15. Wahlperiode

Drucksache **15/3705**

HESSISCHER LANDTAG

06. 03. 2002

Dreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt am 31. Dezember 2001
nach § 30 des Hessischen Datenschutzgesetzes vom 7. Januar 1999

Eingegangen am 6. März 2002 · Ausgegeben am 19. März 2002
Druck: Druck- und Verlagshaus Chmielorz GmbH · 65205 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

INHALTSVERZEICHNIS

KERNPUNKTE DES 30. TÄTIGKEITSBERICHTS

1. Das Terrorismusbekämpfungsgesetz lässt - über Lichtbild und Unterschrift hinaus - die Aufnahme weiterer biometrischer Merkmale in Pässe und Personalausweise zu. Vor einer Festlegung der Merkmale bedarf es einer umfassenden Diskussion über die Geeignetheit dieser Maßnahme für die Terrorismusbekämpfung und ihre Auswirkungen auf das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger (Ziff. 2).

2. Die angestrebte rechtliche Gleichstellung elektronischer Dokumente mit Papierdokumenten wirft eine Vielzahl schwieriger rechtlicher und technischer Fragen auf. Die Ersetzung der Papierform wird bei Dokumenten mit dauerhaftem Beweiswert nur möglich sein, wenn diese auch in elektronischer Form dauerhaft unverfälscht verfügbar und lesbar sind. Ich habe die Landesregierung auf erhebliche Schwachstellen in den im Verwaltungsverfahrensänderungsgesetz vorgesehenen Vorschriften zur Gleichstellung der elektronischen Kommunikation im Rechtsverkehr mit den herkömmlichen Papierdokumenten hingewiesen und Verbesserungsvorschläge unterbreitet (Ziff. 4).

3. Die neuen Befugnisse für Polizei- und Gefahrenabwehrbehörden zum Einsatz von Videoüberwachungsanlagen werden von den Gemeinden zunehmend - zum Teil sehr extensiv - genutzt. Die Polizeipräsidien zeigen deutlich größere Zurückhaltung. Jedes Projekt wird von mir unter Berücksichtigung der örtlichen Besonderheiten und der beteiligten Stellen bewertet (Ziff. 5.1).

4. Bei der Landratswahl im Kreis Marburg-Biedenkopf am 16. September 2001 konnten Briefwähler erstmals in Hessen testweise ihre Stimme auch über das Internet abgeben. Durch pseudonyme Stimmabgabe, anonyme Stimmauszählung und verschlüsselte Datenübertragung konnte das Briefwahlgeheimnis gewährleistet werden (Ziff. 6.1).

5. Der Gesetzentwurf zur Änderung des Verfassungsschutzgesetzes sieht eine Zuständigkeit des Verfassungsschutzes für die Bekämpfung der organisierten Kriminalität vor. Die Befugnisse des Verfassungsschutzes zum Abhören und zur Anfertigung von Bildaufzeichnungen in Wohnungen werden deutlich erweitert. Außerdem sollen nicht näher eingegrenzte Auskunftspflichten für Geldinstitute, Postdienstleistungs- und Luftverkehrsunternehmen eingeführt werden. Ich habe gegenüber der Landesregierung kritisch zum Entwurf Stellung genommen (Ziff. 9.1).

6. Im Berichtsjahr fanden intensive Gespräche über die lange geforderte Anpassung der Abgabenordnung an die datenschutzrechtlichen Standards im Allgemeinen Verwaltungsrecht statt (Ziff. 10.2).

7. Die Übermittlung der für das Modellprojekt Mammographie-Screening erforderlichen Meldedaten an den Projektträger wirft datenschutzrechtliche Probleme auf. Das unter meiner Mitwirkung erstellte neue Konzept des Projektträgers stellt sicher, dass keine schutzwürdigen Belange der betroffenen Frauen beeinträchtigt werden (Ziff. 11.1).

8. Anmeldeprozeduren an IT-Systeme sind von entscheidender Bedeutung für die IT-Sicherheit. Passwörter werden immer häufiger durch biometrische Verfahren und Chipkarten ersetzt. Jede technische Lösung hat Schwachstellen. Die höchste Sicherheit kann derzeit mit dem Einsatz von Chipkarten in Kombination mit Passwörtern oder biometrischen Merkmalen erreicht werden (Ziff. 14.1).

9. Der Einsatz geeigneter Software bei der Prüfung TCP/IP-basierender Netze kann Schwächen der Netzsicherheit aufdecken. Als Ergebnis ist festzuhalten, dass die Administratoren ihre Netze in der Regel recht gut absichern. Die Flut neu erkannter Schwachstellen von Netzsoftware und Betriebssystemen erfordert die kontinuierliche Pflege der Netzkomponenten (Ziff. 14.5).

10. Eine Evaluation der Lehre an den Hochschulen darf nur mit Kenntnis der Betroffenen und nach fachlichen Kriterien erfolgen. Sie stellt eine dienstliche Bewertung der gezeigten Leistungen dar. Eine personenbezogene Veröffentlichung der Ergebnisse ist deswegen nicht zulässig (Ziff. 19.1).

11. Die Einführung neuer Prüfungsmethoden in die Abgabenordnung (AO) im Rahmen der Außenprüfung birgt nach wie vor Schwierigkeiten. Nach § 147 Abs. 6 AO erhalten Betriebsprüfer ab Januar 2002 unter anderem das Recht, im Rahmen einer Außenprüfung unmittelbar die gesamte EDV-Buchhaltung als elektronische Kopie zur weiteren Auswertung im Finanzamt auf einem Datenträger mitzunehmen (Ziff. 26.5).

12. Auch die Datenschutzbeauftragten des Bundes und der Länder unterstützen den Kampf des demokratischen Rechtsstaats gegen Terrorismus und organisierte Kriminalität. Die Sicherheits- und Strafverfolgungsbehörden verfügen schon heute über weitreichende Befugnisse zur Terrorismusbekämpfung (bspw. Rasterfahndung, Abhörbefugnisse, Datenübermittlung). Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Auch die Einführung biometrischer Abgleiche, die keine zusätzlichen Sicherheiten schaffen, ist rechtsstaatlich nicht zu legitimieren (Ziff. 27.12).

13. Vor dem Hintergrund der Lipobay-Diskussion hat das Bundesministerium für Gesundheit die Einführung eines "Arzneimittelpasses" in Form einer (elektronisch nutzbaren) Medikamentenchipkarte befürwortet; auf der Karte sollen alle ärztlichen Verordnungen verzeichnet werden. Damit soll eine größere Transparenz der Arzneimittelverordnungen erreicht werden. Wie die Datenschutzbeauftragten des Bundes und der Länder habe ich erhebliche Bedenken gegen eine Medikamentenchipkarte als Pflichtkarte geäußert und datenschutzrechtliche Anforderungen an den Einsatz eines Arzneimittelpasses formuliert (Ziff. 27.13).

1. Vorwort

Das Berichtsjahr war für die Dienststelle und mich durch die Terroranschläge in New York und die daran anschließenden gesetzlichen Neuregelungen und dem vorausgehenden Beratungen auch in datenschutzrechtlicher Hinsicht sehr stark geprägt. Jenseits dessen standen umfangreiche Beratungstätigkeiten in Gesetzgebung und Verwaltung an. Die laufende Kontrolltätigkeit erfasste eine Vielzahl von Verwaltungsbereichen. Zum Ende des Jahres traten vor allem im Bereich der Versorgungsverwaltung und der Sozialverwaltung gravierendere Probleme auf (Ziff. 19.2). Im letzen Quartal habe ich mich zu den Fragen des Datenschutzes in der Gerichtsbarkeit erstmals ausführlicher festgelegt (Ziff. 28.2).

Die begleitende Gesetzesberatung bezog sich zunächst auf die Antiterrorgesetze des Bundes und die Umsetzung bestehender Regelungen im Hessischen Sicherheits- und Ordnungsbehördengesetz (HSOG) durch das Land (Ziff. 27.12 und 27.17). Besondere Streitfragen, die vor allem von den Betroffenen an uns herangetragen worden sind, hat die Rasterfahndung aufgeworfen. Obwohl richterliche Anordnungen die Ermächtigungen für den Datenabgleich konkretisiert haben, ist der Vollzug durch das Landeskriminalamt der Kontrolle durch den Datenschutz unterworfen und wird daher von mir im Einzelnen verfolgt. Besondere Schwierigkeiten wirft die Subsumtion zu § 26 HSOG auf, denn diese Vorschrift setzt eine gegenwärtige, konkrete Gefahr voraus. Da sowohl der Bundesinnenminister als auch der Staatssekretär des Hessischen Innenministerium erklärt haben, dass gegenwärtig keine tatsächlichen Anhaltspunkte für Anschläge in Deutschland existierten, sind die gesetzlichen Voraussetzungen nur schwer begründbar. Im Einzelvollzug stellt sich vor allem die Frage, wann die Daten derjenigen Betroffenen, die im Zuge des Rasterabgleichs ausgeschieden worden sind und nicht durch weitere Ermittlungen verfolgt werden sollen, zu löschen sind. Während ich die Auffassung vertrete, dass Daten solcher Personen nicht mehr erforderlich und deswegen zu löschen sind, ist das Innenministerium der Meinung, dass der Gesamtdatenbestand bis zum Schluss des Abgleichs zusammengehalten werden müsse. Die rechtliche Notwendigkeit dieser Auffassung erschließt sich mir nicht. Nach wie vor äußerst umstritten ist die Verwendung biometrischer Merkmale in Personalausweisen. Die zunächst in erster Linie angedachten Fingerprints lassen sich nur mit hohem technischen Aufwand auf Personalausweisen unterbringen, haben zudem hohe Unsicherheitsquotienten und sind international bei anderen europäischen Mitgliedsländern nicht durchsetzbar. Bevor Gesichtserkennungssysteme eingeführt werden, müsste zunächst im Verwaltungsvollzug sichergestellt werden, dass die auf Ausweisen verwendeten Portraitfotos eine Qualität aufweisen, die fototechnischem Standard entspricht. Zur Fälschungssicherheit bedarf es keiner biometrischen Merkmale, da die Fälschungsquote schon jetzt gegen Null geht. Die nächsten Monate werden zeigen, ob die genannten und weitere kritische Punkte datenschutzgerecht konkretisiert und definiert werden können (s. Ziff. 2, 27.18 sowie 14.1 zur generellen Problematik von biometrischen Verfahren).

Besondere Probleme hat die Umsetzung des Bundesverfassungsgerichtsurteils zu den Überprüfungsbefugnissen des Bundesnachrichtendienstes (BVerfG NJW 2000 S. 55 ff.) im Landesverfassungsschutzrecht aufgeworfen. Das Urteil des Bundesverfassungsgerichts zieht zum einen strenge Maßstäbe für die Erforderlichkeit, die bei der Erweiterung der Zuständigkeiten des Landesamtes nicht immer eingehalten worden sind, zum anderen verlangt es eine Kennzeichnung der Daten nach ihrer Herkunft. Auch wenn diese Forderung nur auf Daten nach dem Gesetz zu Art. 10 GG bezogen ist, verdient sie bei sensiblen Quellen der Erweiterung. Eine solche Kennzeichnung versieht die Daten mit einem Warnhinweis, der die nachfolgenden Verwender zu besonderer Sorgsamkeit veranlassen wird. Deswegen schützt er auch die Quelle, aus der die Daten stammen. Im Zuge der Erweiterung des Zuständigkeitsbereiches des Landesamtes für Verfassungsschutz hat sich als problematisch erwiesen, dass bei Verfolgung der organisierten Kriminalität Paralleltätigkeiten mit dem Hessischen Landeskriminalamt auftreten werden. Da keine grundlegenden Unterschiede bei den Aufklärungsinstrumenten bestehen, birgt eine solche konkurrierende Zuständigkeit die Gefahr der Ineffizienz. Besonders fragwürdig ist die Herabsetzung des Alters, ab dem personenbezogene Daten gespeichert werden können: Nunmehr sollen zwölf Lebensjahre die Grenze sein. Damit werden Kinder zum Gegenstand von Personenakten des Verfassungsschutzes (Ziff. 9.1 und 27.1).

Mehrfach beschäftigt haben mich die verschiedenen Anläufe zur Schaffung eines „Transparenzgesetzes“ im Gesundheitswesen. Mit der im Internet veröffentlichten Entwurfsfassung soll eine Vielzahl neuer Erfassungsstellen und -ebenen geschaffen werden. Zum Teil sollen diese mit Klardaten, zum Teil mit pseudonymisierten Daten arbeiten. Beabsichtigt ist u.a., den gesetzlichen Krankenkassen einen personenbezogenen Überblick über die Krankenversorgung einzelner Versicherter zu geben; das bedingt einen Einblick in die Krankheitsprofile der Versicherten. Mit einer solchen - unter dem Aspekt der Gesundheitsberatung - eingeführten Kontrolle der Krankenversorgung einzelner Versicherter durch die Krankenkassen wird ein grundlegender Wechsel in der Informationsverarbeitung durch die Krankenkassen eingeleitet. Während diese bislang Arztbriefe verschlossen an die Versicherten weiterzuleiten hatten, sofern diese Aufklärung über die ärztliche Krankenversorgung beanspruchten, wird künftig voller Einblick gestattet. Es ist zweifelhaft, ob das im Zuge der Beratungsaufgaben der Kasse erforderlich ist und ihrer Sachkompetenz entspricht (s. auch Ziff. 27.6). - Auf vergleichbarer Ebene liegt die nunmehr konzipierte Erfassung der Gesundheits- und Krankheitsdaten in zentralen Speichern. Diese Speicher sollen durch individuelle Gesundheitspässe von den einzelnen Leistungserbringern abgerufen werden können. Die Einrichtung zentraler Speicher ist selbst bei Verschlüsselung der Daten geeignet, Gesundheitsprofile einzelner Versicherter zusammenzutragen und bei Bedarf verfügbar zu machen. Hier ist die Forderung unabdingbar, dass dem einzelnen Versicherten die Möglichkeit technisch offen gehalten wird, eine selektive Datenfreigabe zu verfügen, d. h. nur jenen Ärzten Einblick zu gewähren, denen die Kenntnis nach Auffassung des Patienten für die Behandlung hilfreich sein kann. Die Anforderungen an das technische System sind bisher so wenig präzisiert, dass eine substanzielle Kritik noch nicht formuliert werden kann (s. auch Ziff. 27.13).

Auf ganz anderer Ebene liegen die Neuregelungen, die zunächst auf Bundesebene für elektronische Verwaltungsakte und deren Handhabung konzipiert worden sind. Da das Land der Gesetzgebung des Bundes in Kürze folgen muss, haben meine Dienststelle und ich sich intensiv in die Vorbereitung der Bundesnovelle eingeschaltet. Die zahlreichen Mängel, die festgestellt werden mussten, sind mittlerweile zum Teil, aber noch nicht ganz behoben (vgl. dazu Ziff. 4).

Meine Bemühungen, die Regierungskoalition zu einem Informationszugangsgesetz in Hessen zu bewegen, sind bedauerlicherweise genauso erfolglos geblieben wie ein Entwurf der Fraktion Bündnis 90/Die Grünen im Hessischen Landtag (Ziff. 26.2). Die CDU-Fraktion war der Auffassung, dass die bestehenden Informationsrechte aufgrund des Verwaltungsverfahrens- und des Umweltinformationsrechts ausreichten, um den Beratungsbedarf von Bürgerinnen und Bürgern zu stillen. Ich selbst bin der Auffassung, dass im Zuge der Ausweitung elektronischer Verwaltung mit unmittelbarer Interaktion zwischen Bürgerinnen, Bürgern und Administration der Informationsbedarf über die elektronischen Medien, aber auch in Form traditioneller Akteneinsicht deutlich ansteigen wird. Ohne verbesserte Informationsbeschaffung wird sich die mediale Innovation nicht durchsetzen lassen. Informationszugangsgesetze sind daher notwendige Bedingung für diese Reformansätze.

Seit vielen Jahren steht eine Anpassung der Abgabenordnung (AO) an die verfassungsrechtlichen Grundsätze informationeller Selbstbestimmung aus. Während in den Vorjahren aus der Konferenz der Referenten der Landesfinanzverwaltungen zur Abgabenordnung intensiver Widerstand gegen eine Anpassung in der Abgabenordnung geleistet worden ist, hat sich in jüngerer Zeit eine gewisse Wende vollzogen. Im Zuge der Erörterungen um die Neufassungen des § 88b AO (inzwischen durch eine besondere Regelung im Umsatzsteuerrecht ersetzt) und des § 147 Abs. 6 AO ist das Bewusstsein gewachsen, dass der erweiterte Zugriff auf steuererhebliche Daten durch die Finanzverwaltung Widerstände erzeugt, die nicht der eigensüchtigen Abwehr steuerlicher Zugriffe dienen, sondern zum Schutz des Persönlichkeitsrechts geltend gemacht werden. Der inzwischen in Hessen liegende Vorsitz des Arbeitskreises Steuer der Datenschutzbeauftragten des Bundes und der Länder hat die Anpassung der finanzverfahrensrechtlichen Regelungen zu den Schwerpunkten der Gegenwart und der kommenden Monate gemacht. Es ist damit zu rechnen, dass noch im ersten Vierteljahr des Jahres 2002 ein Vorschlagskatalog präsentiert wird, aus dem sich die datenschutzrechtlich begründeten Änderungen der Abgabenordnung ergeben. Gespräche mit dem Landesfinanzminister haben eine erfreuliche Sensibilität für die datenschutzrechtlichen Fragen erkennen lassen (Ziff. 10).

Bei der Beratung der Landesregierung vor der Neufassung von Verwaltungsrichtlinien standen vor allem die kriminalpolizeilichen Sammlungen und der Datenschutz in der Gerichtsbarkeit im Vordergrund. Im Zuge der Neufassung der KPS-Richtlinien war vor allem die datenschutzrechtliche Neuregelung in der Strafprozessordnung umzusetzen. Mit dieser Neuregelung ist für einen wichtigen Bereich der Gerichtsbarkeit und der staatsanwaltschaftlichen Tätigkeit eine erste datenschutzrechtliche Kodifikation erfolgt, die nach und nach nicht nur die KPS-Richtlinien, sondern auch die Speicherungen im INPOL- und POLAS-System beeinflussen werden (Ziff. 8.4). Das POLAS-System, das von Hamburg übernommen worden ist, ist in datenschutzrechtlicher Hinsicht überprüft worden; Einzelfragen harren noch der Beantwortung (Ziff. 8.1). Hinsichtlich des Datenschutzes in der Justiz habe ich eine Orientierungshilfe formuliert, die derzeit in der Gerichtsbarkeit erörtert wird. Es ist damit zu rechnen, dass in der ersten Jahreshälfte 2002 ein gemeinsames Papier erarbeitet werden kann, das dann für die gesamte Gerichtsbarkeit verfügbar sein wird (vgl. dazu Ziff. 28.2).

Besondere Probleme wirft nach wie vor die rechtspolitische Frage auf, ob die Aufsicht im öffentlichen und im nicht-öffentlichen Bereich vereinheitlicht werden soll. Die Europäische Datenschutzrichtlinie fordert zwingend, dass auch der Datenschutz im nicht-öffentlichen Bereich in „völliger Unabhängigkeit“ überwacht wird. Dem genügt die gegenwärtige Eingliederung der Aufsichtsbehörden in die Regierungspräsidien nicht - wie ein jüngst versandtes Schreiben der Europäischen Kommission an den Berliner Datenschutzbeauftragten dokumentiert. Es wird daher in jedem Fall erforderlich, die Aufsichtsbehörden für den nicht-öffentlichen Bereich aus den Regierungspräsidien herauszulösen und als völlig unabhängige Stellen zu organisieren. Unabhängig davon ist zu entscheiden, ob dabei aus Gründen der Verwaltungseffizienz eine Zusammenlegung mit meiner Dienststelle erfolgen soll. Da sich zunehmend Überschneidungen zwischen den Aufgabenfeldern ergeben, etwa bei Banken, Versicherungen, Krankenkassen, Flughäfen, privaten und öffentlichen Sicherheitsdiensten, und auch die eingesetzten Instrumente sich immer stärker angleichen, etwa bei Chipkarten, Videoüberwachung und Versichertendatenbanken, drängt sich aus Gründen des besseren Personaleinsatzes eine Zusammenfassung beider Dienststellen auf. Die abschließende Entscheidung des Landes ist noch nicht gefallen, obwohl drei Fraktionen des Hessischen Landtages die Zusammenlegung befürworten.

Eigene Probleme wirft der zunehmende Chipkarteneinsatz auf. Neben den Chipkarten, die im Gesundheitswesen vom Bund geplant sind (Ziff. 27.13), werden von den hessischen Hochschulen Pilotprojekte verfolgt, die die traditionellen Studentenausweise durch Chipkarten ersetzen sollen (Ziff. 23.1). Dabei ist nicht nur der schmale Datensatz von Name, Matrikelnummer, Wohnort und Studienrichtung vorgesehen. Vielmehr ist daran gedacht, die Chipkarten um eine Geldkartenfunktion, eine Authentifizierungsfunktion und eine private Verschlüsselungssoftware zu erweitern. Außerdem soll ein Zugangslegitimationssystem aufgebracht werden. Unabhängig von den Grenzen, die die gegenwärtige Fassung der Verordnung den Studentenausweisen zieht, bedingen die technischen Zusatzlösungen, dass der Einsatz durch die einzelnen Studierenden freiwillig erfolgt.

Gewisse Erregung hat meine Stellungnahme zur Evaluation der Lehre an den Hochschulen hervorgerufen. Meine Einwendungen betreffen nicht die gesetzlich vorgesehene Forderung, die Hochschullehre zu evaluieren, sondern das Verfahren und die weitere Verwendung der dadurch gewonnenen personenbezogenen Daten. Die Evaluation soll Auskunft über die Qualität geben, mit der die dienstlichen Pflichten durch die Hochschullehrerinnen und Hochschullehrer erfüllt werden. Die Evaluationsdaten müssen daher wie Personalaktendaten auch sonst behandelt werden. Das bedeutet vor allem, dass sie nicht universitätsweit veröffentlicht werden dürfen. Eine solche Veröffentlichung würde die einzelnen Hochschullehrer „an den Pranger“ stellen; das darf nicht sein. Die Hochschulen werden daher die erforderlichen Verfahren in ihrer Satzung datenschutzgerecht formulieren müssen. Bislang ist keine Hochschule in ihren Planungen so weit fortgeschritten, dass über die Evaluation insgesamt berichtet werden könnte (Ziff. 19.1).

Zunehmend wird in der politischen und der Rechtswissenschaft, aber auch im Datenschutz erörtert, inwieweit Wahlen künftig über das Internet abgewickelt werden können. Im Zuge von Wahlen für die Selbstverwaltungsgremien in der gesetzlichen Versicherung ist erstmals ein Internet-Wahlverfahren bundesweit durchgeführt worden. Für politische Wahlen ist in Marburg in Zusammenarbeit mit der Universität ein Testwahlverfahren entwickelt worden, das parallel zur Briefwahl durchgeführt worden ist (Ziff. 6.1).

Das Internet hat weitere Probleme aufgeworfen; amtliche Veröffentlichungen, die im Internet erfolgen, gewinnen zunehmende Bedeutung. Erstmals ist im Zuge einer Novelle zur Insolvenzordnung die Veröffentlichung von insolventen Schuldnern im Internet vorgesehen worden. Da Veröffentlichungen im Internet nicht zurückholbar sind und von Dritten jederzeit kopiert und gesondert aufbewahrt werden können, erweist sich jede amtliche Veröffentlichung als solche mit „Ewigkeitswert“. Das ist in allen Lebensbereichen, die auf Rehabilitation der Betroffenen angelegt sind, hoch problematisch. Bislang sind technische Verfahren, mit denen Kopiersperren gelegt werden können, nicht verfügbar. Deswegen ist meine diesbezügliche Forderung allenfalls für die Zukunft realisierbar (Ziff. 7.1).

Die Internetnutzung in den Dienststellen wirft schwierige Probleme auf, wenn neben der amtlichen auch die private Nutzung gestattet wird. In diesem Fall wird die Dienststelle zum Teledienstanbieter und damit Pflichten unterworfen, die sich mit der amtlichen Nutzung nicht vereinbaren lassen. Gegenüber der privaten Nutzung gelten die strengen Grenzen, die der Datenerfassung durch Diensteanbieter gezogen sind: Es dürfen nur Bestandsdaten über die nutzungsberechtigten Personen und Verbindungsdaten, soweit sie zur Abrechnung oder zur Missbrauchskontrolle erforderlich sind, gespeichert werden. Inhaltsdaten dürfen nur soweit erfasst werden, als dies zur Erfüllung der Dienstleistung erforderlich ist. Diese datenschutzrechtliche Strenge des Teledienstrechts macht die volle Erfassung der amtlichen E-Mails und sonstigen Internetnutzungen unmöglich, soweit sie im Gemenge mit privaten Nutzungen stehen. Auch eine Einwilligung kann keine Abhilfe schaffen. Die von mir empfohlene Lösung geht dahin, entweder eine private Zusatzadresse einzurichten, auf die nur der Bedienstete Zugriff hat, oder zu gestatten, dass vom dienstlichen PC aus die Mailbox abgerufen wird, die der betreffende Bedienstete privat unterhält (Ziff. 13.3 und 28.1).

In technischer Hinsicht hat meine Dienststelle im Jahr 2001 erstmals für zahlreiche Verwaltungsstellen ein informationstechnisches Kontrollverfahren angeboten und durchgeführt. Mit diesem Verfahren kann der Zugang zu den Verwaltungsnetzen von außen mit Hilfe eines Port-Scanners auf Lücken in der Firewall untersucht werden (Ziff. 14.5). Dabei hat sich gezeigt, dass vor allem in kleineren Dienststellen die Administration von Firewalls noch Schwächen aufweist. Das informationstechnische Angebot ist von den einzelnen Dienststellen gut angenommen worden. Es wäre sachgerecht, für die gesamte Landes- und Kommunalverwaltung gleichartige Überprüfungsverfahren vorzusehen. Da die Kosten der angemieteten Software und der Zeitaufwand nicht gering sind, würde der flächendeckende Einsatz meine Dienststelle allerdings finanziell wie personell überfordern.

Das Wiesbadener Forum zum Datenschutz, das der Landtagspräsident gemeinsam mit mir jährlich im Hessischen Landtag veranstaltet, hat auch dieses Jahr wieder eine große Resonanz gefunden. Thematisch befasste es sich mit der hoch umstrittenen Problematik, inwieweit Presse und andere Medien die datenschutzrechtlichen Anforderungen wie andere Unternehmen erfüllen müssen. Dabei steht zum einen in Frage, ob Presse und andere Medien interne Datenschutzbeauftragte ernennen müssen. Für die öffentlichen Rundfunkanstalten ist das staatsvertraglich bereits vorgesehen, die Presse bestreitet die datenschutzrechtliche Notwendigkeit und die verfassungsrechtliche Zulässigkeit interner Beauftragter. Streitig ist weiter, ob die Aufsichtsbehörden des Staates Missbrauchskontrollen gegenüber der Presse vorsehen dürfen. Die Europäische Richtlinie geht von einer nachträglichen Kontrolle als europäischem Standard aus. Materiell schaffen die umfangreiche Datensammlungen, die in Presseunternehmen üblich geworden sind, Schwierigkeiten. Da eine Vielzahl der gesammelten Daten personenbezogen ist, wäre mit einem Verbot der Datensammlung auf Vorrat ein großer Teil der Archivarbeit unterbunden. Für die Anforderungen an die Datensammlungen wie für die gesamte Medienarbeit gilt der allgemeine Rechtsgrundsatz, dass Persönlichkeitsrechte nicht verletzt werden dürfen. Er wird allerdings bislang nur durch die Zivil- und Strafgerichte mit Sanktionen belegt. Aus dem Kreis der Datenschutzbeauftragten wird die Forderung erhoben, missbräuchliche Eingriffe in das Persönlichkeitsrecht auch im Wege aufsichtlicher Einwirkung abzustellen. Dabei wird allerdings die Grenze zur verbotenen Vorzensur große Vorsicht nahe legen. Das Forum hat die unterschiedlichen Sichtweisen hinterfragt und in ausgiebigen Diskussionen zu hohem Problembewusstsein geführt. Unmittelbar umsetzbare rechtspolitische Empfehlungen für die Landesgesetzgebung haben sich nicht gewinnen lassen.

Auch in diesem Jahr möchte ich allen meinen Mitarbeiterinnen und Mitarbeitern für die im Berichtszeitraum geleistete Arbeit danken. Die engagierte Begleitung meiner Tätigkeit schlägt sich im nachstehenden Bericht nicht in allen Facetten nieder. Veröffentlicht sind nur jene Teile der Arbeit, die sich als besonders hervorhebenswert erwiesen haben.

Auch den Abgeordneten des Hessischen Landtages gilt mein Dank für die fruchtbare Zusammenarbeit, die sich vor allem in den Ausschüssen ergeben hat. Die Gespräche mit der Landesregierung waren stets sachorientiert, selbst dort, wo unterschiedliche Auffassungen aufgetreten sind. Auch in Zukunft möge das Recht auf informationelle Selbstbestimmung gemeinsames Anliegen bleiben.

2. Terrorismusbekämpfung

Biometrische Merkmale in Pässen und Personalausweisen

Im Zuge der Beratungen zur Änderung des Pass- und Personalausweisgesetzes, das jetzt die Aufnahme weiterer biometrischer Merkmale in Ausweispapiere grundsätzlich zulässt, bin ich verstärkt mit der Fragestellung konfrontiert worden, inwieweit sich dies mit dem Recht auf informationelle Selbstbestimmung vereinbaren lässt.

Der Bundestag hat mit dem zweiten Terrorismusbekämpfungsgesetz vom 11. Januar 2002 (BGBl. Teil I S. 361 ff.) beschlossen, dass in Pässe und Personalausweise neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale aufgenommen werden dürfen. Bislang hat sich der Bundestag noch nicht festgelegt, welche Merkmale das im einzelnen sein sollen. Diese zusätzlichen Daten dürfen nur zur Überprüfung der Identität des Inhabers und der Echtheit des Dokuments genutzt werden und nicht für erkennungsdienstliche Zwecke zur Gefahrenabwehr oder Strafverfolgung.

Zunächst enthielt der Gesetzentwurf kein Verbot der Speicherung dieser Daten in einer bundesweiten Referenzdatei. Auf Drängen von Datenschutz- und Bürgerrechtsorganisationen wurde jedoch ein Zusatz aufgenommen, dass eine bundesweite Datei nicht eingerichtet wird.

§ 4 Abs. 3 und 4 Passgesetz
(entspricht § 1 Abs. 4 und 5 Personalausweisgesetz)

(3) Der Pass darf neben dem Lichtbild und der Unterschrift auch weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden. Auch die in Abs. 1 Satz 2 aufgeführten Angaben über die Person dürfen in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden.

(4) Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form nach Abs. 3 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt. Eine bundesweite Datei wird nicht eingerichtet.

Im Gesetzgebungsverfahren wurde die Geeignetheit dieser Maßnahmen zur Terrorismusbekämpfung nicht ausreichend diskutiert. Die Auswirkungen, die die Aufnahme derartige Merkmale auf das Recht auf informationelle Selbstbestimmungsrecht haben kann, wurden nicht angemessen berücksichtigt.
Die folgenden Aspekte sind berücksichtigenswert:

1. Die Fälschungssicherheit ist durch biometrische Merkmale kaum zu erhöhen; da schon heute die Ausgestaltung der Bundespersonalausweise das Risiko „gen Null“ gehen lässt (so die Bundesdruckerei), sind zusätzliche Maßnahmen gegen Fälschungen im datenschutzrechtlichen Sinn „nicht erforderlich“.
2. Fingerprints sind wegen der Notwendigkeit internationaler Vereinheitlichung nicht näher in Erwägung zu ziehen, da z. B. Frankreich, ein Partner des Schengener Vertrages, sich festgelegt hat, dass er Fingerprints in keinem Fall in Ausweispapiere aufnehmen will. Außerdem liegt die Fehlerquote bei den angewandten Leseverfahren lt. Fraunhofer-Institut bei ca. 5 %. Die Zurückweisungsquote ist also hoch. Bei Kontrollen kann daher nicht auf Personal verzichtet werden.
3. Biometrische Systeme sind bislang weder hinsichtlich ihrer Zurückweisungsrate noch hinsichtlich der Überwindungssicherheit ausreichend überprüft, um flächendeckend eingeführt werden zu können.
4. Auch für Gesichtserkennungssysteme, die auf laufende Personenkontrollen bezogen sind, bedarf es näherer Untersuchungen, mit denen geklärt wird, wie hoch der Maschineneinsatz zu veranschlagen ist, der für eine hinreichend sichere Wiedererkennung oder Ersterkennung notwendig ist.
5. Die Begrenzung biometrischer Erkennungssysteme auf deutsche Staatsangehörige kann Gefahren, die aus internationalen Anschlägen durch ausländische Staatsbürger, die in Deutschland ihren Wohnsitz haben, entsehen können, nicht abwehren. Deutschland hat keine Verfügungsbefugnisse über Ausweispapiere ausländischer Mitbürger oder Besucher.

6. Biometrische Merkmale enthalten stets Zusatzinformationen (z. B. Iris: Krankheitsindikator; Fingerprint: Unfallindikator und Beschäftigungsindikator). Es muss weitestgehend unterbunden werden, dass die gespeicherten Daten Rückschlüsse darauf erlauben.

7. Aktive Systeme sind zu bevorzugen, da sie sicherstellen, dass der zu Verifizierende auf das Verfahren aufmerksam wird und sich subjektiv darauf einstellt. Außerdem ist datenschutzrechtlich geboten, empfindliche Daten - um diese handelt es sich hier - nur in Kenntnis der Betroffenen zu erheben. Das sichern aktive Systeme.

8. Die Verwendung der Merkmale für andere Staatszwecke (insbesondere Kriminalistik) oder privatrechtliche Zwecke (Versicherungen, Gesundheitssystem) ist auszuschließen. Die gegenwärtig bereits bestehende Beschränkung auf Verifikationszwecke muss aufrecht erhalten bleiben.

9. Identifikationssysteme benötigen zentrale Datenbestände, während Verifikationssysteme auch mit dezentralen Speichern (z. B. Chipkarte/Ausweis) auskommen. Auch deshalb sind Verifikationssysteme im Zusammenhang mit Ausweisdokumenten aus Datenschutzsicht der einzig mögliche Weg.

10. Es bestehen starke Zweifel, dass die vorgesehenen Chipkarten über den Gültigkeitszeitraum von Ausweisen (zehn Jahre) funktionsfähig bleiben. Als Konsequenz müsste der Gültigkeitszeitraum verkürzt werden oder eine andere Technik (z. B. 2D-Barcode) eingesetzt werden.

11. Um einen Fremdzugriff auf biometrische Daten zu verhindern, müssten die Daten verschlüsselt gespeichert werden. Da andererseits europaweit Kontrollen geplant sind, werden die Entschlüsselungsprogramme weit gestreut sein. Wie eine funktionsfähige Infrastruktur aussehen kann, die auch gegen gestohlene Lesegeräte einen Schutz bietet, und welche Kosten damit verbunden sind, ist unklar.

12. Bei der wissenschaftlichen Untersuchung biometrischer Merkmale ist auch zu klären, inwieweit sie sich im Lauf der Zeit ändern und welchen Einfluss das auf Erkennungsraten und Funktionsfähigkeit hat.

Ich werde mich dafür einsetzen, dass die Konferenz der Datenschutzbeauftragten diese Kritikpunkte in einer Entschließung aufgreift.

3. Novelle des Bundesdatenschutzgesetzes

Mit der Novellierung des Bundesdatenschutzgesetzes, die am 23. Mai 2001 in Kraft getreten ist, hat der Bundesgesetzgeber die EG-Datenschutzrichtlinie in nationales Recht umgesetzt und in einigen Vorschriften Anpassungen an die Fortentwicklung der Informationstechnik vorgenommen. In einer zweiten Stufe beabsichtigt er, weiteren Novellierungsbedarf umzusetzen und die Datenschutzvorschriften zu vereinfachen.

3.1 Gesetzgebungsverfahren

Seit der Verabschiedung der EG-Datenschutzrichtlinie vom 24. Oktober 1995 arbeitete das Bundesinnenministerium an einer Umsetzung der Richtlinie in nationales Recht. Trotz zahlreicher Vorentwürfe kam das Gesetzgebungsverfahren erst so spät in Gang, dass die Umsetzungsfrist, die am 24. Oktober 1998 abgelaufen war, weit überschritten wurde. Die Datenschutzbeauftragten des Bundes und der Länder hatten ihre Forderungen für das Gesetzgebungsverfahren bereits frühzeitig artikuliert und seit 1997 mehrfach auch in Entschließungen zum Ausdruck gebracht (vgl. 26. Tätigkeitsbericht, Ziff. 25.7; 27. Tätigkeitsbericht, Ziff. 26.4; 28. Tätigkeitsbericht, Ziff. 24.1 und 29. Tätigkeitsbericht, Ziff. 21.11). Das Gesetz zur Änderung des Bundesdatenschutzgesetzes ist im Bundesgesetzblatt vom 22. Mai 2001 (BGBl. I S. 904 ff.) veröffentlicht. es ist beabsichtigt, eine Neufassung des Bundesdatenschutzgesetzes zu veröffentlichen; diese lag aber bis zum Redaktionsschluss dieses Tätigkeitsberichtes noch nicht vor.

3.2 Wesentliche Änderungen

3.2.1 Anpassung an die EG-Datenschutzrichtlinie

3.2.1.1 Anpassung von Struktur und Begriffen

Die EG-Datenschutzrichtlinie kennt keine Unterscheidung zwischen öffentlichem und nicht-öffentlichem Bereich. Das Bundesdatenschutzgesetz trennt diese Bereiche weiterhin; bei der Umsetzung hat der Bundesgesetzgeber aber mehr Regelungen in den für beide Bereiche geltenden Teil des Bundesdatenschutzgesetzes zusammengezogen.

Eine Ausweitung des Anwendungsbereichs hat die Anpassung der Begriffe der automatisierten Verarbeitung und der Datei zur Folge. Dabei hat der Bundesgesetzgeber leider den einheitlichen Verarbeitungsbegriff der EG-Richtlinie, der jede Verwendung von Daten vom Erheben bis zum Löschen umfasst (der im Übrigen im hessischen Datenschutzrecht schon lange problemlos verwendet wird) nicht übernommen, sondern arbeitet weiterhin mit den Einzelbegriffen "Erheben, Verarbeiten

oder Nutzen". Vom Anwendungsbereich des Bundesdatenschutzgesetzes wird jetzt aber jede automatisierte Verarbeitung sowie die nicht automatisierte gleichartig aufgebaute und nach bestimmten Merkmalen zugängliche und auswertbare Sammlung personenbezogener Daten erfasst. Auch hier setzt das Bundesdatenschutzgesetz die Richtlinie nicht eins zu eins um, denn der Dateibegriff erfordert nach der Richtlinie lediglich eine Strukturierung und die Zugänglichkeit nach bestimmten Kriterien.

Neu ist der besondere Schutz der sensitiven Daten (besondere Arten personenbezogener Daten, § 3 Abs. 9), für die strengere Regeln der Zulässigkeit der Datenverarbeitung zu beachten sind: z. B. nach § 4a Abs. 3 bei der Einwilligung, nach § 4d Abs. 5 die zwingende Vorabkontrolle, nach § 12 Abs. 2 für das Erheben, nach § 28 Abs. 6 bis 9 für die Verarbeitung durch nicht-öffentliche Stellen.

3.2.1.2
Information und Einwilligung

Das neue Bundesdatenschutzgesetz sieht umfassendere Informationspflichten schon bei der Datenerhebung (§ 4 Abs. 3) und - wenn die Daten ausnahmsweise nicht bei Betroffenen erhoben werden - grundsätzlich die Benachrichtigung vor (§ 19a bzw. § 33).

Eine Einwilligung als Rechtsgrundlage für eine Datenverarbeitung ist nur wirksam erteilt, wenn sie auf der freien und auf ausreichender Information basierenden Entscheidung des Betroffenen beruht (§ 4a).

3.2.1.3
Interner Datenschutzbeauftragter, Meldepflicht, Vorabkontrolle

Der Bundesgesetzgeber hat jetzt auch für die öffentlichen Stellen des Bundes die Pflicht zur Bestellung eines oder einer internen Datenschutzbeauftragten eingeführt, wie sie im nicht-öffentlichen Bereich und auch in vielen Landesdatenschutzgesetzen bereits bestand (§ 4f). Der oder die Datenschutzbeauftragte ist unmittelbar der Leitung der Stelle zu unterstellen, unterliegt keinen Weisungen, ist bei der Erfüllung der Aufgabe mit den erforderlichen sachlichen und personellen Mitteln zu unterstützen und insbesondere auch rechtzeitig zu unterrichten. Für ihn oder sie gilt eine Verschwiegenheitspflicht sowie ein Benachteiligungsverbot. Ist eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter bestellt, so hat die von der EG-Datenschutzrichtlinie vorgesehene Meldepflicht für automatisierte Verarbeitungen personenbezogener Daten nicht an die zentralen Kontrollstellen, sondern an sie bzw. ihn zu erfolgen und das entsprechende Register ist dort zu führen (§ 4g Abs. 2). Die internen Datenschutzbeauftragten sind für die Durchführung von Vorabkontrollen für automatisierte Datenverarbeitungen zuständig, die mit besonderen Risiken behaftet sind (§ 4d Abs. 5), und haben Auskünfte aus dem Register zu erteilen (§ 4g Abs. 2). Damit haben sie einen besseren Überblick über die in ihrem Zuständigkeitsbereich vorhandenen Verfahren und können ihre Kontrollaufgabe besser ausführen, insbesondere auch sicherstellen, dass risikobehaftete Verfahren vor ihrem Einsatz datenschutzgerecht eingerichtet werden. Ist kein Datenschutzbeauftragter vorhanden, hat die Meldung über automatisierte Verarbeitungen an die Kontrollstelle zu erfolgen. Um das zu vermeiden, ist auch kleineren Betrieben zu raten, betriebliche Datenschutzbeauftragte zu berufen.

3.2.1.4
Verbot von automatisierten Einzelentscheidungen und besonderes Widerspruchsrecht

Aus der EG-Datenschutzrichtlinie sind die Einführung des Rechtes, bei Vorliegen von besonderen Gründen einer rechtmäßigen Datenverarbeitung im Einzelfall zu widersprechen (§ 20 Abs. 5) und das grundsätzliche Verbot von ausschließlich automatisiert getroffenen Einzelfallentscheidungen (vgl. § 6a) übernommen worden.

3.2.1.5
Neue Übermittlungsregelungen

Die Übermittlungsvorschriften im Bundesdatenschutzgesetz wurden nach dem Prinzip umgestaltet, dass Übermittlungen innerhalb des Geltungsbereichs der EG-Datenschutzrichtlinie wie Übermittlungen im Inland zu behandeln sind und bei Übermittlungen außerhalb dieses Bereichs jeweils zu prüfen ist, ob ein angemessenes Datenschutzniveau besteht (vgl. § 4b).

3.2.1.6
Kontrollstellen/Beurteilung berufsständischer Verhaltensregelungen

Die Kontrollstelle für den Datenschutz im öffentlichen Bereich, der Bundesbeauftragte für den Datenschutz, bleibt weiterhin beim Bundesinnenministerium angesiedelt. Für die Kontrollstellen für den nicht-öffentlichen Bereich sind - entgegen zwi-

schenzeitlichen Entwürfen im Gesetzgebungsverfahren - nun doch keine Vorgaben hinsichtlich der von der EG-Datenschutzrichtlinie vorgeschriebenen „völligen Unabhängigkeit“ gemacht worden. Allerdings ist die Beschränkung der Tätigkeit der Aufsichtsbehörden auf die Anlasskontrolle zu Gunsten eines umfassenden Kontrollrechts weggefallen (§ 38 Abs. 1). Es bestehen Zweifel, ob damit die EG-Datenschutz-richtlinie ordnungsgemäß in nationales Recht umgesetzt ist. Die Einführung präventiver Kontrollen wird zu einer deutlichen Aufgabenvermehrung führen.

Neu ist die Eröffnung der Möglichkeit für berufsständische Vereinigungen, Verhaltensregelungen hinsichtlich des Datenschutzes zu erlassen, die von den Kontrollstellen auf die Übereinstimmung mit geltendem Datenschutzrecht geprüft werden (§ 38a).

3.2.2
Weiterentwicklung des Datenschutzrechts

3.2.2.1
Anpassung der technischen und organisatorischen Maßnahmen

Die Anlage zu § 9 wurde den Anforderungen des Art. 17 der EG-Datenschutzrichtlinie angepasst und enthält jetzt einen in acht Maßnahmen konzentrierten Katalog. Leider hat der Bundesgesetzgeber diesen Katalog wiederum nur als „Anlage“ zu dem Gesetz deklariert und damit die Frage der rechtlichen Qualität dieser Anlage weiterhin offen gelassen. Durch die späte Verabschiedung des Bundesdatenschutzgesetzes ist jetzt auch die Situation entstanden, dass die Landesdatenschutzgesetze unterschiedliche Begriffe verwenden. Auch wenn die Inhalte weitgehend deckungsgleich sind, führt das nicht zur Vereinfachung im Umgang mit den Vorschriften; besondere Probleme entstehen dort, wo öffentliche und nicht-öffentliche Stellen im Verbund arbeiten.

3.2.2.2
Datenvermeidung, Datensparsamkeit, Anonymisierung, Pseudonymisierung

Aufgrund der Beobachtung, dass immer häufiger Datenverarbeitungssysteme eingesetzt wurden, die einen umfassenden Datenkatalog erforderten und ebenso umfassende Auswertungen ermöglichten, ist nunmehr auch im Bundesdatenschutzgesetz ausdrücklich das aus dem Erforderlichkeitsprinzip hergeleitete Prinzip der Datenvermeidung und Datensparsamkeit für die Gestaltung und Auswahl von Datenverarbeitungssystemen festgeschrieben (§ 3a). Damit soll sichergestellt werden, dass unzulässige Datenverarbeitung ausgeschlossen ist, insbesondere die Speicherung und Verarbeitung von mehr Daten als sie Rechtsgrundlage und Zweck erfordern. Gleichzeitig ist klargestellt, dass der Personenbezug von Daten nur so lange als wirklich notwendig zulässig ist. Die Vorschrift weist ausdrücklich auf die Möglichkeiten der Anonymisierung und Pseudonymisierung hin. Die Definition der Pseudonymisierung wurde in die Begriffsbestimmungen neu eingeführt (vgl. § 3 Abs. 6a).

3.2.2.3
Videoüberwachung

Das alte Bundesdatenschutzgesetz bot keinen Schutz gegen konventionelle Videoüberwachung, da Videoaufnahmen - jedenfalls sofern sie nicht digitalisiert waren - nicht unter den alten Dateibegriff einzuordnen waren. Mit § 6b hat der Bundesgesetzgeber nunmehr klargestellt, dass die Beobachtung öffentlich zugänglicher Räume per Videoüberwachung nur unter bestimmten Voraussetzungen zulässig ist. Dabei ist allerdings der Katalog der Rechtfertigungsgründe zu ausufernd geraten, weil die Befugnisnorm im öffentlichen Bereich durch Verweis auf die öffentlichen Aufgaben offen ist und weil auch das Hausrecht und "berechtigte Interessen" zur Videoüberwachung berechtigen.

3.2.2.4
Chipkarten

Chipkarten (mobile personenbezogene Speicher- und Verarbeitungsmedien) weisen Besonderheiten hinsichtlich der Transparenz der Datenverarbeitung, der Ausübung der Auskunftsrechte sowie der Information der Betroffenen auf. Diese waren mit dem alten Bundesdatenschutzgesetz nicht abgefangen. Aus diesem Grund ist im Bundesdatenschutzgesetz die neue Vorschrift des § 6c geschaffen worden, die diese Besonderheiten berücksichtigt. Allerdings wäre eine Klarstellung hilfreich gewesen, dass Datenverarbeitung mittels Chipkarten mit besonderen Risiken behaftet ist, die eine Vorabkontrolle zwingend machen.

3.2.2.5
Datenschutzaudit

Neben dem Instrument der Selbstregulierung durch berufsständische Regelungen hat der Bundesgesetzgeber das Datenschutzaudit eröffnet (§ 9a). Die Vorschrift ist § 17 des Mediendienste-Staatsvertrages nachgebildet und verfolgt das Ziel, Produkte auf dem Markt zu fördern, die höhere Datenschutzstandards verwirklichen als gesetzlich vorgegeben. Die Bewertung von Datenverarbeitungssystemen und -programmen sowie von Datenschutzkonzepten von Anbietern und datenverarbeitenden Stellen soll durch unabhängige Gutachter erfolgen. Allerdings ist diese Vorschrift noch eine leere Hülse, weil das nähere Verfahren durch ein besonderes Gesetz geregelt werden soll, das es bisher noch nicht gibt. Als geeignetes Beispiel könnte der Gesetzgeber das Umweltaudit-Verfahren in das Datenschutzrecht übernehmen.

3.3
Ausblick

Eine ganze Reihe von Anliegen der Datenschutzbeauftragten hat der Bundesgesetzgeber im neuen Bundesdatenschutzgesetz nicht gelöst, sondern auf eine zweite Stufe der Novellierung verschoben. Hier sei nur genannt die Straffung und verständliche Formulierung des Gesetzes, die Regelung des Arbeitnehmerdatenschutzes und eine weitere Anpassung an die Technikentwicklung. Die Vorarbeiten hierzu hat er einem Gutachterausschuss übertragen, der im Oktober 2001 sein Gutachten abgeliefert hat. Außerdem prüft derzeit die EG-Kommission, ob die EG-Datenschutzrichtlinie korrekt in nationales Recht umgesetzt ist. Hinsichtlich der Organisation der Datenschutzkontrollstellen im nicht-öffentlichen Bereich sind dazu erhebliche Bedenken bereits formuliert worden. Es bleibt abzuwarten, ob dem Gesetzgeber noch innerhalb der laufenden Legislaturperiode die notwendige grundlegende Überarbeitung des Datenschutzes in vollständiger Umsetzung der EG-Datenschutzrichtlinie unter Berücksichtigung der Freiheitsrechte der Bürger und einer sachgerechten Interessenabwägung gelingt. Auch für den presserechtlichen Datenschutz bestehen große Lücken, die der Landesgesetzgeber schließen muss - etwa nach dem Vorbild der §§ 47 bis 47f des Rundfunkstaatsvertrages.

4. Elektronische Signatur und Verwaltungsverfahrensänderungsgesetz

Die Landesregierung habe ich auf erhebliche Schwachstellen bei den bisher entworfenen Bundesvorschriften zur Gleichstellung der elektronischen Kommunikation im Rechtsverkehr mit den herkömmlichen Papierdokumenten hingewiesen und Verbesserungsvorschläge unterbreitet. Die angestrebte rechtliche Gleichstellung elektronischer Dokumente mit Papierdokumenten wird bei Dokumenten mit dauerhaftem Beweiswert nur möglich sein, wenn diese auch in elektronischer Form dauerhaft unverfälscht verfügbar und lesbar sind.

4.1
Anlass für die rechtliche Gleichstellung von Papierform und elektronischer Form

Die zunehmende Nutzung der elektronischen Kommunikation, beispielsweise in Form von E-Mail (elektronischer Post) oder PC-Fax auch zwischen Bürgern und Behörden macht es nicht nur sinnvoll, sondern auch erforderlich, Rahmenbedingungen für ihre Rechtsverbindlichkeit festzulegen.

Ein Referentenentwurf für das Verwaltungsverfahrensänderungsgesetz wird derzeit vom Bundesinnenministerium in Abstimmung mit den Ländern erarbeitet. Er wird für die übermittelten elektronischen Dokumente in verschiedenen Gesetzen - z. B. im Verwaltungsverfahrensgesetz (VwVfG), im Sozialgesetzbuch X, in der Abgabenordnung und in Fachgesetzen - Anforderungen formulieren, die eine rechtliche Gleichstellung mit der „Schriftform“ bei herkömmlichen Papierdokumenten ermöglichen. Dies kann sowohl die Bürgerfreundlichkeit als auch die Effektivität der Behörden steigern.

Nachzubilden sind Regelungen, wie sie für Briefe und Urkunden einerseits aber auch für den Nachweis der Zustellung oder für den besonderen Beweiswert von Schriftstücken andererseits gelten. Sie betreffen Anforderungen an Verfügbarkeit (dauerhafte Speicherung und Lesbarkeit), Vertraulichkeit (insbesondere auf den Übermittlungswegen) sowie Integrität und Authentizität des Dokuments (Unverfälschtheit) und Nachweis der Urheberschaft.

Zusätzlich zu diesen Anforderungen an die neuen elektronischen Dokumente müssen jetzt selbstverständlich auch rechtsverbindliche Verfahren für die Überführung eines elektronischen Dokuments in ein Schriftstück und umgekehrt, also für den „Medienbruch“ zwischen Papier und Elektronik, gefunden werden.

Dem Änderungsgesetz zum VwVfG kommt insofern eine wesentliche Rolle zu, als es einen erheblichen Teil des Schriftverkehrs von und mit öffentlichen Dienststellen erfasst und als Bundesgesetz Vorbildfunktion für die Ländergesetze haben wird.

Aus diesem Grunde habe ich frühzeitig konstruktive Vorschläge unterbreitet, die inzwischen von vielen anderen Datenschutzbeauftragten aufgegriffen wurden.

4.2
Grundlegende Begriffe

Schriftliche Dokumente einerseits und elektronische Dokumente andererseits haben jeweils unterschiedliche Stärken und Schwächen. Diese lassen sich weder genau aufeinander abbilden, noch lassen sich die Stärken des einen durch das andere nachbilden. Hier liegen die besonderen Schwierigkeiten einer rechtlichen Gleichstellung.

Beim schriftlichen Dokument wird die Urheberschaft durch die Unterschrift (und ggf. einen Stempel) dokumentiert. Um den Zusammenhang der Urkunde zu sichern, werden einzelne Blätter ggf. fest verbunden. Es sind nur Papier, Stift und evtl. ein Stempel erforderlich.

Bei einem elektronischen Dokument fehlt die materielle Verbindung zwischen Text und Unterschrift. Um im elektronischen Rechts- und Geschäftsverkehr den Urheber und die Integrität von Daten festzustellen, wurde die „elektronische Signatur“ entwickelt. Die Funktion und Anwendungsmöglichkeiten der elektronischen Signatur habe ich bereits in meinem 24. Tätigkeits-bericht, Ziff. 17.1 ausführlich dargestellt.

Inzwischen wurde das Signaturgesetz (SigG) novelliert, um die gemeinschaftlichen Rahmenbedingungen der EG-Signaturrichtlinie 1999/93/EG umzusetzen. Das neue SigG vom 16. Mai 2001 unterscheidet einfache, fortgeschrittene und qualifizierte elektronische Signaturen. Die einfachen elektronischen Signaturen sind völlig ungeregelt. Die fortgeschrittenen elektronischen Signaturen lassen auch juristische Personen als Signaturschlüsselinhaber zu; sie verlangen weder eine zuverlässige Identifikation des Inhabers noch den Einsatz sicherer Komponenten. Diese beiden Signaturen sind für eine rechtsverbindliche Kommunikation *nicht* geeignet.

Die qualifizierten elektronischen Signaturen werden danach unterschieden, ob ihre Zertifikate von Diensteanbietern mit oder ohne Akkreditierung stammen. Solche *ohne* Akkreditierung entsprechen dem *Mindeststandard der EG-Signaturrichtlinie*. Sie sind nach Ablauf des Gültigkeitszeitraums des Zertifikats noch mindestens fünf Jahre überprüfbar. Dagegen wird bei *Signaturen mit Anbieter-Akkreditierung* der Anbieter vor Aufnahme der Tätigkeit und danach spätestens nach jeweils drei Jahren umfassend auf technische und administrative Sicherheit überprüft; er darf nur geprüfte und bestätigte Produkte verwenden. Ferner müssen Signaturen, deren Zertifikate von einem akkreditierten Diensteanbieter ausgestellt sind, 25 Jahre länger überprüfbar sein als jene nach EG-Mindeststandard.

Die qualifizierten elektronischen Signaturen und die zugehörige IT-Sicherheitsinfrastruktur (Zertifizierungsdienste, technische Komponenten, geeignete Prüf- und Bestätigungsstellen) sind der eigentliche Gegenstand des Gesetzes und werden ab § 4 bzw. in der zugehörigen Signaturverordnung geregelt.
Die Regelungen des alten Gesetzes zur digitalen Signatur entsprechen im Wesentlichen denen für qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung im neuen Signaturgesetz.

4.3
Anforderung an die Gleichstellung elektronischer Dokumente

4.3.1
Zustellungsfiktion

Meiner Anregung folgend ist die zunächst im Entwurf vorgesehene verkürzte Frist für die Zustellungsfiktion elektronischer Dokumente, die den ständigen „Blick“ in den elektronischen Briefkasten erzwungen hätte, wieder entfallen. Außerdem wurde - unabhängig von der Zustellung im In- oder Ausland - eine einheitliche Frist bei elektronischen Dokumenten gewählt. Die 3-Tages-Frist trägt dem Umstand Rechnung, dass elektronische Kommunikation bei Fehlern in der Technik nicht in jedem Fall schneller ist als die herkömmliche Post. Für die elektronische Post muss eindeutig festgelegt werden, wann die Frist zu laufen beginnt, d. h. was als Zeitpunkt der Absendung bei elektronischen Dokumenten gilt und auch wie bei diesen der Zugang nachgewiesen werden kann.

4.3.2
Aufnahme eines Verschlüsselungsgebotes

Elektronische Post ist eher mit einer Postkarte als mit einem Brief zu vergleichen, weil nicht sichergestellt ist, dass nur der Adressat vom Inhalt Kenntnis nehmen kann. Aus diesem Grund sollte zumindest für die Kommunikation von der Behörde zur Bürgerin bzw. dem Bürger ein Verschlüsselungsgebot aufgenommen werden.

Umgekehrt sollte festgelegt werden, dass auch die Bürgerinnen und Bürger mit der Verwaltung verschlüsselt kommunizieren können; dazu müssen die Behörden ihnen für die gängigen (marktüblichen) Verschlüsselungsverfahren öffentliche Schlüssel zur Verfügung stellen.

4.3.3
Einwilligung

Elektronische Kommunikation darf dem Adressaten nicht ohne ausdrückliche Einwilligung aufgedrängt werden. Es genügt nicht, dass Adressaten selbst mit der Behörde auf elektronischem Weg in Kontakt getreten sind, um zu unterstellen, dass sie die Kommunikation mit der Behörde generell auf diesem Weg führen möchten. Insbesondere vor dem Hintergrund technischer Anforderungen wie der Verfügbarkeit bestimmter Entschlüsselungs- oder Signaturverfahren oder der Notwendigkeit, den elektronischen Briefkasten zeitnah zu „leeren“, muss der Adressat die ausdrückliche Einwilligung unter Kenntnis aller Rechtsfolgen geben.

Wünschenswert wäre es, wenn Adressaten ihre Einwilligung zur elektronischen Kommunikation auf allgemeine Kommunikation ohne besondere Anforderungen oder Rechtsfolgen (z. B. besondere Formerfordernisse wie Schriftform oder beglaubigte Unterschrift, Fristenlauf) beschränken können.

4.3.4
Anforderungen an die Beglaubigung beim „Medienbruch“

Werden in Papierform erstellte Dokumente in elektronische Form überführt oder umgekehrt, so sind die Besonderheiten elektronischer Dokumente und der Ersatzformen für die Unterzeichnung solcher Dokumente zu beachten.

Ein Papierdokument wird unterzeichnet, in besonderen Fällen mit Beglaubigung der Unterschrift zur Identitätsprüfung. Die gleichen Anforderungen an die Beglaubigung sind im VwVfG geregelt. Daneben gibt es bei herkömmlichen Dokumenten den Fall, dass eine Kopie des Dokuments mit einem Beglaubigungsvermerk versehen wird, der die Übereinstimmung mit dem Original bestätigt. Auch die Anforderungen hieran sind im VwVfG geregelt.

Bei der Einführung elektronischer Dokumente sind im VwVfG folgende neue Fälle zu unterscheiden:

- Anforderungen an die Umsetzung eines beglaubigten Papierdokuments in elektronische Form,
- Ersatz der Beglaubigung elektronischer Dokumente bei Vervielfältigung,
- Ersatz der Beglaubigung der Unterschrift bei elektronischen Dokumenten,
- Anforderungen an die Umsetzung eines „beglaubigten“ elektronischen Dokuments in die Papierform.

Bei den genannten Fällen kommt der qualifizierten elektronischen Signatur, ihrer dauerhaften Überprüfbarkeit, der Sicherheit beim Anbieter sowie der eingesetzten Produkte entscheidende Bedeutung zu. Durch diese Signatur sind Dokumente gleichzeitig gegen unbemerkte Veränderungen geschützt. Die gleichen Anforderungen wie bei einer Beglaubigung können nur bei Einsatz von qualifizierten Signaturen mit Anbieter-Akkreditierung (s.u. Ziff. 4.4.1) erreicht werden. Dies hat der Gesetzgeber bisher noch nicht gesehen. Zu beachten ist auch, dass sich bei der elektronischen Form eine Kopie nicht von einem Original unterscheidet, es also beliebig viele gleiche „Originale“ geben kann. Deshalb ist eine besondere Beglaubigung einer „Kopie“ bei derart signierten Dokumenten überflüssig. Letzteres hat der Gesetzgeber inzwischen berücksichtigt.

Zur Regelung der übrigen Fälle habe ich Formulierungsvorschläge unterbreitet.

4.4
Praktische und rechtliche Probleme

4.4.1
Qualität der Signatur

Einfache und fortgeschrittene elektronische Signaturen erzeugen nur Scheinsicherheit und sind für eine rechtsverbindliche Kommunikation nicht einsetzbar (s.o. Ziff. 4.2). Dies gilt auch für die SPHINX-Signatur, die als reine Softwarelösung höchstens eine fortgeschrittene Signatur sein kann. Bei Speicherung des Signaturschlüssels auf der Festplatte muss selbst das bezweifelt werden, insbesondere wenn der Rechner in einem Inhouse-Netz hängt. Denn dann kann nicht mehr davon ausgegangen werden, dass die Signatur „mit Mitteln erzeugt wird, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann“.

Die qualifizierte elektronische Signatur ist der EG-Mindeststandard, der der eigenhändigen Unterschrift gleichsteht. Nur für qualifizierte elektronische Signaturen *mit Anbieter-Akkreditierung* ist nach § 4 Signaturverordnung eine *langfristige* Über-

prüfbarkeit gewährleistet, auch wenn für eine wirklich *dauerhafte* Überprüfbarkeit noch zusätzliche Regelungen getroffen werden müssen. Diese Signaturform bietet auch den Vorteil, dass die Sicherheit der Zertifizierungsdienste und der eingesetzten Produkte im Vorhinein nachgewiesen ist. Sie ist überall dort zu empfehlen, wo hohe Sicherheit oder langfristige Überprüfbarkeit erforderlich sind. Sie ist für *alle* Anwendungsbereiche geeignet, schafft Rechtssicherheit und ist grundsätzlich nicht teurer als der EG-Mindeststandard.

Deshalb sprechen sich renommierte Institutionen wie die Arbeitsgemeinschaft der Verbraucherverbände (AgV), die Stiftung Warentest, der Deutsche Städtetag, die Gesellschaft für Informatik (GI) und die Bundesnotarkammer nachdrücklich für die Anwendung der Signaturen mit nachweislich hoher Sicherheit aus.

4.4.2
Fehlende Anwendungs-Produkte

Wichtig wird auch die Entwicklung von Anwendungs-Produkten, die die qualifizierte Signatur sinnvoll nutzen. So ist es beispielsweise wünschenswert und evtl. auch aus Datenschutzgründen erforderlich, dass man einzelne Dokumente signieren und dann, z. B. als Anlage einer E-Mail, versenden kann, statt eine E-Mail mit allen Anlagen zu signieren und dann zu versenden.

4.4.3
Archivierung

Qualifiziert signierte elektronische Dokumente als „Originale“ genießen im Falle einer rechtlichen Auseinandersetzung denselben Beweiswert wie Original-Papierdokumente. Damit wird ihre langfristige sichere Archivierung erforderlich. Der einfache Papierausdruck eines elektronischen Dokuments ist wertlos; er steht einer unbeglaubigten Kopie eines unterschriebenen Papierdokuments - selbst wenn Signatur und Zertifikat mit angedruckt werden - gleich, weil eine Prüfung der Signatur auf dem Papier nicht mehr möglich ist. Selbst eine beglaubigte Überführung in die Papierform ersetzt nach den derzeitigen Regelungen nicht das Original.

Hier müssen alsbald Verfahren und Dienstleistungen zur langfristigen sicheren Archivierung entwickelt werden. Zudem müssen sowohl die Bürgerinnen und Bürger als auch die Mitarbeiterinnen und Mitarbeiter von Behörden informiert werden, dass sie elektronische „Originale“ nicht löschen dürfen. Sie müssen auf die Vernichtung des Beweiswertes hingewiesen werden, die mit einer Löschung einhergeht.

Will man lediglich die Unverfälschtheit und Authentizität von Daten während des Transports von Sender zum Empfänger sichern, ist die Anwendung der qualifizierten elektronischen Signatur unproblematisch. Wenn das signierte Dokument für Beweiszwecke aufbewahrt werden soll, müssen zusätzliche technische und organisatorische Vorkehrungen getroffen werden.

Bei der Archivierung elektronischer Dokumente stellt sich neben der dauerhaften Überprüfbarkeit der Signatur auch die Frage nach der Verfügbarkeit und Nutzbarkeit der früher verwendeten Hard- und Software, um das Dokument nach langer Zeit wieder in der ursprünglichen Form anzeigen zu können. Diese Frage ist wegen der kurzen Innovationszyklen von Hard- und Software nicht einfach zu lösen und wirft dort praktische Probleme auf, wo die Würdigung des Inhalts eines alten signierten archivierten Dokuments notwendig wird.

4.4.4
Interoperable Produkte

Wichtig - und nicht von vornherein selbstverständlich - ist schließlich, dass nicht eine Vielzahl verschiedener technischer Ausstattungen vorgehalten werden muss, um mit *allen* Partnern rechtsverbindlich kommunizieren zu können. Dies ist mit *einer* einzigen technischen Ausstattung möglich, wenn man Produkte einsetzt, die die einheitliche Interoperabilitätsspezifikation „ISIS-MTT“ einhalten. Diese Spezifikation bezieht sich auf die Sicherheitsfunktionen elektronische Signatur, Authentisierung und Verschlüsselung, nicht aber auf die Datenaustauschformate. Sie sollte bei Ausschreibungen und Beschaffungen zugrunde gelegt werden, um Fehlinvestitionen zu vermeiden.

5. Videoüberwachung

5.1
Videoüberwachung auf Grundlage des § 14 Abs. 3 und 4 HSOG

Die neuen Befugnisse für Polizei und Gefahrenabwehrbehörden zum Einsatz von Videoüberwachungsanlagen werden zunehmend - zum Teil sehr extensiv - genutzt. Jedes Projekt wird von mir unter Berücksichtigung der örtlichen Besonderheiten und der beteiligten Stellen bewertet.

Wie zu erwarten war, hat die Einfügung der Abs. 3 und 4 in § 14 des Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) im vergangenen Jahr dazu geführt, dass an vielen Stellen Forderungen zum Einsatz von Videokameras laut geworden sind.

§ 14 Abs. 3 und 4 HSOG

(3) Die Polizeibehörden können zur Abwehr einer Gefahr oder wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten drohen, öffentlich zugängliche Orte mittels Bildübertragung offen beobachten und aufzeichnen. Abs. 1 Satz 2 und 3 gilt entsprechend.

(4) Die Gefahrenabwehrbehörden können mittels Bildübertragung offen beobachten und aufzeichnen:
1. zur Sicherung öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, sofern tatsächliche Anhaltspunkte für weitere Straftaten bestehen,
2. zum Schutz besonders gefährdeter öffentlicher Einrichtungen,
3. zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs, soweit Bestimmungen des Straßenverkehrsrechts nicht entgegenstehen.
Gefahrenabwehrbehörde im Sinne der Nr. 2 ist auch der Inhaber des Hausrechts. Abs. 1 Satz 2 und 3 gilt entsprechend.

Durch solche Kameras erhoffen sich viele einen Beitrag zur Sicherheit im öffentlichen Raum. Dies zeigt sich etwa auch an der verharmlosenden Verwendung des Wortes „Videoschutzanlage“ anstelle von „Kamera-“ oder „Videoüberwachung“. Bei einzelnen Projekten bin ich vorab um eine Stellungnahme gebeten worden. Von anderen erfahre auch ich nur durch die öffentliche Diskussion in der Presse. Der Rückgriff auf die Möglichkeiten des Polizeirechts ist immer im Einzelfall anhand der vorhandenen Gegebenheiten und Konzeptionen zu bewerten. Dabei ist darauf zu achten, dass die unterschiedlichen Anforderungen, die die Regelungen in § 14 Abs. 3 und 4 HSOG für die Polizei und die, Gefahrenabwehrbehörden benennen, auch eingehalten werden.

Für viele dieser Projekte gilt, dass Polizei und Kommune als Gefahrenabwehrbehörde zusammenarbeiten, und zwar sowohl bei der Entscheidung, ob und welche Räumlichkeiten überwacht werden sollen, als auch bei der technischen Realisierung des Kameraeinsatzes.

5.1.1
Bahnhofsvorplatz in Limburg

Bei diesem Projekt bin ich vorab über den städtischen Datenschutzbeauftragten um Beratung gebeten worden.

In Limburg wird seit einiger Zeit die Zusammenarbeit von Ordnungsamt und Polizei intensiviert. Dabei geht es vor allem um die Bekämpfung der Drogenkriminalität im Bereich des Bahnhofsvorplatzes und in einer Unterführung am Bahnhof. Die Bekämpfung dieser Kriminalität soll nun durch den Einsatz von Videokameras unterstützt werden.

Aufgestellt werden sollten nach ersten Plänen bis zu 16 Kameras in der Bahnhofsunterführung und auf dem Bahnhofsvorplatz. Damit wäre bis in die Einkaufsstraßen hinein eine umfassende Beobachtung eines großen Teils der Innenstadt möglich gewesen. Die Planung und voraussichtlich auch die Beschaffung erfolgen durch die Kommune unter Beteiligung der Polizei. Die konkrete Überwachung an den Bildschirmen bzw. die Aufzeichnung soll durch die Polizei erfolgen. Ursprünglich war geplant, dass die Monitore durch Personal des Ordnungsamtes überwacht werden sollen, wenn der Polizeiposten wegen anderer Einsatzorte der Beamten nicht besetzt ist. Davon wurde inzwischen Abstand genommen.

Die weite Dimension der geplanten Maßnahme relativierte sich in einem Gespräch vor Ort. Bei der Besichtigung des zu überwachenden Platzes wurde deutlich, dass eine Vielzahl von Kameras allein auf Grund der baulichen Gegebenheiten und der sehr winkligen Unterführung benötigt werden. Auf dem Bahnhofsvorplatz konnten gemeinsam Einschränkungen des Bereichs erarbeitet werden, der erfasst wird. Durch technische Möglichkeiten wie z. B. Beschränkung des Schwenkbereichs, Ausblendung von Wohnhäusern etc. war es möglich, die Überwachung auf den ursprünglichen Zweck, die Beobachtung der Drogenszene auf dem Vorplatz und der Unterführung, einzugrenzen.

Die Maßnahme soll voraussichtlich im kommenden Jahr realisiert werden. Unter der Voraussetzung, dass die vor Ort mit mir diskutierten und oben beschriebenen Beschränkungen des erfassbaren Bereichs in die Praxis umgesetzt werden, halte ich die Installierung der Videokameras für rechtlich zulässig. Für die weitere Zukunft sollte an den Einsatz von Kamerasystemen gedacht werden, die die Gesichter rastern. Die Entschlüsselung der gleichzeitig aufgezeichneten Klardaten sollte besonders dazu berufenen Bediensteten der Gefahrenabwehr- und Strafverfolgungsbehörden vorbehalten bleiben.

5.1.2
Rhein-Main Flughafen

Am Frankfurter Flughafen kommen Videokameras naturgemäß aus sehr unterschiedlichen Zwecken zum Einsatz. Interesse daran haben Polizei und Bundesgrenzschutz ebenso wie die Fraport AG selbst. Das gilt auch für die am Flughafenbahnhof im Rahmen des Sicherheitskonzepts der Deutschen Bahn eingesetzte Videotechnik.

Die Anlage am Flughafen wird von der Fraport AG betrieben, die anderen Nutzer können (teilweise) auf die Kameras zugreifen. Die Kameras der Fraport AG sind Analogkameras, die an zentrale Systeme angeschlossen sind. Ein Teil der Kameras ist steuerbar, während andere Kameras immer den gleichen Bereich abbilden. An diesen Systemen sind neben den Kameras, die die Bildsignale liefern, auch alle Monitore angeschlossen.

Die Monitore sind in vier Leitstellen der Fraport AG sowie der Polizeistation Flughafen und der Leitstelle des BGS zusammengefasst:

- Integrierte Leitstelle (Passagierführung) - Beobachtung vor allem des Abfertigungsbereichs
- Parkierungsleitwarte (Autoführung) - Beobachtung Zufahrt Parkhäuser sowie Teile der B 43
- Sicherheitsleitstelle (Security und Safety)
- Vorfeldkontrolle
- Polizeidirektion Flughafen
- Leitstelle BGS-Flughafen

Bilder von Kameras, die den Stauraum (Fahrzeugüberwachung) überwachen, werden teilweise 24 Stunden aufgezeichnet; es sind aber keine Details zu erkennen.

Da die unterschiedlichsten Stellen beteiligt sind, sind für die Überprüfung der datenschutzrechtlichen Belange verschiedene Aufsichtsbehörden zuständig. Ich habe mich daher gemeinsam mit dem Bundesbeauftragten für den Datenschutz und der Aufsichtsbehörde beim Regierungspräsidium über die Details dieses Kameraeinsatzes informiert.

In der Regel erfolgt kein Mitschnitt der Bilder. Dies kann im Einzelfall durch jede der beteiligten Stellen veranlasst werden; im Bereich der Sicherheitskontrollen der Fluggäste erfolgt die Aufzeichnung immer dann, wenn vom Personal ein Alarm ausgelöst wird. Gespeichert wird durch die Fraport AG, die die Aufnahmen dann an die Stelle weitergibt, die sie veranlasst hat.

Die Steuerung der Kameras erfolgt über die zentralen Systeme. Dort ist festgelegt:
- an welchen Monitoren die Bilder einer bestimmten Kamera wiedergegeben werden können,
- welcher Arbeitsplatz das Bild einer bestimmten Kamera anfordern kann,
- wer mit welcher Priorität eine Kamera steuern kann,
- an welchem Monitor das Bild einer Kamera angezeigt wird, wenn ein Alarm ausgelöst wird. (Wenn ein Notfallmelder betätigt wird, erfolgt automatisch die Aufschaltung eines Monitors in der Sicherheitsleitstelle sowie auf einen Monitor der Leitstelle des BGS auf die zugeordnete Kamera und es wird eine Aufzeichnung angestoßen.)
- bei Kameras in deren Aufnahmebereich auch Arbeitsplätze von Fraport AG-Mitarbeitern liegen, leuchtet eine rote Lampe auf, sobald das Bild an Monitore übertragen wird,
- dass die integrierte Leitstelle auf alle Kameras zugreifen kann,
- ein Mitschnitt erfolgt u.U. auch auf Anforderung des BGS oder der Polizei (Auftragsdatenverarbeitung),
- Mitschnitte werden auch für die Information der Rettungsleitstellen nach dem Hessischen Rettungsdienstgesetz durchgeführt.

Die Dokumentation der Fraport AG zur Videoanlage umfasst insbesondere Unterlagen, wer mit welcher Priorität auf welche Kameras zugreifen kann.

Vor einer abschließenden Bewertung durch die verschiedenen Datenschutzkontrollinstanzen wird die Fraport AG die Detailregelungen zu den oben skizzierten Verfahrensweisen beschreiben. Erst dann kann geklärt werden, ob das bisherige Verfahren beibehalten werden kann oder ob zusätzlicher Regelungsbedarf besteht.

5.2
Der Videoeinsatz zur Gefahrenabwehr hält auch bei den Hochschulen Einzug

Eine Universität darf zur Verhinderung künftiger Straftaten Videokameras auf dem Hochschulgelände installieren.

Die Johann Wolfgang Goethe-Universität in Frankfurt hat mich um Prüfung gebeten, inwieweit Videokameras auf dem Hochschulgelände installiert werden dürfen.
Die Hochschulverwaltung hatte festgestellt, dass in der Vergangenheit zahlreiche DV-Geräte mit beachtlichem Wert aus den Hochschulräumen entwendet worden waren. Sie vermutete, dass die Diebe den Notausgang benutzt hatten, der von der Pförtnerloge nicht einsehbar ist. Ferner waren aus einem Biozentrum gefährliche chemische Tinkturen entwendet worden, die sich später auf einem öffentlichen Platz wiederfanden. Zur Verhinderung künftiger Straftaten sollten Videokameras an geeigneten Stellen installiert werden. Dabei sollten die überwiegend außerhalb der Dienstzeiten entstandenen Bilder aufgezeichnet und spätestens nach 14 Tagen wieder gelöscht werden.

§ 14 Abs. 4 HSOG

Die Gefahrenabwehrbehörden dürfen offen Bildaufzeichnungen anfertigen:
1. Zur Sicherung öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, sofern tatsächliche Anhaltspunkte für weitere Straftaten bestehen,
2. zum Schutz besonders gefährdeter öffentlicher Einrichtungen,
3. zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs, soweit Bestimmungen des Straßenverkehrs nicht entgegenstehen.

Gefahrenabwehrbehörde im Sinne der Nr. 2 ist auch der Inhaber des Hausrechtes. Abs. 1 Satz 2 und 3 gilt entsprechend.

Die Universität Frankfurt als Inhaberin des Hausrechts hinsichtlich der von ihr verwalteten Hochschulgebäude und des Inventars ist zuständig (§ 14 Abs. 4 Satz 2).

Als eine besondere Gefährdung der öffentlichen Einrichtung „Hochschule“ kann gewertet werden, dass in der Vergangenheit Sachgüter der Hochschule mit erheblichem Wert beschädigt bzw. gestohlen wurden und konkret zu befürchten steht, dass gleichartige Straftaten auch künftig begangen werden. Geeignete andere Mittel zur Verhinderung der Straftaten stehen nicht zur Verfügung. Ich habe den Videoeinsatz daher für zulässig gehalten, allerdings mit der Maßgabe, dass die Hochschulverwaltung vor Ort einen leicht erkennbaren Hinweis auf die Videoüberwachung anbringt. Dies verlangt § 14 Abs. 4 Satz 1 HSOG; der Präventiveffekt wird zudem besser durch offene Überwachung erreicht. Die von der Hochschulverwaltung einzuhaltende Löschungsfrist von maximal zwei Monaten war gewährleistet, da der Film nach spätestens zwei Wochen überspielt werden soll.

§ 14 Abs. 1 Satz 2 HSOG

... Die Unterlagen sind spätestens zwei Monate nach Beendigung der Veranstaltung oder Ansammlung zu vernichten, soweit sie nicht zur Verfolgung einer Straftat oder Ordnungswidrigkeit oder zur Strafvollstreckung benötigt werden.

6. Internet

6.1
Internettestwahl in Marburg

Bei der Landratswahl im Kreis Marburg-Biedenkopf am 16. September 2001 konnten Briefwähler erstmals in Hessen testweise ihre Stimme auch über das Internet abgeben. Durch pseudonyme Stimmabgabe, anonyme Stimmauszählung und verschlüsselte Datenübertragung konnte das Briefwahlgeheimnis gewährleistet werden.

Meine Dienststelle wurde im Vorfeld über die geplante Testwahl informiert und ebenso wie der Landeswahlleiter durch die Projektgruppe (Universität Marburg, eine Softwarefirma, Stadt und Kreis Marburg) in die Planungen mit einbezogen. Im Rahmen der ersten Internetwahl sollte ausschließlich das Briefwahlverfahren simuliert werden, weil sich nur bei diesem Verfahren die derzeit geltenden Wahlrechtsvorgaben nahezu spiegelbildlich umsetzen ließen. Schwerpunkt meiner Beratung war die Frage, welche Maßnahmen getroffen werden müssen, damit das Wahlgeheimnis gewahrt bleibt.

6.1.1
Ausgestaltung der Testwahl

Die wesentlichen Maßnahmen zur Gewährleistung des Wahlgeheimnisses waren:
- **Pseudonyme Stimmabgabe:** Die Informationen auf dem Wahlserver erlauben es nicht, den Wähler zu erkennen.
- **Anonyme Stimmauszählung:** Es ist nicht bekannt, wer welchen Stimmzettel abgegeben hat.
- **Verschlüsselte Datenübertragung:** Ein Zugriff Dritter auf die Stimmdaten ist unmöglich.

Um an der Internet-Testwahl teilnehmen zu können, erhielten die Wähler einen PIN-Brief mit einer Zahlenkombination (PIN und TAN), die sie als Testwähler auswies. Auf dem PIN-Brief war eine laufende Nummer gedruckt. Wem welcher PIN-Brief zugesandt wurde, war nur dem Wahlamt bekannt; es notierte, welche laufende Nummer welchem Wähler zugeordnet wurde, kannte die PIN und TAN aber nicht.
Wenn der Wähler über das Internet auf den Wahlserver zugriff, wurde die Verbindung über das SSL-Protokoll gesichert, eine im Internet etablierte Technik zur verschlüsselten Übertragung von Daten, damit Unbefugte die Daten nicht lesen können.
Der Wähler hatte sich durch die Eingabe der PIN/TAN-Kombination als Testwähler auszuweisen. Auf dem Wahlserver wurde anschließend geprüft, ob es sich um eine gültige Kombination handelt. Dazu waren auf dem Server die laufenden Nummern mit den zugehörigen PIN/TAN-Kombinationen gespeichert, es gab aber keine Hinweise, welchem Wähler welcher PIN-Brief ausgehändigt wurde.

Nachdem der Wähler gewählt hatte, wurden die Stimmdaten zum Server verschlüsselt übertragen und dort erneut verschlüsselt gespeichert. Zu diesem Zeitpunkt gab es noch eine Referenz zwischen der laufenden Nummer und den verschlüsselten Stimmdaten. Diese ist erforderlich, da es bis 18:00 Uhr am Wahltag noch möglich sein muss, Stimmen für ungültig zu erklären und nicht zu zählen.
Das Wahlamt teilte nach Schließung der Wahllokale dem Wahlvorstand mit, welche der im herkömmlichen Verfahren abgegebenen Stimmzettel ungültig waren und welche PIN-Briefe nicht ausgegeben wurden. Vor der Stimmauszählung wurden die für ungültig erklärten Stimmzettel aussortiert. Bevor der Wahlvorstand die Internetdaten erhielt, um sie zu entschlüsseln und als Stimmen zu zählen, wurden Hinweise auf die laufende Nummer und PIN/TAN gelöscht. Danach war es nicht mehr möglich zu rekonstruieren, welcher Wähler wie gewählt hatte.

6.1.2
Probleme, die vor einer Echtwahl gelöst werden müssen

Bei einer Echtwahl mit elektronischer Stimmabgabe muss befürchtet werden, dass versucht wird, durch unberechtigte Zugriffe die Ergebnisse zu fälschen oder aufzudecken, wer wie gewählt hat. Um dem zu begegnen, muss ein Sicherheitskonzept erstellt werden, das die Risiken benennt und die erforderlichen Gegenmaßnahmen festlegt. Es reicht nicht, durch eine Firewall unberechtigte Zugriffe von außen abwehren zu wollen.

Dafür einsetzbare Vorkehrungen sind zum Beispiel:
- Intrusion Detection Systeme einzusetzen (vgl. 28. Tätigkeitsbericht, Ziff. 10.3),
- den Server in gesicherten Räumen unterzubringen, zu denen nur Wahlhelfer Zutritt haben,
- nur solche Software auf dem Server zu speichern und zu starten, die für die Abwicklung der Wahl erforderlich ist,
- alle Komponenten der für die Wahl benötigten Software hinsichtlich Funktion und Sicherheit zu evaluieren und zu zertifizieren,
- die Protokollierung auf das absolute Minimum zu beschränken oder auf anderen Rechnern durchzuführen, damit eine Zusammenführung der Daten erschwert wird,
- bei Zugriffen auf den Server ein 4-Augen-Prinzip (z. B. Doppelpasswort) umzusetzen,
- die Verschlüsselung der Stimmdaten über eine Chipkarte vorzunehmen, damit die Schlüssel nicht kopiert werden können.

Die Details zur Datensicherheit müssen auf Bundes- bzw. Landesebene einheitlich festgelegt werden.
Um zu verhindern, dass die für die Wahl gültigen PIN/TAN-Kombinationen bekannt werden, sollten diese ähnlich wie beim Online-Banking durch vertrauenswürdige Institutionen erstellt werden, die keine Kenntnis der Zuordnung zwischen laufender Nummer und Wähler haben.
Um die Stimme abgeben zu können, muss der Wähler Java-Script zulassen. Damit ergeben sich potentielle Sicherheitsprobleme. (27. Tätigkeitsbericht, Ziff. 8.2 und Anhang 2) Es sollte bei einer Echtwahl dem Wähler die Möglichkeit gegeben werden, die Herkunft und Unversehrtheit des Codes vor der Ausführung zu verifizieren.

Die Versicherung an Eides statt, dass der Wahlberechtigte auch tatsächlich selbst gewählt hat, findet im Internet ohne Unterschrift statt. Dies ist eine erhebliche Abweichung von der Briefwahl, zu der eine technische oder rechtliche Lösung gefunden werden muss.
Das Verfahren bietet auch nicht die Möglichkeit, dass eine Hilfsperson eine Erklärung an Eides statt abgeben kann. Dies ist ebenfalls eine erhebliche Abweichung von der Briefwahl.

6.1.3
Ergebnis der Testwahl

Die Testwahl verlief nach übereinstimmender Meinung aller Beteiligten erfolgreich. 234 Wähler in Marburg, das waren ca. 7 % aller Briefwähler, haben an der Internetwahl teilgenommen. Die vergleichsweise hohe Quote wurde insbesondere darauf zurückgeführt, dass die Wähler keine besondere Hard- und Software für die Wahl benötigten.

Bei den Abläufen kam es zwar zu Verzögerungen, aber man beabsichtigt durch entsprechende Checklisten die Ursachen in den Griff zu bekommen.

6.1.4
Fazit

Die Briefwahl per Internet ist ein erfolgversprechender Ansatz. Vor einer Echtwahl müssen allerdings noch einige Probleme angegangen und beseitigt werden.

6.2
Anonymität bzw. das Recht auf informationelle Selbstbestimmung im Internet

Das Telekommunikations- und Teledienstrecht schreibt vor, das Internet anonym oder pseudonym nutzen zu können. Die technischen Lösungsansätze sind heute noch nicht ausreichend.

Bereits im letzten Tätigkeitsbericht (Ziff. 11.4) ist die Möglichkeit des anonymen Surfens dargestellt worden. Der nachfolgende Beitrag ist eine Fortsetzung. Ob Internet-Nutzer die Möglichkeit haben sollten, anonym zu surfen oder E-Mails zu verschicken, wird aufgrund der Geschehnisse des 11. September 2001 und der Gefahr terroristischer Angriffe auf Rechnersysteme zur Zeit kontrovers diskutiert. Umstritten ist auch die rechtliche Zuordnung der Dienste zu Telekommunikations- oder Teledienstleistungen.

6.2.1
Spannungsfeld

Durch anonyme oder pseudonyme Nutzung des Internet kann die Privatsphäre des Einzelnen effektiv geschützt werden. Allerdings haben die letzten Monate gezeigt, dass Anonymisierungen Sicherheitsrisiken mit sich bringen. Der ordnungsgemäße Betrieb der Datenverarbeitung erfordert ein Mindestmaß an Protokollierung personenbezogener Daten (Server, Filter, Leistungen etc.). Darauf richtet sich das Interesse der Strafverfolgungsbehörden, bei Ermittlungen wegen Terrorismus, Rechtsradikalismus, Kinderpornographie und Computerkriminalität auf die personenbezogenen Spuren der Internet-Nutzer zugreifen zu können.

6.2.2
Personenbezogene Daten bei der Internetnutzung

Während der Internetnutzung fallen bei den Internet-Zugangs-Providern, Internet-Service-Providern, System-Administratoren und Client-Rechnern personenbezogene Daten an. Bei den Internet-Zugangsprovidern sind dies Dienste- und Inhaltsdaten.

Zu den Daten, die die Abwicklung der Dienstleistung ermöglichen, gehören die Bestandsdaten, die Nutzungsdaten und die Abrechnungsdaten.

Datenart		**Beschreibung**	**Beispiele**	**Rechtsgrundlage**
Dienstedaten	Bestandsdaten	Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erforderlich sind.	Name, Anschrift der Nutzer, statische IP-Nummer, Kontonummer, Kreditkartennummer	TDDSG, MDStV
	Nutzungsdaten	Nutzungsdaten, die für die Inanspruchnahme von Diensten erforderlich sind.	Name oder IP-Adresse des anfragenden Clients, Username, Anfrage und deren Status	TDDSG, MDStV
	Abrechnungsdaten	Nutzerdaten für die Abrechnung von Diensten	Zeitpunkt und Dauer von Verbindungen, Datenvolumen	TKG, TDDSG, MDStV
Inhaltsdaten		Aus den Internetangeboten abgerufene Informationen	Bytes, Zeichen, Bilder, Töne	Landesdatenschutzgesetze, BDSG, Fachgesetze

Weitere Datenspuren entstehen durch die an den Diensteanbieter beim Surfen übermittelten Daten wie beispielsweise
- Browsermeldungen (Browsertyp und Version)
- Hardware, Betriebssystem und Anwendungsprogramm
- eingestellte Sprache
- aktuelle IP-Adresse (dynamisch oder statisch)
- E-Mail-Adresse (soweit sie im Browser gespeichert ist).

Hinzu kommen weitere Datenspuren in den auf den Servern gespeicherten Protokolldateien; sie zeichnen oft weitergehende Informationen über die Nutzer, beispielsweise die aufgerufene URL mit genauer Zeitangabe, auf. Durch diese und weitere Daten, die mit Hilfe von Cookies und Web-Bugs auf den Client-Rechnern entstehen, ist dem Anbieter eine Analyse des Nutzer- und Konsumverhaltens möglich. Durch das Zusammenführen der verschiedenen Datenspuren lassen sich Nutzerprofile erstellen. Das geschieht im Wesentlichen durch die Auswertung von Cookies, Web-Bugs, Log-Files (Protokolldaten) und Online-Bestellungen (s. 29. Tätigkeitsbericht, Ziff. 11.4).

Cookies (engl. cookie = Keks)

Kleine Dateien, die zusammen mit den eigentlich angeforderten Daten aus dem Internet verschleiert an den Computer des Benutzers übermittelt werden. Dort werden diese Daten gespeichert und für einen späteren Abruf bereitgehalten. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Nutzers (exakt: des Browsers auf dem Computer, den er verwendet) auf das Internet-Angebot erkennbar.

Web-Bugs

Winzige, auf den Seiten des Anbieters versteckte Bilder mit hinterlegten Programmbefehlen, die vom Benutzer beim Abruf der Seiten nicht oder kaum wahrgenommen werden. Wenn sie mit einem Browser angesehen werden, könnten sie die IP-Adresse, die www-Adresse der besuchten Webseite, den Zeitpunkt des Ansehens und Informationen eines zuvor gesetzten Cookies an die www-Adresse eines vorgegebenen Servers senden. Sie können auch in E-Mails untergebracht werden.

Client-Rechner

In einem lokalen Netzwerk und im Internet stellt ein Client-Rechner einen Computer dar, der auf die von einem anderen Computer (dem sog. Server) bereitgestellten, gemeinsam genutzten Netzwerkressourcen zugreift.

6.2.3
Vermeidung von Datenspuren und Nutzerprofilen

6.2.3.1
Überblick der Lösungsmöglichkeiten

Es gibt mehrere Möglichkeiten, Datenspuren und Nutzerprofile zu vermeiden:

Lösungsansatz	**Technische Umsetzung**
Anonymisierungsverfahren	Mixe JAP
Neue Standards	P3P
Client-Software	Webwasher u. a.

6.2.3.2
Anonymisierungsverfahren
6.2.3.2.1
Mixe

Anonymisierungsverfahren sind in der Regel Mixe nach dem Konzept von David Chaum von 1981 (s. Orientierungshilfe für datenschutzfreundliche Technologien in der Telekommunikation, Ziff. 4.1.4; http:\www.datenschutz.hessen.de\o-hilfen\dft-tk.htm)

Mixe

Netzknoten, die zum Schutz der Kommunikationsbeziehung dienen, in dem sie die Verkettbarkeit zwischen Sender und Empfänger einer Nachricht verhindern.

6.2.3.2.2
JAP

Das Projekt JAVA ANON PROXY ist eine Soft- und Hardware-Entwicklung der Technische Universität Dresden in Zusammenarbeit mit dem unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. Die Kommunikation bei JAP

erfolgt nicht direkt zwischen dem Client und dem Web-Surfer, sondern über eine Mix-Proxy-Kaskade. Die Anonymität entsteht durch die gleichzeitige Nutzung vieler Teilnehmer. Jeder Betreiber eines Mix-Proxy-Server verpflichtet sich zudem, keine Log-Dateien zu speichern und keine Daten mit anderen Mix-Proxy-Betreibern auszutauschen. Es erfolgt eine Überprüfung durch unabhängige Prüfstellen.

6.2.3.3
Neuer Standard P3P

6.2.3.3.1
Definition

Ein weiterer datenschutzfreundlicher Ansatz ist der Standard P3P. Er steht für Plattform für Privacy Preferences. Das World Wide Web Consortium betreibt diesen Standardisierungsprozess unter Beteiligung von Firmen und Datenschutzbeauftragten. Dieser technische Basisstandard sorgt durch Datenschutzpolicies für Transparenz bei dem Nutzer und setzt auf Selbstregulierung. Unverzichtbar sind ergänzende Datenschutzkontrollen, um die in Deutschland bereits bestehenden präzisen Rechtsnormen nicht leer laufen zu lassen.

6.2.3.3.2
Funktion

Das neue Verfahren sieht vor, dass künftig von Nutzern Voreinstellungen des Browsers vorgenommen werden können, mit denen das Datenschutzniveau den individuellen Anforderungen angepasst werden kann. Beim Aufruf einer Web-Page wird der Browser künftig die vom Nutzer voreingestellten Datenschutzforderungen mit der Policy des jeweiligen Betreibers der Web-Page vergleichen. Leider ist dieses Verfahren noch nicht verfügbar. Erste Implementa-tionsversuche des Standards gab es bereits im Dezember 2000. Der Standard besteht aus einem Set von Multiple-Choice-Fragen zum Thema Privacy an Daten verarbeitende Unternehmen und Behörden. Die Antworten werden via XML als maschinenlesbare Privacy-Policy in beliebige Web-Page eingebunden.

6.2.3.3.3
Ausblick

Der Standard findet die Zustimmung der Browser-Firmen AOL, Netscape und Opera, wurde aber bis jetzt noch nicht in der Software berücksichtigt. Bisher ist nur im Internet Explorer 6.0 eine erste abgespeckte Version P3P, die sich im Wesentlichen mit der Behandlung von Cookies beschäftigt, implementiert. Außerdem können die Datenschutzpolicies einzelner Anbieter damit leichter aufgerufen werden.

6.2.3.4
Client-Software

Auf den Client-Rechnern fallen - wie beschrieben - beim Surfen Daten an, die Aufschluss über das Verhalten des Nutzers erlauben. Die beim Nutzer eingespeicherten Cookies, Web-Bugs und der geräteeigene Cachespeicher sind sehr „geschwätzig“. Deshalb sollen nach jeder Internet-Session die verräterischen Spuren gelöscht werden. Dies kann der Nutzer manuell oder mit Hilfe von speziellen Softwareprodukten selbst durchführen. Als Beispiel sei hier der kostenlose „Webwasher“ genannt. Aber auch andere kommerzielle Produkte wie z. B. Internet Cleanup 2.0 erfüllen hier die gewünschten Anforderungen.

6.2.4
Ergebnis

Das TDDSG und der MDStV sehen die Möglichkeit vor, das Internet sowohl anonym als auch pseudonym zu nutzen. Die technischen Varianten sind Teillösungen und werden den verschiedenen Rollen bzw. Identitäten, die der Nutzer annehmen kann, nicht im ausreichendem Maße gerecht. Sog. Identifikationsmanagement-Systeme scheinen für die Zukunft die geeignete Lösung zu sein. Sie sollen die Nutzer befähigen, die Verwaltung ihrer personenbezogenen Daten in der Online-Welt selbst in die Hand zu nehmen. Sie beschreiben die verschiedenen Rollen und bieten hierfür die jeweils passenden Sicherheitslösungen an. Mit diesen Systemen wird auch in Zukunft eine Identifizierung zu bestimmten rechtlich zulässigen Zwecken möglich sein. Die Entwicklungen im Bereich der Identifikationsmanagement-Systeme der Technische Universität Dresden und Universität Freiburg werden hoffentlich bald verfügbar sein.

6.3
Dienstliche und private Nutzung von E-Mail und www

Die im 29. Tätigkeitsbericht (Ziff. 22.2) abgedruckte Orientierungshilfe für dienstliche und private Nutzung von E-Mail und www wurde überarbeitet.

Sich häufende Anfragen zu den datenschutzrechtlichen Anforderungen privater und dienstlicher Nutzung der Internetdienste E-Mail und World Wide Web hatten mich veranlasst, im letzten Tätigkeitsbericht und auf meiner Webseite eine Orientierungshilfe zu veröffentlichen. In der anschließenden Diskussion zeigte sich, dass einige der darin angesprochenen Punkte einer Änderung, Präzisierung oder Ergänzung bedurften. Ziff. 28.1 dieses Berichts enthält deshalb eine überarbeitete Neufassung, die seit dem 24. Oktober 2001 auch auf der Homepage im World Wide Web zu finden ist (www.datenschutz.hessen.de).

Die überarbeitete Orientierungshilfe stellt klar, dass die dienstliche Nutzung des E-Mail-Dienstes ähnlich zu beurteilen ist wie der herkömmliche Briefverkehr. Sie enthält Empfehlungen zur Lösung des zuvor nicht behandelten Problems, wie der E-Mail-Verkehr mit Funktionsträgern, die in der Dienststelle eine besondere Vertrauensstellung haben, z. B. Personalräten oder Suchtbeauftragten, organisiert werden sollte. Diese Personen sollten eine eigene E-Mail-Adresse erhalten und es sollte durch organisatorische Maßnahmen sichergestellt werden, dass die an sie gerichteten E-Mails Dritten in der Dienststelle nicht zugänglich sind.

Zu den möglichen Organisationsformen wird nunmehr deutlicher zwischen Verbindungsdaten, die bei der Nutzung des Dienstes anfallen, und den Inhalten, die mittels der Dienste transportiert werden, differenziert. Die Orientierungshilfe macht deutlich, dass es unüberwindbare rechtliche Hindernisse gibt, private und dienstliche E-Mail-Nutzungen unter einer einheitlichen E-Mail-Adresse auf ein und demselben E-Mail-Server abzuwickeln. Bei Verbundnutzung gibt es keine technische Möglichkeit, zwischen dienstlicher und privater E-Mail zu unterscheiden, mit der Folge, dass an die E-Mail-Adresse des Bediensteten gerichtete dienstliche E-Mails wie private behandelt werden müssten. Nicht nur wären sämtliche Verbindungsdaten grundsätzlich unmittelbar nach Beendigung der Nutzung zu löschen, die Dienststelle dürfte auch dienstliche E-Mails nicht einsehen. Dies ließe keinen ordnungsgemäßen Dienstbetrieb zu. Das Problem lässt sich nicht dadurch lösen, dass die Bediensteten der Dienststelle gestatten, die Inhalte aller privaten E-Mails zur Kenntnis zu nehmen. Eine solche Einwilligung, welche die einheitliche Behandlung nach den für dienstliche E-Mails geltenden Regeln ermöglichen würde, wäre wegen der damit verbundenen völligen Aufhebung des Fernmeldegeheimnisses gegen das Telekommunikationsgesetz.

Da aus Kostengründen keine Dienststelle einen Server für private und einen für dienstliche E-Mails bereitstellen kann, bietet sich - wenn die private Nutzung dennoch zugelassen werden soll - als einfachster technischer Ausweg die Einrichtung einer zusätzlichen separaten E-Mail-Adresse für private Nutzung an. Dadurch wird weitgehend ausgeschlossen, dass unbefugte Dritte Kenntnis vom Inhalt der privaten E-Mails erlangen. Die Verbindungsdaten müssten zwar weiterhin über das für private E-Mails gesetzlich zulässige Maß hinaus gespeichert werden, dies wäre mit Einwilligung des einzelnen Bediensteten jedoch vertretbar.

Die neugefasste Orientierungshilfe macht außerdem auf eine weitere, noch problemlosere Alternative aufmerksam: Die Dienststelle könnte den Bediensteten gestatten, mittels des www private E-Mails von einem externen (häuslichen) Webmail-Anschluss abzurufen. Bedienstete, die diesen Weg nutzen, können die Zwischenspeicherung auf dem dienstlichen PC unverzüglich löschen und so Einsichtnahmen weiterhin ausschließen.

7. Justiz

7.1
Insolvenzveröffentlichungen im Internet

Die Novelle zur Insolvenzordnung soll ermöglichen, das Medium Internet auch für notwendige Veröffentlichungen im Insolvenzverfahren zu nutzen. Die zur Konkretisierung der Rahmenbedingungen beabsichtigte Rechtsverordnung trägt jedoch dem besonderen Gefährdungs-potential einer Veröffentlichung im Internet nicht ausreichend Rechnung.

Durch die am 1. Dezember 2001 in Kraft getretene Novelle der Insolvenzordnung (InsO) (BGBl. 2001 I S. 2710 ff.) wird angestrebt, die im Laufe des Verfahrens anfallenden Kosten - vor allem auch im Interesse des Verbraucherinsolvenzverfahrens - zu senken. Dies soll unter anderem durch geänderte Bekanntmachungsmodalitäten geschehen, da die bisherigen Veröffentlichungsformen erhebliche Kosten verursachen. Die Einstellung entsprechender Informationen durch die zuständigen Gerichte ins Internet würde bedeutend weniger Kosten verursachen als die Veröffentlichungen in den Printmedien.

Informationen aus Insolvenzverfahren im Internet sind weltweit abrufbar. Dritte, etwa Auskunfteien oder Wirtschaftsinformationsdienste, können die veröffentlichten Daten unbegrenzt kopieren, speichern, auswerten und auch nach Abschluss des

Insolvenzverfahrens beliebig lange zum Abruf vorhalten. Dies führt zu einem Eingriff in das Persönlichkeitsrecht des Schuldners, der über die Beeinträchtigung hinausgeht, die er nach der jetzigen Gesetzeslage im Hinblick auf die begrenzten Auswertungsmöglichkeiten der Veröffentlichungen in Zeitungen oder Amtsblättern hinnehmen muss. Die Veröffentlichung der Daten des Insolvenzschuldners im Internet übertrifft damit in ihrer Wirkung sogar den Eingriff, den seine Eintragung in das Schuldnerverzeichnis bedeuten würde. Ein solcher Eintrag erfolgt aber in diesem Zusammenhang gerade nicht. Dies kennzeichnet den Schuldner wegen seiner Insolvenz auf Dauer im Geschäftsverkehr und steht darüber hinaus auch in Widerspruch zu dem mit der Restschuldbefreiung angestrebten Zweck, dem Schuldner zu ermöglichen, wieder unbeschwert am Geschäftsverkehr teilzunehmen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einem Beschluss vom 24. April 2001 (vgl. Ziff. 27.10) die Aufnahme datenschutzgerechter Rahmenregelungen in das Gesetz gefordert. Der Gesetzgeber muss eine Entscheidung treffen, welches Datenprofil ins Internet eingestellt werden darf. Dabei muss der bezweckte Grad der Publizität der jeweiligen Daten zum Kriterium gemacht werden. Der Gesetzgeber sollte für eine Veröffentlichung über das Internet vorsehen, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern. Außerdem sollte eine automatische Übernahme der Daten, etwa durch Kopierschutz, verhindert werden; mit den gegenwärtigen technischen Möglichkeiten ist das allerdings noch nicht realisierbar.

Aufgrund dessen wurde in den Beratungen des Rechtsausschusses des Bundestages die im Gesetzentwurf (vgl. BTDrucks. 14/5680) vorgesehene Regelung modifiziert. § 9 Abs. 2 S. 2 InsO Fassung ermächtigt nunmehr zum Erlass von Vorschriften, die im Interesse des Rechts auf informationelle Selbstbestimmung die Sicherstellung der Datenintegrität und Datenauthentizität, und - soweit nach dem Stand der Technik möglich - einen Kopierschutz herstellen. Diese Konkretisierung soll in der Verordnung und nicht in der Insolvenzordnung selbst erfolgen, um flexibel auf technische Entwicklungen reagieren zu können, so ausdrücklich die Begründung im Rechtsausschuss (vgl. BTDrucks. 14/6468).

Für die Verordnung hat das Bundesjustizministerium im Sommer einen Entwurf vorgelegt; es will sicherstellen, dass zeitnah mit In-Kraft-Treten der Änderungen in der Insolvenzordnung auch baldmöglichst die praktische Umsetzung durch Nutzung der neuen Veröffentlichungsmöglichkeit erfolgen kann. Der vorgelegte Entwurf ist jedoch unzureichend. Er trifft gerade nicht die notwendigen Festlegungen, sondern wiederholt die Beschreibung der Rahmenbedingungen des Gesetzes. Insbesondere werden keine Vorgaben gemacht, wie die technischen Rahmenbedingungen zu erfüllen sind, sondern lediglich der Text der Verordnungsermächtigung übernommen.
Zwar werden in der Begründung zum Entwurf einige wenige technische Lösungen vorgeschlagen, z. B. die eingestellten Texte zu spiegeln; dies stellt aber keine ausreichende Festlegung dar. Eine Verbesserung wäre zum Beispiel durch eine Signatur erreichbar, dies ist auch heute schon technisch realisierbar.

Nach meiner Ansicht sollte die Verordnung ausdrücklich fordern, dass ein ausreichender Kopierschutz binnen Kürze geschaffen wird. Nur so kann das Gefährdungspotential, das in einer Veröffentlichung dieser Daten steckt, eingegrenzt werden.

Nicht zufriedenstellend ist auch die Dauer der Einstellung im Internet. Vorgesehen ist eine Löschung drei Monate nach Aufhebung des Verfahrens oder der Rechtskraft der Einstellung des Insolvenzverfahrens. Diese Frist ist zu lang. Sobald die Entscheidung über die Aufhebung des Verfahrens Rechtskraft erlangt hat, kann eine Löschung unverzüglich erfolgen. Es besteht keine Notwendigkeit, drei Monate nach Rechtskraft abzuwarten.

7.2
Der Einsatz von EUREKA in der Verwaltungsgerichtsbarkeit

Das im Bereich der Verwaltungsgerichtsbarkeit eingesetzte Verfahren EUREKA-Fach ist an einigen Punkten dringend überarbeitungsbedürftig. Vor dem jeweiligen Einsatz bei einem Gericht sind organisatorische Überlegungen notwendig, um die mit dem Verfahren mögliche Differenzierung der Nutzungsrechte sinnvoll umzusetzen.

Bei der hessischen Verwaltungsgerichtsbarkeit soll nunmehr flächendeckend das Verfahren EUREKA-Fach zum Einsatz kommen. Vorbereitet und koordiniert wird dieser Einsatz durch den Verwaltungsgerichtshof. Für den Bereich der Verwaltungsgerichtsbarkeit gibt es eine allgemeine Dienstanweisung Datenschutz und Datensicherung im Bereich der verwaltungsgerichtlichen Informationstechnik (DA-IT), über deren ursprüngliche Erarbeitung ich schon im Jahre 1996 berichtet habe (vgl. 25. Tätigkeitsbericht, Ziff. 3.2). Diese wurde für das Verfahren EUREKA ergänzt um eine Dienstvereinbarung „Über die Ausgestaltung der Benutzerrechte beim Einsatz der EDV am richterlichen Arbeitsplatz im Gericht“, die an einigen Punkten durch örtliche Dienstvereinbarung ergänzt werden kann.

Das Verfahren EUREKA ist ein erprobtes Verfahren, das in Zusammenarbeit mit anderen Bundesländern den Gegebenheiten der modernen Verwaltungsgerichtsbarkeit angepasst werden soll. Das Verfahren leistet eine Verwaltung von Verfahrens-

stammdaten. Eine Speicherung von Dokumenten ist nur durch eine Verknüpfung mit dem Textverarbeitungssystem Word möglich.

Bei einem Verwaltungsgericht habe ich den Einsatz des Verfahrens überprüft. Zudem bin ich mehrmals aus der Richterschaft um Beratung bei der Abfassung örtlicher Vereinbarungen ergänzend zur allgemeinen Dienstvereinbarung gebeten worden. Gegenstand der Überprüfung waren Funktionsweise, Einsatz des Verfahrens und getroffene technische und organisatorische Datensicherheitsmaßnahmen. Dabei ergaben sich die nachfolgenden Feststellungen:

- **Bemerkungsfelder**
  Die im Verfahren enthaltenen Bemerkungsfelder sind uneingeschränkt recherchierbar. Hier sollte näher festgelegt werden, welche Art von Zusatzinformationen dort abgelegt werden dürfen. Es muss ausgeschlossen werden, dass in diesen Feldern z. B. subjektive Wertungen über Prozessbeteiligte gespeichert werden.

- **Adressdatei**
  Das System enthält eine Adressdatei, in der alle Personen - unabhängig von der Rolle, in der sie an einem Verfahren beteiligt sind -, gespeichert werden. Bei der Suche, ob eine Person dem System schon bekannt ist, wird automatisch die gesamte Liste aller Beteiligten in allen Verfahren angezeigt, in der dann geblättert werden kann. Diese Art von Auswahl entspricht nicht dem heutigen Standard.
  Ich halte eine Änderung dergestalt für erforderlich, dass bestimmte Anfragedaten in das System eingegeben werden müssen und dann nur die Datensätze vom System angezeigt werden, die den Anfragedaten entsprechen. Der Eingeber kann dann weitere Angaben vergleichen und entscheiden, ob er die schon vorhandenen Adressdaten übernehmen will.

  Zu klären ist noch, wie die Aufbewahrungsdauer bzw. die Löschung der Adressdaten gesteuert wird.

- **Aufbewahrung der Dokumente in der Textverarbeitung**
  Für die von EUREKA angestoßenen und in Word gespeicherten Dokumente (Entscheidungstexte usw.) fehlt eine Aussage zur Speicherungsdauer; es sind Löschfristen festzulegen. Diese sollten sich an der Erforderlichkeit der Aufbewahrung der einzelnen Dokumente in elektronischer Form orientieren. Denn die in den Aufbewahrungsbestimmungen vorgesehenen, zum Teil sehr langen Fristen beziehen sich auf die Akten in Papierform und nicht auf die elektronisch gespeicherte Textverarbeitung.

- **Zugriffsmöglichkeiten auf die Anwendung**
  Innerhalb des Systems EUREKA gibt es differenzierte Zugriffsmöglichkeiten. Das Datenbanktool erlaubt es, in einer Berechtigungstabelle einzelnen Benutzern bzw. Gruppen unterschiedliche Zugriffsrechte zuzuordnen. Damit lassen sich innerhalb des Verfahrens hinreichende Zugriffsbegrenzungen realisieren. Diese Zugriffsbegrenzungen sind allerdings nicht vollständig auf dem NT-Dateibaum abgebildet. Durch die Zuordnung des Netzlaufwerks zum lokalen Rechner sind Teile der Anwendung im Zugriff aller berechtigten Nutzer. Damit sind für den Einzelnen über den Explorer in der Regel mehr Daten verfügbar als ihm nach seiner Aufgabenstellung zugänglich sein dürfen. Ein gezielter Zugriff ist zwar nur mit einer gewissen Sachkenntnis und ggf. mit zusätzlichen Tools möglich, andererseits besteht nicht nur eine Manipulationsmöglichkeit, sondern auch das Risiko eines unbemerkten ggf. auch versehentlichen Datenverlustes.

- **Löschprogramm**
  Derzeit ist keine automatisierte Löschung nach Ablauf der Aufbewahrungsdauer realisiert. Hier ist eine Nachbesserung des Systems erforderlich.

Soweit die Beseitigung der Schwachstellen technische Änderungen im Verfahren erfordert, habe ich darauf hingewiesen, dass dieses spätestens mit dem zur Zeit in der Planung befindlichen neuen Datenbanksystems erfolgen muss, um den jetzigen technischen Standard zu übernehmen.

Da das Verfahren im Verbund entwickelt wird, ist es nicht immer einfach, entsprechende Anforderungen zu realisieren. Um dabei die Reibungsverluste zu minimieren, arbeite ich mit den Datenschutzbeauftragten anderer Länder, in denen das Verfahren eingesetzt wird, zusammen.

Die angesprochenen örtlichen Dienstvereinbarungen zielen vor allem auf Festlegungen, wem in welchem Umfang Zugriff auf die vom Verfahren erstellten Überblickslisten (die sogenannten Streitlisten) über anhängige oder abgeschlossene Streitfälle gewährt wird. Bei der Geschäftsverteilung innerhalb der Gerichte ist die Anzahl der in den Kammern (Senaten) anhängigen Verfahren ein Faktor. Solche Erhebungen sind daher normal. Die automatisierte Aufbereitung weckt aber selbstverständlich Begehrlichkeiten, über die Anzahl der anhängigen Verfahren hinausgehende Informationen verfügbar zu machen. Das System ermöglicht eine Aufschlüsselung nach Verfahrensdauer, Sachverhalten, Kammern, Senaten, Berichterstattern und anderen Merkmalen. Das erlaubt eine Kontrolle der Arbeitsleistung der einzelnen Richter. Wesentliches Kriterium bei der Bewertung dieser Zugriffsrechte sind die richterliche Unabhängigkeit und die dienstrechtliche Bewertung der Leistung. Deshalb sieht die Dienstvereinbarung vor, dass der Zugriff auf diese Listen nur zur Organisation der Geschäftsverteilung

oder zur Wahrnehmung der Dienstaufsicht durch einen eng festgelegten Benutzerkreis erfolgen darf. Auch insoweit unterliegen die Listen einem besonderen Geheimhaltungsbedürfnis und müssen vor der Weitergabe an Richtervertretung, Präsidiumsmitglieder und Vorsitzende anonymisiert werden.

Spruchkörperintern könne entsprechende Zugriffsrechte auf die Listen nur auf Grundlage örtlicher Vereinbarungen gewährt werden.

7.3
Das elektronische Grundbuch

Die Führung des Grundbuches wird auf ein neues, elektronisches System umgestellt. Dieses ermöglicht auch die Einsicht in die Register durch Dritte in automatisierter Form. Die neue Version erfüllt im Wesentlichen die datenschutzrechtlichen Anforderungen.

Das Grundbuch hat nach § 873 des Bürgerlichen Gesetzbuches (BGB) eine wichtige Funktion. Es dokumentiert alle Rechte an einem Grundstück einschließlich der im Laufe der Zeit sich ergebenden Entwicklungen durch Eigentümerwechsel, sei es durch Verkauf oder Erbschaft, Belastungen, die auf dem Grundstück liegen, oder Rechte Dritter wie etwa ein Wegerecht.

§ 873 Abs. 1 BGB

Zur Übertragung des Eigentums an einem Grundstücke, zur Belastung eines Grundstücks mit einem Rechte sowie zur Übertragung oder Belastung eines solchen Rechtes ist die Einigung des Berechtigten und des anderen Teiles über den Eintritt der Rechtsänderung und die Eintragung der Rechtsänderung in das Grundbuch erforderlich, soweit nicht das Gesetz ein anderes vorschreibt.

§ 891 BGB

(1) Ist im Grundbuche für jemand ein Recht eingetragen, so wird vermutet, dass ihm das Recht zustehe.

(2) Ist im Grundbuch ein eingetragenes Recht gelöscht, so wird vermutet, dass das Recht nicht bestehe.

Da das Grundbuch gemäß § 891 BGB öffentlichen Glauben genießt - die Richtigkeit einer Eintragung wird vermutet -, sind die Anforderungen an die Richtigkeit der Eintragung hoch. Dem wird durch das in der Grundbuchordnung geregelte komplexe Verfahren der Grundbuchführung Rechnung getragen.
Aus all dem ergibt sich zwangsläufig, dass eine Fülle von Daten zu verarbeiten sind. Sie sind so darzustellen, dass die Einsichtsberechtigten die Eintragungen nachvollziehen können.

Ursprünglich wurde das Grundbuch in großen Folianten handschriftlich geführt. Damit Löschungen nachvollziehbar blieben, wurden die entsprechenden Eintragungen rot durchgestrichen - gerötet. Dies erfolgt auch heute noch so.

Nachdem schon vor einiger Zeit das Grundbuch in Loseblattform überführt wurde, mit dem Vorteil, die Blätter mit technischem Gerät schreiben zu können, wurde nunmehr mit dem Verfahren SOLUM-Star ein weiterer neuer Entwicklungsweg begangen.
Das Grundbuch wird nicht mehr auf Papier, sondern auf elektronischen Datenträgern geführt.

Speichermedium sind einmal beschreibbare Datenträger, so genannte WORM-Platten (**W**rite **O**nce **R**ead **M**any; vgl. auch 21. Tätigkeitsbericht, Ziff. 16.1). Um die Grundbuchblätter zu übernehmen, wird zunächst der Bestand an Grundbuchblättern eingescannt und als Graphik abgelegt. Darauf folgende Änderungen werden in einer Datenbank abgelegt. Bei Aufruf einer Grundbucheintragung werden die verschiedenen vorhandenen Informationen so zusammengespielt, dass am Bildschirm eine Darstellung erfolgt, die dem bis jetzt gewohnten Blick ins Grundbuch entspricht. Die Eingaben in die Grundbuchdatei werden durch eine elektronische Signatur gegen Manipulationen geschützt.

Technik des Verfahrens

SOLUM-Star ist eine Client-Server Anwendung, bei der die Daten auf Servern im Rechenzentrum der Justiz gespeichert werden. Als Server dienen UNIX-Rechner, während an den Arbeitsplätzen ein Windows-Betriebssystem genutzt wird. Die Gerichte und das Rechenzentrum sind über das HCN 2000 vernetzt. Hinsichtlich der Anbindung der Arbeitsplätze gibt es zur Zeit zwei Varianten:

1. Variante
Die Arbeitsplätze sind als „normale“ Clients am Server angebunden. Als Konsequenz werden beispielsweise Grundbuchblätter immer komplett zum Arbeitsplatz übertragen, wodurch hohe Anforderungen an die Übertragungsleistung gestellt werden. Dies gilt für die ersten Installa-tionen.

2. Variante
Bei einem weiteren Grundbuchamt wurden testweise die Arbeitsplätze über einen Terminalserver angeschlossen. Dadurch laufen die wesentlichen Verarbeitungsschritte auf den Terminalservern im Rechenzentrum; nur die Bildschirminhalte werden an den Arbeitsplatz übertragen. Die benötigte Übertragungsleistung ist geringer als in der ersten Variante und die Daten können mit den produktspezifischen Verschlüsselungsmechanismen bei der Übertragung gesichert werden.

Änderungen im Elektronischen Grundbuch werden durch elektronische Signaturen signiert, deren Zertifikate ein proprietäres Format haben, das nicht konform zum Signaturgesetz von 1997 ist. Die Zertifikate wurden im Rechenzentrum generiert und gespeichert. Vor einer Signatur laufen mehrere Schritte ab. Bei der Anmeldung im System wird dem Sachbearbeiter einer Benutzerkennung, ein geheimer Schlüssel, zugeordnet. Will er eine Änderung signieren, so muss er ein zusätzliches Passwort eingeben. Die jetzige Realisierung der elektronischen Signatur hat Schwächen, so dass sie insbesondere nicht den Anforderungen an qualifizierte Signaturen entspricht. Ich habe daher gefordert, bei der Fortentwicklung des Verfahrens das Signaturgesetz und die entsprechenden Änderungen in den Verwaltungsgesetzen zu berücksichtigen.

Es ist beabsichtigt, Chipkarten zur Authentisierung auszugeben. Die geheimen Signatur-Schlüssel sollen aber nicht auf den Chipkarten gespeichert werden.

Die Archivierung der Dokumente findet in einem proprietären Format statt, was bei einer Langzeitarchivierung Probleme bereiten kann.
Neben den Softwarekomponenten für die Sachbearbeitung gibt es ein Abrufverfahren zur Realisierung der Grundbucheinsicht bzw. zur Auskunftserteilung. Dieses Verfahren kommt entweder direkt im Grundbuchamt zur Anwendung oder bei externen, ausdrücklich zum Abruf zugelassenen Personen. Die Mitarbeiter des Grundbuchamts müssen vor einer Einsicht die Berechtigung überprüfen. Bei unbeschränkt zur Einsicht berechtigten Personen (z. B. Notare) müssen die Personalien und die Zugehörigkeit zur Kanzlei, bei anderen Einsichtsberechtigten das berechtigte Interesse geprüft werden. Bei der direkten Einsicht muss der Name des Einsehenden angegeben werden, der mit der Abfrage protokolliert wird. Die Teilnehmer am externen Abrufverfahren müssen jeweils ihr Aktenzeichen und ggf. ein Bearbeiterkürzel eingeben, Teilnehmer am eingeschränkten Abrufverfahren müssen zudem mit vorgegebenen Texten eine Erklärung abgeben, die das berechtigte Interesse an dieser Einsicht begründet. Diese Angaben werden gemeinsam mit den jeweils eingesehenen Seiten protokolliert. Das Oberlandesgericht ist berechtigt, diese Abrufe zu überprüfen.

Prüfungen von elektronischen Signaturen finden nicht in dem Abrufmodul statt, sondern nur im Modul für die Sachbearbeitung. Die Teilnehmer am Abrufverfahren haben keine Möglichkeit festzustellen, ob die Dokumente unverändert sind.

Problematisch war in der eingesetzten Version 2.11, dass alle Daten einer Datenbank so behandelt wurden, als würden sie zu einem Amt gehören. Wenn also ein Benutzer die Befugnis hatte, ihm erlaubte Änderungen vorzunehmen, so konnte er auch Änderungen an Daten anderer Ämter durchführen. Seit Mitte 2001 wird die Version 2.12 eingesetzt, bei der ein gerichtsübergreifender Zugriff nicht mehr möglich ist.

Um mit SOLUM-Star arbeiten zu können, müssen Benutzerkennungen und deren Zugriffsrechte im lokalen Netz und auf dem Server im Rechenzentrum eingetragen werden. Die Vorgaben werden von den Präsidenten der Gerichte gemacht. Nach diesen Vorgaben werden die Benutzerkennungen und die Zugriffsrechte in SOLUM-Star vom zentralen Support eingetragen, während die Eintragung der Benutzerkennungen und Zugriffsrechte im lokalen Netz durch die Systemadministration bei den Gerichten erfolgt.

Eine Umstellung auf die Anbindung mit Terminalserver hat zur Konsequenz, dass die Prüfung, ob sich ein Benutzer von einem zugelassenen Arbeitsplatz (IP-Adresse; Adresse eines Rechners im Netz) aus angemeldet hat, nicht mehr funktioniert. Dies liegt daran, dass alle Benutzer mit der IP-Adresse des Terminalservers gegenüber dem Programm auf die Daten zugreifen. Dadurch könnte sich ein Mitarbeiter, der eine Kennung aus einem anderen Amt im Gedächtnis hat, weil er vorher dort gearbeitet hat, mit dieser Kennung an SOLUM-Star anmelden und auf die Daten des anderen Amts zugreifen. Die Voraussetzung, dass beide Ämter über dieselben Terminalserver angeschlossen sind, dürfte die Regel sein, da für eine optimale Lastverteilung alle Server zugelassen sein müssen. Das Justizministerium prüft, mit welchen Maßnahmen das bisherige Schutzniveau wieder hergestellt werden kann.

7.4
Datenübermittlung an gefährdete Personen

Eine Justizvollzugsanstalt ist befugt, eine von dem Strafgefangenen bedrohte Person über Vollzugslockerungen zu informieren.

Der Insasse einer Justizvollzugsanstalt hat sich an mich gewandt, weil er sich in seinen datenschutzrechtlichen Belangen beeinträchtigt sah. Seiner Darstellung zufolge wurde der Leiter der Justizvollzugsanstalt, in der er zuvor untergebracht war,

über sämtliche seine Person betreffende Vollzugslockerungen durch die Anstaltsleitung informiert. Er räumte ein, dass er den früheren Anstaltsleiter geohrfeigt hatte, meinte aber, nach seiner Verlegung in eine andere Anstalt und seiner Verurteilung wegen dieses Übergriffes seien Informationen über Vollzugslockerungen an den früheren Anstaltsleiter nicht zulässig.

Die Anstaltsleitung teilte mit, dass der Gefangene schon die Ermittlungsrichterin tätlich angegriffen hatte und er einem Vollzugsbeamten mit der Faust ins Gesicht geschlagen und ihn danach schriftlich und telefonisch bedroht habe. Die zugestandene Ohrfeige sei ein Schlag gegen den Kopf gewesen, der den Angegriffenen niedergestreckt habe; ferner bestehe der Verdacht, dass er auch die Ehefrau des Gefängnisdirektors telefonisch bedroht habe. Aufgrund dieser Vorkommnisse war für den bedrohten Anstaltsleiter Personenschutz angeordnet worden. Dementsprechend seien die Mitteilungen an die gefährdete Person aus Fürsorgegründen erforderlich gewesen.

Daran war aus meiner Sicht nichts auszusetzen. Das Gefährdungspotential wird durch die Information gemindert. Sie warnt das potentielle Opfer, um der möglichen Gefahr vorbeugen zu können. Ich habe dem Gefangenen mitgeteilt, dass er diese Datenübermittlung wegen seines aggressiven Verhaltens hinnehmen muss. Sie war gemäß § 180 Abs. 1 und 2 Nr. 3 des Strafvollzugsgesetz zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich und damit zulässig.

7.5
Zweckwidrige Verwendung von Daten im Strafvollzug

Das Landgericht Gießen verlangte von der Justizvollzugsanstalt Butzbach die Übersendung des Protokolls einer Behandlungskonferenz über einen Strafgefangenen. Da das Protokoll nicht auffindbar war, übersandte die Justizvollzugsanstalt ein nicht zureichend anonymisiertes Protokoll über einen anderen Gefangenen. Dies war rechtswidrig.

Ein Insasse der Justizvollzugsanstalt Butzbach hat gerügt, dass ein Mitgefangener in den Besitz eines ihn betreffenden Protokolls der Behandlungskonferenz gekommen war. Das Protokoll enthielt zahlreiche personenbezogene Daten. Ihm war beispielsweise zu entnehmen, dass der Betroffene sich erstmals in Haft befindet, zuvor nicht vorbestraft war, wann er festgenommen und zu welcher Freiheitsstrafe er verurteilt wurde, wann der Endstrafzeitpunkt und der Zweidrittelstrafzeitpunkt ist, dass er die Straftat geleugnet hat, seit wann er sich in therapeutischer Behandlung befindet, welchen Beruf er ausübte und in welchem Zusammenhang es zu den Straftaten kam. Es folgen vollzugsfachliche Einschätzungen und Beurteilungen sowie der Beschluss der Behandlungskonferenz.

Die von mir um Stellungnahme gebetene Justizvollzugsanstalt rechtfertigte sich damit, dass sie in der Strafsache des Mitgefangenen vom Landgericht Gießen um Übersendung des Protokolles der Behandlungskonferenz gebeten worden sei. Da die Unterlagen über den betreffenden Gefangenen nicht aufgefunden werden konnten, habe man dem Gericht ein Protokoll zu einem anderen Gefangenen übersandt. Zwar wurde angeführt, dass es sich um ein „Muster, das einen anderen Gefangenen betrifft“ handelt. Auch wurde der Name des Betroffenen geschwärzt, doch sind die Angaben derart detailliert und individuell, dass durch die bloße Schwärzung des Namens von einer Anonymisierung keine Rede sein konnte. Der Betroffene wurde von seinem Mitgefangenen identifiziert und mit der Information konfrontiert, dass „sein“ Protokoll in Sachen des Anderen Verwendung fand.

Es war sachlich keinesfalls zu rechtfertigen, dem Landgericht Gießen das den einen Gefangenen betreffende Behandlungsprotokoll in der Sache des anderen Gefangenen zu übersenden. Die Anstalt hätte wissen müssen, dass das Gericht dem Antragsteller eine Kopie überlässt. Das Interesse der Anstalt, dem Auskunftsverlangen des Gerichts nachzukommen, hätte durch Übersendung einer vollständig anonymisierten Ausfertigung oder eine auf sonstige Weise abstrahierte Darstellung gewahrt werden können. Jedenfalls liegt ein Rechtsgrund im Sinne des § 180 Strafvollzugsgesetz zur Verarbeitung - hier der Übermittlung - der personenbezogenen Daten des Mitgefangenen nicht vor. Es fehlte daher an einer Rechtsgrundlage für die Datenübermittlung.

Gemäß § 27 Abs. 1 Nr. 1 Hessisches Datenschutzgesetz habe ich die unzulässige Datenübermittlung gegenüber dem Hessischen Justizministerium beanstandet. In seiner Stellungnahme hat das Ministerium den Sachverhalt bestätigt, meine Rechtsauffassung geteilt und fest-gestellt, Ursache sei eine Fehleinschätzung der handelnden Bediensteten gewesen, die vom Behördenleiter entsprechend belehrt worden sind.

7.6
Datenübermittlungen im Zusammenhang mit Geldüberweisungen

Strafgefangene, die angespartes Geld auf ihr Bankkonto überweisen wollen, sind nicht verpflichtet, dem Geldinstitut zu offenbaren, dass sie im Gefängnis einsitzen. Trotzdem gab sich die Justizvollzugsanstalt Butzbach im Falle eines Strafgefangenen mehrere Male als Absender der Überweisungen aus.

Ein Häftling führte im Herbst 2000 in einer Eingabe an meine Behörde an, er habe die Justizvollzugsanstalt (JVA) darum gebeten, von seinem Eigen- und Hausgeld Beträge auf sein Konto bei der Postbank AG einzuzahlen. Dabei hat er von dem von der Anstaltsleitung schriftlich unterbreiteten Angebot Gebrauch gemacht, dies als Bareinzahlung abzuwickeln. Dadurch wird verhindert, dass auf dem Überweisungsträger die Justizvollzugsanstalt als Absender erscheint. Trotzdem hat die Anstalt in zwei Fällen kenntlich gemacht, dass der Absender einsitzt. In der von mir erbetenen Stellungnahme führte die Anstaltsleitung aus, ursprünglich seien keine Bedenken zu der Absenderangabe gesehen worden, da Einzahler und Empfänger identisch waren. Es sei jedoch nicht bedacht worden, dass Angestellte der Post Rückschlüsse auf eine mögliche Inhaftierung ziehen können.

Die JVA hätte auf die Angabe der dortigen Institution verzichten müssen. Die Bediensteten der Zahlstelle wurden aufgrund meiner Intervention angewiesen, zukünftig Herkunftsangaben neutral zu formulieren, um datenschutzrechtliche Belange nicht zu verletzen. Kurz danach beschwerte sich jedoch der Betroffene erneut. Die Anstalt habe bei einer Eigengeldüberweisung den von ihm vorbereiteten Einzahlungsvordruck nicht verwendet, stattdessen den Betrag unter der Angabe „Auftraggeber Justizvollzugsanstalt …“ überwiesen. In der erneuten Stellungnahme räumte die Anstalt ein abermaliges Versehen ein und versprach Abhilfe. Anfang des Jahres 2001 wandte sich der Betroffenen ein drittes Mal an mich. Er teilte mit, dass er zwei neue Einzahlungsaufträge erteilt hätte. Die Kasse händige ihm die Belege nicht aus, vermutlich um weitere Fehler zu verdecken. In ihrer Stellungnahme bestätigte die Anstalt, dass erneut die JVA als Absender genannt wurde. Als Ursache führte sie die Fehleinschätzung eines Bediensteten an.

Mit der Absenderangabe „Justizvollzugsanstalt …“ auf den Überweisungsträgern wird gegenüber dem Geldinstitut offenbart, dass der Betroffene sich in der JVA befindet. Diese Datenübermittlung ist vermeidbar und damit für Zwecke des Vollzugs der Freiheitsstrafe nicht erforderlich. Es scheidet daher § 180 des Strafvollzugsgesetzes als Rechtsgrundlage der Verarbeitung (hier der Übermittlung) der Information aus. Auch eine andere Rechtsgrundlage ist nicht ersichtlich. Die unzulässigen Datenübermittlungen wurden gegenüber dem Hessischen Justizministerium gemäß § 27 Abs. 1 Nr. 1 Hessisches Datenschutzgesetz beanstandet. Das Ministerium teilte mit, der Anstaltsleiter habe nun in einer Verfügung auf die Datenschutzverletzungen hingewiesen und die Weisung erteilt, die Überweisungen soweit zu anonymisieren, dass der Absender nicht als Insasse einer JVA erkennbar ist. Die Weisung ist allen in Frage kommenden Bediensteten gegen Empfangsbescheinigung ausgehändigt worden.

8. Polizei- und Strafverfolgungsbehörden

8.1
Neue Informationssysteme für die Hessische Polizei - Das Verfahren POLAS

Aus den Schwierigkeiten mit der Weiterentwicklung der vorhandenen Informationssysteme und der Zusammenarbeit mit dem Projekt INPOL-neu wurden Konsequenzen gezogen und ein neues modernes Informationssystem für die Hessische Polizei implementiert.

8.1.1
Das Ende des Hessischen Polizeiinformationssystems HEPOLIS

Wiederholt haben sich die Tätigkeitsberichte mit den Entwicklungen und dabei auftretenden Probleme der Informations- und Vorgangsbearbeitungssysteme der Polizei in Hessen befasst. Wegen der vom Vorhaben INPOL-neu gestellten Anforderungen war es notwendig, die Parallelstrukturen der Hessischen Polizei neu zu gestalten.

Zum Ende des vergangenen Jahres wurde entschieden, das bisherige Verfahren HEPOLIS abzulösen und die Vorgangsbearbeitung HEPOLAS nicht weiter zu realisieren. Nunmehr ist das Land Hessen eine Kooperation mit Hamburg eingegangen mit dem Ziel, die dortigen Verfahren zur Landesdatenhaltung und zur Vorgangsbearbeitung in Hessen einzusetzen.

Begonnen wurde zunächst mit dem Einsatz der Landesdatenhaltung POLAS. Bei der Projektabwicklung waren aus datenschutzrechtlicher Sicht die hessischen Rahmenbedingungen einzuhalten: Der Umfang der zu verarbeitenden Daten richtet sich nach dem Hessischen Gesetz über die öffentliche Sicherheit und Ordnung (HSOG). Die Struktur der Zugriffsrechte etc. muss die hessische Verwaltungsstruktur wiedergeben. Insofern waren insbesondere die Strukturen des Stadtstaates Hamburg und des Flächenlandes Hessen mit ihren unterschiedlichen Zugriffsbefugnissen wiederzugeben.

Für die Überführung des vorhandenen Datenbestandes in das neue Verfahren wurde vereinbart, dass die Anforderungen, die zwischen mir und der Hessischen Polizei bezüglich der alten Verfahren HEPOLIS und HEPOLAS abgesprochen waren, soweit wie möglich eins zu eins umgesetzt werden sollen. Soweit dies nicht realisierbar erscheint, sollen gemeinsame Lösungsmöglichkeiten entwickelt werden.

Nach der Umstellung auf das Verfahren POLAS konnten sich meine Mitarbeiter im August bei einem ersten Termin davon überzeugen, dass das Verfahren POLAS offensichtlich in der inhaltlichen Ausgestaltung diesen Anforderungen entspricht. Das war so zu erwarten, da die Entwicklung von POLAS vom Hamburger Datenschutzbeauftragten intensiv begleitet worden war. Detailfragen, die sich auch aus den aufgrund der Entwicklung der Sicherheitspolitik ergebenden Anforderungen stellen, werden noch zu erörtern sein.

Eine vergleichbare Vorgehensweise ist auch für den im kommenden Jahr beabsichtigten Einsatz der Vorgangsbearbeitung ComVor verabredet.

Ergänzend wird ein IT-Sicherheitskonzept für die Hessische Polizei erarbeitet, das nicht nur für POLAS, sondern für alle IT-Anwendungen den Rahmen bilden soll. Eine Unternehmensberatung erstellt das Konzept mit Unterstützung des Präsidiums für Technik, Logistik und Verwaltung (PTLV). Für die bisherige Vorgangsbearbeitung HEPOLAS existierte ein Sicherheitskonzept, von dem Teile übernommen wurden. Das Sicherheitskonzept wurde im Dezember 2001 abschließend erstellt und wird von mir geprüft.

8.1.2
Weitere Entwicklung des Projektes INPOL-neu

INPOL-neu konnte nicht wie geplant im April diesen Jahres gestartet werden. Die Gründe lagen in der Entwicklung des Projektes selbst. Die dabei aufgetretenen Schwierigkeiten vor allem in der technischen Umsetzung haben zu erheblichen Verzögerungen geführt (voraussichtlich bis 2004).

8.2
Zusammenarbeit bei der Produktion von Fernsehsendungen - Reality-TV

Wenn die Polizei bei so genannten Reality-TV Produktionen mitwirkt, müssen alle Betroffenen ihr Einverständnis erteilt haben. Sonst dürfen nur Übersichtsaufnahmen gesendet werden oder die personenbezogenen Bildausschnitte müssen gelöscht oder unkenntlich gemacht werden. Vor der Ausstrahlung ist der fertige Film der Polizei zur Abnahme vorzulegen.

Immer realitätsnäher wünschen sich Fernsehproduzenten ihre Aufnahmen beim so genannten Reality-TV. „Life dabei sein“, bei einer echten Verhaftung, einer Razzia oder einer Durchsuchung, lautet das Motto: Je authentischer die Aufnahme, desto größer der Heißhunger des Publikums. Allerdings können beim Reality-TV datenschutzrechtliche Belange der betroffenen Bürgerinnen und Bürger und der Bediensteten beeinträchtigt werden. Eine Rechtsgrundlage für diese Beeinträchtigung existiert nicht. Es ist daher zwingend, dass die Betroffenen in die Verarbeitung ihrer personenbezogenen Daten vorab einwilligen. Der Hessische Innenminister hat auf meine Initiative hin die „Richtlinien über Mitteilungen der Polizei an die Presse und den Rundfunk“ vom 21. Dezember 1999 (StAnz. 2000 S. 99) durch Erlass vom 10. Mai 2001 (StAnz. 2001 S. 1906) um Regelungen über die Zusammenarbeit mit Fernseheinrichtungen ergänzt. Eine Zusammenarbeit darf nur erfolgen, wenn dies im öffentlichen Interesse liegt und die Fernseheinrichtung zuvor bestimmte Voraussetzungen schriftlich anerkannt hat.

Zusammenarbeit bei der Produktion von Sendungen über polizeiliche Einsätze

Den Wünschen von Fernseheinrichtungen, vorab über polizeiliche Einsätze unterrichtet zu werden, um diese filmen zu können (so genanntes Reality-TV) ist nur dann zu entsprechen, wenn dies, zum Beispiel wegen der Präventionswirkung, im öffentlichen Interesse liegt und datenschutzrechtliche Belange der betroffenen Personen nicht beeinträchtigt werden.

Datenschutzrechtliche Belange der betroffenen Personen werden nicht beeinträchtigt, wenn die Fernseheinrichtung folgende Voraussetzungen schriftlich anerkannt hat:

- Keine Person - Bürger oder Beamter - darf aufgenommen werden, die nicht vorher nach Aufklärung über den Umfang, Zweck und Dauer der Aufnahmen ihr Einverständnis erklärt hat. Auf die Freiwilligkeit der Einwilligung ist die betroffene Person hinzuweisen.

- Solange keine Einwilligung eingeholt worden ist, weil die betroffene Person vom Aufnahmeteam noch nicht angesprochen werden konnte, dürfen nur Übersichtsaufnahmen erstellt werden, die die betroffene Person nicht klar erkennen lassen.

- Personen oder andere personenbezogene Umstände (insbesondere amtliche Kennzeichen) dürfen ohne zusätzliche schriftliche Einwilligung nicht gesendet werden. Sie sind durch Schnitt zu löschen oder unkenntlich zu machen. Personenbezogenes Aufnahmematerial ist nach der Auswertung für die Sendung zu löschen. Die Löschung ist zu dokumentieren.

- Der fertige Film ist der Polizeibehörde zur Abnahme in datenschutzrechtlicher Hinsicht so rechtzeitig vorzulegen, dass Änderungen noch vor der Sendung möglich sind. Forderungen der Polizei nach Anonymisierung von Personen oder Sachen mit Personenbezug hat die Fernseheinrichtung zu entsprechen.

Damit wird den Belangen der Betroffenen in sachgerechter Weise Rechnung getragen.

8.3
Der Hausmeister der Universität als Ermittler der Polizei

Das Polizeipräsidium Gießen erhielt eine Presseerklärung eines AStA-Mitgliedes, die einige allgemeine politische Aussagen enthielt. Ohne weiteren Anlass stellte es Ermittlungen gegen die presserechtlich verantwortliche Person an, informierte dritte Personen über ihren Verdacht einer extremistischen Betätigung, ermittelte im Hoheitsbereich der Fachhochschule Gießen und setzte den Hausmeister der Fachhochschule als Ermittler ein. Die Beeinträchtigung der Rechte der Betroffenen war unzulässig.

Eine Studentin wurde vom Sekretariat des Allgemeinen Studentenausschusses der Fachhochschule Gießen darauf hingewiesen, dass sich ein Hausarbeiter der Fachhochschule nach ihrer Adresse erkundigt habe. Er brauche die Anschrift, um sie seinem Bekannten, der bei der Polizei sei, weiterzugeben. Auf Nachfrage nannte der Betreffende der Studentin den Namen des Polizeibeamten; dieser sei bei der Gießener Polizei für politische Veranstaltungen und Personenüberwachung zuständig, habe ihm einen Zettel mit ihrem Namen gegeben und gebeten, im Büro des Studentenausschusses ihre Anschrift zu erfragen. Die Studentin zweifelte an, dass dieses Vorgehen mit datenschutzrechtlichen Bestimmungen in Einklang steht.

Das Polizeipräsidium teilte mir mit, eine Presseerklärung von einer außerhessischen Polizeibehörde eines „Bündnisses für Politik und Meinungsfreiheit“ zur Kenntnisnahme und Auswertung erhalten zu haben. Die Studentin war namentlich und unter Angabe des Allgemeinen Studentenausschusses der Fachhochschule Gießen für diese Presseerklärung verantwortlich. Da zu der Schrift und der Organisation keine Erkenntnisse vorlagen, wurde ein Beamter beauftragt abzuklären, ob sich Anhaltspunkte für eine extremistische Ausrichtung der Organisation ergäben oder ob von der Organisation Aktionen ausgehen könnten, die die öffentliche Sicherheit und Ordnung stören würden. Erkundigungen bei der Fachhochschule und beim Studentenausschuss blieben ohne Erfolg. Deshalb wurde ein auf der Dienststelle persönlich bekannter Hausmeister der Fachhochschule vom Staatsschutzkommissariat gebeten, sich bei der Geschäftstelle des Studentenausschusses nach ihr zu erkundigen. Es habe sich lediglich um Vorfeldaufklärungen einfachster Art gehandelt.

Die unter dem Titel „Wissenschaft kann nicht unpolitisch sein“ veröffentlichte Presseerklärung enthielt zwar politische Aussagen, diese waren jedoch selbst bei sehr kritischer Betrachtung nicht als extremistisch einzuordnen. Das sah auch das Polizeipräsidium Gießen so. Es gab auch zu, dass der Weg über den Haumeister ungewöhnlich war. Trotzdem habe man wenigstens die Existenz der presserechtlich Verantwortlichen nachvollziehen wollen.

Die Annahme einer extremistischen Ausrichtung der Organisation war aus der Luft gegriffen. Die Mitteilung an den Hausmeister, dass das Staatsschutzkommissariat der Gießener Polizei gegen die Studentin ermittele, sowie dessen Beauftragung mit weiteren Datenerhebungen waren unzulässig. Sie entbehrten jeder Rechtsgrundlage. Der Studentenausschuss ist Organ der Fachhochschule. Der Leiter der Fachhochschule hätte daher von den Ermittlungen gegen ein Organ der Hochschule oder dessen Mitglied in Kenntnis gesetzt werden müssen, denn die Ausübung von Hoheitsfunktionen im Bereich anderer Hoheitsträger ist grundsätzlich nicht zulässig. Das gilt auch für strafrechtliche Ermittlungen, die ohne Kenntnis des Leitungsorgans nur in Ausnahmefällen gerechtfertigt werden können.

Ich habe das Vorgehen der Gießener Polizei gegenüber dem Hessischen Innenministerium gerügt. Der Hessische Innenminister stimmte mir zu, dass dieses Vorgehen, Daten über die Studentin zu erheben, nicht gerechtfertigt war. Einen Eingriff in den Hoheitsbereich der Fachhochschule sah er allerdings nicht. Dieser Darlegung ist aus allgemein verwaltungsrechtlichen Gründen zu widersprechen.

8.4
Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen

Das Hessische Innenministerium hat einen Entwurf neuer Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen vorgelegt. Änderungen zur vorgesehenen Aufbewahrung von erkennungsdienstlichen Unterlagen, zur Übermittlung von Informationen aus Kriminalakten und zur Auswertung der Verfahrensausgangsmitteilung der Staatsanwaltschaft sind nach meiner Beurteilung nötig.

Nachdem das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) nebst den dazu ergangenen Verwaltungsvorschriften novelliert worden ist, beabsichtigen das Hessische Landeskriminalamt und das Hessische Innenministerium

auch die Anpassung der „Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen“. Das Innenministerium hat mich um eine Stellungnahme zu seinem Entwurf gebeten.

Die Richtlinie sieht wie bisher vor, dass erkennungsdienstliche Unterlagen (z. B. Lichtbilder, Fingerabdrücke) ebenso lange aufbewahrt werden wie die Kriminalakten. Auch an den Voraussetzungen der Aufbewahrung hat sich nichts geändert. Nach der Rechtsprechung zu § 81b Strafprozessordnung (StPO) müssen Anhaltspunkte dafür vorliegen, dass der Beschuldigte künftig strafrechtlich in Erscheinung treten wird und die erkennungsdienstlichen Unterlagen die Ermittlungen der Polizei fördern können. Für die Aufbewahrung von Informationen in Akten gilt die Schranke der Erforderlichkeit. Eine Konkretisierung des Erforderlichkeitsgrundsatzes, etwa dass die Besorgnis der Begehung weiterer Straftaten besteht (§ 20 Abs. 4 HSOG-alt), wurde durch die letzte HSOG-Novelle gegen meine Bedenken gestrichen. Die Aufbewahrung von erkennungsdienstlichen Unterlagen ist damit an strengere Voraussetzungen geknüpft als die Aufbewahrung von Akten.

Die Richtlinie legt die Voraussetzungen fest, unter denen anderen Stellen Informationen aus Kriminalakten übermittelt werden dürfen. Ich habe empfohlen, dass bei der Übermittlung von Daten aus Ermittlungsverfahren immer zusätzlich mitzuteilen ist, wie das Verfahren ausgegangen ist bzw. dass der Verfahrensausgang unbekannt ist. Datenweitergaben ohne diese Zusätze haben immer wieder zu Rügen seitens der Betroffenen und zu datenschutzrechtlichen Beanstandungen geführt.
Die Richtlinie regelt, welche Folgen der Ausgang des Strafverfahrens für die weitere Aufbewahrung der Unterlagen hat. Danach soll bei den in der Praxis sehr häufig vorkommenden Verfahrenseinstellungen durch die Staatsanwaltschaft nach § 170 Abs. 2 StPO die Aussonderung nur erfolgen, wenn der Tatverdacht ausgeräumt wurde.

§ 170 StPO

(1) Bieten die Ermittlungen genügend Anlass zur Erhebung der öffentlichen Klage, so erhebt die Staatsanwaltschaft sie durch Einreichung einer Anklageschrift bei dem zuständigen Gericht.

(2) Andernfalls stellt die Staatsanwaltschaft das Verfahren ein. Hiervon setzt sie den Beschuldigten in Kenntnis, wenn er als solcher vernommen worden ist oder ein Haftbefehl gegen ihn erlassen war; dasselbe gilt, wenn er um einen Bescheid gebeten hat oder wenn ein besonderes Interesse an der Bekanntgabe ersichtlich ist.

Erfolgt die Einstellung aus sonstigen Gründen, soll der Vorgang in der Kriminalakte verbleiben bzw. die Akte weiter aufbewahrt werden. Diese Regelung ist aus datenschutzrechtlicher Sicht nicht zufriedenstellend. Sehr häufig ist die in der Richtlinie vorgesehene Voraussetzung der Löschung (Verdacht ausgeräumt) nicht erfüllt, etwa wenn ein zur Aufnahme von Ermittlungen ausreichender Anfangsverdacht sich nicht bestätigt oder nicht ausgeräumt werden kann (z. B. bei böswilligen Beschuldigungen oder widerrufenen Zeugenaussagen oder bei Schöpfung von Verdacht nach der Berufs- oder Lebenserfahrung). Oft wird einem ersten Verdacht nachgegangen, dessen „Widerlegung“ aber nicht bewiesen werden kann. Immer dann ist der „Verdacht nicht ausgeräumt“, so dass die gesetzliche Löschungspflicht nicht greift (§ 20 Abs. 4 HSOG). Der Umkehrschluss, dass in allen anderen Fällen eine weitere Aufbewahrung erforderlich und zulässig ist, widerspricht jedoch dem Verhältnismäßigkeitsgrundsatz. Wenn die von der Staatsanwaltschaft einzuschätzende Beweislage dazu führt, dass ein Verfahren ohne jede Auflage eingestellt wird, darf der Vorgang nicht genauso behandelt werden als wäre der Beschuldigte verurteilt worden.

Bis zum Redaktionsschluss dieses Berichtes lag mir noch keine Antwort des Ministeriums auf meine Änderungsvorschläge vor.

8.5
Datenübermittlung aus dem Zentralen Verkehrsinformationssystem (ZEVIS) beim Kraftfahrtbundesamt

Die Polizei darf nur zu ihrer eigenen Aufgabenerfüllung Auskünfte im automatisierten Verfahren gemäß § 36 Straßenverkehrsgesetz aus dem Zentralen Verkehrsinformationssystem einholen. Die zweckfremde Nutzung von ZEVIS-Daten ist nicht zulässig.

Im vergangenen Jahr wurden zwei Konstellationen an mich herangetragen, in denen die Polizei Auskünfte im automatisierten Verfahren aus dem Zentralen Verkehrsinformationssystem einholt, obwohl sie diese Auskünfte nicht zu ihrer eigenen Aufgabenerfüllung benötigt.

Kommunen müssen häufig das Abschleppen eines nicht zugelassenen Fahrzeugs veranlassen. Ist das letzte amtliche Kennzeichen des abzuschleppenden Fahrzeugs bekannt, kann der letzte Halter durch eine Anfrage bei der Kfz-Zulassungsstelle festgestellt werden. Eine Anfrage bei der Kfz-Zulassungsstelle bleibt jedoch erfolglos, wenn der Kommune nur die Fahrzeugidentifi-zierungsnummer bekannt ist, da eine Halterfeststellung im Verfahren AUGE (**Au**skunft **Ge**meinde) nur über das Kennzeichen möglich ist. Um auch in solchen Fällen den letzten Halter festzustellen, müssen die Kommunen beim Kraftfahrtbundesamt in Flensburg (KBA), das das zentrale Fahrzeugregister führt, anfragen. Die Beantwortung dieser Anfragen durch das KBA nimmt einige Tage in Anspruch. Für die bis zur Halterfeststellung sichergestellten Fahrzeuge fallen

Verwahrkosten an, die der Halter zu tragen hat. Um diese Kosten so gering wie möglich zu halten, bitten die Kommunen – wenn ihnen lediglich die Fahrzeugidentifizierungsnummer bekannt ist - teilweise die örtlichen Polizeibehörden, die benötigten Auskünfte im automatisierten Verfahren gemäß § 36 Straßenverkehrsgesetz (StVG) aus ZEVIS einzuholen. Dieses Verfahren ist zwar grundsätzlich bürgerfreundlich, aber es ist derzeit so im Gesetz nicht vorgesehen. In § 36 Abs. 2 Ziff. 1 StVG ist abschließend aufgezählt, zu welchen Zwecken ein Abruf im automatisierten Verfahren erfolgen darf.

§ 36 Abs. 2 Ziff. 1 StVG

Die Übermittlung nach § 35 Abs. 1 Nr. 1 bis 4 aus dem Zentralen Fahrzeugregister darf durch Abruf im automatisierten Verfahren erfolgen
1. an die Polizeien des Bundes und der Länder sowie an den Zoll, soweit er grenzpolizeiliche Aufgaben wahrnimmt,
a) zur Kontrolle, ob die Fahrzeuge einschließlich ihrer Ladung und die Fahrzeugpapiere vorschriftsmäßig sind,
b) zur Verfolgung von Ordnungswidrigkeiten nach §§ 24 oder 24a,
c) zur Verfolgung von Straftaten oder zur Vollstreckung oder zum Vollzug von Strafen oder
d) zur Abwehr von Gefahren für die öffentliche Sicherheit,
...
Da im konkreten Fall keiner der in § 36 Abs. 2 Ziff. 1 genannten Zwecke verfolgt wurde, war das Verfahren rechtswidrig. Das wurde den beteiligten Stellen dargelegt.

Bei dem zweiten Fall geht es um eine Datenübermittlung zwischen der deutschen Polizei und der amerikanischen Militärpolizei. Fraglich war, inwieweit eine hessische Polizeidienststelle befugt ist, für das amerikanische Zollfahndungsamt auf ZEVIS-Daten zuzugreifen und diese an die amerikanische Behörde zu übermitteln. Hintergrund ist die Überprüfung von Zollprivilegien bei Benzincoupons oder Fahrzeugankäufen; geklärt werden soll der Verdacht eines Missbrauchs, insbesondere einer Steuerhinterziehung. Anlass für eine Überprüfung sind Fahrzeuge mit deutschen Kennzeichen, die bei den amerikanischen Tankstellen vorfahren und Benzincoupons einlösen. Darüber hinaus werden Zollprivilegien überprüft, wenn Fahrzeuge mit einer bestimmten Fahrzeugidentifikationsnummer im deutschen Verkehr zugelassen werden.

Um an die Halterdaten zu gelangen, hat sich die amerikanische Zollbehörde bisher mit einem Auskunftsersuchen an deutsche Polizeidienststellen gewandt. Dieses Vorgehen ist nach den gesetzlichen Vorschriften nicht zulässig. Das amerikanische Zollfahndungsamt muss sich gem. Art. 7 Abs. 6a des NATO-Truppenstatut an die deutschen Zollfahndungsdienststellen wenden. Der kurze Dienstweg zu den Polizeibehörden ist nicht zulässig, da sich die im NATO-Truppenstatut festgeschriebene gegenseitige Unterstützungspflicht auf die jeweils zuständigen Behörden bezieht. Das sind für die hier fraglichen Feststellungen die deutschen Zollfahndungsdienststellen. Ihnen sind gemäß § 36 Abs. 2 StVG ZEVIS-Daten zur Verfolgung von Steuer- und Wirtschaftsstraftaten durch Abruf im automatisierten Verfahren zu übermitteln. Da die deutschen Zollfahndungsdienststellen ihre Anfragen über den bundesweiten zentralen ZEVIS-Anschluss beim Zollkriminalamt in Köln stellen müssen, erzeugt das einen Zeitaufwand von zwei bis drei Tagen. Für einen Ermittlungserfolg ist diese Zeitspanne teilweise zu lang. Angesichts der gesetzlichen Regelung ist das aber unvermeidbar.

Sowohl die anfragende amerikanische Zollbehörde als auch die beteiligte Polizeidienststelle wurde entsprechend unterrichtet und darauf hingewiesen, dass zeitliche Verzögerungen bei der Beantwortung von Anfragen keine Umgehung der gesetzlichen Vorschriften rechtfertigen.

9. Verfassungsschutz

9.1
Änderung des Verfassungsschutzgesetzes

Der Gesetzentwurf zur Änderung des Verfassungsschutzgesetzes sieht eine Zuständigkeit des Verfassungsschutzes für die Bekämpfung der organisierten Kriminalität vor. Die Befugnisse des Verfassungsschutzes zum Abhören und zur Anfertigung von Bildaufzeichnungen in Wohnungen werden deutlich erweitert. Außerdem sollen nicht näher eingegrenzte Auskunftspflichten für Geldinstitute, Postdienstleistungs- und Luftverkehrsunternehmen eingeführt werden. Ich habe gegenüber der Landesregierung kritisch zum Entwurf Stellung genommen.

9.1.1
Einbeziehung der organisierten Kriminalität in den Aufgabenbereich des Verfassungsschutzes

Die Aufgaben des Landesamtes für Verfassungsschutz beschränkten sich bisher auf die Be-obachtung verfassungsfeindlicher Bestrebungen, gewaltbereiten Ausländerextremismus, Spionagehandlungen und die Beteiligung an der Durchführung von Sicherheitsüberprüfungen.

Der Entwurf bindet das Landesamt für Verfassungsschutz nun erstmals in die Bekämpfung von Straftaten ein, die der organisierten Kriminalität zuzurechnen sind. Damit verliert sich der Sachzusammenhang zu den tradierten Aufgaben des Verfassungsschutzes. Außer Bayern und dem Saarland verfährt kein weiteres Bundesland so. In Thüringen gibt es einen entsprechenden Gesetzentwurf.

Meine Bedenken gegen eine derartige Aufgabenerweiterung lassen sich wie folgt zusammenfassen:

- Das Landesamt für Verfassungsschutz erhält mit der Bekämpfung von Straftaten ein ganz neues Betätigungsfeld. Es geht um eine qualitative Umstrukturierung, die ihn in unmittelbarer Verwandtschaft zum Landeskriminalamt bringt. Es werden konkurrierende Zuständigkeiten aufgebaut, die die gesamtstaatliche Effizienz stören.

- Die Aufgabenerweiterung des Landesamtes für Verfassungsschutz in die Bekämpfung der organisierten Kriminalität macht nur Sinn, wenn sie zu einer informationellen Verflechtung zwischen Landesamt für Verfassungsschutz, Staatsanwaltschaft und Polizei führt. Ein stark erweiterter Informationsaustausch zwischen Verfassungsschutz und den anderen Sicherheitsbehörden tangiert das Trennungsgebot zwischen Polizei und Geheimdienst. Das Trennungsgebot antwortet auf Erfahrungen, die die Allmacht der Gestapo schuf.

- Die Vorfeldbefugnisse der Polizei nach dem Hessischen Gesetz über die öffentliche Sicherheit und Ordnung und nach der Strafprozessordnung sind unlängst stark ausgeweitet worden. Es sind kaum Fälle denkbar, in denen das HSOG ein Eingreifen der Polizei verbietet. In jedem Fall wäre eine Nachbesserung des HSOG sachgerechter, statt die Zuständigkeit einer anderen Behörde zusätzlich zu begründen.

- Die Unschärfe des Begriff der organisierten Kriminalität macht die Zuständigkeitsabgrenzung schwer, zumal es um eine frühe Vorfeldbeobachtung geht.

- Schließlich stellt sich die praktische Frage nach der Verwertbarkeit der vom Landesamt für Verfassungsschutz gewonnenen Informationen, die oftmals der Geheimhaltung unterliegen, im Gerichtsverfahren.

9.1.2
Erweiterung der Befugnisse zum Abhören und Anfertigen von Bildaufnahmen in Wohnungen

Das hessische Verfassungsschutzgesetz (VerfSchG) enthält bislang eine restriktive Regelung zum Abhören in Wohnungen. Nach § 5 Abs. 2 VerfSchG ist der „Lauschangriff“ nur zugelassen, wenn es zur Abwehr einer gegenwärtigen gemeinen Gefahr oder einer gegenwärtigen Lebensgefahr für einzelne Personen unerlässlich ist und polizeiliche Hilfe für das bedrohte Rechtsgut nicht rechtzeitig erlangt werden kann. Der Entwurf sieht eine deutliche Ausweitung der Ausspähbefugnisse in Wohnungen für unterschiedlichste Fallgestaltungen vor. Der Entwurf schöpft alle durch die Änderung von Art. 13 Grundgesetz eröffneten Eingriffsmöglichkeiten aus:

- Nach § 5 Abs. 2 Nr. 3 des Entwurfs ist das Ausspähen in Wohnungen bei Verdacht der Planung oder Begehung von Straftaten i.S.v. § 100a StPO sowie fast allen Vermögensdelikten zulässig. Eine echte Begrenzung der Überwachung ist nicht mehr zu sehen.

- Der Entwurf sieht das optische und akustische Ausspähen in Wohnungen vor, „wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre“. Hier habe ich die Streichung des Begriffs „wesentliche Erschwerung“ vorgeschlagen. Immerhin handelt es sich um einen höchst intensiven Eingriff in die Wohnungsfreiheit. Voraussetzung sollte dafür sein, dass die Sachverhaltsaufklärung auf andere Weise nicht erfolgen könnte, und nicht nur, dass sie wesentlich erschwert ist.

- Abs. 3 des Entwurfs sieht vor, dass die Anordnungsbefugnis für den Einsatz besonderer nachrichtendienstlicher Mittel bei Gefahr im Verzug vom Richter auf den Leiter des Landesamtes für Verfassungsschutz übergeht. Ein derartiger Eilfall ist schwer zu begründen. Das für derartige Anordnungsbefugnisse zuständige Gericht ist das Amtsgericht Wiesbaden, das jederzeit erreicht werden kann.

- Daten, die aufgrund von Abhörmaßnahmen in Wohnungen erhoben wurden, sollten als solche gekennzeichnet werden. Auch für die Empfänger sollten die Art und Weise der Erhebung erkennbar sein. Diese Kennzeichnung ist nach einer Übermittlung der Daten an weitere Empfänger aufrecht zu erhalten. Was für den Bundesnachrichtendienst bei Eingriffen in das Fernmeldegeheimnis durch § 4 Abs. 2 des Gesetzes zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses vorgeschrieben ist, muss auch für Fallgestaltungen gelten, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen.

9.1.3
Auskunftspflichten gegenüber dem Landesamt für Verfassungsschutz

In den Planungen des Hessischen Innenministeriums ist vorgesehen, dass Banken und andere Geldinstitute, Postdienste und Luftverkehrsunternehmen verpflichtet werden können, bestimmte Auskünfte über ihre Kunden dem Landesamt für Verfas-

sungsschutz mitzuteilen. Banken sind beispielsweise nicht nur angehalten, den Namen von Konteninhabern weiterzugeben, sondern auch Ausführungen zu Geldbewegungen zu machen. Der derzeitige Entwurf zur Änderung des Bundesverfassungsschutzgesetzes vom 15. November 2001 sieht bestimmte Auskunftspflichten vor, ist aber datenschutzrechtlich deutlich besser und rechtsstaatlicher als der hessische Entwurf. Beispielsweise sind auf Bundesebene derartige Auskunftspflichten nicht bei allen Aufgaben des Verfassungsschutzes - wie etwa der Beobachtung extremistischer Bestrebungen - vorgesehen. Nach den hessischen Überlegungen sollen die Auskunftspflichten für das gesamte Aufgabenspektrum des Verfassungsschutzes gelten.

Unter dem Gesichtspunkt der Verhältnismäßigkeit wäre auf jeden Fall eine Eingrenzung dieser Verpflichtungen durch die Festlegung einer erhöhten Verdachtsschwelle und die Beschränkung auf schwerwiegende Gefahren für bestimmte Schutzgüter vorzusehen.

Auskunftsersuchen sollten nur als ultima ratio gestellt werden können. Geregelt werden sollte weiterhin, dass die Anordnung der Auskunftsverpflichtung durch eine übergeordnete Stelle erfolgen muss. Eine Mitteilungspflicht des Landesamts für Verfassungsschutz gegenüber dem Betroffenen fehlt völlig.
Die Auskunftsverpflichtung für die Unternehmen, die geschäftsmäßig Postdienstleistungen erbringen, sieht weitgehende Eingriffe in Art. 10 Grundgesetz vor. Erforderlich sind deshalb den Grundrechtseingriff flankierende Maßnahmen; dies trifft sowohl die Zweckbindung als auch die Regelung von Prüfungs- und Löschungspflichten und die Kennzeichnungspflicht.

9.1.4
Herabsetzung des speicherungsrelevanten Alters von Jugendlichen

Neu vorgesehen werden soll, dass Minderjährige bereits ab dem zwölften Lebensjahr und nicht mehr wie bisher ab dem sechzehnten Lebensjahr Erwachsenen bezüglich der Speicherung von Daten zu ihrer Person weitgehend gleichgestellt werden. Ab dem zwölften Lebensjahr sollen unter den gleichen Voraussetzungen wie bei Erwachsenen Personenakten angelegt werden dürfen und Dateispeicherungen stattfinden. Auch wenn sie kürzeren Prüf- und Löschfristen unterliegen, stellt das eine Ausweitung der Erfassung dar, die dem kindlichen Alter nicht gemäß ist. Die Herabsetzung des Alters birgt die Gefahr einer Stigmatisierung von Jugendlichen und sollte dringend überdacht werden. Hessen wäre zudem das einzige Land, dass eine derartige Regelung vorsähe.

9.1.5
Verlängerung der Lösch- und Prüffristen

Durch die vorgesehene Regelung werden die Prüf- bzw. Löschpflichten für Datensätze in automatisierten Dateien und in Akten von 5 auf 10 bzw. von 10 auf 15 Jahre verlängert. Auch angesichts der äußerst niedrigen Verdachtsschwelle mit der der Verfassungsschutz arbeitet, ist das kaum nachzuvollziehen. Nach meinen Erfahrungen werden schon nach fünf Jahren bei der ersten Prüfung auf die weitere Erforderlichkeit der Speicherung hin eine Reihe von Datensätzen und Personenakten gelöscht. Die Heraufsetzung der Fristen mit dem Hinweis auf den erheblichen personellen Aufwand halte ich gerade bei der Arbeit des Verfassungsschutzes im Vorfeldbereich und der naturgemäß niedrigen Verdachtsschwelle für nicht akzeptabel.

9.2
Prüfung von Akten des Landesamtes für Verfassungsschutz

Beim Hessischen Landesamt für Verfassungsschutz wurden die Akten über die Sicherheitsüberprüfung von Mitarbeitern des öffentlichen Dienstes kontrolliert. Seit der letzten Prüfung sind weitere Verbesserungen zu verzeichnen. Bei der Prüfung von Nachweisen über die Einsichtnahme des Landesamtes für Verfassungsschutz in Register und Akten öffentlicher Stellen wurde eine Reihe datenschutzrechtlicher Probleme festgestellt.

9.2.1
Kontrolle der Sicherheitsüberprüfungsakten

Für Sicherheitsüberprüfungen ist in Hessen nach wie vor, worauf meine Amtsvorgänger und ich schon seit vielen Jahren hinweisen, keine gesetzliche Grundlage vorhanden. Es ist kaum nachvollziehbar, dass in einem derart sensiblen Bereich, in dem fühlbare Grundrechtseingriffe auftreten, immer noch keine Rechtsgrundlage existiert.

Im 21. Tätigkeitsbericht (Ziff. 2) habe ich von einer Kontrolle der Sicherheitsüberprüfungsakten beim Landesamt für Verfassungsschutz berichtet. Ich hatte damals eine Reihe von Mängeln festgestellt. Die erneute Überprüfung diente dem Zweck festzustellen, ob die Mängel behoben sind.

Meine Mitarbeiter wählten aus dem derzeitigen Bestand von 7.000 bis 8.000 Sicherheitsüberprüfungsakten stichprobenartig 28 Akten aus.
Die Überprüfung hat ergeben, dass inzwischen weniger Informationen erhoben werden. Insbesondere die Berichte über die Gespräche von Mitarbeitern des Landesamtes für Verfassungsschutz mit Referenz– und Auskunftspersonen sind viel seltener geworden. In den Fällen, in denen sie noch stattfinden (Geheimhaltungsstufe „streng geheim"), ist der Inhalt sehr viel knapper und sachlicher gehalten.

Wenig überzeugend ist der Umgang mit den sogenannten Sicherheitserklärungen, die von der Person, die der Sicherheitsüberprüfung unterzogen wird, auszufüllen ist. Für alle drei Überprüfungsarten („vertraulich", „geheim", „streng geheim") wird die gleiche Art von Formularen verwandt. Dies führt dazu, dass Daten erhoben werden, die für die jeweilige Überprüfungsart gar nicht erforderlich sind. So hat der Betroffene die Namen von Referenzpersonen im Regelfall nur dann anzugeben, wenn es um eine Überprüfung der Geheimhaltungsstufe „streng geheim" geht. Nach meinen Feststellungen werden die Namen von Referenzpersonen aber auch in anderen Sicherheitsstufen abverlangt, wo dies nicht erforderlich ist. Darin liegen unzulässige Datensammlungen „auf Vorrat".
Ich habe dem Landesamt für Verfassungsschutz und dem Hessischen Innenministerium verschiedene Änderungsvorschläge unterbreitet.

9.2.2
Prüfung der Einsichtnahme des Landesamtes für Verfassungsschutz in Register und Akten öffentlicher Stellen sowie die darüber anzufertigenden Nachweise

Die Mitarbeiter des Landesamtes für Verfassungsschutz können unter bestimmten Voraussetzungen in Akten und Register öffentlicher Stellen einsehen. Über diese Einsichtnahme ist ein Nachweis zu führen.

§ 4 Gesetz über das Landesamt für Verfassungsschutz

(2) ... Würde durch die Erhebung nach Satz 1 der Zweck der Maßnahme gefährdet oder die betroffene Person unverhältnismäßig beeinträchtigt, darf das Landesamt für Verfassungsschutz Akten und Register öffentlicher Stellen einsehen.

(3) ... Über die Einsichtnahme nach Abs. 2 Satz 2 hat das Landesamt für Verfassungsschutz einen Nachweis zu führen, aus dem der Zweck, die ersuchte Behörde und die Aktenfundstelle hervorgehen; der Nachweis ist gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr seiner Erstellung folgt, zu vernichten.

Ansatzpunkt für meine Prüfung waren diese Nachweise. Aus dem mir vorgelegten Material wählte ich stichprobenartig 23 Nachweise und bat um Vorlage der entsprechenden Akten.
Alle eingesehenen Stichproben zeigten, dass die Voraussetzungen für Einsichtnahmen in Register öffentlicher Stellen vorlagen. Allerdings war festzustellen, dass von der ersuchten Behörde häufig mehr Daten an das Landesamt für Verfassungsschutz übermittelt werden, als überhaupt angefordert wurden. So enthielten die Datensatzausdrucke der Meldebehörden beispielsweise Angaben über die Zugehörigkeit zu einer Religionsgesellschaft, die Information, dass Untersuchungsberechtigungsscheine nach dem Jugendarbeitsschutzgesetz ausgestellt sind, Pass- und Ausweisdaten einschließlich der Passversagungsgründe oder auch Daten, die dem Steuergeheimnis unterliegen. Ein Nachweis enthielt die Information, dass der Betroffene ein uneheliches Kind hat, und Name, Geburtsdatum und Anschrift der Mutter waren ebenfalls in der Akte enthalten.

In zwei Fällen wurden Daten bei der Polizei erhoben. In beiden Fällen enthielten die Protokolle über die Einsichtnahme komplette Datensatzausdrucke aus HEPOLIS und INPOL. Ausdrucke aus polizeiinternen Dateien dürfen nach den Richtlinien über kriminalpolizeiliche Sammlungen aber nicht an Stellen außerhalb der Polizei übermittelt werden.
Ich habe dem Landesamt für Verfassungsschutz vorgeschlagen, die Einsichtnahme in Akten und Register bei anderen Behörden beispielsweise durch die Benutzung einheitlicher Formulare datenschutzgerecht zu gestalten. Da die Verantwortung für einen Teil der Mängel nicht beim Landesamt für Verfassungsschutz liegt, habe ich darum gebeten, die entsprechenden Stellen des Hessischen Innenministeriums zu beteiligen, um eine Lösung des Problems herbei zu führen.

10. Finanzwesen

10.1
Die Allgemeine Nachschau in der Abgabenordnung

Der Entwurf eines Steuerverkürzungsbekämpfungsgesetzes sieht überraschende Kontrollbesuche ohne Anlass bei Gewerbetreibenden und Selbständigen vor. Solange keine konkreten Voraussetzungen für die Kontrollbesuche festgelegt sind, ist die Regelung ein unverhältnismäßiger Eingriff.

Mit dem Entwurf eines Artikelgesetzes zur Bekämpfung von Steuerverkürzungen bei der Umsatzsteuer und anderen Steuern (Steuerverkürzungsbekämpfungsgesetz - StVBG, Stand 10. September 2001, BTDrucks. 14/6883) beabsichtigt der Gesetzgeber mit § 88b Abgabenordnung (AO) eine sogenannte „allgemeine Nachschau“ in die Abgabenordnung einzuführen. Die neue Vorschrift soll es den Finanzbehörden zur Sicherstellung einer gleichmäßigen Festsetzung und Erhebung der Umsatzsteuer ermöglichen, ohne vorherige Ankündigung und außerhalb einer Außenprüfung Grundstücke und Räume von Personen, die eine gewerbliche oder berufliche Tätigkeit selbständig ausüben, während der Geschäfts- und Arbeitszeiten zu betreten, um Sachverhalte festzustellen, die für die Besteuerung erheblich sein können. Das Finanzamt soll in die Lage versetzt werden, den Geschäftsbetrieb zu prüfen, ohne dem Inhaber die Möglichkeit zu geben, sich auf die Kontrolle einzustellen. Mit einem schriftlichen Hinweis, aber ohne vorherige Prüfungsanordnung, kann die Maßnahme in eine Außenprüfung übergehen.

Im Gegensatz zu dem ausgehenden Referentenentwurf hat der vorgelegte Gesetzentwurf datenschutzrechtliche Nachbesserungen erfahren: Er beschränkt die neue Maßnahme auf die Festsetzung und Erhebung der Umsatzsteuer und berücksichtigt den grundrechtlichen Schutzbereich der privaten Wohnräume (Art. 13 GG). Nach wie vor fehlt es jedoch an genauen tatbestandlichen Voraussetzungen, unter denen eine allgemeine Nachschau angeordnet werden kann. Mit der Neuregelung wird parallel zur Außenprüfung (§ 194 AO) und zur Steueraufsicht (§§ 209 ff. AO) ein neuartiges Ermittlungsverfahren eingeführt, das für die Steuerpflichtigen wegen des unangekündigten Zugriffs der Finanzbehörden eine deutlich stärkere Belastung aufweist. Die herkömmliche Außenprüfung erlaubt dem Steuerpflichtigen eine Vorbereitung der Prüfung und die Einschaltung eines Steuerberaters. Er kann erforderlichenfalls Ergänzungen bei fehlerhaften Ansätzen und Bewertungen veranlassen und aufgetretene Mängel in der Buchführung rechtzeitig beheben. Deswegen muss die Anordnung der Außenprüfung vorab und mit Rechtsmittelbelehrung erfolgen (§ 197 AO). Demgegenüber setzt die Neuregelung auf den Überraschungseffekt einer unangekündigten Kontrolle.

Gegenüber Steuerpflichtigen, bei denen hinreichende tatsächliche Anhaltspunkte für den Verdacht bestehen, dass sie sich aktiver Steuerverkürzung schuldig gemacht haben, ist ein solches Vorgehen sachgerecht und grundrechtlich legitimierbar, nicht hingegen bei rechtstreuen Steuerpflichtigen. Während die zollamtliche Steueraufsicht nach § 209 ff. AO ihre besondere Rechtfertigung darin hat, dass Waren und Leistungen das Zollgebiet verlassen oder erreichen, soll die neue Steueraufsicht den gesamten Gewerbe- und Freiberufssektor ohne vorausgehendes Fehlverhalten einer jederzeitigen möglichen und ohne tatbestandliche Voraussetzungen zulässigen Kontrolle unterwerfen. Darin liegt nach der soeben durchgesetzten Verschärfung der Prüfungsbefugnisse nach § 147 Abs. 6 AO (s.a. Ziff. 26.5) ein weiterer Schritt zum „gläsernen Betrieb“. Die Neuregelung ist verfassungsrechtlich nur tragbar, wenn genaue tatbestandliche Voraussetzungen genannt werden, unter denen die allgemeine Nachschau angeordnet werden kann. Dies könnte z. B. der begründete Verdacht einer Steuerverkürzung oder der Verdacht einer Mitwirkung an einer solchen sein.

Ich habe in diesem Sinne zu dem Gesetzentwurf öffentlich und dem Hessischen Ministerium der Finanzen gegenüber Stellung genommen.

10.2
Abgabenordnung und Datenschutz - ein altes Thema neu belebt

Im Berichtsjahr fanden intensive Gespräche über die lange geforderte Novellierung der Abgabenordnung statt.

Die Novellierung der Abgabenordnung (AO) unter datenschutzrechtlichen Gesichtspunkten ist nunmehr seit über 20 Jahren überfällig. Die Anpassung an das Datenschutzrecht ist zum - leider ergebnislosen - Dauerthema zwischen den Datenschutzbeauftragten des Bundes und der Länder sowie den Bundes- und Landesfinanzministerien geworden. Inzwischen gibt es zwischen den Parteien einen neuen Vorstoß, der durchaus vielversprechend erscheint. Unlängst fanden Gespräche statt, die jenseits des festgefahrenen und polarisierenden Meinungsstandes („Datenschutz ist Steuerhinterzieherschutz“ kontra „Steuerdaten ohne Datenschutz“) auch Gemeinsamkeiten und Erfahrungen mit datenschutzrechtlichen Regelungen berücksichtigen.

Die Herausforderung besteht insbesondere darin, Regeln und Verfahren zu finden, die auf der einen Seite die Durchführung einer ordnungsgemäßen und vollständigen Besteuerung im Massenverfahren reibungslos zulassen, und auf der anderen Seite den einzelnen Steuerpflichtigen in seinem verfassungsrechtlich geschützten Recht auf informationelle Selbstbestimmung nicht verletzen. Als Vorsitzender des Arbeitskreises Steuern habe ich Vorgespräche mit einem Vertreter des Bundesfinanzministeriums und Mitarbeitern des Hessischen Finanzministeriums geführt. Ausführlich erörtert wurde insbesondere das bisher nicht geregelte Recht auf Akteneinsicht, das auch von der europäischen Datenschutzrichtlinie als fundamentales Recht betrachtet wird. Die Durchführung einer Akteneinsicht darf allerdings die sonstige Arbeit der Finanzbehörden nicht mehr als notwenig behindern. Daten Dritter - etwa in Kontrollmitteilungen - dürfen bei dieser Gelegenheit nicht offenbart werden. Angedacht wurde eine Regelung zur Akteneinsicht, die als Rechtsanspruch mit entsprechenden Ausnahmeregelungen formuliert wird.

Weiterer Regelungsbedarf besteht im Rahmen des fast grenzenlosen Ermittlungswunsches der Steuerverwaltung (s.a. Ziff. 10.3). Unter Hinweis auf den gesetzlichen Auftrag, die Steuern gleichmäßig und vollständig festzusetzen und zu erheben (§ 85 AO) und auf die grundsätzliche Auskunftspflicht der Beteiligten und anderer Personen (§ 93 AO) wird von der Finanzverwaltung eine Vielzahl von Informationen mit personenbezogenen Daten von Steuerpflichtigen auf Vorrat abgefragt, ohne dass dabei die datenschutzrechtlichen Grundsätze wie Erforderlichkeit der Datenerhebung, Datenerhebung beim Betroffenen, Zweckbindung der Daten und Datensparsamkeit berücksichtigt werden. Wie wiederkehrende Bürgerbeschwerden zu diesem Thema zeigen, sind die Anfragen der Finanzämter oft sehr pauschal. Der Auskunftsverpflichtete wird mitunter in eine Zeugenposition gedrängt, ohne dass ihm Weigerungsrechte, über Daten Dritter Auskunft zu geben, zustehen. Bereits die Angabe einer spezifischen Begründung für das Auskunftsverlangen, die auch die datenschutzrechtlichen Belange berücksichtigt, könnte hier weiterhelfen.

Schließlich fordert die fortschreitende Automatisierung in der Steuerverwaltung die Beachtung datenschutzrechtlicher Gesichtspunkte. Mein Eindruck ist, dass im Rahmen der Automation die datenschutzrechtlichen Anforderungen an die Datensicherheit - zumindest in Hessen - durchaus beachtet werden. Ungeachtet dessen müssen durchgängig verpflichtende Regelungen geschaffen werden, die den Datenschutz innerhalb der gesamten Steuerverwaltung nachvollziehbar und kontrollierbar machen.

10.3
Steuerliche Ermittlungen: Auskunftsersuchen, Rasterfahndung oder Zeugenbefragung ohne Grenzen?

In der Steuerverwaltung verwischen zusehends die Grenzen zwischen begründeten Auskunftsbegehren einerseits und Rasterfahndungen, Zeugenbefragungen und strafrechtlichen Ermittlungen andererseits. Das geltende Recht enthält undifferenzierte Ermächtigungen, die den Finanzbehörden zu weitreichende Zugriffe gestatten.

Ein Bauunternehmer legte mir die Aufforderung des Finanzamts Wetzlar (Steuerfahndungsstelle) vor, die ihn zur Auskunft über die von ihm innerhalb eines bestimmten Zeitraums eingesetzten Subunternehmen Auskunft gemäß §§ 85, 88, 90, 92, 93, 97 i.V.m. § 208 Abs. 1 Satz 1 Nr. 3 Abgabenordnung (AO) 1977 verpflichtete. Vergleichbare Schreiben haben offensichtlich ca. 8.000 weitere Steuerpflichtige aus dem Bauhaupt- und Baunebengewerbe erhalten. In dem übersandten Fragebogen war einzutragen, ob und welche Subunternehmer (Name, Anschrift) der Steuerpflichtige beauftragt hatte, und welche handelnden Personen für die Subunternehmer aufgetreten waren, z. B. Zahlungen erhalten hatten. Mit einer Kopie einer aktuellen Rechnung waren die Angaben zu belegen.

Ein konkreter Verdacht auf einen Gesetzesverstoß lag den Anforderungen der Finanzämter nicht zugrunde. In den gleichzeitig versandten Erläuterungen ist dargelegt, dass aufgrund einer Vielzahl anderer Ermittlungsverfahren festgestellt worden sei, dass auch im dortigen Raum steuer- und sozialversicherungsrechtlich unzutreffend deklarierte Subunternehmer tätig sind. Die Aktion soll der Bekämpfung illegaler Beschäftigung dienen. In einem beigefügten Merkblatt wurde der Petent über die Rechte und Pflichten Steuerpflichtiger bei Prüfungen durch die Steuerfahndung nach § 208 Abs. 1 Nr. 3 AO unterrichtet.

Diese Vorgehensweise ist mit den datenschutzrechtlichen Anforderungen, Erforderlichkeit, Zweckbindung und Transparenz der Datenverarbeitung, nicht zu vereinbaren. Die Fragen nach Subunternehmen durch die Steuerfahndung ist eine Erhebung personenbezogener Daten. Hingegen ist die Überprüfung der Subunternehmer auf sozialversicherungsrechtliches Fehlverhalten keine Aufgabe der Steuerverwaltung und kann als Zweck der Maßnahme nicht herangezogen werden. Eine Rechtsvorschrift, die die Erhebung der Daten wegen steuerlichen Fehlverhaltens Dritter zulässt, existiert nicht. Die §§ 208 Abs. 1 Nr. 3, 93 Abs. 1 Satz 1 AO sind allgemeine Ermittlungsnormen in Bezug auf Dritte, denen es an der erforderlichen Normenklarheit fehlt. Die Vorschriften lassen schon gar nicht ein Massenauskunftsverlangen zu, das - ohne konkreten Verdacht - die pauschale Durchforstung der baugewerblichen Unternehmen nach Subunternehmen ermöglicht. Es handelt sich meines Erachtens um eine gesetzlich nicht vorgesehene und auch von der Rechtsprechung nicht legitimierte, daher unzulässige Rasterfahndung. Aus seriösen Subunternehmen sollen evtl. „schwarze Schafe“ herausgefiltert werden, ohne dass ein Zusammenhang zu einem bestimmten Verfahren oder ein konkreter Verdacht vorliegt. Die Steuerverwaltung will die Daten hinter dem Rücken der Betroffenen erheben und sie ohne deren Wissen auswerten. Die Erforderlichkeit einer derartigen generellen Erhebung ist zu verneinen. Dass das Auskunftsverlangen für die Erfüllung der Aufgaben der Steuerverwaltung unerlässlich ist, darf zudem bezweifelt werden. So wird z. B. nicht dargelegt, ob oder warum als milderes Mittel nicht die Auswertung der bereits im jeweiligen Besteuerungsverfahren enthaltenen Angaben des auftraggebenden Unternehmens ausreichen. Die Befragung aller in Betracht kommenden Auftraggeber stellt eine neue Dimension des Auskunftsverlangens dar, die nicht mit den Fällen vergleichbar ist, die in der Vergangenheit von der Rechtsprechung zum Thema Rasterfahndung und Bankengeheimnis entschieden wurden. Während dort jeweils *eine* Bank um Auskunft über ihre Kunden ersucht wurde, wenn ein Sachzusammenhang zu einem ihrer Anleger (z. B. Inhaber von Tafelpapieren) bestand, wäre der hier vergleichbare Fall der, dass *alle* Banken im Zuständigkeitsbereich des Finanzamtes Auskunft über alle ihre Kunden zu erteilen haben, die bei ihnen Tafelgeschäfte getätigt haben, weil es in dieser Geschäftssphäre anderswo zu Unregelmäßigkeiten gekommen ist. Diese undifferenzierte Vorgehensweise ist unverhältnismäßig. Hier hätte wenigstens ein Bezug oder Hinweis zum jeweiligen Auftraggeber bestehen müssen, der eine Abfrage rechtfertigt.

Die jeweiligen Auftraggeber werden außerdem in eine Zeugenfunktion versetzt, ohne Hinweis darauf, dass sie selbst sich u.U. steuerstrafrechtlichen Vorwürfen aussetzen können. Auch die künftigen Geschäftsbeziehungen werden gefährdet, wenn diese von den Auskünften Kenntnis erlangen. Des Weiteren besteht für die Auftraggeber die Gefahr, für die Umsatzsteuerausfälle in Anspruch genommen zu werden, wenn sich der Steueranspruch bei den Subunternehmen nicht realisieren lässt, § 14 Abs. 3 Umsatzsteuergesetz. Über diese weitere Zweckbestimmung der Datenerhebung wird der Steuerpflichtige im Unklaren gelassen. Ihm wird lediglich mitgeteilt, dass vollständige Angaben zu den Subunternehmern auch im eigenen Interesse liegen, den Schutz eines fairen Wettbewerbes im Baugewerbe zu festigen.

Trotz meiner Intervention hält die Finanzverwaltung an ihrem Vorgehen fest. Auskunftsersuchen, in denen - wie im Berichtsfall - Daten Dritter von der Finanzverwaltung gefordert werden, stellen eine Vielzahl der bei mir eingehenden Beschwerden. Ich halte es daher für dringend geboten, in diesem Bereich des Verfahrensrechts (Abgabenordnung) eine Überarbeitung der geltenden Rechtsnormen herbeizuführen, die das Recht auf informationelle Selbstbestimmung stärker berücksichtigen.

11. Gesundheit

11.1
Modellprojekt Mammographie-Screening

Gegen eine Übermittlung der für das Projekt erforderlichen Meldedaten an den Projektträger bestehen keine datenschutzrechtlichen Bedenken. Durch das neue Konzept des Projektträgers wird sichergestellt, dass keine schutzwürdigen Belange der betroffenen Frauen beeinträchtigt werden.

Bereits im Frühjahr 2000 bin ich von den Projektbeteiligten um eine Stellungnahme zu den datenschutzrechtlichen Anforderungen an die Durchführung des Modellprojekts zur Einführung einer qualitätsgesicherten Brustkrebsfrüherkennung mittels Mammographie-Screening gebeten worden. Gegenstand des Modellprojekts ist die Erprobung von Strukturen, innerhalb deren künftig qualitätsgesichertes Mammographie-Screening in Deutschland flächendeckend durchgeführt werden kann. Parallel sollen Modellprojekte in Bremen und der Region Weser-Ems erfolgen.
Für die Durchführung des Projekts wurde von dem Projektträger die Übermittlung der Meldedaten aller Frauen im Alter von 49 bis 69 Jahren mit Hauptwohnsitz in Wiesbaden oder dem Rheingau-Taunus-Kreis von den Einwohnermeldeämtern beantragt. In einer ersten Stellungnahme im Oktober 2000 habe ich gegenüber dem Hessischen Sozialministerium, der Stadt Wiesbaden und den Projektbeteiligten dargelegt, dass ich aufgrund der mir vorliegenden Unterlagen und der Besprechungsergebnisse noch eine Reihe klärungsbedürftiger Fragen sehe und bisher kein Datenschutzkonzept vorgelegt wurde, sodass ich eine Übermittlung der Meldedaten noch nicht als zulässig ansehe. Die Fragen betrafen insbesondere

- den Inhalt und die Dauer des Projekts,
- den Kreis der Projektbeteiligten und deren jeweilige Aufgaben innerhalb des Projekts
- die Rechte der Frauen, die zu der betroffenen Altersgruppe gehören und nicht an dem Projekt teilnehmen wollen, auf Löschung ihrer Daten in der Einladungsdatenbank des Projektträgers,
- die Texte der Informationsblätter und der Formulare für die Einwilligungserklärungen der betroffenen Frauen sowie
- die vorgesehenen technisch-organisatorischen Datensicherheitsmaßnahmen.

In der Zwischenzeit sind diese Fragen geklärt und es liegt ein überarbeitetes detailliertes Konzept für das Projekt vor. Projektträger ist der Verein Mammographie-Screening Wiesbaden/Rheingau-Taunus-Kreis e. V.; Projektbeteiligte sind niedergelassene Ärzte, Kliniken, die Kassenärztliche Vereinigung Hessen und die Krankenkassen in Hessen. Das Projekt wird im Auftrag des Bundesausschusses der Ärzte und Krankenkassen durchgeführt und hat das Ziel, die bundesweite Einführung der Mammographie in die Früherkennungsuntersuchung der gesetzlichen Krankenversicherung zu unterstützen. Allen Frauen zwischen 49 und 69 Jahren wird ein Untersuchungstermin zur Früherkennung von Brustkrebs nach den Qualitätsstandards der europäischen Leitlinien zur Qualitätssicherung des Mammographie-Screenings durch den Projektträger schriftlich angeboten. Zu diesem Zweck werden sukzessive während des Projekts Meldedaten (Vorname, Familienname, Titel, Staatsangehörigkeit, Anschrift, Alter) der betroffenen Frauen an den Verein übermittelt. Die Teilnahme an dem Projekt ist freiwillig. Die Frauen werden in einem Informationsblatt über die Ziele des Modellprojekts, die Organisation und insbesondere auch die Verarbeitung ihrer personenbezogenen Daten informiert und um ihre schriftliche Einwilligung gebeten.

Ich habe dem Hessischen Sozialministerium, der Stadt Wiesbaden und den Projektbeteiligten mitgeteilt, dass ich eine Übermittlung der Meldedaten auf der Grundlage des § 34 Abs. 3 Hessisches Meldegesetz (HMG) als zulässig ansehe.

§ 34 Abs. 3 und 4 HMG

(3) Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohnerinnen und Einwohner (Gruppenauskunft) darf nur erteilt werden, soweit sie im öffentlichen Interesse liegt. Für die Zusammensetzung der Personengruppe dürfen die folgenden Daten herangezogen werden:
1. Tag der Geburt,

2. Geschlecht,
3. Staatsangehörigkeiten,
4. Abschriften,
5. Tag des Ein- und Auszugs,
6. Familienstand, beschränkt auf die Angabe, ob verheiratet oder nicht,
7. erwerbstätig/nicht erwerbstätig und
8. Verknüpfungen zu Familienangehörigen (Ehegatten, Kinder, Eltern).

Mitgeteilt werden dürfen außer der Tatsache der Zugehörigkeit zu der Gruppe folgende Daten:
1. Vor- und Familienname,
2. Doktorgrad,
3. Alter,
4. Geschlecht,
5. Staatsangehörigkeiten,
6. Anschriften und
7. gesetzliche Vertreterin/gesetzlicher Vertreter oder Betreuerin oder Betreuer.

(4) Bei Melderegisterauskünften nach Abs. 2 und 3 darf der Empfänger die Daten nur für den Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt wurden.

Ein öffentliches Interesse an der Melderegisterauskunft ist gegeben. Das Modellprojekt soll zur Bekämpfung der Brustkrebssterblichkeit beitragen. Es wird vom Bundesgesundheitsministerium gefördert und u. a. auch vom Hessischen Sozialministerium befürwortet. Durch das neue Konzept ist gewährleistet, dass schutzwürdige Belange der betroffenen Frauen i. S. v. § 7 HMG nicht beeinträchtigt werden.

§ 7 HMG

Schutzwürdige Belange Betroffener dürfen durch die Verarbeitung personenbezogener Daten nicht beeinträchtigt werden. Schutzwürdige Belange werden insbesondere beeinträchtigt, wenn die Verarbeitung gemessen an ihrer Eignung und ihrer Erforderlichkeit zu dem vorgesehenen Zweck, Betroffene unverhältnismäßig belastet. Die Prüfung, ob schutzwürdige Belange Betroffener beeinträchtigt werden, entfällt, wenn die Verarbeitung durch Rechtsvorschrift vorgeschrieben ist.

Insbesondere sieht das nachgebesserte, nunmehrige Konzept vor, dass die Daten der eingeladenen Frauen, die

- eine Teilnahme an dem Projekt explizit gegenüber dem Projektträger ablehnen oder
- zum Einladungstermin nicht erschienen sind und sich auch nicht telefonisch oder schriftlich geäußert haben und auch auf einen weiteren Terminvorschlag nicht reagiert haben,

in der Datenbank des Projektträgers gelöscht werden. Informationsblatt und Text der Einwilligungserklärungen sind aus datenschutzrechtlicher Sicht korrekt formuliert. In dem Konzept sind angemessene Datensicherheitsmaßnahmen vorgesehen.

Die Umsetzung des Konzepts wird von dem für den privaten Bereich - und damit auch für den Verein Mammographie-Screening - zuständigen Dezernat Datenschutz des Regierungspräsidiums Darmstadt und- soweit es grundsätzliche Fragen des Konzepts betrifft - auch von mir überprüft.

11.2
Auswertung von Mitglieder- und Leistungskarten von Zwangsarbeitern durch den Internationalen Suchdienst des Roten Kreuzes

Die Auswertung von Mitglieder- und Leistungskarten der ehemaligen Ortskrankenkassen über die in den Datenbeständen geführten Zwangsarbeiter durch den Internationalen Suchdienst des Roten Kreuzes in Bad Arolsen ist möglich. Nach § 69 Abs. 1 Nr. 1 SGB X in Verbindung mit § 69 Abs. 2 Nr. 1 SGB X ist eine Datenübermittlung für die Erfüllung sozialer Aufgaben zulässig.

11.2.1
Anfrage des Internationalen Suchdienstes

Die AOK Hessen musste über eine Anfrage des Internationalen Suchdienstes (ISD) in Bad Arolsen befinden. Der ISD beabsichtigte, aus den Archivbeständen der AOK Hessen Unterlagen zu übernehmen, die Informationen über ehemalige Zwangsarbeiter enthalten.

11.2.2
Art und Umfang der Datenbestände

Bei den Unterlagen, für die sich der ISD interessierte, handelt es sich überwiegend um Datenkarten. Diese Datenkarten sind in bestimmte Felder unterteilt, in die u.a. neben dem Namen des Betroffenen auch die Versicherten-Nummer sowie Behandlungsdaten per Hand eingetragen waren. Die Unterlagen lagen in zahlreichen Standorten der AOK, die sich über ganz Hessen verteilen. Über die Anzahl der Karten konnten keine endgültigen Angaben gemacht werden, da die Datenkarten der ehemaligen Zwangsarbeiter, die zwischen 1939 und 1945 in hessischen Betrieben arbeiteten, zusammen mit denen der anderen Versicherten gelagert waren. Man ging aber davon aus, dass 500 laufende Meter Mitglieder- und Leistungskarten sowie erhebliche verfilmte Bestände vorhanden sind.

11.2.3
Datenschutzrechtliche Bewertung einer Übermittlung an den Internationalen Suchdienst

Bei den Daten ehemaliger Zwangsarbeiter handelt es sich um geschützte Sozialdaten im Sinne des Sozialgesetzbuches (SGB). Nach § 69 Abs. 1 Nr. 1 ist eine Übermittlung von Sozialdaten zulässig, soweit sie erforderlich für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem SGB X erforderlich ist.
Die Übermittlung der genannten Daten dient der Erfüllung einer sozialen Aufgabe i.S.d. § 69 Abs. 1 SGB X. Der ISD in Bad Arolsen soll die Daten ausschließlich für den Zweck erhalten, eine Entschädigung der Betroffenen zu ermöglichen. Damit erfüllt die Datenübermittlung eine soziale Aufgabe, nämlich die Möglichkeit, ehemalige Betroffene in den Genuss einer finanziellen Wiedergutmachung zu bringen.

11.2.4
Abwicklung der Datenübermittlung

Nach Gesprächen der AOK Hessen mit meinem Haus und der Besprechung mit dem ISD ist folgende Lösung im Wege einer förmlichen Vereinbarung abgesprochen worden:
Der ISD erhält von der AOK Hessen die Erlaubnis, die Unterlagen ausländischer Personen aus den Jahren 1939 bis 1945 zu sichten und das für den ISD relevante Material über Zwangsarbeiter in den Bestand des ISD zu übernehmen. Die Sichtung der Bestände erfolgt in den AOK-Standorten durch Mitarbeiter des ISD. Die überlassenen Unterlagen werden ausschließlich zur Erfüllung der dem ISD übertragenen Aufgaben verwendet. Der Suchdienst wertet die übernommenen Daten nur aufgrund bei ihm eingehender Anfragen aus. Er erteilt Bestätigungen über Haft, Zwangsarbeit oder Verschleppung nur den ehemaligen Verfolgten gegenüber. Einzelauskünfte können auch an Organisationen wie Wiedergutmachungsbehörden, die im Interesse der Verfolgten anfragen, erteilt werden.

Technisch wird das Verfahren so abgewickelt, dass die aus dem Gesamtbestand ausgewählten Karten vom ISD verfilmt werden. Ein Film über die vom ISD zusammengeführte „Zwangsarbeiterkartei“ wird dem hessischen Hauptstaatsarchiv übergeben.

11.3
Fragebogen der AOK Hessen zur Krankenbeförderung mit Taxi oder Mietwagen

Von der AOK Hessen konzipierte Formulare für die automatisierte Abrechnung von Krankenbeförderungen sahen vor, dass die Fahrer detaillierte medizinische Daten der Patienten erheben. In Gesprächen mit den Datenschutzbeauftragten der AOK sowie einem Mitarbeiter der zuständigen Fachabteilung wurden die Erhebungsmerkmale in den Formularen reduziert.

11.3.1
Verfahren

Durch die Beschwerden mehrerer Taxiunternehmen, einzelner Taxifahrer sowie des Fachverbandes PKW-Verkehr bin ich auf ein Vorhaben der AOK Hessen aufmerksam geworden, mit dem bei der Abrechnung von Beförderungsleistungen mehr Transparenz und Möglichkeiten zur Kontrolle erreicht werden sollten. Zu diesem Zweck hatte die AOK ein Formular entwickelt, in dem durch das Beförderungsunternehmen umfangreiche Angaben zu Fahrer, Fahrzeug und Patient eingetragen werden sollten. Das Formular sollte vom Fahrer an die AOK zur Erfassung weitergeleitet werden.

11.3.2
Erfassungsbogen

Vor der Neuorganisation erhielt der Patient von seinem behandelnden Arzt eine ärztliche Verordnung zur Krankenbeförderung ausgehändigt, in der personenbezogene Daten enthalten sind. Neben den persönlichen Angaben wie Name und Vorna-

me sowie Geburtsdatum hatte der Arzt auch die Gründe für die Krankenbeförderung zu vermerken. Der Beförderer ließ sich auf der Verordnung die Fahrt quittieren. Die Verordnung wird an die Krankenkasse weitergeleitet. In Abänderung dieses Verfahrens hat die AOK zusammen mit einem Thüringer Verlag ein maschinenlesbares Formular entwickelt, auf dem neben den Angaben der ärztlichen Verordnung zusätzliche Daten über den beförderten Patienten erhoben werden sollten. So sollte beispielsweise die Frage beantwortet werden, zu welcher Art von Therapie oder Behandlung der Patient befördert wird, ob es sich um eine Dialyse, Chemotherapie oder Strahlentherapie handele. Auch andere über die ärztliche Verordnung hinausgehende Fragen sollten beantwortet werden.

11.3.3
Rechtliche Bewertung

Bei ihrem Auskunftsverlangen berief sich die AOK auf die Vorgaben des § 302 Sozialgesetzbuch V (SGB V). Danach sind Leistungserbringer verpflichtet, maschinenlesbar in den Abrechnungsbelegen die von ihnen erbrachten Leistungen nach Art, Menge und Preis zu bezeichnen und den Tag der Leistungserbringung sowie die Arztnummer des verordnenden Arztes und die Angaben nach § 291 Abs. 2 Nr. 1 bis 6 SGB V anzugeben. Deswegen sollte der Fahrer die erforderlichen Daten über die Patienten auf dem Formular dokumentieren. Zahlreiche Daten standen in keinem Zusammenhang mit der Beförderung. Das widerspricht der Regelung des § 302 Abs. 1 SGB V, demzufolge die Leistungserbringer nur die von ihnen erbrachten Leistungen zu bezeichnen haben. Bei diesem Verfahren wären die Patienten faktisch gezwungen gewesen, gegenüber dem Fahrer ihre detaillierten Krankheitsdaten zu offenbaren.

11.3.4
Weitere Vorgehensweise

In Gesprächen mit Vertretern der AOK Hessen wurde eine Einigung erzielt. Der Erfassungsbogen wurde um nicht erforderliche Patientendaten reduziert. Auf die Abrechnung mit dem maschinenlesbaren Erfassungsbogen wurde verzichtet, da die Anpassung der Software zu aufwendig gewesen wäre. Die manuelle Verwendung des inhaltlich reduzierten Formulars wurde den Vertragspartnern freigestellt.

11.4
Zusammenarbeit von Sozialämtern mit privaten Dienstleistern

Sozialämter dürfen die finanzielle Abwicklung der medizinischen Behandlung von Sozialhilfeempfängern und Asylbewerbern privaten Dienstleistern übertragen, wenn die Voraussetzungen des § 80 Sozialgesetzbuch X eingehalten werden und die Datensicherheit gewährleistet ist.

Seit einigen Jahren übertragen hessische Sozialämter die finanzielle Abwicklung der medizinischen Behandlung von Sozialhilfehilfeempfängern und Asylbewerbern privaten Dienst-leistern. In vielen Fällen wurde das Deutsche Dienstleistungszentrum für das Gesundheitswesen (DDG) mit Sitz in Essen beauftragt. Ich habe die Ausgestaltung der Zusammenarbeit und die Vertragstexte überprüft und Sozialämter bei der Formulierung der Verträge beraten.

11.4.1
Grundlage der Zusammenarbeit - Datenverarbeitung im Auftrag

Die DDG wickelt für einige Sozialämter das komplette Rechnungswesen im Zusammenhang mit der ärztlichen Versorgung von Sozialhilfeempfängern und Asylbewerbern ab. Die Leistungserbringer (Ärzte, Krankenhäuser, Apotheken usw.) erhalten ihre Auslagen - nach entsprechender Prüfung - vom Sozialamt unter Einschaltung der DDG ersetzt. Die Prüfung erfolgt anhand der vom Sozialamt festgelegten Kriterien. Das Sozialamt führt eine Datei, in der die Anspruchsberechtigten gespeichert sind. Diese Datei wird ständig aktualisiert und monatlich an die DDG übermittelt. Der Auftragnehmer prüft danach, ob die für eine bestimmte Person erbrachte Leistung auch erbracht werden durfte. Werden Fehler festgestellt, wird die Zahlung verweigert und der Leistungserbringer sowie das Sozialamt hiervon in Kenntnis gesetzt.

Die Abrechnungen der Leistungserbringer werden in einer automatisierten Datei bei der DDG gespeichert. Die DDG prüft die rechnerische Richtigkeit der abgerechneten Beträge. Werden Fehler festgestellt, reicht die DDG die Rechnung unbezahlt zurück und informiert den Auftraggeber hierüber. Soweit die DDG Beschwerden der Leistungserbringer bearbeitet, tritt sie nach außen als Auftragnehmerin des Sozialamtes auf.

11.4.2
Organisation bei der DDG

Täglich erreichen ca. 22.000 bis 25.000 Belege die DDG, die auch für große Krankenkassen die komplette Rechnungsabwicklung durchführt. Städte und Landkreise machen derzeit etwa 6 bis 7 % des Volumens aus. Vor allem aus Nordrhein-Westfalen, aber auch aus Hessen und anderen Bundesländern lassen Städte und Landkreise Sozialdaten bei der DDG verarbeiten.

Die Belege werden sortiert den einzelnen Abrechnungsstellen zugeordnet. Danach gehen die Unterlagen zur Erfassung nach Ordnungsnummern. Zentrales Identifikationsmerkmal ist die sogenannte Eingangsbuch-Nummer. Diese Nummer ist einmalig und kann durch niemanden ein zweites Mal vergeben werden. Damit ist die Authentizität jedes Beleges als unverwechselbares Dokument gewährleistet. Nach Erstellung eines Begleitbeleges für interne Zwecke erfolgt in einer anderen Gruppe die inhaltliche Kontrolle, bei der die Unterlagen auf formale Inhalte und sachliche Richtigkeit geprüft werden (Unterschriften, Arztstempel etc.). Ist alles stimmig, wird ein Datensatz erstellt und abgerechnet. Ist dies nicht der Fall, erfolgt eine weitere Prüfung.

11.4.3
Rechtliche Zulässigkeit der Auftragsdatenverarbeitung

Datenverarbeitung im Auftrag ist im Regelfall mit der Kenntnisnahme personenbezogener Daten durch den Auftragnehmer verbunden. Der Gesetzgeber hat das zugelassen, in § 80 Sozialgesetzbuch X (SGB X) jedoch strikte Vorgaben für die Auftragsdatenverarbeitung festgelegt, weil es sich bei den Sozialdaten um besonders sensitive, dem Sozialgeheimnis unterliegende Daten handelt.

§ 80 SGB X

...
(2) Eine Auftragserteilung für die Erhebung, Verarbeitung oder Nutzung von Sozialdaten ist nur zulässig, wenn der Datenschutz beim Auftragnehmer nach der Art der zu erhebenden, zu verarbeitenden oder zu nutzenden Daten den Anforderungen genügt, die für den Auftraggeber gelten. Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Der Auftraggeber ist verpflichtet, erforderlichenfalls Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zu erteilen. Die Auftragserteilung an eine nicht-öffentliche Stelle setzt außerdem voraus, dass der Auftragnehmer dem Auftraggeber schriftlich das Recht eingeräumt hat
1. Auskünfte bei ihm einzuholen,
2. während der Betriebs- oder Geschäftszeiten seine Grundstücke oder Geschäftsräume zu betreten und dort Besichtigungen und Prüfungen vorzunehmen und
3. geschäftliche Unterlagen sowie die gespeicherten Sozialdaten und Datenverarbeitungsprogramme einzusehen,

soweit es im Rahmen des Auftrags für die Überwachung des Datenschutzes erforderlich ist.

…

(5) Die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nicht-öffentliche Stellen ist nur zulässig, wenn
1. beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder
2. die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des gesamten Datenbestandes muss beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist, und die Daten zur weiteren Verarbeitung im Auftrag an nicht-öffentliche Auftragnehmer weitergibt, verbleiben.

Zentraler Punkt meiner Prüfung war die Frage, ob die Verantwortung der Sozialämter für die Verarbeitung der Daten gewahrt bleibt. Eine vollständige Aufgabenübertragung auf den Dienstleister ist nicht zulässig. Inhaltliche Entscheidungen müssen von den Sozialämtern getroffen werden. Der Dienstleister darf nur entsprechend den Weisungen der Sozialämter tätig werden. Andernfalls findet eine Funktionsübertragung statt. Die vereinbarte Zusammenarbeit zwischen den Sozialämtern und der DDG kann als Auftragsdatenverarbeitung i. S. v. § 80 SGB X qualifiziert werden, denn die DDG entscheidet jeden Einzelfall nach den von den Sozialämtern vorgegebenen Kriterien. Sie tritt nach außen als Auftragnehmerin auf und gibt unklare Fälle an die Sozialämter zur weiteren Abklärung zurück.

Allerdings hat die DDG den Auftraggebern angeboten, zusätzlich eine sog. „Ersatzanspruchsverdachtsprüfung“ vorzunehmen. Die Belege sollen manuell auf bestimmte Hinweise hin überprüft werden, wenn ein Fremdverschulden vermutet wird (etwa bei Stichverletzungen, Unfällen). Die DDG informiert den Auftraggeber, der diese zusätzliche Leistung vereinbart hat, über den Verdacht eines Fremdverschuldens und einen eventuellen Ersatzanspruch gegenüber einem Dritten.

Ich halte die Nutzung dieses Moduls in dieser Form nicht mit einer Auftragsdatenverarbeitung im Sinne von § 80 SGB X für vereinbar. Der an die DDG erteilte Auftrag kann aber vertraglich erweitert werden, soweit sichergestellt wird, dass die DDG ausschließlich weisungsgebunden nach den vom Sozialamt vorgegebenen Kriterien Auswertungen vornimmt.

Die weiteren in § 80 SGB X enthaltenen Vorgaben sind ebenfalls eingehalten. Es liegen detaillierte schriftliche Verträge vor, die die Rechte und Pflichten von Auftraggebern und Auftragnehmern eindeutig regeln und den Anforderungen des § 80 SGB X entsprechen. Der überwiegende Teil des Datenbestandes verbleibt bei den Sozialämtern. Dazu zählen die Antragsunterlagen des Betroffenen ebenso wie der Bescheid der Sozialverwaltung über die Gewährung der Hilfeleistung. Zudem werden alle entscheidungsrelevanten Vorgänge in der Sachakte gesammelt. Die übertragenen Aufgaben können von der DDG erheblich kostengünstiger erledigt werden. So hat eine Berechnung der Stadt Kassel für das Jahr 2000 ergeben, dass bei einem Volumen von ca. 9 Millionen Mark und nach Abzug der Kosten für die Dienstleistung der DDG eine Einsparung von etwa 700.000 Mark erreicht wurde.

11.4.4
Datensicherheitsmaßnahmen bei der DDG

Die vom Auftragnehmer getroffenen Datensicherheitsmaßnahmen müssen die Anforderungen des § 78a SGB X erfüllen.

11.4.4.1
Server

Für die Datenverarbeitung im Bereich der Kommunen und Landkreise stehen derzeit drei Novell-Server (Version 3.12 mit Update 2000) zur Verfügung. Die laufende Datenverarbeitung wird durch eine Nachtsicherung ergänzt (Kopie der laufenden Daten). Die Archivierung der Sicherungskopien erfolgt auf Band. Das Archiv wird für die Datenbestandshaltung sowie Statistikauswertungen genutzt (Datenvolumen 80 bis 90 MB monatlich).

11.4.4.2
Arbeitsplätze

Etwa 40 Client-Rechner MS-DOS ohne CD-ROM Laufwerke stehen zur Verfügung, die teilweise keine lokale Festplatte haben. Der Startvorgang führt direkt in das Programm-Menü.

11.4.4.3
Netzwerk

Es wird ein FDDI-Glasfaser-Netzwerk mit IPX/SPX als einziges Transportprotokoll genutzt.

11.4.4.4
Zugriffsregelung

Die erste Zugriffsregelung ist Hardware-bezogen und betrifft den Standort des PC. Den jeweiligen Rechnern steht nur die zur Aufgabenerfüllung notwendige Menü-Auswahl zur Verfügung.

Die zweite Authentifizierung erfolgt über die Benutzerkennung und ein Passwort, das fünf Stellen lang ist. Es wird jedem Mitarbeiter vierteljährlich in einem verschlossenen Briefumschlag zugewiesen.

11.4.4.5
Protokollierung

Die Protokollierung erfolgt serverseitig (Zugriff auf die Datenbestände) und vom EVA-NOVA aus. Die Protokolle umfassen Zugangs-, Authentifizierungs- und Verarbeitungsdaten.

11.4.4.6
Datentransfer

Der Datenaustausch erfolgt über Disketten (unverschlüsselt).

11.4.4.7
Lagerung der Belege

Die bearbeiteten Belege werden von der DDG (aufgrund vertraglicher Regelungen) im Keller eines Gebäudes in der Nähe des Firmensitzes eingelagert. In zwei großen Kellerräumen sind mehrere tausend Aktenordner untergebracht. Dabei stehen

die Ordner, die nach einer datumsorientierten Ablage sortiert sind, blockweise nach einzelnen Auftraggebern. Jeder Ordner ist mit einer Kunden-Nummer, einer laufenden Ordner-Nummer sowie einer Eingangskontroll-Nummer versehen.

Die Ordner sind gegenüber den Unterlagen von Städten und Landkreisen anderer Bundesländer nicht abgeschottet. Allerdings verhindert die blockweise Unterbringung Verwechslungen. Als Option ist vorgesehen, die Belege mit einer digitalen Signatur versehen auf CD-ROM zu speichern. Die DDG führt dies bereits im Auftrag von zwei Krankenkassen durch und hat bei der Entwicklung des Verfahrens sowohl mit dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) als auch mit Tochterunternehmen der Deutschen Telekom (telsec) zusammengearbeitet. Die Kosten sind unwesentlich höher. Ein zusätzlicher Vorteil liegt darin, dass der Auftraggeber selbst seine Belege platzsparend auf CD-Rom archivieren kann.

11.4.4.8
Defizite der Datensicherheitsmaßnahmen

Die Prüfung zeigte einige Schwachpunkte auf, die allerdings von der DDG und in Absprache mit den Kommunen und Landkreisen behoben werden können:

1. Der Datentransfer zwischen Auftraggeber und DDG erfolgt bislang per Diskette. Bei der Art der übermittelten Daten handelt es sich um Sozialdaten nach dem SGB, die in besonderem Maße schutzwürdig sind. Aus diesem Grund müssen die Daten generell verschlüsselt werden. Hierzu kann man sich ohne großen organisatorischen und finanziellen Aufwand öffentlicher Schlüssel wie z. B. PGP bedienen.
   Die DDG hat zugesagt, im Zusammenwirken mit den Auftraggebern so schnell wie möglich eine Verschlüsselung der Daten vorzunehmen und damit den Datentransport noch sicherer zu machen.

2. Die Verwendung fünfstelliger Passworte beim „log-in“ entspricht nicht dem Stand der Technik und den Sicherheitsbedürfnissen. Die DDG hat eine unverzügliche Heraufsetzung der Passwortlänge auf acht Stellen zugesagt und auch umgesetzt.

11.4.5
Abschließende Bewertung

Gegen die Beauftragung privater Dienstleister durch die Sozialämter gibt es aus datenschutzrechtlicher Sicht keine Einwände, sofern die vertraglichen Absicherungen einen hinreichenden Datenschutz garantieren. Dass es dazu sehr genauer vertraglicher Festlegungen bedarf, zeigt der von mir entwickelte Mustervertrag. Dieser kann auf meiner Homepage unter www.datenschutz.hessen.de eingesehen und abgerufen werden (s. auch 28. Tätigkeitsbericht, Ziff. 25.2). Die Städte und Landkreise, die an einer Zusammenarbeit mit der DDG interessiert waren, im Hinblick auf meine Prüfung und die daraus abgeleiteten Ergebnisse jedoch abgewartet haben, sind entsprechend unterrichtet worden.

12. Statistik

Volkszählung: Zensusvorbereitungsgesetz

Mit dem Zensusvorbereitungsgesetz vom 27. Juli 2001 strebt der Bundesgesetzgeber für die nächste Volkszählung einen Methodenwechsel an. Die Daten sollen nicht wie bisher durch eine Befragung aller Einwohner, sondern primär aus vorhandenen Verwaltungsdateien gewonnen werden. Dagegen bestehen keine datenschutzrechtlichen Bedenken.

12.1
Hintergrund

Volkszählungen erfüllen eine Reihe von Funktionen: Sie sind sowohl national als auch international die Grundlage der amtlichen Statistik. Für die politische Planung liefern sie unverzichtbare Basisdaten über Bevölkerung, Erwerbstätigkeit und Wohnsituation. Die aufgrund der Volkszählung festgestellte amtliche Einwohnerzahl ist die maßgebliche Bemessungsgrundlage für den horizontalen und vertikalen Finanzausgleich und für die Einteilung der Wahlkreise. Auch die Europäische Union benötigt für ihre Regional- und Sozialpolitik Basisdaten über die Bevölkerung der Mitgliedstaaten. Deshalb plante sie für das Jahr 2001 einen gemeinschaftsweiten Zensus. Das war der Anstoß, in Deutschland zum ersten Mal nach 1987 wieder eine Volkszählung durchzuführen. Aus Kostengründen und angesichts der Akzeptanzprobleme bei der letzten Volkszählung 1987 soll sie nicht als primärstatistische Vollerhebung durchgeführt werden, stattdessen ist eine registergestützte Datengewinnung beabsichtigt. Da damit Neuland betreten wird, sind zunächst umfangreiche Tests notwendig, für die das Zensusvorbereitungsgesetz die Rechtsgrundlage schafft.

12.2
Testerhebungen

Das Gesetz zur Vorbereitung eines registergestützten Zensus (Zensusvorbereitungsgesetz) ist am 3. August 2001 in Kraft getreten (BGBl. I S. 1882). Zentrale Datenquelle für die demographischen Grunddaten der kommenden Volkszählung sollen die kommunalen Melderegister sein. Deren Verlässlichkeit wird allerdings von der Polizei und Statistikern immer wieder bezweifelt. Durch Stichprobenhebungen bei den Meldebehörden soll deshalb eine Qualitätsprüfung erfolgen. Gleichzeitig sollen Verfahren entwickelt und getestet werden, mit denen die Melderegisterdaten statistisch um Mehrfachfälle, Übererfassungen und Fehlbestände bereinigt werden können. Zur Überprüfung von Mehrfachmeldungen wird zu den Stichtagen 5. Dezember 2001 und 31. März 2002 bei allen Meldebehörden eine Stichprobe durchgeführt. Erfasst werden die Einwohner aller Geburtsjahrgänge, die am 1. Januar, 15. Mai und 1. September geboren sind, sowie alle Einwohner mit unvollständig eingetragenem Geburtsdatum, insgesamt etwa 1,5 % der Bevölkerung. Erhebungsmerkmale sind Geburtsmonat und -jahr, Geschlecht, Staatsangehörigkeit, Geburtsstaat bei im Ausland Geborenen, Familienstand, Wohnort, Status der Wohnung (alleinige Wohnung, Haupt- oder Nebenwohnung). Darüber hinaus wird eine Vielzahl von personenbezogenen Hilfsmerkmalen, das sind Merkmale, die der technischen Durchführung dienen, erhoben.

Die von der künftigen Volkszählung erwarteten Informationen über die Erwerbstätigkeit der Bevölkerung sollen aus Dateien der Bundesanstalt für Arbeit gewonnen werden. Getestet werden soll deshalb die Qualität der Daten aus der Datei für sozialversicherungspflichtig Beschäftigte, der Arbeitslosendatei und der Datei für Teilnehmer an Maßnahmen zur beruflichen Weiterbildung. Betroffen sind Personen aus maximal 230 ausgewählten Gemeinden und 16.000 Gebäuden.

Der dritte Teil des Erhebungsprogramms der Volkszählung betrifft Daten zur Wohnsituation. Hier ist eine registergestützte Erhebung nicht möglich, denn für Gebäude und Wohnungen gibt es in Deutschland keine Register, die kleinräumige Bestands- und Strukturdaten enthalten. Bei früheren Volkszählungen wurden daher alle Gebäudeeigentümer und Wohnungsinhaber befragt. Künftig sollen Gebäudedaten und Wohnungsgrunddaten nur bei den Gebäudeeigentümern erfragt werden. Eine postalische Testerhebung zum Stichtag 5. Dezember 2001 bei den Eigentümern von maximal 16.000 ausgewählten Gebäuden in 230 Gemeinden soll Aufschlüsse über Verfahrenstechniken geben und zeigen, ob die Befragung der Eigentümer zu anderen Ergebnissen führt als die bislang übliche Befragung der Wohnungsinhaber.

12.3
Zusammenführung der Daten

Die aus den Melderegistern, den Dateien der Bundesanstalt für Arbeit und aus der Gebäude- und Wohnungserhebung gewonnenen Daten werden einzelpersonenbezogen und haushaltsbezogen zusammengeführt. Bei den früheren Volkszählungen war dies nicht erforderlich, denn alle Daten wurden im Haushaltszusammenhang direkt bei den Personen und Haushalten erhoben. Die Zusammenführung der Daten aus verschiedenen Quellen widerspricht nicht den Grundsätzen, die das Bundesverfassungsgericht in seinem Volkszählungsurteil 1983 formuliert hat. Das Gericht sah zwar in der Übernahme sämtlicher Daten aus bereits vorhandenen Dateien der Verwaltung eine unzulässige Alternative zur Totalerhebung. Die Gründe, die es dafür anführte, treffen auf die geplante registergestützte Volkzählung allerdings nicht zu. Das Gericht ging davon aus, dass die Zusammenführung der Daten aus verschiedenen Registern die Schaffung eines einheitlichen, für alle Register und Dateien geltenden Personenkennzeichens oder eines Substituts erforderlich mache. Es sah darin einen entscheidenden Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren (BVerfGE 65, 1, 56 f.). Das Zensusvorbereitungsgesetz sieht kein Personenkennzeichen vor. Es gibt auch kein Substitut, das die Verknüpfung der Daten aus allen Registern und Dateien ermöglichen würde. Es werden lediglich Daten aus den Melderegistern und drei Dateien der Bundesanstalt für Arbeit mittels der im Gesetz festgelegten Hilfsmerkmale zusammengeführt. Außerdem ist der Datensatz gegenüber der vorangegangenen Volkszählung erheblich, um ein Drittel, reduziert worden. Man wird kaum behaupten können, dass damit der Bürger in seiner ganzen Persönlichkeit registriert wird.

12.4
Hilfsmerkmale

Gegenüber einem herkömmlichen Zensus ist die Zahl der Hilfsmerkmale erheblich angestiegen. Weil Erhebungsmerkmale aus unterschiedlichen Registern und Dateien zusammengeführt werden müssen, ist dies nicht verwunderlich. Soweit möglicherweise mehr Hilfsmerkmale erhoben werden, als für die künftige Volkszählung notwendig sein werden, ist dies akzeptabel, denn es handelt sich um ein Testprogramm, das gerade zeigen soll, welche Hilfsmerkmale künftig benötigt werden.

12.5
Statistikgeheimnis

Man mag darüber streiten, ob es besser gewesen wäre, im Zensusvorbereitungsgesetz auf das Statistikgeheimnis zu verweisen. Es nicht ganz eindeutig, ob es sich bei den Testerhebungen um Bundesstatistiken handelt und damit die erhobenen Da-

ten dem Statistikgeheimnis nach § 16 Bundesstatistikgesetz (BStatG) unterliegen. Immerhin findet sich in der Begründung zum Gesetzentwurf eine Klarstellung: Die Bundesregierung weist dort ausdrücklich darauf hin, dass alle für die Testuntersuchungen erhobenen Daten unter die statistische Geheimhaltung fallen (BTDrucks. 14/5736, S. 12).

§ 16 Abs. 1 BStatG

Einzelangaben über persönliche und sachliche Verhältnisse, die für eine Bundesstatistik gemacht werden, sind von den Amtsträgern und für den öffentlichen Dienst besonders Verpflichteten, die mit der Durchführung von Bundesstatistiken betraut sind, geheim zu halten, soweit durch besondere Rechtsvorschriften nichts anderes bestimmt ist. ...

Die Daten werden ausschließlich in besonders abgeschotteten Bereichen der Statistikämter der Länder und des Statistischen Bundesamtes verarbeitet und sobald wie möglich faktisch anonymisiert. Überprüfungen und Berichtigungen der Daten im Rahmen der methodischen Untersuchungen erfolgen ausschließlich im Bereich der Statistikämter, die registerführenden Verwaltungsbehörden erhalten keine Rückmeldung.

13. Telekommunikation

13.1
Telekommunikations-Überwachungsverordnung

Zu dem Ende Januar 2001 vom Bundesministerium für Wirtschaft und Technologie vorgelegten Entwurf einer Telekommunikations-Überwachungsverordnung (TKÜV) hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die unter Ziff. 27.11 dieses Berichts abgedruckte Entschließung gefasst. Darin wurde besonders kritisiert, dass auch Anbieter von Internetdiensten verpflichtet sein sollten, technische Einrichtungen zur Umsetzung von Überwachungsmaßnahmen vorzuhalten, sodass es (technisch) möglich gewesen wäre, den gesamten Internetverkehr zu überwachen.

Inzwischen hat das Bundesministerium für Wirtschaft und Technologie einen überarbeiteten Entwurf vorgelegt (Stand 6. September 2001). Neben Betreibern von „nichtöffentlichen" Telekommunikationsanlagen werden danach auch Internet-Access-Provider von der Verpflichtung zur Vorhaltung technischer Einrichtungen zur Überwachung der Telekommunikation freigestellt. Verpflichtet sollen nur noch Zugangsanbieter sein, die einem Teilnehmer unter Umgehung der Vermittlungsfunktionen des Zugangsnetzes den unmittelbaren Zugang zum Internet ermöglichen, wie z. B. mit dem xDSL-Angebot. Unklar bleibt jedoch weiterhin, ob für die Überwachung von Mobilfunkteilnehmern statt der Rufnummer die Gerätekennung IMEI (International Mobil Equipment Identity) ausreicht (bejahend der Bundesgerichtshof (BGH) in einem Beschluss vom 7. September 1998 - 2 BGs 211/98). Die Überwachungsmöglichkeit soll dagegen auch darauf erstreckt werden, in welcher Funkzelle sich das Mobiltelefon befindet, und zwar unabhängig davon, ob telefoniert wird oder nicht (entsprechend einem Beschluss des BGH vom 21. Februar 2001 - 2 BGs 42/2001).

13.2
Einsatz des sog. IMSI-Catchers durch Strafverfolgungsbehörden und Polizei

Für den Eingriff in das Fernmeldegeheimnis durch den Einsatz des sog. IMSI-Catchers zur Ermittlung von Handy-Kennungen durch die Strafverfolgungsbehörden fehlt es derzeit an einer Rechtsgrundlage. Insbesondere für die Berufung auf den rechtfertigenden Notstand gemäß § 34 Strafgesetzbuch als Grundlage polizeilichen Handelns ist kein Raum.

Beim Gebrauch von Handys fallen Informationen an, die bei der Verwendung von „normalen" Telefonen nicht entstehen. Dazu gehört unter anderem die sog. Aktivmeldung, mit der sich jedes Handy bei einem Provider als empfangsbereit in einer bestimmten Funkzelle anmeldet. Anhand der Aktivmeldung lässt sich der Aufenthaltsort des Gerätes und damit auch seines Nutzers bestimmen. Diese Informationen können für die Strafverfolgungsbehörden und für die Polizei von Interesse sein. Die rechtlichen Rahmenbedingungen für den Einsatz habe ich mit verschiedenen Stellen diskutiert.

13.2.1
Einsatz zu repressiven Zwecken

Für die Strafverfolgungsbehörden können die Aktivmeldungen z. B. bei Fahndungen hilfreich sein (s.a. 24. Tätigkeitsbericht, Ziff. 12.1), ferner auch bei geplanten Überwachungen des Telefonverkehrs: Soll das Telefon eines Verdächtigen abgehört werden, so schreibt die Strafprozessordnung u.a. vor, dass die richterliche Anordnung die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten muss (§ 100b Abs. 2 Strafprozessordnung [StPO]).

§ 100b Abs. 2 StPO

Die Anordnung ergeht schriftlich. Sie muss Namen und Anschrift des Betroffenen, gegen den sie sich richtet, und die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten. In ihr sind Art, Umfang und Dauer der

Maßnahmen zu bestimmen. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die in § 100a bezeichneten Voraussetzungen fortbestehen.

Bei „normalen“ Telefonen ist die Zuordnung des Anschlusses zu einem bestimmten räumlichen Standort leicht zu ermitteln. Dies gilt zwar grundsätzlich auch bei der Verwendung von Handys. Beschuldigten ist es jedoch leicht möglich, abwechselnd verschiedene Handys oder solche, die eine andere Person beschafft hat, zu verwenden. Häufig ist es deshalb den Strafverfolgungsbehörden nicht möglich, die tatsächlich benötigte Anschlusskennung zu bezeichnen. Wenn die Anschlusskennung nicht bekannt ist, kann keine richterliche Anordnung erwirkt werden.

In diesen Fällen, kann der sog. IMSI-Catcher die notwendigen Informationen liefern. Das Gerät simuliert eine Funkzelle mit starker Feldstärke, so dass sich alle Handys in einem bestimmten Umkreis nicht bei der echten Funkzelle, sondern beim IMSI-Catcher melden. Die so „eingefangenen“ Telefon- und Gerätenummern können dann Basis für die entsprechenden gerichtlichen Anordnungen sein.

Unabhängig von der Frage des Umfangs des Eingriffs in das Telekommunikationsgeheimnis ist für den Einsatz des Geräts als eines telekommunikationsrechtlichen Betriebes eine ergänzende Genehmigung der Regulierungsbehörde für Telekommunikation und Post erforderlich. Eine solche liegt derzeit nicht vor.

Nach Auskunft des Hessischen Landeskriminalamts gab es in Hessen Fälle, in denen jeweils für ein konkretes Ermittlungsverfahren in Absprache mit der jeweils zuständigen Staatsanwaltschaft der sog. IMSI-Catcher eingesetzt worden ist. Zum rechtlichen Hintergrund des Einsatzes dieser Ermittlungsmethode hat das Landeskriminalamt Folgendes ausgeführt: Entweder habe die Staatsanwaltschaft die Anordnung gegengezeichnet und dabei ausdrücklich auf eine Strafverfolgung der Beamten verzichtet sowie den Einsatz des IMSI-Catchers befürwortet oder sie habe dem Einsatz vorab zugestimmt und ihren Verzicht auf eine Verfolgung der beteiligten Beamten ausgesprochen. Das um Zustimmung ersuchte Innenministerium habe den Einsatz mit dem Hinweis genehmigt, dass es sich bei dem IMSI-Catcher um ein „technisches Mittel“ i.S.d. § 15 Hessisches Gesetz über die öffentliche Sicherung und Ordnung (HSOG) handele, mit dem nach der Änderung des § 10 HSOG in Art. 15 Grundgesetz (GG) eingegriffen werden dürfe. Wegen der fehlenden fernmelderechtlichen Genehmigung sei ein Rückgriff auf den in § 34 Strafgesetzbuch (StGB) geregelten rechtfertigenden Notstand gleichwohl erforderlich.

§ 34 StGB

Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden.

Aufgrund der besonderen Umstände dieser Ermittlungsverfahren habe ich den konkreten Einsatz nicht beanstandet. Es kommt aber für die Rechtmäßigkeit einer Maßnahme nicht darauf an, dass der einzelne Beamte sich subjektiv nicht strafbar macht. Ich habe in der dazu abgegebenen Stellungnahme hervorgehoben, dass jeder Eingriff in das Telekommunikationsgeheimnis auf einer tragfähigen rechtsstaatlichen Basis beruhen muss.
Der Einsatz des IMSI-Catchers ist nach meiner Ansicht für die repressive Tätigkeit der Polizei nicht durch die Berufung auf die Notstandsregelung des § 34 StGB zu legitimieren, da er keine Befugnisnorm darstellt. Für die Frage, ob die Polizei eine Ermittlungshandlung rechtmäßig vornehmen kann, ist entscheidend, ob sie im Rahmen ihrer gesetzlichen Befugnisse handelt.

13.2.2
Einsatz zu präventiven Zwecken

Soweit der Einsatz des IMSI-Catchers im präventiven Bereich erfolgt, kommt grundsätzlich § 15 HSOG als Rechtsgrundlage in Betracht.

§ 15 HSOG

(1) Im Sinne dieser Bestimmung ist
... Einsatz technischer Mittel ihre für die betroffene Person nicht erkennbare Anwendung, insbesondere zur Anfertigung von Bildaufnahmen oder -aufzeichnungen sowie zum Abhören oder Aufzeichnen des gesprochenen Wortes.
...
(5) Maßnahmen nach Abs. 4 sowie das Abhören oder Aufzeichnen des nicht öffentlich gesprochenen Wortes durch den Einsatz technischer Mittel dürfen außer bei Gefahr im Verzug nur durch richterliche Anordnung getroffen werden. ... Die Anordnung ergeht schriftlich. Sie muss die Personen, gegen die sich die Maßnahmen richten sollen, so genau bezeichnen, wie dies nach den zur Zeit der Anordnung vorhandenen Erkenntnissen möglich ist. Art und Dauer der Maßnahmen sind festzulegen. ...
Der IMSI-Catcher ist ein technisches Mittel i. S. d. § 15 Abs. 1 Ziff. 2 HSOG. Sein Einsatz bedarf zunächst auch keiner richterlichen Anordnung, da § 15 Abs. 5 HSOG dies nur verlangt, soweit das nicht öffentlich gesprochene Wort abgehört oder aufgezeichnet wird. Dies

erfolgt zumindest durch den derzeit eingesetzten IMSI-Catcher nicht. Anders als in § 100b Abs. 2 S. 2 StPO vorgesehen muss eine richterliche Anordnung nach § 15 Abs. 5 HSOG die Anschlusskennung nicht zwingend benennen.
Ein Problem ergibt sich jedoch daraus, dass vorab nicht bekannt ist, ob sich die vom Einsatz des IMSI-Catchers betroffenen Handys innerhalb einer Wohnung befinden. Es wird daher generell davon ausgegangen werden müssen, dass Daten aus Wohnungen (mit)erhoben werden. Nach § 15 Abs. 4 und 5 HSOG dürfen Polizeibehörden Daten aus Wohnungen nur erheben, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist und eine richterliche Anordnung vorliegt.
Nötig ist eine verfassungskonforme Gesamtregelung zum Einsatz des IMSI-Catchers im präventiven Bereich ebenso wie die Ergänzung der Strafprozessordnung, die inzwischen in Angriff genommen worden ist. Die gleichen Anforderungen muss auch die geplante bereichsspezifische Neuregelung in § 5 Abs. 10 LfVG erfüllen.

14. Entwicklungen im Bereich der Technik

14.1
Sicherheit von Anmeldeprozeduren an IT-Systemen

Anmeldeprozeduren an IT-Systeme sind von entscheidender Bedeutung für die IT-Sicherheit. Nachdem in der Vergangenheit fast ausschließlich Passwörter genutzt wurden, werden immer häufiger biometrische Verfahren und Chipkarten eingesetzt. Jede technische Lösung hat Schwachstellen. Die höchste Sicherheit kann derzeit mit dem Einsatz von Chipkarten in Kombination mit Passwörtern oder biometrischen Merkmalen erreicht werden.

Wenn ein Benutzer mit einem IT-System arbeiten will, muss er eine Anmeldeprozedur durchlaufen. Dabei wird eine Identifikation und eine Authentisierung verlangt.

Identifikation

Der Benutzer gibt eine Identität an, unter der er arbeiten will. Hierbei handelt es sich um eine Benutzerkennung, die dem System bekannt sein muss.

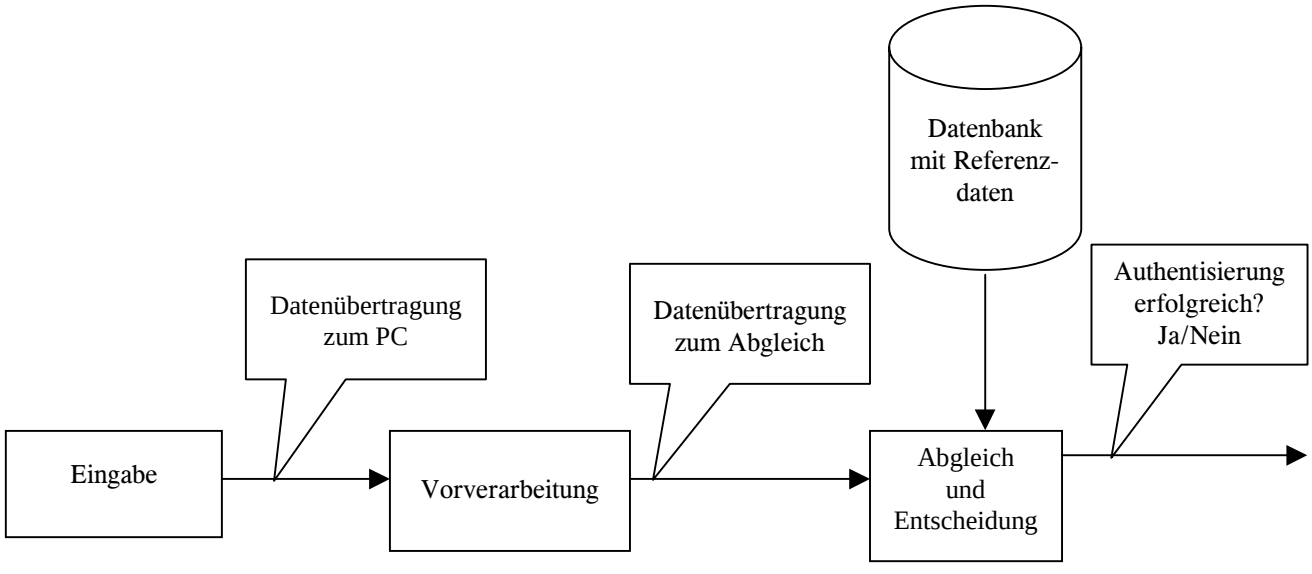
Authentisierung

Zu der Benutzerkennung (Identifizierung) muss bewiesen werden, dass tatsächlich der richtige Mensch das IT-System benutzen will. Eine Authentisierung kann durch
- Wissen (z. B. Passwort)
- Besitz (z. B. Chipkarte) oder
- Biometrische Merkmale (Iris, Fingerabdruck etc.)

erfolgen.

Für die Sicherheit von IT-Systemen ist die Anmeldeprozedur ein zentraler, vielleicht sogar der wichtigste Baustein. Wesentliche Sicherheitsfunktionen knüpfen an die Benutzerkennung an. Dies gilt beispielsweise für die Prüfung des Rechts, auf bestimmte Dateien zugreifen zu dürfen oder bestimmte Anwendungen ausführen zu können. Auch die Protokollierung von durchgeführten Aktionen bezieht sich im Regelfall auf Benutzerkennungen. Damit die IT-Sicherheit das vom Datenverarbeiter gewünschte Niveau erreicht, muss die Qualität der Anmeldeprozedur, und dabei besonders die der Authentisierung, den von ihm gestellten Anforderungen genügen.

Die technischen Abläufe bei einer Authentisierung lassen sich grob mit folgendem Schema beschreiben.



Das Eingabegerät kann beispielsweise ein biometrischer Sensor, eine Tastatur für die Passworteingabe oder ein Chipkartenlesegerät sein. Die Daten werden zur weiteren Verarbeitung üblicherweise an einen PC übertragen. Von dort erfolgt in Rechnernetzen eine Datenübertragung der für den Abgleich benötigten Daten an einen Server, die Vergleichseinheit, auf dem der eigentliche Abgleich mit den Referenzdaten stattfindet. Die Vorverarbeitung und der Abgleich können auch auf demselben Rechner erfolgen, wie es bei Einzelplatzgeräten der Fall ist. Nach dem Vergleich fällt die Entscheidung, ob die Authentisierung erfolgreich war.
Unabhängig von der eingesetzten Technik zur Authentisierung müssen gegen typische Angriffe Maßnahmen ergriffen werden. Beispiele solcher Angriffe und Gegenmaßnahmen sind:

- **Manipulationen der Datenbank**
  Es darf nicht möglich sein, Referenzmuster auszutauschen, zu verändern oder zu entziffern. Ausnahmen kann es nur geben, wenn es für die Funktionsfähigkeit der Anmel-deprozedur (Benutzerkontrolle i. S. v. § 10 Abs. 2 Nr. 2 HDSG) unumgänglich ist.

- **Replay-Angriffe**
  Es muss verhindert werden, dass Daten während der Übertragung durch Unberechtigte aufgezeichnet werden, um damit später Anmeldungen zu simulieren.
  Eine verschlüsselte Übertragung der Passwörter zwischen PC und Server ist in neueren Betriebssystemen vorgesehen und daher Stand der Technik. In besonders gesicherten Systemen, beispielsweise Geldausgabeautomaten, werden die Daten sogar schon bei der Eingabe verschlüsselt. Ein erneutes Einspielen der verschlüsselten Daten kann jedoch nur wirksam verhindert werden, wenn sich diese bei jeder Anmeldung unterscheiden. Das leisten beispielsweise Challenge-Response-Verfahren. Bei biometrischen Verfahren sind zu 100 % identische Daten ein Hinweis auf einen Angriff, da es keine vollständige Übereinstimmung von Merkmalen bei der Erfassung gibt.

Als Schutzmaßnahmen werden sowohl bei der Speicherung als auch bei der Übertragung kryptographische Verfahren eingesetzt. Deren Güte ist ebenfalls entscheidend für ein gutes Gesamtsystem (vgl. 23. Tätigkeitsbericht, Ziff. 27)

14.1.1
Passwort

Passwörter sind die derzeit am weitesten verbreitete Technik für eine Authentisierung. Sie haben jedoch einige Schwächen. Als größte Herausforderung zeichnet sich die „Passwortinflation“ ab. Es gibt Untersuchungen, wonach in zehn Jahren jede Person sich über 100 Passwörter/PINs merken muss, wenn sich die Entwicklung wie bisher fortsetzt. Deshalb wurden sog. Single-Sign-On-Systeme entwickelt, bei denen man sich nur einmal anmeldet und alle weiteren Anmeldungen automatisiert im Hintergrund ablaufen. Bei diesen Systemen gibt es dann neue Risiken, denen durch entsprechende Maßnahmen begegnet werden muss.

Es ist bekannt, dass Passwörter eine gewisse Komplexität haben müssen, damit sie ihre Funktion ausüben können (zu Details siehe Ziff. 14.2). Sie sollten z. B. mindestens sechs, besser acht bis zwölf Stellen lang sein, aus Buchstaben, Ziffern und Sonderzeichen bestehen, nicht in Wörterbüchern vorkommen und sich möglichst nicht wiederholen. Sie sollten nicht notiert werden. Hier beginnt nun das Problem. In der Regel muss sich jeder Benutzer mehrere Passwörter merken. Sind die Passwörter aber nicht einfach, so führt kaum ein Weg daran vorbei, sie sich zu notieren. Bei Prüfungen konnte ich daher oft mit einem Blick auf Zettel am Bildschirm, in der rechten Schreibtischschublade oder unter der Schreibunterlage das Passwort erfahren. Erschwerend kommt hinzu, dass der Benutzer oft nicht erkennt, dass ein Unbefugter sein Passwort ausspioniert hat; daher sollten Passwörter regelmäßig in nicht zu großen Abständen (alle 30 bis 90 Tage) gewechselt werden.

Es gibt eine Reihe von Möglichkeiten, Passwörter auszuforschen. Eine beliebte Vorgehensweise besteht darin, den Benutzer anzurufen und sich als Mitarbeiter der IT-Abteilung, oder, wenn es beispielsweise um die PIN einer Geldkarte geht, Mitarbeiter der Bank auszugeben. Nach einer kurzen Einleitung folgt dann die Behauptung, man benötige das Passwort bzw. die PIN, um einen Fehler zu beheben.
Es gibt jedoch keinen Grund, einer anderen Person das eigene Passwort zu nennen. Mit dem Passwort kann diese Person eine fremde Identität vortäuschen und damit Geld abheben, Dokumente ändern und löschen.

Neben den Angriffen, die auf zwischenmenschlichen Kontakten aufbauen, gibt es auch Angriffe mit technischen Mitteln. Über zwei Varianten berichte ich unter Ziff. 14.2 und 14.3. Dabei ist das Aufzeichnen der Tastatureingaben deshalb besonders kritisch, weil es ohne großen technischen Aufwand und ohne Zugriffsrechte auf dem Rechner stattfinden kann.

Aus den beschriebenen Schwächen darf aber nicht geschlossen werden, dass Passwörter unbrauchbar sind. Wenn die Benutzer gute Passwörter wählen und die Systeme gut administriert sind, ergibt sich ein für viele Anwendungsfälle ausreichendes Sicherheitsniveau. Besteht jedoch ein höherer Sicherheitsbedarf , so muss die Anmeldung um weitere Sicherheitsmechanismen ergänzt werden.

14.1.2
Biometrie

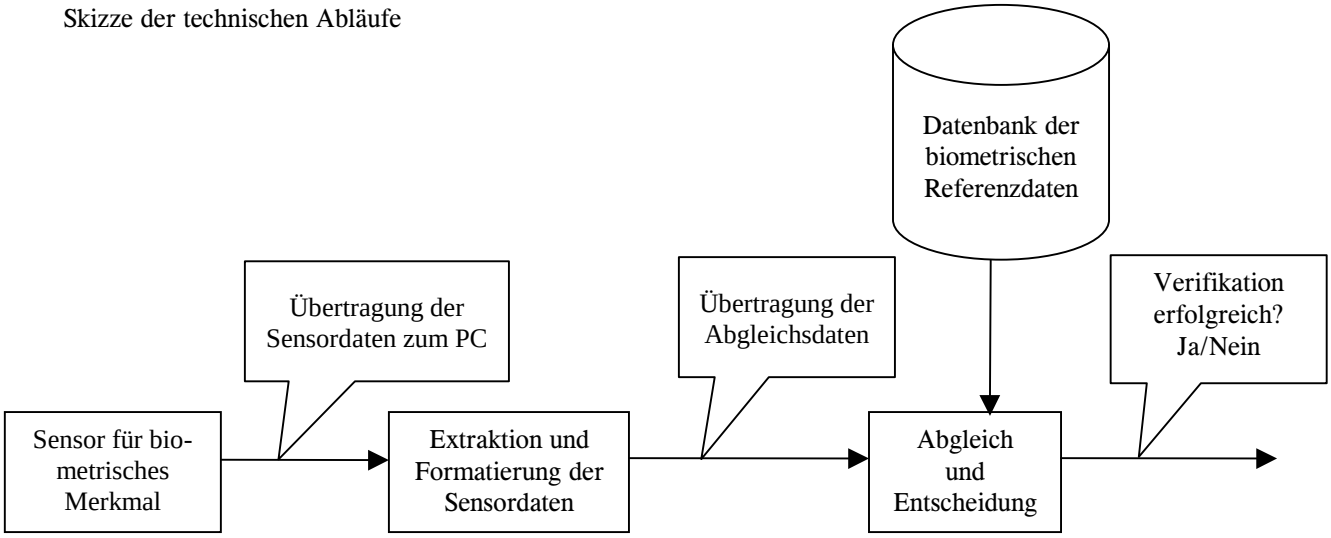
Als eine weitere Möglichkeit, Anmeldeprozeduren am System benutzerfreundlich und sicher zu gestalten, ist die Biometrie inzwischen herangereift. Es sind aber noch nicht alle Probleme befriedigend gelöst, so dass die Biometrie insbesondere bei höheren Sicherheitsanforderungen derzeit noch als eine Ergänzung zu den anderen Techniken zu sehen ist. Die Entwicklung schreitet schnell fort, weshalb sich die Situation bald ändern kann.

Biometrische Merkmale charakterisieren den Menschen als Individuum. Beispiele sind:

- Gesicht
- Stimme
- Fingerabdruck
- Iris
- Retina
- Handgeometrie
- Unterschriftsdynamik
- Dynamik der Tastatureingabe

Biometrische Merkmale sind prinzipiell gut geeignet, einen Menschen zu erkennen. Vorteile biometrischer Verfahren gegenüber Passwörtern liegen vor allem in der Benutzerfreundlichkeit. Man muss sich nicht viele Passwörter merken, sondern hat sein Merkmal immer „dabei“ und kann es auch nicht vergessen.

Skizze der technischen Abläufe



Der technische Ablauf ist wie folgt:

- Ein Sensor erfasst ein biometrisches Merkmal. Beispielsweise nimmt eine Kamera das Gesicht auf.
- Die Daten werden zur Verarbeitungseinheit übertragen.
- Die Verarbeitungseinheit reduziert bzw. extrahiert die Daten und formatiert sie in den für den Vergleich benötigten „Merkmalsvektor“
- Der Merkmalsvektor wird an die Vergleichseinheit übertragen, die den Abgleich vornimmt.
- Der Abgleich wird vorgenommen. Die Referenzdaten können zentral oder dezentral, beispielsweise in einer Chipkarte gespeichert sein. Die Übertragung zwischen Referenzdatenbank und Vergleichseinheit sollte verschlüsselt erfolgen.
- Das Ergebnis wird an das Betriebssystem übertragen.

Zu unterscheiden ist zwischen einer Identifizierung, d.h. Herr Meier befindet sich in der Gruppe, und einer Verifikation, d.h. der Geprüfte ist Herr Meier. Bei der technischen Realisierung von Anmeldeprozeduren wird üblicherweise eine Verifikation verlangt: Man gibt eine Benutzerkennung ein und das System muss erkennen, ob sich tatsächlich diese Person anmelden will. Wesentliches Kriterium für die technische Ausgestaltung ist die zuverlässige Erkennung der als berechtigt anerkannten (eingelernten) Benutzer. Die Rate fälschlich zurückgewiesener Benutzer (FRR, **F**alse **R**ejection **R**ate) muss niedrig sein, damit das System als praktikabel akzeptiert wird. Darüber hinaus muss die Überwindungssicherheit, d.h. die Abweisung von nicht bekannten Personen und Fälschungen hoch sein. (Die Überwindungssicherheit wird teilweise mit der Rate der fälschlicherweise akzeptierten Personen (FAR, **F**alse **A**cceptance **R**ate) gleichgesetzt. Nach einer anderen Interpretation gibt es die FAR nur, wenn mit biometrischen Verfahren eine Identifikation stattfindet.) Leider ist es so, dass eine hohe Überwindungssicherheit eine hohe Zahl fälschlicherweise zurückgewiesener Benutzer verursacht, während eine niedrige FRR eine geringere Überwindungssicherheit mit sich bringt. Hier gilt es, die für das jeweilige System optimale Einstellung zu finden.

Technische Maßnahmen gegen Überwindungsversuche am Sensor müssen die für biometrische Merkmale spezifischen Rahmenbedingungen berücksichtigen. Man muss sich vor Augen halten, dass die meisten Merkmale nicht geheim zu halten sind. Sie sind quasi öffentlich. Mit wenig Aufwand können Fingerabdrücke besorgt werden oder Fotos geschossen werden.

Die Prüfung eines Passwortes setzt immer eine 100 %ige Übereinstimmung des eingegebenen Passwortes mit dem gespeicherten Passwort voraus. Beim Ablesen von biometrischen Merkmalen gibt es demgegenüber keine völlige Übereinstimmung mit den Referenzdaten, sondern nur eine Ähnlichkeit. Es muss festgelegt werden, wann sich die Muster so sehr ähneln, dass sie als zu einer Person gehörig angesehen werden.

Biometrische Merkmale sind auch nicht bei jeder Person gleich gut ausgeprägt. Es gibt immer eine Anzahl Personen, bei denen das Merkmal nicht geprüft werden kann. Die Prozentzahlen, die genannt werden, schwanken je nach Merkmal zwischen 1 % und 5 %. Außerdem kann sich ein biometrisches Merkmal auch durch eine Krankheit (Entzündung des Auges), einen Unfall (Schnitt in der Fingerkuppe) oder aus anderen Gründen (Veränderung des Fingerabdrucks durch ungewohnte körperliche Arbeit) für eine kurze Zeit oder auf Dauer ändern. Um mit solchen Fällen umgehen zu können, müssen die Systeme alternative Möglichkeiten zur Anmeldung vorsehen.

Biometrische Verfahren sollten evaluiert und zertifiziert werden, damit ihre Qualität eingeschätzt werden kann. Hierzu haben das Bundesamt für Sicherheit in der Informationstechnik (BSI) und andere Stellen bereits Vorbereitungen getroffen.

14.1.3
Chipkarten (Smartcards)

Chipkarten ermöglichen qualitativ hochwertige Anmeldeprozeduren. Ihr Einsatz erfordert insbesondere organisatorische Maßnahmen, die regeln, durch wen und wie die Karten ausgegeben, gesperrt und eingezogen werden.

Gegenüber biometrischen Merkmalen haben Chipkarten den Nachteil, dass man sie vergessen oder verlieren kann. Um Missbräuche zu vermeiden, müssen Chipkarten unbedingt durch Eingabe eines Passworts/einer PIN oder durch Prüfung eines biometrischen Merkmals freigeschaltet werden. Eine potentielle Schwachstelle liegt in der Übertragung der PIN von der Tastatur an die Chipkarte, da der Übertragungsweg schwer zu schützen ist. Hier können Kartenleser mit integrierter Zahlentastatur helfen. Es gibt mittlerweile auch Chipkarten mit integriertem Fingerabdrucksensor, die den Fingerabdruck erfassen und auf der Karte prüfen sollen.

Im Vergleich zum Passwort hat die Chipkarte beim Diebstahl den Vorteil, dass der Benutzer den Verlust im Regelfall schnell bemerkt. Die Karte kann dann umgehend gesperrt und somit die Sicherheitslücken schnell geschlossen werden.

Die Stärke von Chipkarten liegt auch in der Möglichkeit, Datenübertragungen bei der Anmeldeprozedur abzusichern. So können Challenge-Response-Verfahren genutzt werden, bei denen alle Daten verschlüsselt übertragen werden und Replay-Attacken unmöglich sind.

Die Sicherheit steht und fällt damit, dass vertrauenswürdige Institutionen die Karten produzieren und personalisieren. Es darf nicht geschehen, dass Duplikate von Karten existieren.

14.1.4
Fazit

Passwörter gehören noch nicht zum alten Eisen, aber sie sind in Bereichen mit einem hohen Sicherheitsbedarf allein nicht ausreichend. Anmeldeprozeduren auf Basis biometrischer Merkmale sind in vielen Fällen benutzerfreundlicher als Passwörter, aber ihre Sicherheit ist nicht einfach einzuschätzen. Die höchste Sicherheit versprechen Lösungen, die Chipkarten nutzen. Diese sind dann aber mit Passwörtern oder Biometrie gekoppelt.

Jede technische Lösung der Anmeldeprozeduren muss permanent auf Schwachstellen kontrolliert werden und ggf. sind Änderungen an der Anwendung vorzunehmen.

14.2
Sicherheit von Windows NT Passwörtern

Die mit dem Service Pack 3 erweiterte Passwortsicherheit erhöht deren Zugriffsschutz erheblich. Neueste Entwicklungen von Programmen auf diesem Sektor lassen allerdings wieder Lücken in der Systemsicherheit erkennen. Daher ist - immer noch und immer wieder - die richtige Auswahl eines Passwortes von essenzieller Bedeutung.
Im Rahmen der präventiven IT-Sicherheitsprüfungen sind die Unsicherheiten der Passwortlegitimation untersucht worden.

14.2.1
Neue Struktur mit Problemen

Mit Einführung des Betriebssystems Windows NT änderte sich die gesamte Windows-Passwortstruktur. Die Passwörter werden nicht mehr in allgemein zugänglichen Dateien (mit der Endung „pwl“ für „password list“) abgelegt, sondern in der Systemregistrierung als sog. „Hashes“.

Hash

eindeutige Umwandlung einer Zeichenfolge, hier in Hexadezimalwerte

Sie sind dort grundsätzlich nur dem System zugänglich. Administratoren können sich jedoch über Berechtigungsänderungen mit dem Registrierungseditor (32bit-Version REGEDT32) Zugang zu den dort abgelegten Daten verschaffen.
Zudem verursacht die in der Anfangszeit von NT erforderliche und von Microsoft daher standardmäßig vorgesehene Kompatibilität zum LANManager-Protokoll eine erhebliche Schwäche des Systems. Das LANManager-Protokoll kann nur maximal sieben Zeichen als Passwort verarbeiten. Zudem werden alle Buchstaben in Großbuchstaben umgewandelt, d.h. der zur Verfügung stehende Zeichensatz wird erheblich reduziert. Das (maximal 14 Zeichen lange) NT-Passwort wird außerdem „LANManager-kompatibel“ gespeichert, d.h. in zwei Gruppen zu je sieben Zeichen geteilt und jeweils in der NT- **und** LAN-Manager-Form abgelegt.
Diese Verfahrensweise schwächt die Passwortsicherheit weiter, da der zweite Teil eines NT-Passwortes in dieser Form eine sehr kurze Zeichenkette (NT-Passwortlänge - 7) darstellt, die gegen Attacken noch anfälliger ist. Dieser zweite Teil des Passwortes wird im Zuge von Angriffen meist als erstes entschlüsselt (s. Abbildung 2 weiter unten bei „user2“ und „user4“).

14.2.2
Der Anfang

Diese Schwächen ausnutzend tauchten 1995/96 die ersten Werkzeuge auf, um die von Microsoft bis dahin als sicher dargestellten Passwörter anzugreifen.

Die Zugänge zu den Passwörtern waren (und sind !):

- der direkte Zugriff auf die SAM-Datenbank (Security Account Manager) in der Systemregistrierung - mit Administratorprivilegien,
- Netzwerksniffer, die in der Lage sind, SMB-Pakete (Server Message Block), die die Windows-Anmeldeinformationen enthalten, aus dem Netzverkehr zu filtern.
  Sie setzen keine Administratorrechte voraus, sondern nur eine Netzwerkkarte, die den „promiscuous mode“ beherrscht und Pakete ans System weiterleitet, die nicht für den Rechner selbst vorgesehen sind, und
- Programme, die in der Lage sind, SAM-Informationen auszulesen.

Der Angriff auf Passworte erfolgt über:

- Wörterbücher, d.h. Vergleich der Passworte mit gängigen Wörterlisten
- BruteForce-Angriffe, d.h. Ausprobieren aller möglichen Zeichenkombinationen in verschiedenen Stufen (nur Buchstaben bis zum kompletten Tastaturzeichensatz)

Ein Beispiel einer (mit Administratorrechten) extrahierten Benutzerdatenbank stellt sich etwa wie folgt dar:

User Name	LanMan Pas...	<8	NT Password	LanMan Hash
Administrator				A16BA9F67F15BF4C8B4C5FC57CE52905
Gast	NO PASSWORD		NO PASSWORD	NO PASSWORD
surfer	NULL PASSWORD		NULL PASSWORD	NULL PASSWORD
user1				DC88C45E1907D8790581AC077E125C22
user2				55456EE90DFA0978A404E5878E17A6CA
user3				E4C5A902304FEBEBBE367EE3A947DC2E
user4				3A4D73247D1F15DE329834CB76966135
user5		x		4C64F8B7E803CB1CAAD3B435B51404EE

Abbildung 1

Ein Angriff mit einem geeigneten Wörterbuch (hier ca. 415.000 Wörter) bringt - ent-sprechende Hardware vorausgesetzt - bereits nach einigen Minuten recht brauchbare Ergebnisse (Hinweis: Der sich an die Wörterbuchattacke anschließende BruteForce-Angriff wurde jeweils erst nach Bearbeitung der Zeichenfolge „KURZ“ abgebrochen, um die Wirkung auf das Passwort „ZuKurz“ von „user5“ zu zeigen):

Brute Force: ??JGHZA 7.44 % Done 0 H 59 M Left Rate: 2182801 Tries/sec

User Name	LanMan Password	<8	NT Password	LanMan Hash
Administrator				A16BA9F67F15BF4C8B4C5FC57CE52905
Gast	NO PASSWORD		NO PASSWORD	NO PASSWORD
surfer	NULL PASSWORD		NULL PASSWORD	
user1	DEZEMBER12		dezember12	DC88C45E1907D8790581AC077E125C22
user2	???????USSS			55456EE90DFA0978A404E5878E17A6CA
user3	???????TURE			E4C5A902304FEBEBBE367EE3A947DC2E
user4	CROISSANT99		croissant99	3A4D73247D1F15DE329834CB76966135
user5	ZUKURZ	x	ZuKurz	4C64F8B7E803CB1CAAD3B435B51404EE

Abbildung 2

14.2.3
Windows NT Service Pack 3

Auf diese, über das Internet schnell verbreiteten, Angriffsmöglichkeiten reagierte Microsoft mit einer weiteren Verschlüsselung der Benutzerdatenbank, die mit Service Pack 3 ausgeliefert wurde. SYSKEY.EXE bietet die Möglichkeit, das zur Ver- und Entschlüsselung (schon beim Systemstart) nötige Passwort manuell einzugeben, auf einer Diskette oder im System selbst abzulegen:

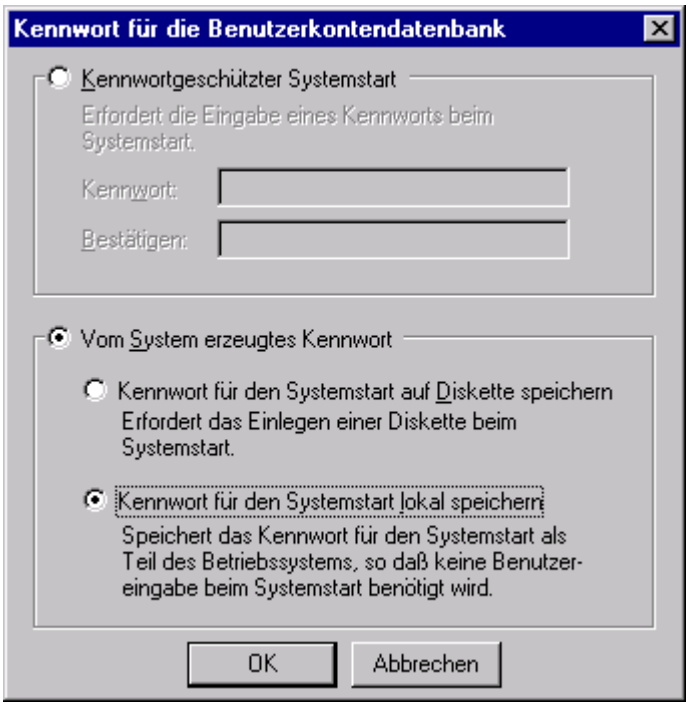


Abbildung 3

Diese doppelte Verschlüsselung machte den Angriff auf Benutzerpasswörter vorübergehend wirkungslos.
Nachteil von SYSKEY ist allerdings, dass das Programm manuell vom Administrator (in Domänen auf allen Domänencontrollern) aktiviert werden muss.

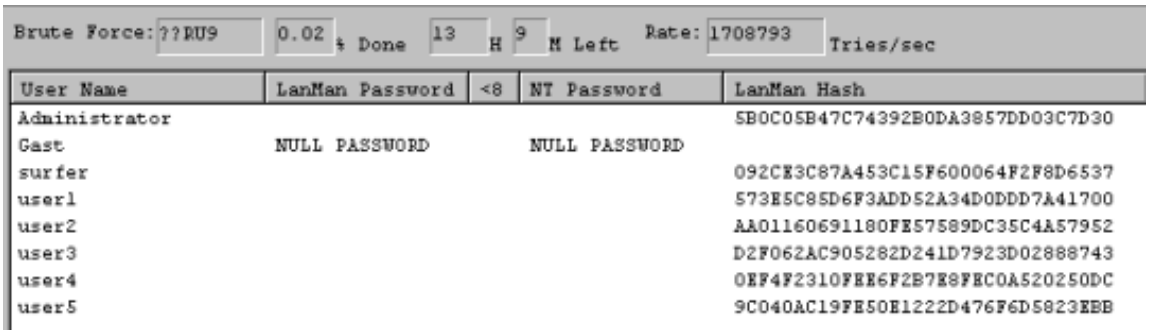
Der nach Aktivierung von SYSKEY erstellte Auszug der obigen Benutzerdatenbank stellt sich nun wie folgt dar:

User Name	LanMan Password	<8	NT Password	LanMan Hash
Administrator				5B0C05B47C74392B0DA3857DD03C7D30
Gast	NULL PASSWORD		NULL PASSWORD	NULL PASSWORD
surfer				092CE3C87A453C15F600064F2F8D6537
user1				573E5C85D6F3ADD52A34D0DDD7A41700
user2				AA0116069118OFE57589DC35C4A57952
user3				D2F062AC905282D241D7923D02888743
user4				0EF4F2310FEE6F2B7E8FEC0A520250DC
user5				9C040AC19FE50E1222D476F6D5823EBB

Abbildung 4

Wesentliche Unterschiede sind neben den veränderten Hash-Werten der (gleich gebliebenen) Passwörter sofort beim Benutzer „user5“ erkennbar: Das kurze Passwort (vgl. Spalte „<8“ in Abbildung 1 und 2) ist nicht mehr ersichtlich.

Die Liste stellt sich nach der Wörterbuchattacke und dem Anfang der BruteForce-Attacke unverändert dar:



Brute Force: ??RU9 0.02 % Done 13 H 9 M Left Rate: 1708793 Tries/sec

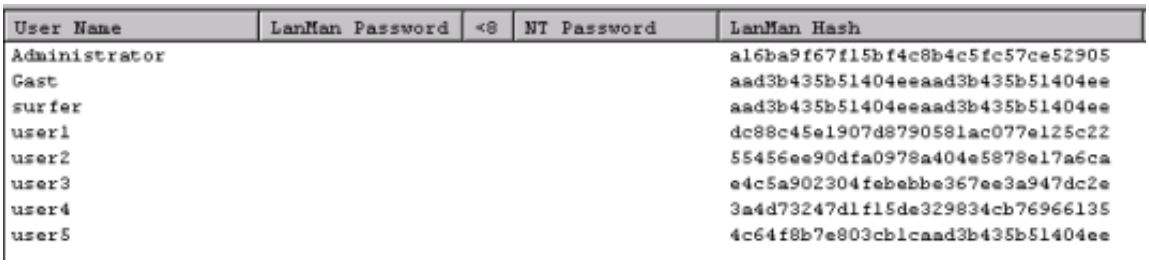
User Name	LanMan Password	<8	NT Password	LanMan Hash
Administrator				5B0C05B47C74392B0DA3857DD03C7D30
Gast	NULL PASSWORD		NULL PASSWORD	
surfer				092CE3C87A453C15F600064F2F8D6537
user1				573E5C85D6F3ADD52A34D0DDD7A41700
user2				AA0116069118OFE57589DC35C4A57952
user3				D2F062AC905282D241D7923D02888743
user4				0EF4F2310FEE6F2B7E8FEC0A520250DC
user5				9C040AC19FE50E1222D476F6D5823EBB

Abbildung 5

Damit war zunächst die Sicherheit - wenn auch mit Schwächen bei der Implementierung (Syskey ist ohne Kenntnis der entsprechenden Veröffentlichungen kaum bekannt und wird nicht automatisch installiert) - wiederhergestellt.

14.2.4
Der nächste Schritt

Bereits einige Zeit später fanden sich im Internet - neben neuen Versionen der gängigen „Passwortknacker" - Zusatzprogramme, die in der Lage sind, die mit SYSKEY modifizierten Hashwerte aus der Systemregistrierung zu extrahieren. Dies setzt neben dem Zugang zum System (lokal oder über das Netzwerk) auch einige Windows NT-Rechte voraus, da diese Programme Funktionen des NT-Sicherheitssystems (**L**ocal **S**ecurity **A**uthority **S**ub**s**ystem - LSASS.EXE) nutzen.
Die so erstellten Listen können dann wiederum zur Dekodierung der Passworte benutzt werden:

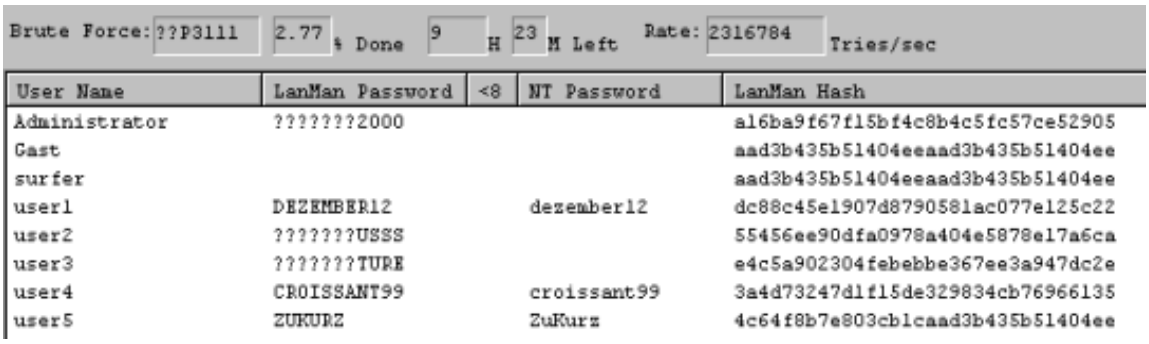


User Name	LanMan Password	<8	NT Password	LanMan Hash
Administrator				al6ba9f67f15bf4c8b4c5fc57ce52905
Gast				aad3b435b51404eeaad3b435b51404ee
surfer				aad3b435b51404eeaad3b435b51404ee
user1				dc88c45e1907d8790581ac077e125c22
user2				55456ee90dfa0978a404e5878e17a6ca
user3				e4c5a902304febebbe367ee3a947dc2e
user4				3a4d73247d1f15de329834cb76966135
user5				4c64f8b7e803cb1caad3b435b51404ee

Abbildung 6

Im Vergleich zu Abbildung 1 fällt auf:
- Die Hash-Werte sind wiederum identisch
- bei den Benutzern „Gast" und „surfer" fällt das nicht vorhandene Passwort nicht sofort auf. Jedoch weisen die identischen Hash-Werte auf eine leere Zeichenfolge hin, da es sehr unwahrscheinlich ist, dass zwei Benutzer das gleiche Passwort verwenden.

Die Attacken erzeugen folgendes Bild:



Brute Force: ??P3111 2.77 % Done 9 H 23 M Left Rate: 2316784 Tries/sec

User Name	LanMan Password	<8	NT Password	LanMan Hash
Administrator	???????2000			al6ba9f67f15bf4c8b4c5fc57ce52905
Gast				aad3b435b51404eeaad3b435b51404ee
surfer				aad3b435b51404eeaad3b435b51404ee
user1	DEZEMBER12		dezember12	dc88c45e1907d8790581ac077e125c22
user2	???????USSS			55456ee90dfa0978a404e5878e17a6ca
user3	???????TURE			e4c5a902304febebbe367ee3a947dc2e
user4	CROISSANT99		croissant99	3a4d73247d1f15de329834cb76966135
user5	ZUKURZ		ZuKurz	4c64f8b7e803cb1caad3b435b51404ee

Abbildung 7

Im Unterschied zu den alten Versionen ist die (wesentlich gefährlichere) Option, Passworte über das Netzwerk abzufangen, allerdings wirkungslos, da sie doppelt verschlüsselte Passworte liefert (normale Verschlüsselung und SYSKEY).

Die durchgängige Implementierung von SYSKEY sollte daher - wie das jeweils aktuelle Service Pack - zur Standardimplementierung gehören.
Darüber hinaus sollte die Vergabe von Windows-NT-Rechten, die Benutzern Zugang zu Systemfunktionen ermöglichen, restriktiv gehandhabt werden, da diese für die normale Nutzung des Systems nicht erforderlich sind.

14.2.5
Das Passwort

Verschärfung der Passwortregeln ruft bei den Nutzern immer erheblichen Unwillen hervor. Einfache Passwörter (wie in den Beispielen „ZuKurz“, „dezember12“ o.ä.) sind zwar leicht zu merken, aber ebenso leicht zu ermitteln - nicht nur mit dem Blick über die Schulter.
Komplizierte Buchstabenkombinationen führen neben dem ständigen Freischalten von Benutzern zum Zettel unter der Tastatur oder am Bildschirm.
Ideal ist das komplizierte Passwort, das leicht zu merken ist.
Es soll

- mindestens acht Zeichen lang sein
- kein sinnvolles Wort sein
- mindestens drei der vier Gruppen „Großbuchstaben“, „Kleinbuchstaben“, „Ziffern“ und „Sonderzeichen“ enthalten

Dies lässt sich auf verschiedenen Wegen erreichen:

- Einfügen/Ändern von Zeichen in einem sinnvollen Wort, z. B. „oster12ei“ weil Ostern am 12. des Monats ist oder „7schlaefer#“
- Verwenden von Anfangsbuchstaben eines Satzes, z. B. ergibt „Ich war schon zwölf Mal im Urlaub auf Mallorca“ das Passwort „Iws12MiUaM“

Sofern nicht erforderlich (homogene Windows NT-Umgebung vorhanden), sollte zudem die Vorhaltung (und damit Übermittlung) von LAN-Manager-kompatiblen Passwörtern im System deaktiviert werden.

14.2.6
Weitere Hinweise

Viele Programme bedürfen keiner Installationsroutine. Sie können daher auf beliebigen Wegen in ein System gelangen.
Für den Zugriff auf die Passwörter ist der direkte Zugang zum System am effektivsten. Der besondere Zugangsschutz (passwortgesicherte Bildschirmschoner, gesicherte Räumlichkeiten) ist für die NT-Domänencontroller daher von besonderer Bedeutung.
Ferner sind heute Programme verfügbar, die in der Lage sind, Paketsniffer im Netzwerk zu erkennen.
Ferner sollte Standardbenutzern auch über die Systemrichtlinien (POLEDIT.EXE) der Zugriff auf die Systemregistrierung verweigert werden.

14.3
Mitschneiden von Tastatureingaben

Es gibt im Versandhandel technische Komponenten, die alle Eingaben protokollieren, die über eine Tastatur erfolgen, ohne dass es der Benutzer bemerkt. Dieser Gefahr muss in Sicherheitskonzepten und bei der täglichen Arbeit begegnet werden.

Im letzten Jahr wurde ich durch eine Werbeanzeige auf ein Bauteil aufmerksam, das der Hersteller als Mittel beschreibt, um das unberechtigte Benutzen eines Rechners feststellen zu können. Das Bauteil wird zwischen Tastatur und Rechner gesteckt und zeichnet bis zu 32.000 Tastaturanschläge auf; das entspricht ca. 10 DIN-A4-Seiten Text. Laptops können daher mit diesem Bauteil nicht ausspioniert werden. Das Bauteil benötigt keinen Strom oder besondere Programme zum Funktionieren. Es speichert auch die beim Startvorgang eingegebenen Zeichen. Hiermit ist es beispielsweise möglich, Passwörter auszuforschen oder auch den Text von Dokumenten mit zu lesen, die später auf dem Rechner verschlüsselt gespeichert oder versandt werden.

Um das Bauteil installieren zu können, muss man Zutritt zum Rechner haben und der Rechner muss ausgeschaltet sein. Der Einbau dauert nur Sekunden. In der täglichen Arbeit ist es praktisch nicht möglich, den Einbau des Teils zu bemerken. Niemand wird jeden Tag seinen Rechner auf unbekannte Adapter auf der Rückseite untersuchen. Nach einiger Zeit kann man das Bauteil ebenso schnell wieder abbauen. Die Anzeige der Tastatureingaben kann nur an einem Rechner erfolgen, an dem das Teil installiert ist. Da es zur Auswertung an jedem Rechner eingebaut werden kann, auch dem des Abhörers, verringert das die Gefahr einer unbefugten Ausforschung nicht.
Es ist durchaus denkbar, dass die Komponente im Einzelfall - wie vom Hersteller beschrieben - zur Feststellung einer unberechtigten Nutzung eines Rechners eingesetzt wird, etwa bei Verdacht auf Industriespionage. Die Fälle, in denen eine Nutzung der Komponente rechtlich unproblematisch ist, sind jedoch rar. Sehr viel wahrscheinlicher ist, dass damit Personen ohne deren Wissen überwacht werden oder dass Angreifer versuchen, in fremde Rechnernetze einzudringen. Konsequenz ist, dass das Passwort als alleiniger Schutz gegen unberechtigte Anmeldeversuche, zumindest in Bereichen mit höheren Sicherheitsanforderungen, nicht mehr ausreichend ist.

Leider gibt es keine einfachen, praktikablen Sicherheitsmaßnahmen, die einen Schutz gegen das Bauteil bieten. Aber da die interessierten Kreise das Bauteil und seine Möglichkeiten kennen, habe ich mich entschieden, darüber zu berichten. Vielleicht wird mehr Aufmerksamkeit einige Probleme lösen.

Die folgenden Punkte sind erste kleine Schritte auf dem Weg zur Sicherheit:

- Die Zutrittskontrolle muss genau überwacht werden; unbefugte Personen dürfen nicht allein an den Rechner gelangen. Dies wird bisher jedoch nur in Sicherheitsbereichen konsequent umgesetzt werden.

- Wenn verfügbar, sollten die Rechner in verschlossenen Gehäusen untergebracht werden, die auch die Schnittstellen blockieren. Leider hat ein mir bekannter Anbieter für solche Gehäuse kürzlich die Produkte aus seinem Angebot genommen.

- Es sollte geprüft werden, ob und in welchem Fällen Laptops zu bevorzugen sind. Die Gefahr der Protokollierung aller Eingaben über die Tastatur besteht dann nicht.

- Die Schnittstellen zwischen Rechner und Tastatur sollten immer wieder daraufhin kontrolliert werden, ob Adapter angebracht wurden.

- Um eine höhere Sicherheitsstufe zu erreichen, sollte die Anmeldeprozedur ergänzt werden, etwa durch biometrische Merkmale, Chipkarten oder die Verwendung von Einmalpasswörtern.

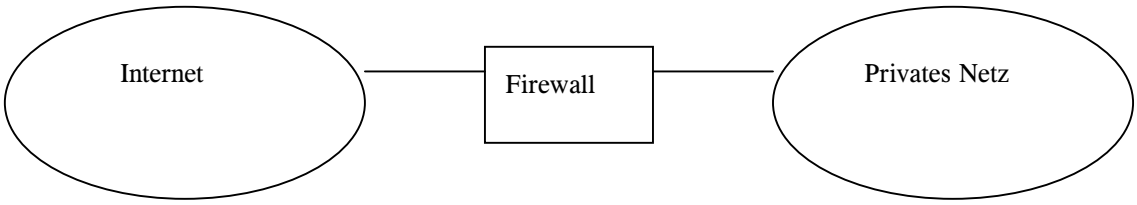
- Administratoren und andere Personen, deren Benutzerkennungen hohe Privilegien haben, sollten das Passwort ändern, nachdem sie sich von unsicheren Rechnern aus angemeldet haben.

14.4
Personal Firewalls

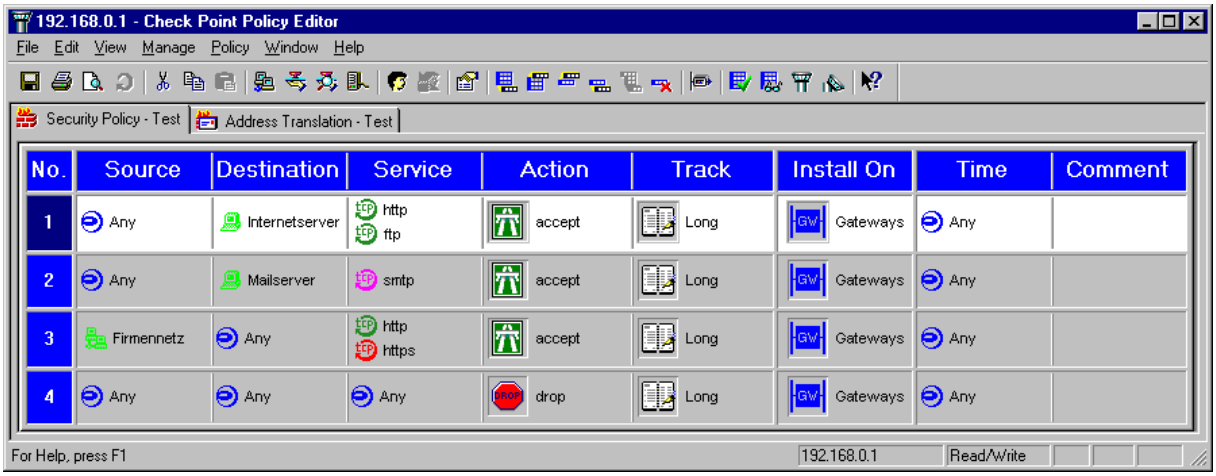
Personal Firewalls sind eine sinnvolle Ergänzung des PC-Schutzes durch Virenscanner bei der Arbeit mit Internet-Anwendungen. Da sie nicht vorkonfigurierbar sind, stellen sie aber gewisse Anforderungen an den Anwender. Eine falsche Auswahl bzw. eine unvollständige/falsche Konfiguration können gefährlicher sein als der Verzicht auf den Einsatz eines solchen Produktes, da sie vermeintliche Sicherheit vorgaukeln.

14.4.1
Eine Firewall - Was ist das?

Unter dem Begriff „Firewall“ ist im Bereich der Netzwerktechnologie eine Anwendung zu verstehen, die den Netzwerkverkehr überwacht. Diese Überwachung findet an den Übergängen von Netzwerken statt - meist vom Internet (öffentliches Netz) zum eigenen Firmen-, Behörden- oder auch sonstigem Netzwerk (privates Netz)



Ähnlich einem Pförtner in einem Gebäude wirkt eine Firewall anhand von Regeln, die der Administrator definiert:



Die Firewall untersucht anhand dieser Regeln alle Netzwerkpakete auf Quelladresse („Source“), Zieladresse („Destination“) sowie den angeforderten Dienst („Service“), führt die festgelegte Aktion („Action“) aus und protokolliert ggf. („Track“). Alle Einträge werden nacheinander durchsucht, am Ende der Liste steht die sog. „Clearing Rule“, die alle nicht vorher explizit erlaubten Verbindungen ablehnt.

14.4.2
Funktion einer Personal Firewall

„Mir wird schon nichts passieren“, „Im Internet falle ich sowieso niemandem auf“, „Wer interessiert sich schon für meinen Rechner“. Das sind Argumente, mit denen man sich bisher gerne um die Anschaffung eines Virenscanners oder die Frage nach Sinn und Zweck weiteren Rechnerschutzes „gedrückt“ hat.

Zu beachten ist aber, dass die Risiken zunehmen, weil
- vermehrt Rechner über Flatrates als Quasi-Standleitungen mit dem Internet verbunden sind,
- die Zahl der dDOS-Angriffe zunimmt,

Distributed Denial Of Service

Lahmlegung eines Internetdienstes durch zentral gesteuerte massenhafte und gleichzeitig Zugriffe von Drittrechnern aus, die über Viren oder trojanische Pferde fernsteuerbar sind.

- E-Mail-Nutzung und -Integration in das Betriebssystem immer intensiver werden (Verbreitung von Viren und Trojanern über automatisierte Skripte und Anwendungen) und
- immer mehr sicherheitsrelevante Anwendungen für das Internet (Home-Banking, Signaturen usw.) verfügbar sind.

14.4.3
Was kann eine Personal Firewall?

Eine Personal Firewall (gelegentlich auch „Desktop Firewall“) kann Aufgaben einer professionellen Firewall - in eingeschränktem Maße - auch für den PC zu Hause oder im Büro übernehmen.

Das Spektrum des Schutzes reicht von der reinen Anwendungsebene (d. h. es werden Regeln für Programme definiert; beispielsweise: Der Anwendung „Netscape Navigator“ ist es gestattet, Verbindung zum Internet aufzunehmen) bis zur Protokollebene wie bei der „echten“ Firewall (d. h. jede gewünschte - oder unerwünschte - Verbindung muss explizit gestattet oder verboten werden; beispielsweise: Der Anwendung „Internet Explorer“ ist es gestattet, auf dem Port 80 [= Zugriff auf Internetseiten] Verbindung zum Server „x.y.z“ aufzunehmen).

Einige Produkte bieten darüber hinaus weitere Funktionen wie bspw. den Schutz des lokalen Dateisystems (Festplattenzugriffe) oder Cookie-Filter.

Cookies beinhalten Informationen, die ein Webserver auf der Festplatte des Benutzers ablegen kann, z. B. Informationen über den letzten Besuch auf der Seite, Kundeninformationen bei Internet-Einkäufen usw. Auf diese Weise kann ein Web-Anbieter schnell und einfach Informationen über das Surfverhalten eines Nutzers auf seiner Seite sammeln.

14.4.4
Konfiguration

Anders als Virenscanner, die mit der Installation (und natürlich der zeitnahen Aktualisierung der Erkennungsdateien) sofort betriebsbereit und so vorbereitet sind, dass sie infizierte Dateien tilgen, muss die Personal Firewall vom Administrator mit Regeln versehen werden, bevor sie ihren Dienst versehen kann.

Viele Produkte bieten neben der festen Einstellungen einen sog. „interaktiven Modus“ oder „Lernmodus“ an. Dies bedeutet, dass zunächst alles erlaubt ist und der Anwender keinen Einschränkungen in seiner Arbeit unterworfen ist. Jede Aktion, die der Firewall unbekannt ist, wird dem Anwender angezeigt, er muss nun entscheiden, ob er diese Aktion einmalig erlauben oder verbieten oder eine allgemeine Regel für künftige gleiche Ereignisse treffen will.

Hier liegt eine nicht zu unterschätzende Gefahr. Die individuelle Entscheidung, ob eine Aktion zulässig sein soll oder nicht, setzt genaue Grundverständnisse voraus. Eine falsche Anwendung kann den Nutzer beeinträchtigen, in dem nötige Funktionen blockiert werden, die später zu aufwendiger Fehlersuche führen, oder einen Zugang für Eindringlinge oder bereits vorhandene Schädlinge (trojanische Pferde) öffnen.

Beispiele:
Beim Datei-Download von einem FTP-Server wird zunächst eine Verbindung vom PC zum Server über Port 21 aufgebaut.

File **T**ransfer **P**rotocol
für die Übertragung von Daten optimiertes Protokoll, das ohne „aufwendige" grafische Oberflächen auskommt.
Diesem folgt beim Datenrückfluss eine umgekehrte Verbindungsaufnahme auf Port 20. Sofern dieser Weg nicht bekannt ist, führt die Blockierung der vermeintlich unzulässigen externen Verbindungsaufnahme zu Fehlern beim Herunterladen. Umgekehrt können trojanische Pferde - die sich zudem meist im Systemverzeichnis einnisten - Verbindungen zu Rechnern im Internet aufbauen. Tragen diese außerdem noch „sprechende" Namen („Win…exe" o. Ä.) kann das dazu verleiten, solche Kontaktversuche als legitim anzusehen und den Schutz der Firewall irrtümlich auszuhebeln.

Ein weiteres, nicht zu unterschätzendes Problem solcher Interaktiv-Modi ist die Tatsache, dass mit Konstanz auftretende Meldungsfenster irgendwann nur flüchtig oder gar nicht mehr gelesen werden, zumal sie das „normale" Arbeiten stören.

14.4.5
Überwachung der Protokolle

Im Einsatz bedarf eine Personal Firewall der kontinuierlichen Überwachung anhand der erzeugten Protokolle. Anders als z. B. ein Virenscanner, der sich in der Systemleiste visuell bemerkbar macht (aktiv oder nicht aktiv), arbeitet die Firewall nach ihren Standardeinstellungen im Verborgenen. Wie effizient oder unvollständig die individuell beeinflussten Einstellungen sind kann nur durch Auswertung der Protokolle festgestellt werden. Einige Anwendungen sind sogar in der Lage, eine installierte Personal Firewall zu erkennen und diese (unbemerkt vom Anwender) zu deaktivieren bzw. Regeln einzufügen, um ihre Aktivitäten zu tarnen.

Beispiel:
Eine Firewall kann selbst nicht
- zwischen einem (prinzipiell erlaubten) einmaligen Zugriff auf einen Webserver und dem (unzulässigen) massenhaften Zugriff als dDOS-Attacke
- zwischen dem Versand einer E-Mail an einen einzelnen Empfänger und den skriptgesteuerten „Massenversand" an alle Adressbucheinträge durch ein Virus

unterscheiden.

Zur Überwachung der Internet-Aktivitäten gehört auch die Verfolgung von aktuellen Meldungen und verfügbaren Aktualisierungen des gewählten Produktes.
Ebenso wie professionelle Firewalls stehen Personal Firewalls im Blickpunkt von Angriffen, da sie richtig eingesetzt ein nicht zu unterschätzendes Hindernis für Eindringlinge darstellen.

14.4.6
Produktauswahl

Sowohl im **Internet** als auch in diversen **PC-Zeitschriften** gibt es **Testberichte** wie auch **Test- und Vollversionen** zu aktuell verfügbaren Produkten.

Hierzu gehört auch als nicht unwesentlicher Faktor der derzeit anstehende Umbruch im Bereich des Betriebssystems für Heimanwendersysteme. Mit der Einführung von Windows XP für Heimanwender ist davon auszugehen, dass die Masse der derzeit am Markt befindlichen Personal Firewalls nicht mehr nutzbar sind, da in Windows XP der komplette Betriebssystemkern erneuert wurde.

Mein Internetangebot unter „http://www.datenschutz.hessen.de" enthält u.a. die Tätigkeitsberichte und ein Schlagwortverzeichnis für die Stichwortsuche.

14.5
Ergebnisse von Prüfungen der Datensicherheit mit Hilfe eines Portscanners

Der Einsatz einer Software bei der Prüfung TCP/IP-basierender Netze kann die Prüfungstätigkeit sinnvoll unterstützen und hat interessante Erkenntnisse gebracht. Die Administratoren sichern ihre Netze in der Regel recht gut ab, aber die Flut neu erkannter Schwachstellen von Netzsoftware und Betriebssystemen erfordert die kontinuierliche Pflege der Netzkomponenten.
Nach einigen Tests im Jahr 2000 habe ich im abgelaufenen Kalenderjahr erstmals die Prüfungen und Beratungen im Bereich der Netzwerkadministration gezielt durch den Einsatz einer Software unterstützt, die verschiedenste Einstellungen im Umfeld von Microsoft NT-Installationen oder von Unix-Derivaten überprüft. Neben dem Ermitteln der jeweils typischen systemspezifischen Einstellungen der Betriebssysteme lassen sich mit dem Programm auch bestimmte Test-Angriffe und das Scannen von TCP/IP-Ports in einem Ablaufprofil zusammenstellen. Das Programm testet dann alle zuvor ausgewählten

Rechner eines Netzes mit dem spezifizierten Profil und erstellt aus den Ergebnissen einen Bericht, der nach verschiedenen Gesichtspunkten für die weitere Auswertung aufbereitet werden kann.

Bei den angemeldeten Prüfungen oder verabredeten Beratungsgesprächen wurde von den jeweiligen Stellen ein interner Netzzugang zur Verfügung gestellt. In Einzelfällen wurde auch der „äußere Anschluss“ einer Firewall als Einstiegspunkt gewählt, um gezielt die Wirksamkeit der Firewall zu prüfen.

Die Prüfungen ergaben insgesamt bei Einbeziehung der konventionell gewonnenen Prüfergebnisse ein überaus positives Bild. Um für den Einsatz der Prüfsoftware ein sinnvolles Umfeld sicherzustellen, wurden kleinere Verwaltungen noch nicht in die Prüfserien mit einbezogen. In der Tendenz zeigt sich, dass mit zunehmendem Grad der Automatisierung und dem damit verbundenen Aufwand die Zahl kritischer oder gar beanstandenswerter Systemeinstellungen abnimmt. Betreiber größerer Netze sind im Allgemeinen zur Sicherstellung der Betriebsfähigkeit gezwungen, sehr sorgfältig und strukturiert zu arbeiten. Lediglich im Bereich der Dokumentation fanden sich vereinzelt Schwächen.

Exemplarisch wurden rund 100 Rechner für die weitere Auswertung der Reports ausgewählt. Neben Servern mit Microsoft- oder Unix-Betriebssystemen wurden bei den Prüfungen einige Firewalls und jeweils mindestens eine Standardworkstation je Dienststelle in die Auswertung einbezogen.

Von den 625 Schwachstellen, die in den Reports festgehalten sind, wurden 50 als besonders schwerwiegend eingeordnet. Weitere 175 Meldungen gehörten zur mittleren Kategorie und der Rest entfiel auf die schwächste Einstufung. Die Kategorisierung durch den Hersteller der Prüfsoftware ist jeweils im Einzelfall zu korrigieren, da die Schwachstellen abhängig von der jeweiligen Netzwerk- und Anwendungsumgebung zu einem Risiko werden können oder beherrschbar sind.

Teilweise ergeben sich schwerwiegende Mängel schon aus der Standardinstallation von Serverprodukten, weil diese Produkte eher „kontaktfreudig“ als „reserviert“ ausgelegt sind. In anderen Fällen können Systemeinstellungen, die mit Risiken behaftet sind, nur dann geändert werden, wenn man bereit ist, auf bestimmte Leistungsmerkmale im internen Netz zu verzichten.

Leider hat sich gezeigt, dass mit etwas abweichenden Softwareprodukten andere Schwachstellen an den untersuchten Servern festzustellen waren. Damit ergeben sich aus den jeweiligen Reports zwar wertvolle Hinweise für die Netzwerkadministration; da die eingesetzte Software nur die jeweils bekannten und in das Prüfprogramm eingearbeiteten Schwachstellen prüft, bleibt für einen Betreiber als ständige Aufgabe, neu auftretende Verwundbarkeiten zu beseitigen. Das können bei einigen Betriebssystemen über 100 pro Jahr sein.

Da das Spektrum einer Prüfung von DV-Technik weit über den Bereich hinaus geht, der durch ein solches Programm abgedeckt wird, bleibt für die konventionelle Prüfung noch sehr viel Raum. So haben die Prüfungen als Nebenergebnis gezeigt, dass es beim Einsatz von Anwendungssoftware viele Verfahren gibt, bei denen zwischen interner Zugriffsabgrenzung und den Einstellungen auf Betriebssystemebene eine Diskrepanz existiert, die auf strukturellen Fehlern der jeweiligen Anwendungssoftware beruht. Ich werde daher dieser Problematik im nächsten Jahr besonders nachgehen und in meinem nächsten Tätigkeitsbericht darüber berichten.

Abschließend ist festzustellen, dass der Einsatz einer Prüfsoftware im Umfeld mittlerer und größerer Netze die Prüfungstätigkeit sinnvoll unterstützt und ergänzt. Dies wird beim zunehmendem Ausstattungsgrad der Dienststellen jedenfalls dann effizient, wenn viele ähnliche Rechner mit dem gleichen Profil in einem Prüflauf untersucht werden können.

14.6
Überprüfung einer übersandten Festplatte

Werden Datenträger vorübergehend oder dauerhaft anderen Aufgabenbereichen zugeführt, ist die physikalische Löschung aller personenbezogenen Daten vorzunehmen, sofern der Empfänger dafür unzuständig ist.

Ein Mitarbeiter einer Hochschule hat mir eine Festplatte zugesandt, die ihm zur Erweiterung seines Arbeitsplatzrechners zur Verfügung gestellt worden war. Offensichtlich war diese Komponente vorher in einem anderen Fachbereich im Einsatz. Die Platte war vor der Übergabe weder neu formatiert noch physikalisch gelöscht worden.

Bei meinen informationstechnischen Recherchen fanden sich relativ schnell eine ganze Reihe von sportmedizinischen Untersuchungsergebnissen, die sowohl die Patienten mit voller Anschrift als auch die Diagnosen, Vorerkrankungen, Medikation und andere ergänzende Angaben enthielten.

Vor der Weitergabe gebrauchter Datenträger ist immer sorgfältig zu prüfen, ob personenbezogene Daten auf diesem Weg in die Hände von nicht zuständigen Personen gelangen können. Derartige Daten sind vor der Überlassung an andere Ressorts

physikalisch zu löschen oder/und zu überschreiben. Über die Möglichkeiten der physikalischen Löschung und die Unterschiede zur logischen Löschung habe ich bereits in meinem 21. Tätigkeitsbericht (Ziff. 16.1) ausführlich berichtet. Seit dieser Zeit sind weitere Tools auf den Markt gekommen, die das physikalische Löschen bzw. das gezielte und wirkungsvolle Überschreiben ermöglichen.

Der Hochschule wurde das nachlässige Vorgehen klar gemacht. Sie schaltete ihren eigenen Datenschutzbeauftragten ein. Auf meine Bitte hat der interne Datenschutzbeauftragte der Hochschule Maßnahmen veranlasst, die sicherstellen, dass künftig in der Hochschule entsprechend verfahren wird.

15. Soziales

15.1
Akteneinsichtsrecht und Auskunftsanspruch

Ein Akteneinsichtsrecht besteht nach geltendem Recht nur im Zusammenhang mit einem laufenden Verwaltungsverfahren; im Übrigen kommt ein Auskunftsanspruch in Betracht.

Das Sozialamt einer Kommune hatte angefragt, inwieweit Betroffenen ein Akteneinsichtsrecht oder nur ein Auskunftsanspruch hinsichtlich der Sozialakte des Antragstellers zusteht.

Das Akteneinsichtsrecht ist eine günstigere Rechtsposition, da es dem Betroffenen möglich ist, den Akteninhalt direkt und authentisch zur Kenntnis zu nehmen. Bei einer Auskunft erhält der Betroffene vom Akteninhalt nur vermittelt Kenntnis, so dass theoretisch z. B. eine gezielte Selektion oder Interpretation des Akteninhalts durch den Auskunft gebenden Bediensteten möglich ist. In jedem Fall wird durch die Möglichkeit der Akteneinsicht umfassendere Transparenz des Verwaltungshandelns für den Bürger gewährleistet.

Das Akteneinsichtsrecht ist in § 25 Sozialgesetzbuch X (SGB X) geregelt.

§ 25 SGB X

(1) Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist.
Satz 1 gilt bis zum Abschluss des Verwaltungsverfahrens nicht für Entwürfe zu Entscheidungen sowie die Arbeiten zu ihrer unmittelbaren Vorbereitung.

(2) Soweit die Akten Angaben über gesundheitliche Verhältnisse eines Beteiligten enthalten, kann die Behörde statt dessen den Inhalt der Akten dem Beteiligten durch einen Arzt vermitteln lassen. Sie soll den Inhalt der Akten durch einen Arzt vermitteln lassen, soweit zu befürchten ist, dass die Akteneinsicht dem Beteiligten einen unverhältnismäßigen Nachteil, insbesondere an der Gesundheit, zufügen würde. Soweit die Akten Angaben enthalten, die die Entwicklung und Entfaltung der Persönlichkeit der Beteiligten beeinträchtigen können, gelten die Sätze 1 und 2 mit der Maßgabe entsprechend, dass der Inhalt der Akten auch durch einen Bediensteten der Behörde vermittelt werden kann, der durch Vorbildung sowie Lebens- und Berufserfahrung dazu geeignet und befähigt ist. Das Recht nach Abs. 1 wird nicht beschränkt.

(3) Die Behörde ist zur Gestattung der Akteneinsicht nicht verpflichtet, soweit die Vorgänge wegen der berechtigten Interessen der Beteiligten oder dritter Personen geheimgehalten werden müssen.

Das Akteneinsichtsrecht knüpft an das Vorliegen eines sog. Verwaltungsverfahrens an. Ein Verwaltungsverfahren ist jede nach außen wirkende Tätigkeit der Behörden, die auf die Prüfung der Voraussetzungen, die Vorbereitung und den Erlass eines Verwaltungsaktes oder auf den Abschluss eines öffentlich-rechtlichen Vertrages gerichtet (§ 8 SGB X). In anderen Fällen besteht kein Anspruch auf Akteneinsicht, sondern nur ein Auskunftsanspruch nach Maßgabe von § 83 SGB X.

§ 83 SGB X

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über
1. die zu seiner Person gespeicherten Sozialdaten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und
2. den Zweck der Speicherung.

…

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung von Sozialdaten an Staatsanwaltschaften und Gerichte im Bereich der Strafverfolgung, an Polizeibehörden, Verfassungsschutzbehörden, den Bundesnachrichtendienst und den Militärischen

Abschirmdienst, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit
1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen,

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.
…

(6) Wird einem Auskunftsberechtigten keine Auskunft erteilt, so kann, soweit es sich um in § 35 des Ersten Buches genannte Stellen handelt, die der Kontrolle des Bundesbeauftragten für den Datenschutz unterliegen, dieser, sonst die nach Landesrecht für die Kontrolle des Datenschutzes zuständige Stelle auf Verlangen der Auskunftsberechtigten prüfen, ob die Ablehnung der Auskunftserteilung rechtmäßig war.

(7) Die Auskunft ist unentgeltlich.

Ich habe das Sozialamt der Kommune entsprechend unterrichtet.

15.2
Planung im Sozialleistungsbereich

Die Übermittlung von Sozialdaten zwecks Befragung der Sozialhilfeempfänger durch ein Privatunternehmen für die Planung im Sozialleistungsbereich ist nur mit Einwilligung der Sozialhilfeempfänger zulässig.

Die Stadt Frankfurt beabsichtigte eine Befragung der Sozialhilfeempfänger durch ein Privatunternehmen über die Qualität der Arbeit des Sozialamtes sowie über sozialhilferechtlich relevante personenbezogene Daten der Sozialhilfeempfänger auf der Grundlage von § 80 Sozialgesetzbuch X (SGB X) (Auftragsdatenverarbeitung). Dem Privatunternehmen sollten die Adressen der Sozialhilfeempfänger zwecks Kontaktaufnahme ohne vorherige Einwilligung zur Verfügung gestellt werden.

Ein solches Vorgehen ist unzulässig. Maßgebend für das angedachte Projekt ist nämlich nicht § 80 SGB X, sondern der hier speziell einschlägige § 75 SGB X, der die Übermittlung von Sozialdaten u.a. für Vorhaben der Planung im Sozialleistungsbereich regelt. Auftragsdatenverarbeitung i. S. v. § 80 SGB X liegt bei dem anvisierten Projekt deshalb nicht vor, weil es nicht um unselbständige, weisungsgebundene Tätigkeit geht. Das Privatunternehmen soll im Wege eigener Gestaltung oder zumindest Mitgestaltung des Forschungsdesigns vorgehen. In einem solchen Fall wäre die Anwendung des § 80 SGB X nicht sachgerecht, weil dadurch die höheren Hürden, die § 75 SGB X für Forschungs- und Planungsvorhaben errichtet hat, umgangen würden. Dafür kann das Instrument der Auftragsverarbeitung nicht verwendet werden.

§ 75 SGB X

(1) Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist für ein bestimmtes Vorhaben
1. der wissenschaftlichen Forschung im Sozialleistungsbereich oder
2. der Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben

und schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung oder Planung das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt. Eine Übermittlung ohne Einwilligung des Betroffenen ist nicht zulässig, soweit es zumutbar ist, die Einwilligung des Betroffenen nach § 67b einzuholen oder den Zweck der Forschung oder Planung auf andere Weise zu erreichen.

(2) Die Übermittlung bedarf der vorherigen Genehmigung durch die oberste Bundes- oder Landesbehörde, die für den Bereich, aus dem die Daten herrühren, zuständig ist. Die Genehmigung darf im Hinblick auf die Wahrung des Sozialgeheimnisses nur versagt werden, wenn die Voraussetzungen des Abs. 1 nicht vorliegen. Sie muss
1. den Dritten, an den die Daten übermittelt werden,
2. die Art der zu übermittelnden Sozialdaten und den Kreis der Betroffenen,
3. die wissenschaftliche Forschung oder die Planung, zu der die übermittelten Sozialdaten verwendet werden dürfen, und
4. den Tag, bis zu dem die übermittelten Sozialdaten aufbewahrt werden dürfen,

genau bezeichnen und steht auch ohne besonderen Hinweis unter dem Vorbehalt der nachträglichen Aufnahme, Änderung oder Ergänzung einer Auflage.

(3) Wird die Übermittlung von Daten an nicht-öffentliche Stellen genehmigt, hat die genehmigende Stelle durch Auflagen sicherzustellen, dass die der Genehmigung durch Abs. 1 gesetzten Grenzen beachtet und die Daten nur für den Übermittlungszweck gespeichert, verändert oder genutzt werden.

Gemäß § 75 Abs. 1 Satz 2 SGB X ist grundsätzlich vor der Übermittlung der Sozialdaten die Einwilligung der Betroffenen einzuholen ist; dass dies unzumutbar ist, ist bei diesem Projekt nicht ersichtlich.

Ich habe die Stadt Frankfurt entsprechend unterrichtet und vorgeschlagen, im Fall der Weiterverfolgung des Projekts zunächst einen Antrag auf Genehmigung an das Sozialministerium zu stellen; ein solcher Antrag liegt aber nach meinen Erkenntnissen bislang nicht vor.

15.3
Bekanntgabe von Heimbeiratsmitgliedern

Die Heimaufsichtsbehörden sind nicht befugt, die Namen der Heimbeiratsmitglieder in den nicht-öffentlichen Bereich zu übermitteln.

Die Bundesinteressenvertretung der Altenheimbewohner e.V. (BIVA) hat um Auskunft gebeten, ob die Heimaufsichtsbehörden sich aus datenschutzrechtlichen Gründen zu recht weigern, der BIVA die Namen der Heimbeiratsmitglieder stationärer Einrichtungen zu nennen. Der Heimbeirat ist von seiner Funktion her für die jeweiligen Heimbewohner etwa das, was der Personalrat für die Bediensteten ist.

Die BIVA ist deshalb an der Nennung der Namen der Heimbeiratsmitglieder interessiert, weil sie jährlich Fachveranstaltungen zu heimspezifischen Themen durchführt, die sich im Wesentlichen an Heimbeiratsmitglieder richten, und diese wolle sie unmittelbar einladen. Den Heimaufsichtsbehörden ist nicht gestattet, die Namen der Heimbeiratsmitglieder ohne deren Einwilligung der BIVA zu nennen. Das ergibt sich aus § 16 Abs. 1 HDSG.

§ 16 Abs. 1 HDSG

Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

Es kann nicht ausgeschlossen werden, dass durch die Datenübermittlungen schutzwürdige Belange der Heimbeiratsmitglieder beeinträchtigt werden. Die Vorschrift setzt eine Einzelfallprüfung voraus.

Das Problem lässt sich datenschutzrechtlich korrekt recht einfach dadurch lösen, dass die BIVA den Heimaufsichtsbehörden Einladungen zuschickt und die Heimaufsichtsbehörden wiederum die Einladungen an die Heimbeiratsmitglieder weiterleiten (sog. Konsulatslösung).

Ich habe der BIVA eine entsprechende Auskunft gegeben.

15.4
Sozialdatenschutz bei der Adoptionsvermittlung

Im Adoptionsvermittlungsrecht gilt der Sozialdatenschutz.

Mitunter fragen Jugendämter an, welche datenschutzrechtlichen Vorschriften bei der Adoptionsvermittlung zu beachten sind.

Dies ist an etwas versteckter Stelle im Sozialgesetzbuch (SGB) ausdrücklich geregelt; § 68 SGB I legt fest, dass u.a. das Adoptionsvermittlungsgesetz bis zu seiner Einordnung in das Sozialgesetzbuch zu dessen besonderen Teilen zählt (Nr. 12).

Nicht eindeutig ist, ob und inwieweit bei der Vollziehung des Adoptionsvermittlungsgesetzes nur das allgemeine Sozialdatenschutzrecht gemäß den §§ 67 ff. SGB X maßgebend ist oder ob primär das spezielle Sozialdatenschutzrecht gemäß dem Kinder- und Jugendhilfegesetz (KJHG, SGB VIII) gilt, §§ 61 ff. KJHG. Die Unsicherheit rührt daher, dass die Vollziehung des Adoptionsvermittlungsgesetzes nicht ausdrücklich in den Aufgabenkatalog der Jugendhilfe nach § 2 KJHG aufgenommen worden ist, wenn auch auf das Adoptionswesen zum Teil Bezug genommen wird (§§ 2 Nr. 7, 51 KJHG).

Unabhängig davon, welche Vorschriften man zu Grunde legt, steht die Förderung des Kindeswohls an erster Stelle. Datenschutzrechtlich ist die Frage von Bedeutung, ob im Adoptionsvermittlungsverfahren ein Recht auf Akteneinsicht besteht. Das Kinder- und Jugendhilferecht verweist in § 67 KJHG nur auf das Auskunftsrecht in § 83 SGB X, nicht jedoch auf das Akteneinsichtsrecht nach § 25 SGB X. Es wäre jedoch paradox, daraus auf die Nichtanwendbarkeit des § 25 SGB X im Kinder- und Jugendhilferecht zu schließen. Denn der spezielle Datenschutz im Kinder- und Jugendhilfegesetz soll die Rechtsposition der Betroffenen gegenüber dem allgemeinen Sozialdatenschutzrecht zusätzlich privilegieren. Von daher wäre es widersinnig, ein so zentrales Recht wie das Recht auf Akteneinsicht für das Adoptions-vermittlungsverfahren zu negieren.

Dementsprechende Auskünfte habe ich den Jugendämtern gegeben.

15.5
Rechtswidrige Übermittlung von Sozialdaten durch das Sozialamt der Kreisstadt Groß-Gerau an die Führerscheinstelle

Ein Sozialamt ist grundsätzlich befugt, im Rahmen einer Güterabwägung die Führerscheinstelle über die Erkrankung eines Sozialhilfeempfängers, der einen PKW führt, zu informieren, wenn erkennbar ist, dass Gefahren für Leib und Leben anderer Verkehrsteilnehmer hierdurch abgewendet werden können.

Ein Sozialhilfeempfänger hat mich im August 2000 gebeten, die Zulässigkeit verschiedener Datenübermittlungen, insbesondere der Weitergabe von ärztlichen Gutachten durch das Sozialamt an die Führerscheinstelle zu überprüfen. Der Sozialhilfeempfänger, der bereits seit längerer Zeit Hilfe zum Lebensunterhalt vom Sozialamt Groß-Gerau bezieht, hat im Jahr 1998 wegen krampfartiger Anfälle beim Sozialamt die Kostenübernahme für eine größere Wohnung beantragt. Im weiteren Verlauf der Bearbeitung seines Antrags hat der Hilfesuchende im September 1999 dem Sozialamt den ärztlichen Abschlussbericht eines Krankenhauses übergeben, aus dem insbesondere der Verdacht einer Epilepsie hervorgeht.

Dem Sozialamt lag neben dem Krankenhausbericht bereits eine amtsärztliche Stellungnahme des Kreisgesundheitsamtes Groß-Gerau vom 12. Dezember 1996 vor. Die amtsärztliche Stellungnahme wurde zur Überprüfung der Erwerbsfähigkeit des Hilfesuchenden gefertigt. Sie beinhaltet die Aussage, dass der Hilfesuchende zum Führen von Kraftfahrzeugen aller Klassen ungeeignet ist. Im weiteren Verlauf der Prüfung des Sozialamtes, ob die Kosten für eine größere Wohnung übernommen werden können, wurde der Hilfesuchende mit Bescheid vom 6. April 2000 aufgefordert, sich einer erneuten medizinischen Begutachtung zu unterziehen.

Am 26. April 2000 hat das Sozialamt der Stadt Groß-Gerau die Führerscheinstelle des Landratsamtes Groß-Gerau dahingehend informiert, dass der Hilfesuchende Hilfe zum Lebensunterhalt erhält, im Besitz der Fahrerlaubnis der Klasse 3 ist, unter Krampfanfällen leidet und deshalb nach Ansicht des Sozialamtes nicht in der körperlichen Verfassung sei, ein Kraftfahrzeug zu führen. Die Stellungnahme des Kreisgesundheitsamtes aus dem Jahre 1996 sowie der Abschlussbericht des Krankenhauses aus dem Jahre 1999 waren dem Schreiben an die Führerscheinstelle in Kopie beigefügt.

Die am 4. September 2000 erbetene Stellungnahme des Sozialamtes ist erst nach zwei schriftlichen Erinnerungen am 22. Februar 2001 abgegeben worden. Darin ist dargelegt, dass eine Urlaubsvertretung in der Altakte des Hilfesuchenden auf das amtsärztliche Gutachten von 1996 gestoßen sei. Aus dem Gutachten und dem Inhalt des Krankenhausberichtes aus dem Jahr 1999 habe gefolgert werden müssen, dass eine akute Gefährdung von Menschenleben vorlag und diese mit dem Hinweis auf Gefahr im Verzug schnellstmöglich zu stoppen sei. Eine vorherige Anhörung, so die Stellungnahme des Sozialamtes, sei wegen der Verzögerung des Verfahrens untunlich gewesen. Der zeitliche Ablauf des Verfahrens lässt jedoch keinesfalls den Schluss zu, dass zum Zeitpunkt der Übermittlung der Sozialdaten vom Sozialamt an die Führerscheinstelle im April des Jahres 2000 besondere Eile geboten war.

Zur Übermittlung der Sozialdaten hat das Sozialamt sich auf § 73 Sozialgesetzbuch X (SGB X) gestützt.

§ 73 SGB X

(1) Eine Übermittlung von Sozialdaten ist zulässig, soweit sie zur Durchführung eines Strafverfahrens wegen eines Verbrechens oder wegen einer sonstigen Straftat von erheblicher Bedeutung erforderlich ist.

(2) Eine Übermittlung von Sozialdaten zur Durchführung eines Strafverfahrens wegen einer anderen Straftat ist zulässig, soweit die Übermittlung auf die in § 72 Abs. 1 Satz 2 genannten Angaben und die Angaben über erbrachte oder demnächst zu erbringende Geldleistungen beschränkt ist.

(3) Die Übermittlung nach den Abs. 1 und 2 ordnet der Richter an.

Der Hilfesuchende habe sich möglicherweise gemäß § 315c Abs. 1 des Strafgesetzbuches (StGB) strafbar gemacht, da er im Straßenverkehr ein Kraftfahrzeug ohne die hierfür erforderliche Eignung führte.

Die Vorschrift des § 73 SGB X kann im vorliegenden Fall jedoch nicht herangezogen werden, da die Übermittlung eine Straftat von erheblicher Bedeutung voraussetzt und zudem der richterlichen Anordnung bedarf. Das Sozialamt hat das zu Unrecht nicht berücksichtigt.
Im Übrigen kann es grundsätzlich nicht Aufgabe eines Sozialamtes sein, die gewonnenen Kenntnisse über einen Leistungsbezieher über die §§ 68 ff. SGB X hinaus an weitere Stellen zu übermitteln.
Die Aufgabenerfüllung eines Sozialamtes ergibt sich insbesondere aus den Bestimmungen im Bundessozialhilfegesetz.

Zukünftig stellt das Sozialamt sicher, dass in gleichgelagerten Fällen Mitteilungen an die Führerscheinstelle erst dann erfolgen, wenn die aktuelle Fahruntüchtigkeit eines Betroffenen feststeht und die Voraussetzungen der Übermittlung nach § 34 StGB vorliegen.

15.6
Datenerhebung der Landesversicherungsanstalt Hessen

Die Landesversicherungsanstalt darf bei der Bearbeitung von Anträgen auf Weiterzahlung der Waisenrente wegen Gebrechlichkeit Informationen über den Gesundheitszustand des Behinderten nur mit seiner Einwilligung erheben.

Nach § 48 Abs. 4 Satz 1 Nr. 2b Sozialgesetzbuch VI (SGB VI) besteht ein Anspruch auf Halb- oder Vollwaisenrente bis zur Vollendung des 27. Lebensjahres, wenn die Waise wegen körperlicher, geistiger oder seelischer Behinderung außer Stande ist, sich selbst zu unterhalten.

Die Mutter eines behinderten Jugendlichen erhielt von der Landesversicherungsanstalt (LVA) knapp drei Monate vor Vollendung des 18. Lebensjahres ihres Sohnes eine Rentenanfrage. Der Anfrage war ein Antragsformular für die Weitergewährung der Waisenrente über die Vollendung des 18. Lebensjahres hinaus beigefügt. Aus dem Antragsvordruck war ersichtlich, dass bei Vorliegen einer Behinderung eine Bescheinigung des behandelnden Arztes vorzulegen ist.

Der daraufhin von der Mutter vorgelegte Bescheid des Amtes für Versorgung und Soziales über die Art der Behinderung ihres Sohnes wurde von der LVA nicht als ausreichend anerkannt. Ihr wurde stattdessen von der Versicherungs- und Rentenabteilung der LVA ein „Ärztlicher Befundbericht zum Rentenantrag“ mit der Bitte übersandt, diesen vom Hausarzt ausfüllen zu lassen und zurückzusenden.

Nach den mir vorliegenden Unterlagen hatten der vom Hausarzt ausgefüllte Befundbericht sowie weitere medizinische Unterlagen der LVA im Januar 2001 vorgelegen. Im Februar 2001 verfügte die LVA, dass die Waisenrente bis zum 31. Dezember 2001 gewährt werde. Eine Begründung für die Befristung der Waisenrente enthält der Bescheid der LVA nicht.

Aufgrund der fehlenden Begründung für die Befristung hat die Mutter des Behinderten bei der LVA fristgerecht Widerspruch eingelegt und gebeten, die Befristung der Waisenrente zu begründen.

Die umfassende Antwort der LVA vom März 2001 an die Widerspruchsführerin ist aus datenschutzrechtlicher Sicht nicht akzeptabel. Die Befristung wurde auf eine von der ärztlichen Untersuchungsstelle Königstein der LVA telefonisch eingeholte Auskunft bei der Wohngruppenleitung der Einrichtung gestützt, in der der Behinderte im letzten Schuljahr der praktisch bildbaren Schule teilnimmt. Die medizinische Beraterin der LVA kam in ihrer Stellungnahme zu dem Ergebnis, dass die derzeitige Einschränkung des Leistungsvermögens des Behinderten nicht länger als drei Jahre andauere und eine weiterreichende Prognose nicht möglich sei.

Die telefonische Datenerhebung der medizinischen Beraterin der LVA über den Zustand des Behinderten fand ohne Wissen und Einwilligung der Mutter, die auch die Betreuerin ihres Sohnes ist, statt. Diese Erhebung wurde maßgeblich für die Entscheidung von der LVA zur Befristung herangezogen. Sie erfolgte ohne Rechtsgrundlage und wurde nicht einmal im Bescheid der LVA erwähnt, obwohl mit ihr weitreichende Konsequenzen verbunden waren.

Auf die Rüge der Mutter des Behinderten zu dem dargestellten Sachverhalt habe ich die LVA um Stellungnahme gebeten. Die LVA hat eingeräumt, dass vom Ärztlichen Dienst übersehen wurde, dass ein Antrag auf Weitergewährung einer Waisenrente gestellt worden war. Im Unterschied zu Anträgen auf erstmalige Rentenbewilligung enthielt das Formular zur Weitergewährung keine Einverständniserklärung. Um zukünftig Verwechslungen zu vermeiden, beabsichtigt die LVA, beim Verband Deutscher Rentenversicherungsträger darauf hinzuwirken, dass auch die Antragsformulare für die Weitergewährung der Waisenrente wegen Gebrechlichkeit durch eine Einverständniserklärung erweitert werden.

Das Widerspruchsverfahren zu dem vorliegenden Sachverhalt war bis Ende Oktober 2001 noch nicht abgeschlossen.

15.7
Verfahren der Unfallkasse Hessen zur Beauftragung eines medizinischen Gutachters

Die Träger der gesetzlichen Unfallversicherung müssen die Betroffenen vor der Erteilung eines Gutachterauftrags auf ihr Widerspruchsrecht hinweisen und sie über den Zweck des Gutachtens informieren.
Ein Versicherter der Unfallkasse Hessen in Frankfurt am Main hat mich nach Eintritt eines Versicherungsfalles um datenschutzrechtliche Prüfung der Bearbeitung seines Leistungsantrags gebeten. Die Unfallkasse Hessen hatte dem Betroffenen einen Widerspruchsbescheid erteilt, ohne ihn am Verfahren zu beteiligen.

In ihrer Stellungnahme teilte die Unfallkasse Hessen mir mit, dass im Verlauf des Widerspruchsverfahrens weitere Ermittlungen zum Sachverhalt unter Beachtung von § 21 Sozialgesetzbuch X (SGB X) nach pflichtgemäßem Ermessen durchgeführt wurden. Dabei habe der Widerspruchsführer auch Kenntnis von einem Gutachterauftrag erhalten, der von der Unfallkasse zur Beurteilung nach Aktenlage veranlasst wurde. Die Unfallkasse räumte ein, dass bei der Vergabe des Gutachtenauftrages die Vorschrift des § 200 Abs. 2 SGB VII außer Acht gelassen wurde, da der Widerspruchsführer auf einen Bescheid drängte. Der Widerspruchsführer habe dem Gutachterauftrag widersprechen können. Eine Anhörung des Widerspruchsführers vor Erteilung des Widerspruchsbescheides habe sich erübrigt, da er durch Telefonate und Schriftverkehr informiert worden sei, dass seinem Widerspruch nicht abgeholfen werde. Die Unfallkasse war daher der Auffassung, dass datenschutzrechtliche Bestimmungen nicht verletzt wurden. Diese Rechtsauffassung ist falsch.

Wie die Unfallkasse selbst zugestanden hat, wurde von ihr die Vorschrift des § 200 Abs. 2 SGB VII außer Acht gelassen.

§ 200 SGB VII

(1) § 76 Abs. 2 Nr. 1 des Zehnten Buches gilt mit der Maßgabe, dass der Unfallversicherungsträger auch auf ein gegenüber einem anderen Sozialleitungsträger bestehendes Widerspruchsrecht hinzuweisen hat, wenn dieser nicht selbst zu einem Hinweis nach § 76 Abs. 2 Nr. 1 des 10. Buches verpflichtet ist.

(2) Vor Erteilung eines Gutachtenauftrages soll der Unfallversicherungsträger dem Versicherten mehrere Gutachter zur Auswahl benennen; der Betroffene ist außerdem auf sein Widerspruchsrecht nach § 76 Abs. 2 des Zehnten Buches hinzuweisen und über den Zweck des Gutachtens zu informieren.

Nach § 200 Abs. 2 SGB VII ist es zwingend erforderlich, dass dem Versicherten vor Erteilung eines Gutachtenauftrages mehrere Gutachter zur Auswahl zu benannt werden. Der Verletzte muss zudem auf sein Widerspruchsrecht hingewiesen werden. Dass der Widerspruchsführer auf Bescheidung drängte, setzt § 200 Abs. 2 SGB VII keinesfalls außer Kraft. Das pflichtgemäße Ermessen, auf das sich die Unfallkasse im Rahmen des § 21 SGB X berufen hat, wird durch die Vorschrift des § 200 Abs. 2 SGB VII bestimmt. Nach der Gesetzesbegründung zu der genannten Vorschrift haben auch die Versicherten das Recht, einen oder mehrere Gutachter vorzuschlagen (BTDrucks. 13/4853, S. 22). Benennt der Versicherte eigene Gutachter, sind diese Vorschläge für den Unfallversicherungsträger allerdings nicht verbindlich.

Die Datenschutzverletzung beruht darauf, dass eine förmliche Anhörung des Betroffenen zu dem von der Unfallkasse eingeholtem Gutachten nicht erfolgte. Jedes Gutachten erhebt und bewertet personenbezogene Informationen. Diese dürfen nicht zum Gegenstand einer Entscheidung gemacht werden, ohne dass dem Verletzten die Möglichkeit zur Gegenäußerung im Anhörungsverfahren gegeben wurde. Die Anhörung erübrigte sich nicht dadurch, dass der Verletzte darüber informiert war, wie er beschieden werden sollte.

Die Unfallkasse wurde darauf hingewiesen, dass die unterbliebene Anhörung nachgeholt und gegebenenfalls der Widerspruchsbescheid neu erlassen werden muss. Meine Kritik an dem Verfahren der Unfallkasse ist auch dem Hessischen Sozialministerium übermittelt worden. Das hat zu einer weiteren Stellungnahme der Unfallkasse an das Sozialministerium geführt. Dort räumt die Unfallkasse ein, dass im Verfahren datenschutzrechtliche Bestimmungen verletzt wurden. Sie versichert, dass die Betroffenen künftig vor Erteilung von Gutachten-aufträgen durch die Unfallkasse auf ihr Widerspruchsrecht hingewiesen werden. Außerdem werden sie über den Zweck des Gutachtens informiert und ihnen sollen in einer bestimmten Reihenfolge mehrere geeignete Gutachter vorgeschlagen werden. Zudem wird zukünftig vermehrt auf die Einschränkung der gesetzlichen Übermittlungsbefugnis bei der Übermittlung von Sozialdaten an einen Gutachter geachtet.

Zum dargestellten Fall ist zur Zeit ein Gerichtsverfahren beim Sozialgericht in Frankfurt am Main anhängig. Ich beabsichtige, die Vorgehensweise der Unfallkasse Hessen in vergleichbaren Fallkonstellationen im ersten Quartal des Jahres 2002 in Frankfurt am Main zu prüfen.

16. Kammern

Datenerhebung und -übermittlung der Industrie- und Handelskammern

Industrie- und Handelskammern können über die im IHK-Gesetz eingeräumten Befugnisse hinaus Daten ihrer Mitglieder erheben. Sie dürfen nicht den Gesamtbestand der Daten, die sie von den Gewerbeüberwachungsbehörden und von den Handelsregistergerichten erhalten, an Wirtschaftsauskunfteien übermitteln.

16.1
Neuorganisation der Stammdatenverarbeitung

Mehrere hessische Industrie- und Handelskammern erwägen, die Verarbeitung der Daten ihrer Mitglieder neu zu organisieren. Die Stammdaten der Kammerzugehörigen erhalten die Industrie- und Handelskammern in erster Linie aus Gewerbeanzeigen, die ihnen die Gewerbeüberwachungsbehörden übermitteln, und aus Mitteilungen der Registergerichte über Eintragungen im Handelsregister. Um Kosten zu sparen und die Datenqualität zu steigern, möchten die Kammern ein privatwirtschaftliches Unternehmen, das hauptsächlich als Wirtschaftsauskunftei tätig ist, mit der Erhebung der Daten aus den Gewerbedateien und Handelsregistern beauftragen. Die Auskunftei würde diese Daten pflegen und durch Daten aus ihrem Bestand ergänzen. Im Gegenzug soll sie die Daten, die sie im Auftrag der Industrie- und Handelskammern von den Gewerbeüberwachungsbehörden und Registergerichten erhält, für eigene Geschäftszwecke verwenden dürfen. Aus datenschutzrechtlichen Gründen lässt sich dieses Datenverarbeitungsvorhaben nur sehr eingeschränkt verwirklichen.

16.2
Gewerbeanzeigen und Handelsregisterdaten

Die Gewerbeüberwachungsbehörden der Kommunen unterrichten die Industrie- und Handelkammern regelmäßig über den Inhalt der eingegangener Gewerbeanzeigen.

Die Mitteilungsformulare fordern
I. Angaben zum Betriebsinhaber und zu den Vertretungsberechtigten:
Im Handelsregister eingetragener Name,
Ort der Eintragung,
Familienname, Vorname, Geburtsname,
Geburtsdatum,
Geburtsort,
Staatsangehörigkeit,
Anschrift der Wohnung;

II. Angaben zum Betrieb:
Zahl der geschäftsführenden Gesellschafter,
vertretungsberechtigte Personen,
Anschrift der Betriebsstätte,
Anschrift der Hauptniederlassung,
Anschrift der früheren Betriebsstätte,
angemeldete Tätigkeit,
Datum des Beginns der angemeldeten Tätigkeit,
Art des angemeldeten Betriebs,
Anzahl der voraussichtlich beschäftigten Arbeitnehmer,
Anmeldung für Haupt-, Zweigniederlassung usw.,
Anmeldung wegen Neuerrichtung oder Übernahme eines Betriebs,
Name des früheren Betriebsinhabers;

III. Angaben über Erlaubnisse:
Erlaubnis für angemeldete Tätigkeit,
Handwerkskarte,
Aufenthaltsgenehmigung,
in der Aufenthaltsgenehmigung enthaltene Auflagen oder Beschränkungen.

Rechtsgrundlage ist § 14 Abs. 5 Satz 1 Nr. 1 Gewerbeordnung (GewO).
Darüber hinaus erhalten die Industrie- und Handelskammern aus dem Handelsregister auf den dort verwendeten Formularen regelmäßig die Angaben zu:
- Name,
- Geschäftsanschrift,
- Firma,
- Sitz,
- Gegenstand,
- Grund- und Stammkapital,
- Vorstand,
- persönlich haftender Gesellschafter,
- Geschäftsführer,
- Abwickler,
- Prokura,

- Rechtsverhältnisse,
- Eintragungstag,
- Bemerkung,
- Gesellschafterliste.

§ 37 der Verfügung über Einrichtung und Führung des Handelsregisters (Handelsregisterverfügung; HRV) verpflichtet die Registergerichte zu diesen Übermittlungen.

16.3
Auftragsdatenverarbeitung

Gegen die im Auftrag der IHK stattfindende Datenerhebung durch eine Wirtschaftsauskunftei bestehen keine rechtlichen Bedenken. Dass es sich um ein privatwirtschaftliches Unternehmen handelt, ist kein Hindernis. Öffentliche Stellen dürfen nicht-öffentliche Stellen nur dann nicht mit der Verarbeitung personenbezogener Daten beauftragen, wenn gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse oder überwiegende schutzwürdige Belange entgegenstehen (§ 4 Abs. 2 Satz 5 Hessisches Datenschutzgesetz [HDSG]). Die Mitgliederdaten der IHK unterliegen keinen besonderen Geheimhaltungsbestimmungen. Es sind auch keine überwiegenden schutzwürdigen Belange der Kammerzugehörigen erkennbar, die eine Beauftragung nicht-öffentlicher Stellen ausschließen würden. Der Auftragnehmer darf die Daten allerdings nur für den Auftraggeber verarbeiten und nicht für eigene Zwecke oder für Dritte nutzen. Er und letztlich der Auftraggeber, die IHK, müssten deshalb sicherstellen, dass die Daten nicht in den Auskunfteibereich gelangen.

16.4
Zusatzerhebungen bei der Auskunftei

Die Wirtschaftsauskunftei soll die von den Gewerbeüberwachungsbehörden und Handelsregistergerichten übermittelten Daten durch folgende Angaben aus ihrem Bestand ohne Einwilligung der Kammerzugehörigen für die Industrie- und Handelskammern ergänzen:
- Kommunikationsdaten (Telefon- und Faxnummern, E-Mail-Adressen),
- Beschäftigtenzahlen,
- Umsatzdaten,
- Tätigkeitsbeschreibungen (Historie),
- Gesellschafternamen,
- Wirtschaftszweigabgrenzung.

Die Kammern erhalten von den Gewerbeüberwachungsbehörden nur die „Anzahl der voraussichtlich beschäftigten Arbeitnehmer". Die Wirtschaftsauskunftei verfügt dagegen über sehr genaue Beschäftigtenzahlen. Die Datenerhebung der Kammern bei der Auskunftei ist mit Ausnahme der E-Mail-Adressen, Beschäftigtenzahlen und Umsatzdaten zulässig.

§ 9 Abs. 1 bis 3 IHKG

(1) Zur Erfüllung der ihnen nach diesem Gesetz übertragenen Aufgaben dürfen die Industrie- und Handelskammern die Daten nach § 14 Abs. 5 Satz 1 Nr. 1 der Gewerbeordnung bei den Kammerzugehörigen erheben, soweit diese Daten ihnen nicht von der zuständigen Behörde übermittelt worden sind. Darüber hinaus dürfen sie Daten über angebotene Waren und Dienstleistungen sowie über die Betriebsgrößenklasse bei den Kammerzugehörigen erheben. Auskunftspflichtig sind der Inhaber und der Leiter des Unternehmens.

(2) Die Industrie- und Handelskammern und ihre Gemeinschaftseinrichtungen, die öffentliche Stellen i. S. d. § 2 Abs. 2 des Bundesdatenschutzgesetzes sind, sind berechtigt, zur Festsetzung der Beiträge der Kammerzugehörigen die in § 3 Abs. 3 genannten Bemessungsgrundlagen bei den Finanzbehörden zu erheben.
(3) Die in den Abs. 1 und 2 genannten Daten dürfen von den Industrie- und Handelskammern gespeichert und genutzt werden, soweit dies zur Erfüllung der ihnen nach diesem Gesetz übertragenen Aufgaben erforderlich ist. Andere als die in Satz 1 genannten Daten dürfen sie nur erheben, verarbeiten und nutzen, soweit andere Rechtsvorschriften dies zulassen.

§ 9 Abs. 1 IHKG bietet keine Rechtsgrundlage für die geplante Datenerhebung. Die Vorschrift regelt lediglich Datenerhebungen bei den Betroffenen. Eine Datenerhebung bei sonstigen Stellen - dies ist eine Auskunftei - sieht die Ermächtigung nicht vor.

Als Rechtsgrundlage kommen somit nur §§ 11 Abs. 1, 12 HDSG in Betracht. Das IHKG regelt die zulässige Datenerhebung der Kammern nicht abschließend. Das ergibt sich aus § 9 Abs. 3 Satz 2 IHKG, wonach die Kammern andere als die in § 9 Abs. 1 und 2 genannten Daten nur erheben dürfen, soweit andere Rechtsvorschriften dies zulassen. Zu den „anderen Rechtsvorschriften" zählen nicht nur bereichsspezifische Regelungen. Das IHKG regelt Erhebungstatbestände, die wegen der angeordneten Auskunftspflicht der Betroffenen (§ 9 Abs. 1) oder wegen der Sensitivität der Steuerdaten (§ 9 Abs. 2)

eine besondere gesetzliche Regelung erfordern. Das lässt Raum für einen Rückgriff auf die Verarbeitungsbefugnisse der allgemeinen Landesdatenschutzgesetze.

Das HDSG erlaubt Datenerhebungen bei Dritten außerhalb des öffentlichen Bereichs nur, wenn der Schutz von Leben und Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen dies im Einzelfall gebieten, eine Rechtsvorschrift dies vorsieht oder, soweit es sich um eine Rechtsvorschrift des Bundes handelt, zwingend voraussetzt (§ 12 Abs. 3 HDSG). Die beabsichtigte Datenerhebung erfüllt keine dieser Anforderungen.

Bis auf die E-Mail-Adressen, Beschäftigtenzahlen und Umsatzdaten sind alle übrigen Daten in allgemein zugänglichen Quellen gespeichert. Die Telefon- und Faxnummern können den gedruckten oder elektronischen öffentlichen Kundenverzeichnissen der Anbieter von Telekommunikationsdiensten entnommen werden, die Tätigkeitsbeschreibungen, Gesellschafternamen und Wirtschaftsabgrenzung dem Handelsregister. Beides sind allgemein zugängliche Quellen, sodass für die Erhebung der Daten die Einschränkungen des § 12 Abs. 3 HDSG nicht gelten (§ 3 Abs. 4 HDSG). Dagegen benötigen die Kammern für die Erhebung der E-Mail-Adressen, Beschäftigtenzahlen und Umsatzdaten die Einwilligung der Kammerzugehörigen.

Die Anwendbarkeit des Hessischen Datenschutzgesetzes ist allerdings nur solange ausgeschlossen, wie die Daten in allgemein zugänglichen Quellen gespeichert sind. Werden sie öffentlich zugänglichen Dateien entnommen und separat gespeichert, muss die Speicherung die Zulässigkeitsanforderungen des HDSG erfüllen. Lediglich für Daten, die von den Betroffenen zur Veröffentlichung bestimmt sind, gilt das HDSG auch dann nicht, wenn die Daten aus der allgemein zugänglichen Quelle entnommen und getrennt gespeichert worden sind. Das sind hier die Telefon- und Faxnummern. Für alle übrigen Daten ist zu prüfen, ob sie gemäß § 11 Abs. 1 Satz 1 HDSG für die Aufgabenerfüllung der Industrie- und Handelskammern erforderlich sind. Für Telefon- und Faxnummern, Beschäftigtenzahlen, Tätigkeitsbeschreibungen und Gesellschafternamen hat dies der Bundesgesetzgeber durch die Erhebungsbefugnis in § 9 Abs. 1 IHKG bejaht.

16.5
Datenübermittlungen an die Auskunftei

Aus dem Datensatz, welchen die Industrie- und Handelskammern von den Gewerbeüberwachungsbehörden und Handelsregistergerichten erhalten, darf die Auskunftei nur die Namen, betriebliche Anschrift und angezeigte Tätigkeit für eigene Geschäftszwecke ohne Einwilligung der Kammerzugehörigen verwenden. Datenschutzrechtlich handelt sich um Datenübermittlungen an eine nicht-öffentliche Stelle. Im Rahmen einer Auftragsdatenverarbeitung dürfen die Industrie- und Handelskammern den Gesamtdatenbestand, den ihnen die Gewerbeüberwachungsbehörden und die Amtsgerichte übermittelt haben, an die Wirtschaftsauskunftei überlassen; eine Übermittlung zu eigenen Geschäftszwecken der Wirtschaftsauskunftei ist hingegen nicht zulässig. Sie dürfen zwar gemäß § 9 Abs. 4 Satz 1 IHKG zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken Namen, Firma, Anschrift und Wirtschaftszweig ihrer Kammerzugehörigen ohne deren Einwilligung und ggf. auch gegen den Willen der Betroffenen an nicht-öffentliche Stellen übermitteln.

§ 9 Abs. 4 IHKG

Die Industrie- und Handelskammern dürfen Name, Firma, Anschrift und Wirtschaftszweig ihrer Kammerzugehörigen zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken an nicht-öffentliche Stellen übermitteln. Die übrigen in Abs. 1 genannten Daten dürfen zu den in Satz 1 genannten Zwecken an nicht-öffentliche Stellen übermittelt werden, sofern der Kammerzugehörige nicht widersprochen hat. Auf die Möglichkeit, der Übermittlung der Daten an nicht-öffentliche Stellen zu widersprechen, sind die Kammerzugehörigen vor der ersten Übermittlung schriftlich hinzuweisen.

Zu denselben Zwecken dürfen sie außerdem die übrigen Daten aus den Gewerbeanzeigen an nicht-öffentliche Stellen übermitteln, sofern die Kammerzugehörigen nicht widersprochen haben (§ 9 Abs. 4 Satz 2 IHKG). Da Wirtschaftsauskunfteien besonders bei der Anbahnung von Geschäftsbeziehungen eine bedeutende Rolle spielen, halten sich die Datenübermittlungen im Rahmen der Zweckbestimmung des IHKG.

§ 9 Abs. 4 Satz 1 und 2 IHKG differenziert nicht zwischen Einzelübermittlungen, Gruppenauskünften oder Übermittlung des Gesamtdatenbestandes. Dennoch ist diese Unterscheidung für die Zulässigkeit der Übermittlung von Bedeutung. Die Gewerbeüberwachungsbehörde, die der IHK die Daten liefert, darf gem. § 14 Abs. 8 GewO an nicht-öffentliche Stellen, soweit sie ein berechtigtes Interesse glaubhaft gemacht haben, aus den Gewerbeanzeigen die drei Grunddaten Name, betriebliche Anschrift und angezeigte Tätigkeit übermitteln. Andere Daten darf sie an nicht-öffentliche Stellen nur übermitteln, wenn diese ein rechtliches Interesse glaubhaft dargelegt haben und kein Grund zu der Annahme besteht, dass überwiegende schutzwürdige Interessen des Gewerbetreibenden einer Übermittlung entgegenstehen. Das Hessische Wirtschaftsministerium weist in Nr. 6.3.3 der Verwaltungsvorschrift zum Vollzug der §§ 14, 15 und 55c der Gewerbeordnung (GewAnzVwV) vom 15. Oktober 1995 (StAnz. 1995 S. 3482) zu Recht darauf hin, dass - beschränkt auf die drei Grunddaten - Einzel- wie Gruppenauskünfte an Markt- und Meinungsforschungsinstitute und Handelsauskunfteien erteilt werden können. Auch wenn in der Verwaltungsvorschrift nicht ausdrücklich erwähnt, spricht außerdem nichts gegen eine Übermittlung des Gesamtbestandes

der drei Grunddaten. Da vor der Übermittlung der übrigen Daten aus den Gewerbeanzeigen zu prüfen ist, ob der Empfänger ein rechtliches Interesse glaubhaft dargelegt hat und keine überwiegenden schutzwürdigen Interessen der Gewerbetreibenden bestehen, kommen hier nur Einzelauskünfte und keine Gruppenauskünfte oder Übermittlungen des Gesamtbestandes in Frage. Der Gesetzgeber wollte mit der Regelung des § 14 Abs. 8 GewO ausschließen, dass neben den Gewerbedateien der Kommunen private Gewerberegister entstehen. Der Schutzzweck der Norm würde unterlaufen, könnten sich Marktforschungsinstitute oder Auskunfteien die Daten, die ihnen die Gewerbeüberwachungsbehörden nicht liefern dürfen, über die Industrie- und Handelskammer besorgen. Bei der Auslegung der Übermittlungsvorschrift des § 9 Abs. 4 IHKG ist daher das gesetzliche Schutzniveau, das für die Datenquelle (Gewerbedatei) gilt, zu berücksichtigen.

Die Handelsregisterdaten, die der IHK von den Registergerichten gem. § 37 HRV übermittelt werden, darf die IHK ebenfalls nicht als Gesamtdatenbestand an die Wirtschaftsauskunftei weiter übermitteln, denn auch in diesem Fall sind die Schutzvorschriften zu beachten, die der Gesetzgeber für die Herkunftsdateien erlassen hat. An sich sieht § 9 Handelsgesetzbuch (HGB) Datenübermittlungen aus dem Handelsregister ohne Nachweis berechtigter Interessen vor. Das Register steht jedermann zur Einsicht offen. Der BGH hat allerdings die datenschutzrechtlich begründete Weigerung der Justizverwaltung, den gesamten Bestand des Handelsregisters zu gewerblichen Zwecken zur Verfügung zu stellen, als ermessensfehlerfreie Anwendung des § 9 HGB gewertet (BGH, Beschluss vom 12. Juli 1989, NJW 1989, 2818 ff.). Die Übermittlung des Gesamtdatenbestandes und anschließende Aktualisierung käme einem automatisierten Abrufverfahren gleich. Dieses ist jedoch nur auf Einzelabrufe beschränkt. Die Landesjustizverwaltung darf die Einrichtung eines Verfahrens, mit dem nichtöffentliche Stellen automatisiert aus dem Handelsregister Daten Abrufen können, nur genehmigen, soweit der Abruf von Daten zur Wahrnehmung eines berechtigten beruflichen oder gewerblichen Interesses des Empfängers erfolgt und kein Grund zu der Annahme besteht, dass die Daten zu anderen als zu den vom Empfänger dargelegten Zwecken abgerufen werden (§ 9a Abs. 2 Nr. 2 HGB). In § 9a Abs. 7 HGB schließt der Gesetzgeber einen unkontrollierbaren Zugriff auf Handelsregisterdaten ausdrücklich aus. Die Vorschrift regelt zwar nur Abrufe aus dem Handelsregister, ihr Schutzzweck würde jedoch unterlaufen, wenn die IHK nicht an dieselben Restriktionen wie das Registergericht gebunden wäre. Damit ist eine Übermittlung des Gesamtbestandes nicht vereinbar.

17. Ausländerrecht

Prüfung der Ausländerbehörden in Offenbach

Bei der Fortsetzung meiner Prüfserie bei Ausländerbehörden bezüglich der Rechtmäßigkeit von Ausschreibungen zur Einreiseverweigerung in das Schengengebiet habe ich erneut zahlreiche fehlerhafte Datenspeicherungen festgestellt.

Die Prüfung der Rechtmäßigkeit von Personenausschreibungen im Schengener Informationssystem (SIS) durch acht Ausländerbehörden (29. Tätigkeitsbericht, Ziff. 12.1) wurde im Berichtszeitraum noch bei den Ausländerbehörden des Landkreises Offenbach und des Oberbürgermeisters der Stadt Offenbach fortgesetzt.

Bei der Ausländerbehörde des Landkreises Offenbach wurden stichprobenweise 86 Ausschreibungen im Schengener Informationssystem überprüft. Nur in 34 Fällen war die Datenspeicherung nicht zu beanstanden, d.h. weit über die Hälfte wies rechtliche Fehler auf. Überwiegend habe ich dieselben Fehler festgestellt, die im letzten Tätigkeitsbericht ausführlich beschrieben wurden: Zum einen fehlt es an der Voraussetzung, dass der Betroffene ausgewiesen, abgeschoben oder zurückgewiesen wurde. Zum anderen unterbleibt die Prüfung der Erforderlichkeit der weiteren Datenspeicherung nach drei Jahren.

In neun Fällen war die Ausschreibung unzulässig, weil es sich um Bürgerinnen und Bürger der Europäischen Gemeinschaft handelte. Eine Ausschreibung zur Einreiseverweigerung in das Schengengebiet kommt nur bei Personen in Betracht, die keinem Schengenstaat angehören.

Der Landrat des Landkreises Offenbach hat zugesagt alle 52 fehlerhaften Datenspeicherungen zu korrigieren. Außerdem hat er auf Verlangen veranlasst, den Gesamtbestand der SIS-Ausschreibungen zu überprüfen.

Bei der Ausländerbehörde des Oberbürgermeisters der Stadt Offenbach wurden 89 Ausschreibungen im Schengener Informationssystem überprüft. Acht Ausschreibungen waren fehlerhaft; sie wurden gelöscht. In elf Fällen fehlte die Prüfung der Rechtmäßigkeit der Datenspeicherung nach Ablauf der Dreijahresfrist. Sie wurde nachgeholt. Veraltete Formulare wurden aktualisiert und alle betroffenen Mitarbeiter wurden - wie übrigens auch beim Landkreis - auf die strikte Einhaltung der Ausschreibungskriterien und die besondere Sorgfaltspflicht bei der Veranlassung von Fahndungsnotizen hingewiesen.

18. Kommunen

Werbe-Mail mit vielen Adressen Dritter

Der Einsatz neuer Techniken kann trotz vorheriger Probeläufe zu erheblichen Verstößen gegen Datenschutzbestimmungen führen.

Nachdem ein Bürger Anfang des Jahres Prospektmaterial bei einem hessischen Fremdenverkehrsamt bestellt hatte, erhielt er im Sommer eine Werbe-Mail dieses Fremdenverkehrsamtes. Das Reklamematerial selbst war unleserlich, dafür konnte der Bürger aber die Adresse von über 1.500 Empfängern erkennen, die die als Rundbrief versandte Mail ebenfalls erhalten hatten. Da er in der Weitergabe seiner Adresse an Dritte eine Verletzung seiner Datenschutzrechte sah, bat er mich, in dieser Angelegenheit tätig zu werden.

Die Rückfrage beim Leiter des Fremdenverkehrsamtes ergab, dass die E-Mail-Adressen aller Personen gespeichert wurden, die über die Homepage Informationsmaterial bestellt hatten. Diese Adressensammlung wurde dann benutzt, um später weiteres Informationsmaterial zu verschicken. Trotz eines erfolgreichen hausinternen Probelaufs kam es bei der Verarbeitung der gesammelten E-Mail-Adressen zu Fehlern. Einige Adressaten erhielten die Mail in der vorgesehenen Form, andere bekamen statt des vorgesehenen Werbematerials die fehlerhafte Mail mit fremden Adressen.

Als Konsequenz hat das Fremdenverkehrsamt alle gesammelten E-Mail-Adressen gelöscht. Darüber hinaus werden künftig Adressen nur noch gespeichert, wenn Anfragende dies ausdrücklich wünschen. Sie müssen ankreuzen, dass sie an der regelmäßigen Zusendung von Informationsmaterial interessiert sind. Außerdem werden weitere Werbeaktionen erst nach einer Klärung des aufgetretenen Fehlers stattfinden.
Eine Überprüfung der Homepage hat ergeben, dass die Gemeinde diese datenschutzgerecht umgestaltet hat.

19. Personalwesen

19.1
Evaluation der Lehre

Eine Evaluation der Lehre darf nur mit Kenntnis der Betroffenen und nach fachlichen Kriterien erfolgen. Sie stellt eine dienstliche Bewertung der gezeigten Leistungen dar. Eine personenbezogene Veröffentlichung der Ergebnisse ist nicht zulässig.

Nachdem ich bereits in meinem letzten Tätigkeitsbericht (Ziff. 16.2) die Evaluation aus datenschutzrechtlicher Sicht angesprochen hatte, bin ich in der Folgezeit erneut mehrfach mit diesem Thema befasst gewesen.

19.1.1
Das Recht auf informationelle Selbstbestimmung

Auch die Lehre an den Hochschulen und deren Evaluation sind datenschutzrechtlich zu schützen.
Bei der Evaluation treffen Amtsfunktionen auf grundrechtliche Gewährleistungen des eingesetzten Lehrpersonals. Bedienstete wie Lehrbeauftragte sind - sofern nicht reine Amtsfunktionen betroffen sind - als Privatpersonen Grundrechtsträger. Dies ist der Hintergrund für die traditionelle Differenzierung, bei Bediensteten des Staates zu unterscheiden, ob sie auch als Privatpersonen betroffen sind (dann Grundrechtsschutz) oder ausschließlich als staatliche Funktionsträger (dann kein Grundrechtsschutz). Bei Hochschullehrern könnte erwogen werden, sie seien bei Lehrveranstaltungen ausschließlich als Amtswalter in Ausübung des Amtes tätig und in diesem Kontext weder datenschutzrechtlich noch grundrechtsgeschützt. Der hessische Landesgesetzgeber hat diesen Aspekt im Archivrecht prägnant aufgenommen, indem er „Amtsträger in Ausübung ihrer Ämter“ von den archivrechtlichen Schutzfristen ausklammert (§ 15 Abs. 2 Hessisches Archivgesetz).

Eine solche Annahme verkürzt die Frage unzulässig. Bei Hochschullehrern kann die gemäß Art. 5 Abs. 3 Grundgesetz (GG) grundrechtlich bewehrte Sphäre von dem grundrechtlich nicht erfassten Bereich der Amtswalterfunktion nicht getrennt werden. Diese Schwierigkeit spiegelt sich beispielhaft in der Gesetzgebungsgeschichte des beamtenrechtlichen Personalaktenrechts wider. Die Frage, ob und inwieweit die im Volkszählungsurteil entwickelten Grundsätze im öffentlichen Dienstrecht überhaupt anwendbar sind, ist seinerzeit explizit aufgeworfen worden. Der Gesetzgeber hat sich dafür entschieden, das Personalaktenrecht „ungeachtet“ dieser Frage neu zu regeln (BRDrucks. 223/90). Die Frage, wie weit der grundrechtliche Schutz bei dienstrechtlichen Wahrnehmungen reicht, ist in der Novellierung dahin entschieden worden, das Persönlichkeitsrecht der Bediensteten zu stärken. Die Rechtsprechung des Bundesverfassungsgerichts, wonach im Zweifel Grundrechte so zu interpretieren sind, dass sie größtmögliche Wirkungskraft entfalten können, wirkt als eine Art „Kompass“, dessen Zeiger in Richtung Datenschutzfreundlichkeit weist. Aus dieser Perspektive sind die beiden Vorschriften im Hessischen Hochschulrecht, die sich mit der Evaluation befassen, datenschutzrechtlich zu deuten.

19.1.2
Die Evaluation im Hessischen Hochschulrecht

In § 3 Hessisches Hochschulgesetz (HHG) liegt die Grundsatznorm für die Evaluation.

§ 3 Abs. 8 HHG

Die Leistungen der Hochschulen in Forschung und Lehre, bei der Förderung des wissenschaftlichen Nachwuchses sowie bei der Durchsetzung der Gleichberechtigung von Frauen und Männern sollen regelmäßig bewertet und die Ergebnisse veröffentlicht werden. Das Präsidium regelt durch Satzung, welche personenbezogenen Daten zu diesem Zweck erhoben, verarbeitet und in welcher Form veröffentlicht werden können.

§ 92 betrifft die Berichtspflicht und Qualitätssicherung. Er lautet wie folgt:

§ 92 HHG

(1) Die Hochschulen berichten regelmäßig über ihre Tätigkeit insbesondere in Forschung und Lehre, bei der Förderung des wissenschaftlichen Nachwuchses sowie der Erfüllung des Gleichstellungsauftrags. Sie berichten über die dabei erbrachten Leistungen und über die Wirtschaftlichkeit und Angemessenheit des Mitteleinsatzes.

(2) Die erbrachten Leistungen sind durch Verfahren der Leistungsbewertung (**Evaluation**) in regelmäßigen Abständen zu überprüfen; bei der Festlegung der Verfahren zur Bewertung der Qualität der Lehre sind die Studierenden zu beteiligen. Die Ergebnisse der Evaluation sind bei den Strukturplänen und den Zielvereinbarungen zu berücksichtigen.

(3) Zur Sicherung der hochschulübergreifenden Vergleichbarkeit der Evaluation legen die Hochschulen im Benehmen mit dem Ministerium hierzu geeignete Kennzahlen und Verfahren fest.

Die Bewertung von Vorlesungen, auch durch die Studenten, hat nach fachlichen Kriterien zu erfolgen. Geschieht das, so stellen die Tatsache der Evaluation und die dadurch ermöglichten Leistungsbewertungen keinen Eingriff in das Recht auf informationelle Selbstbestimmung der Hochschullehrer dar. Deswegen ist eine Evaluation ihrer dienstlichen Leistung auch durch Studenten zulässig, und zwar ohne die Einwilligung der Hochschullehrer. Die Erhebung muss stets mit ihrer Kenntnis erfolgen (§ 12 Abs. 1 Satz 1 HDSG). Dabei ist voraus zu setzen, dass die Art der Bewertung nach vorher festgelegten sachlichen Kriterien erfolgt, die dem Anspruch der Vergleichbarkeit und der Justiziabilität genügen.

Aus der Sicht des Datenschutzes ist der letzte Satz des § 3 Abs. 8 HHG von besonderer Bedeutung; die Satzung muss vorsehen, dass „personenbezogene Daten“ nur veröffentlicht werden, wenn die Betroffenen zugestimmt haben oder keinen Schutzanspruch genießen.

§ 3 Abs. 8 HHG sieht vor, dass die personenbezogenen Daten der Hochschullehrer, die im Rahmen der Bewertung anfallen, verarbeitet und veröffentlicht werden. Bei den Verarbeitungen ist zu berücksichtigen, dass die Evaluation ein besonderes Verfahren der Leistungsbewertung darstellt. Da die Dokumentation von dienstlichen Beurteilungen im allgemeinen Personalaktenrecht datenschutzrechtlich geschützt ist, muss das auch für Evaluationen gelten.

Die in § 3 Abs. 8 Satz 2 HHG angesprochene Satzung darf deswegen nur Regelungen treffen, die mit den grundrechtlichen Vorgaben vereinbar sind. Die Evaluation dient der Optimierung der Hochschullehre und -forschung. Sie ist daher auf die dienstlichen Leistungen und ihre Verbesserung ausgerichtet. Vorgesetzte und für die Forschung und Lehre zur Dienstaufsicht berufene Institutionen sind daher die bestimmungsmäßigen Adressaten der Evaluationsergebnisse. Eine personenbezogene Veröffentlichung von Evaluationsergebnissen ist dafür weder erforderlich noch - insbesondere bei negativen Feststellungen - zumutbar. Als besondere Form der dienstlichen Bewertung muss sie datenschutzrechtlich wie diese behandelt werden. Öffentlich „an den Pranger“ gestellt zu werden, braucht sich kein Amtswalter gefallen zu lassen.

Vorgesehene Veröffentlichungen der Hochschulen erreichen ihren Zweck auch dann, wenn sie in pseudonymisierter Form erfolgen. Durch Bildung von Querschnittswerten können sie aus dem Personenbezug gelöst werden, ohne an Aussagekraft zu verlieren. Personenbezogene Ergebnisse können zu den Personalakten genommen und zum Anlass dienstaufsichtlicher Gespräche genommen werden. Sie können auch in nicht-öffentlichen Sitzungen der Dienstaufsicht Führenden (Präsidium, Dekan) verhandelt werden, soweit die dienstliche Geheimhaltung sicher gestellt ist. Nicht-öffentliche Sitzungen dürfen sich mit personenbezogenen Daten allerdings nur befassen, soweit sie der Vorbereitung personenbezogener dienstrechtlicher Folgerungen dienen, bspw. Umorganisation des Lehrbetriebes, Mittelverteilung für aufwendige Lehrformen. Die dargestellten Einschränkungen bei der Verarbeitung und Veröffentlichung von personenbezogenen Daten sind rechtsförmlich durch Satzung festzulegen. Die Präsidien der Hochschulen haben bei den vorgesehenen Satzungen auf die datenschutzrechtlichen Erfordernisse Rücksicht zu nehmen.

Da es sich um Vorschriften handelt, die generell gelten, sind sie mit dem Hessischen Datenschutzbeauftragten gem. Art. 28 Abs. 2 der Europäischen Datenschutzrichtlinie abzustimmen.

Ich habe die hessischen Hochschulen gebeten, mir ihre Satzungsentwürfe zuzusenden, um sie datenschutzrechtlich würdigen zu können. Das steht noch aus.

19.2
Personaldatenverarbeitung in der Hessischen Versorgungsverwaltung

Sozialleistungsträger haben dafür Sorge zu tragen, dass Gesundheitsdaten schwerbehinderter Mitarbeiterinnen und Mitarbeiter nur dann in das behördeneigene DV-System eingestellt werden, wenn der Zugriff auf die zuständigen Sachbearbeiterinnen und Sachbearbeiter beschränkt wird.

Mehr als sechs Jahre ist erfolglos versucht worden, ein EDV-Verfahren zur Durchführung des Feststellungsverfahrens einer Behinderung (jetzt: § 69 des Sozialgesetzbuches [SGB] IX (Rehabilitation und Teilhabe behinderter Menschen) in der Hessischen Versorgungsverwaltung einzuführen. Nunmehr ist ein in Schleswig-Holstein entwickeltes System übernommen worden. Unter datenschutzrechtlichen Gesichtspunkten ist das misslungen. Die Umsetzung des Verfahrens hat zum gravierendsten Verstoß gegen das Persönlichkeitsrecht geführt, der während des ganzen Jahres bekannt geworden ist.

Am 19. November 2001 wurde ich telefonisch aus dem Mitarbeiterkreis des Hessischen Amtes für Versorgung und Soziales in Darmstadt darüber informiert, dass ein Katalog personenbezogener Daten aller bei der Hessischen Versorgungsverwaltung beschäftigten Schwerbehinderten im System offen eingestellt sei. Zu dem Datenkatalog gehören auch die Diagnosen, die der Schwerbehinderteneigenschaft zugrunde liegen, und die mit der Schwerbehinderteneigenschaft verbundenen Vergünstigungen, soweit sie im Schwerbehindertenausweis dokumentiert sind.

Nicht genug damit. Der komplette Bestand aller Schwerbehindertendaten aus ganz Hessen ist für jeden Benutzer des EDV-Verfahrens sichtbar. Alle Hessischen Ämter für Versorgung und Soziales - Darmstadt, Frankfurt am Main, Fulda, Gießen, Kassel und Wiesbaden - haben Zugriff auf den gesamten Datenbestand. Konkret bedeutet dies, dass etwa die Daten eines schwerbehinderten Amtsangehörigen aus Darmstadt in den fünf weiteren Hessischen Ämtern für Versorgung und Soziales zur Einsicht offen stehen.

Nach der Rüge aus Darmstadt wurde kurzfristig beim Amt für Versorgung und Soziales in Wiesbaden ein Besuchstermin für den 20. November 2001 vereinbart. Das führte dazu, dass die beanstandeten Mitarbeiterdaten in der Nacht vom 19. November auf den 20. November aus dem allgemeinen Zugriff herausgenommen wurden und ab dem 20. November nur noch den Sachbearbeiterinnen und Sachbearbeitern zur Verfügung stehen, die die Schwerbehinderteneigenschaft der Amtsangehörigen festzustellen haben. Diese Beschränkung des Zugriffs wurde anhand von probeweisen Zugriffen auf die entsprechenden Masken an einem EDV-Arbeitsplatz überprüft und bestätigt. Inzwischen hat mir auch der Bezirksvertrauensmann der Schwerbehinderten beim Hessischen Landesamt für Versorgung und Soziales mitgeteilt, dass in allen Hessischen Ämtern für Versorgung und Soziales die Zugriffsmöglichkeiten auf die Gesundheitsdaten der schwerbehinderten Amtsangehörigen abgestellt wurden.

Mit dem Wiesbadener Amt für Versorgung und Soziales wurde Einvernehmen erzielt, dass die Gesundheitsdaten der Amtsangehörigen zum Schutz der Privatsphäre besonders zu schützen sind. Das folgt aus § 35 Abs. 1 Satz 3 SGB I. Hiernach dürfen Sozialdaten der Beschäftigten und ihrer Angehörigen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten weitergegeben werden. Satz 2 der genannten Vorschrift beinhaltet zudem die Verpflichtung eines Sozialleistungsträgers sicherzustellen, dass Sozialdaten nur Befugten zugänglich sind und nur an diese weitergegeben werden. Hinzu kommt in beamtenrechtlicher Hinsicht, dass Personaldaten i. S. v. § 107a des Hessischen Beamtengesetzes (HBG) vorliegen. Sie sind unter besonderem Verschluss zu halten und keinesfalls offen ins Behördennetz einzustellen. Nach § 34 Abs. 1 Hessisches Datenschutzgesetz (HDSG) gelten diese Rechte für alle Arbeitnehmer im öffentlichen Dienst und nicht nur für die Beamten.

Was für die Daten der Bediensteten gilt, muss auch für die sonstigen Behinderten durchgesetzt werden. Das bisherige Verfahren, nach dem in der Hessischen Versorgungsverwaltung der gesamte Schwerbehindertendatenbestand ohne Einschränkung in allen Ämtern zur Verfügung steht, ist nicht länger hinzunehmen. Es sind technische und ggf. auch organisatorische Maßnahmen zu treffen, durch die eine Abschottung der Datenbestände auf die jeweils regional zuständigen Ämter für Versorgung und Soziales und dort auf die jeweils zuständigen Sachbearbeiterinnen und Sachbearbeiter sichergestellt wird. Das muss unverzüglich erfolgen. Das Sozialministerium ist um kurzfristige Neuregelung gebeten worden. In welchem Zeitrahmen die erforderliche Trennung des Gesamtdatenbestandes erfolgen kann, ist gegenwärtig noch nicht abzusehen. Unterlagen zum Betrieb und zur Funktion des Verfahrens lagen mir bis Mitte Dezember 2001 noch nicht vor. Die für meine sachgerechte Beurteilung erforderlichen Unterlagen habe ich bereits im November beim Hessischen Sozialministerium angefordert.

Sobald die Unterlagen vorliegen, wird das Verfahren von mir noch einer eingehenden Prüfung unterzogen.

20. Europa

Schengener Durchführungsübereinkommen

Auch im vergangenen Jahr nahm Hessen - vertreten durch eine meiner Mitarbeiterinnen - zugleich für die anderen Landesdatenschutzbeauftragten an verschiedenen Sitzungen der Gemeinsamen Kontrollinstanz für das Schengener Informationssystem in Brüssel teil.

20.1
Einrichtung einer gemeinsamen Geschäftsstelle für Schengen und Europol

Im letzten Tätigkeitsbericht (Ziff. 19.1) hatte ich von den Anstrengungen der Gemeinsamen Kontrollinstanz berichtet, eine eigene Geschäftsstelle zu erhalten, die aus der Hierarchie des Generalsekretariats der Europäischen Union ausgegliedert und weisungsfrei gestellt wird. Dies wurde im Laufe des Jahres erreicht. Für Schengen, Europol und das Zollinformations-system (dessen Kontrollinstanz erst im Aufbau ist) gibt es jetzt eine gemeinsame Geschäftsstelle. Seit 15. September d.J. ist ein von den beiden bestehenden Kontrollinstanzen berufener Leiter der Geschäftsstelle als sog. Datenschutzsekretär im Amt. Es handelt sich dabei um den bisherigen Delegierten der Niederlande in der Gemeinsamen Kontrollinstanz. Ob die bisher zugebilligten zwei Mitarbeiter(innen) ausreichen, wird sich erweisen.

20.2
Erneuerung des Schengener Informationssystems

Im 28. Tätigkeitsbericht (Ziff. 4.2) hatte ich berichtet, dass im Rahmen des sog. SIS II verschiedene Änderungen des Schengener Informationssystems geplant sind. Die Gemeinsame Kontrollinstanz hat sich hierüber von einem Vertreter des juristischen Dienstes und dem zuständigen Vertreter des Generalsekretariats informieren lassen. Danach werden eine Reihe neuer Leistungsmerkmale für das Schengener Informationssystem in der Ratsgruppe SIS diskutiert. Datenschutzrechtlich relevant sind u.a. folgende Vorschläge:

- Verlängerung der Speicherungsfrist für verschiedene Ausschreibungskategorien, u.a. von zur Einreiseverweigerung ausgeschriebenen Drittausländern nach Art. 96 Schengener Durchführungsübereinkommen (SDÜ) (Änderung der Art. 112 Abs. 1, 113 SDÜ).

- Aufnahme von erkennungsdienstlichen Angaben (Lichtbilder und Fingerabdrücke) in die Ausschreibungen von Personen. Angesprochen wurde in diesem Zusammenhang auch die Einstellung von DNA-Profilen (Änderung des Art. 94 Abs 3 SDÜ).

- Erweiterung des Zugriffs auf das Schengener Informationssystem beispielsweise durch Europol, Schutzeinrichtungen der Kreditwirtschaft (SCHUFA), Rechtsanwälte und Notare, Kfz-Registerbehörden (Änderung des Art. 101 SDÜ). Art. 101 sieht bislang eine Zugriffsberechtigung nur für wenige im Einzelnen bestimmte Stellen vor.

Die Gemeinsame Kontrollinstanz hat weitere schriftliche Informationen angefordert und wird sich zu den Vorschlägen äußern.

20.3
Geltendmachung des Auskunftsrechts

Wie schon berichtet, ist die Zahl der Anträge auf Auskunft über die zu einer Person im Schengener Informationssystem gespeicherten Daten in den einzelnen Schengenstaaten sehr unterschiedlich. Deshalb hat die Gemeinsame Kontrollinstanz eine Umfrage in den Schengenstaaten durchgeführt, um zu erfahren, ob und welche Schritte unternommen wurden, die Bürger über ihre Rechte zu informieren (29. Tätigkeitsbericht, Ziff. 19.3.2). Während Deutschland die in diesem Zusammenhang erstellten Faltblätter mit Informationen über die Rechte der Betroffenen relativ rasch an die entsprechenden Stellen verteilt hat, haben die zuständigen französischen, niederländischen und luxemburgischen Behörden nicht einmal die Mittel für diese Informationskampagne bereit gestellt.

Zur Unterstützung hat die Gemeinsame Kontrollinstanz einen „Leitfaden über das Auskunftsrecht und die Zusammenarbeit zwischen den nationalen Kontrollinstanzen“ erstellt. Hier werden Einzelheiten zum Auskunftsrecht beschrieben. Beispielsweise gibt es eine Darstellung der Rechtslage in jedem einzelnen Schengenstaat. Das Auskunftsrecht richtet sich nach dem nationalen Recht der Vertragspartei, in deren Hoheitsgebiet das Auskunftsrecht beansprucht wird (Art. 109 Abs. 1 SDÜ).

Der Leitfaden ist in erster Linie für Personen bestimmt, die beruflich mit dem Auskunftsrecht zu tun haben, soll aber auch allen anderen Bürgerinnen und Bürgern, die sich für diese Fragen interessieren, als praktisches Hilfsmittel dienen.

20.4
Kontrolle des zentralen Teils des Schengener Informationssystems (CSIS)

Derzeit wird eine erneute Kontrolle durch ein Expertenteam vorbereitet. Sie erfolgt an Hand des Fragebogens, der bereits für die letzte Kontrolle des CSIS in Straßburg und seitdem auch von Europol verwendet wurde.

21. Archive

Weitergabe von archivierten Holocaust-Unterlagen an Drittländer

Die Förderung der internationalen Holocaust-Dokumentation rechtfertigt eine Änderung des Archivgesetzes, um die Verfilmung und Weitergabe von archivierten, personenbezogenen Holocaust-Unterlagen in Drittländer zu ermöglichen.

Schon im Jahre 2000 waren die Gedenkstätte Yad Vashem, Jerusalem und das Holocaust Memorial, Washington an die Bundesrepublik Deutschland und die Bundesländer herangetreten, um die Genehmigung zu erhalten, Holocaust-relevante Dokumente aus den Staatsarchiven, insbesondere auch zu den entsprechenden gerichtlichen Verfahren der Nachkriegszeit, zu verfilmen und in die eigenen Archive zu überführen. Dieses Anliegen wurde wegen der zunehmenden Bedeutung historischer Dokumente aus den Verfahren gegen NS-Täter unterstützt, gleichwohl führte eine rechtliche Prüfung der für diesen Plan einschlägigen Archivgesetze der Länder zu der Erkenntnis, dass rechtliche Hindernisse bestehen. So stellte das Hessische Ministerium für Wissenschaft und Kunst in Abstimmung mit den Staatsarchiven frühzeitig fest, dass § 15 Hessisches Archivgesetz (HArchivG) eine solche Datenübermittlung nicht zulässt. Ausschlaggebend war dabei zum einen der Umstand, dass es sich bei den betroffenen Unterlagen der Archive um sog. personenbezogenes Archivgut handelt, dessen Inhalt sich auf noch lebende Personen beziehen kann. Für diese Unterlagen gilt nach § 15 Abs. 1 Satz 1 HArchivG eine Schutzfrist von zehn Jahren nach dem Tod der betroffenen Person.

§ 15 Abs. 1 Satz 2 HArchivG

Unbeschadet der generellen Schutzfristen dürfen Akten und Dateien, die sich auf eine natürliche Person beziehen (personenbezogenes Archivgut), erst zehn Jahre nach dem Tod der betroffenen Person durch Dritte benutzt werden. Ist der Todestag nicht festzustellen, endet die Schutzfrist 100 Jahre nach der Geburt der betroffenen Person.

Zum zweiten erlaubt zwar § 15 Abs. 4 Satz 1 HArchivG eine Verkürzung der Schutzfrist im Einzelfall, wenn ein öffentliches Interesse vorliegt.

§ 15 Abs. 4 Satz 1 HArchivG

Die festgelegten Schutzfristen können im Einzelfall verkürzt werden, wenn es im öffentlichen Interesse liegt.

Bei personenbezogenem Archivgut setzt § 15 Abs. 4 Satz 2 HArchivG zwingend voraus, dass die Datenverwendung einem bestimmten Forschungsvorhaben dienen muss.

§ 15 Abs. 4 Satz 2 HArchivG

Bei personenbezogenem Archivgut ist eine Verkürzung nur zulässig, wenn die Benutzung für ein bestimmtes Forschungsvorhaben erfolgt. Schutzwürdige Belange der betroffenen Personen nicht beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange erheblich überwiegt; soweit der Forschungszweck dies zulässt, sind die Forschungsergebnisse ohne personenbezogene Angaben aus dem Archivgut zu veröffentlichen.

Unstreitig dient aber die beabsichtigte Verfilmung und die Übernahme der Filme in die genannten Institutionen zunächst lediglich der Dokumentation und Erweiterung der Bestände, nicht jedoch einem konkreten Forschungsvorhaben.

Um dem Anliegen der Gedenkstätten Rechnung tragen zu können, war unabdingbar die Regelung des § 15 HArchivG entsprechend zu erweitern. Das Hessische Ministerium für Wissenschaft und Kunst hat in mehrstufiger Abstimmung mit mir den folgenden Entwurf zu einem § 17a vorgelegt:

§ 17a HArchivG

(1) Das zuständige Ministerium kann nach Anhörung des Hessischen Datenschutzbeauftragten gestatten, dass Archiven, Museen und Forschungsstellen des Auslandes Vervielfältigungen von öffentlichem Archivgut nach § 1 Abs. 2 Satz 1 zur Geschichte der Juden unter der nationalsozialistischen Herrschaft, zur nationalsozialistischen Judenverfolgung sowie zu deren Aufarbeitung in der Nachkriegszeit zu archivarischer Nutzung überlassen werden.

(2) Die Gestattung ist nur zulässig, wenn sichergestellt ist, dass § 17 Abs. 1 - 3 und Abs. 5 sowie bei der Benutzung der Vervielfältigungen die §§ 15 Abs. 1 und 4, 16 Abs. 1 Nr. 1 und 2 und Abs. 2 sinngemäße Anwendung finden. § 17 Abs. 1 und Abs. 2 Satz 1 und 4 Hessisches Datenschutzgesetz ist entsprechend anzuwenden.

(3) Im Einvernehmen mit der zuständigen obersten Bundesbehörde und dem Bundesarchiv dürfen Vervielfältigungen von Unterlagen nachgeordneter Stellen des Bundes (§ 3) überlassen werden.

(4) Ansprüche auf die Gestattung und Überlassung bestehen nicht.

Die neue Vorschrift ist als Ausnahmeregelung zu § 15 Abs. 1 und 4 HArchivG zu verstehen und erlaubt die Übermittlung auch personenbezogenen Archivgutes unabhängig von den geschilderten Schutzfristen in eng gezogenen Grenzen. Der Schutz der von den Unterlagen betroffenen Personen ist durch die im Entwurf festgelegten Voraussetzungen einer Übermittlung ausreichend. Das von mir in Anlehnung an die Regelung des § 17 Abs. 2 Satz 2 Hessisches Datenschutzgesetz gewünschte Anhörungsrecht im Einzelfall ist im Gesetzentwurf enthalten. Auf die Datenübermittlung besteht kein Rechtsan-

spruch. Das für die Genehmigung zuständige Hessische Ministerium für Wissenschaft und Kunst kann aus rechtstaatlich relevanten Gründen die Übermittlung im Rahmen des Ermessens verweigern.

22. Bibliotheken

Prüfung der Stadt- und Universitätsbibliothek Frankfurt

Die Prüfung der Stadt- und Universitätsbibliothek Frankfurt führte zur Feststellung einiger Mängel, die auch für die übrigen hessischen Bibliotheken dieser Art von Bedeutung sind.

In dem Rahmen meiner Prüftätigkeit besuchte ich auch die Stadt- und Universitätsbibliothek Frankfurt.

Die Verwaltungsabläufe im Bereich der Ausleihe sind naturgemäß durch den weitgehenden Einsatz automatisierter Verfahren geprägt. Im Mittelpunkt steht dabei das seit 1995 von den Niederlanden kommende Programm PICA, in das das Hessische Bibliotheksinformationssystem (HEBIS) eingebettet ist. Die hessischen Hochschul-, Fachhochschul-, Fachbereichs- und Landesbibliotheken sowie drei weitere Universitäts- und Staatsbibliotheken aus Rheinland-Pfalz können mittels PICA auf einen gemeinsam erstellten und gemeinsam genutzten Datenbestand zurückgreifen. PICA enthält verschiedene Module, u.a. zur Recherche und zur Ausleihe. Schon bei der Phase der Einrichtung des Systems hatte ich im Rahmen meiner Beteiligung feststellen können, dass das System eine datenschutzgerechte Lösung für das zentrale Problem anbietet, das bei automatisierten Bibliotheksverfahren auf der Hand liegt: Wird nach Rückgabe eines Buches der Titel bei den Entleiherdaten weiterhin gespeichert, entsteht leicht ein Leserprofil. Dies ist datenschutzrechtlich zu vermeiden. Das System stellt sicher, dass die Titelangaben sofort nach Rückgabe des Buches gelöscht werden.

Insgesamt hielt sich das Ergebnis der Prüfung im Rahmen normaler Erfahrungen. Folgende Punkte sind aber erwähnenswert, weil sie vermutlich auch bei anderen Hochschulbibliotheken ein Problem darstellen.

22.1
Auftragsverhältnis mit der Universität Frankfurt

Der gesamte automatisierte Datenbestand im Rahmen von PICA, auch der Entleiher, wird vom Rechenzentrum der Universität Frankfurt dv-technisch betreut. Damit entsteht eine Rechtslage, die ich bereits im 26. Tätigkeitsbericht, Ziff. 16.3.1 eingehend beschrieben hatte. Ist die Behörde, die für die Bibliotheksdaten datenschutzrechtlich verantwortlich ist, nicht identisch mit der Behörde, die die Daten dv-technisch betreut, besteht ein Auftragsverhältnis, das der Bestimmung des § 4 Abs. 1 und 2 Hessisches Datenschutzgesetz (HDSG) unterliegt.

§ 4 HDSG

(1) Die datenverarbeitende Stelle bleibt für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz sowie für die Erfüllung ihrer sich aus § 8 ergebenden Pflichten auch dann verantwortlich, wenn personenbezogene Daten in ihrem Auftrag durch andere Personen oder Stellen verarbeitet werden. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen; dabei sind der Gegenstand und der Umfang der Datenverarbeitung, die technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen. Für ergänzende Weisungen gilt Satz 2 entsprechend. Der Auftraggeber hat zu prüfen, ob beim Auftragnehmer die nach § 10 erforderlichen Maßnahmen getroffen und die erhöhten Anforderungen bei der Verarbeitung von Daten, die besonderen Amts- oder Berufsgeheimnissen unterliegen sowie der in § 7 Abs. 4 genannten Daten eingehalten werden. An nichtöffentliche Stellen darf ein Auftrag nur vergeben werden, wenn weder gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse, noch überwiegende schutzwürdige Belange entgegenstehen.

§ 4 Abs. 2 Satz 2 HDSG verlangt einen schriftlichen Vertrag, der jedoch zwischen den beiden betroffenen Behörden noch nicht abgeschlossen war. Einen Mustervertrag dazu hat das Hessische Ministerium für Wissenschaft und Kunst mit meiner Mitwirkung bereits in früheren Jahren erstellt. Er wurde jedoch offensichtlich nicht weitergegeben. Die Stadt- und Universitätsbibliothek Frankfurt sagte mir zu, den Vertrag unverzüglich abzuschließen.

22.2
Aufklärung nach § 12 Abs. 4 HDSG

Bei der Durchsicht der Formulare, mit denen auf der Grundlage der Benutzungsordnung die Entleiherdaten erhoben werden, fiel mir auf, dass dort die Aufklärung fehlte, die § 12 Abs. 4 HDSG vorgibt.

§ 12 Abs. 4 HDSG

Werden Daten beim Betroffenen mit seiner Kenntnis erhoben, dann ist er von der datenverarbeitenden Stelle in geeigneter Weise über deren Anschrift, den Zweck der Datenerhebung sowie über seine Rechte nach § 8 aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Werden Daten bei dem Betroffenen auf Grund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, dann ist er auf die Rechtsgrundlage hinzuweisen. Im übrigen ist er darauf hinzuweisen, dass er die Auskunft verweigern kann. Sind die Angaben für die Gewährung einer Leistung erforderlich, ist er über die möglichen Folgen einer Nichtbeantwortung aufzuklären.

Die Konsequenz dieses Mangels ist die Rechtswidrigkeit der Datenverarbeitung. Ich habe daher verlangt, diesen Punkt bei der Verwendung künftiger Formulare zur Datenerhebung zu beachten und die Formulare umgehend zu ergänzen.

22.3
Aufbewahrung der Entleiherdaten

Grundsätzlich löscht die Bibliothek die Nutzerdaten, wenn sich der Entleiher abmeldet, etwa der Student bei der Exmatrikulation. Auf Nachfrage, wie lange die Entleiherdaten im System aufbewahrt werden, wenn kein Anlass zur Löschung bekannt wird, zeigt sich indes Unklarheit und eine uneinheitliche Praxis. Da eine spezialgesetzliche Vorschrift fehlt, ist § 19 Abs. 3 HDSG zu beachten.

§ 19 Abs. 3 HDSG

Personenbezogene Daten sind unverzüglich zu löschen, sobald feststeht, dass ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind oder für die sie nach § 13 Abs. 2 und 4 weiterverarbeitet werden dürfen. Wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer aufgrund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht. Satz 1 findet keine Anwendung, wenn Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Ich habe um baldige Behebung der Mängel gebeten.

Zwischenzeitlich wurde mir mitgeteilt, dass mit der Einführung einer neuen PICA-Version im Frühjahr 2002 eine Löschung der Daten automatisch fünf Jahre nach der letzten Entleihe erfolgt, soweit sich der Entleiher nicht vorher abgemeldet hat.

23. Hochschulen

23.1
Einsatz von Chipkarten an Hochschulen

Die gegenwärtige Einführung der Studenten-Chipkarte an hessischen Hochschulen erfährt unterschiedliche technische Ausgestaltungen. Während die Fachhochschule Frankfurt dem Prinzip der Datenminimierung folgt, strebt die Universität Gießen ein komplexeres Verfahren an.

An einigen hessischen Hochschulen werden Studentenausweise durch Chipkarten ersetzt. Dabei kommen zwei unterschiedliche Verfahren zum Einsatz.

Die Vorschriften zu den inhaltlichen und verfahrenstechnischen Voraussetzungen für die Nutzung von Chipkarten im Hochschulbereich liegen in § 4 Abs. 2 der Immatrikulationsverordnung, zu deren Entwicklung und Text ich auf Ziff. 23.2 dieses Tätigkeitsberichtes verweise. Die Verordnung verlangt eine Hochschulsatzung, in der die „Einzelheiten des Nutzungsumfanges der Chipkarte bezüglich allgemeiner Serviceangebote der Hochschule wie etwa Einschreib- und Rückmeldeverfahren, Zugang zu Parkplätzen oder Nutzung von Hochschulrechenzentrum oder Bibliothek sowie der Einbeziehung von Angeboten des Studentenwerkes und der Kosten“ geregelt werden.
Weitere Grundlagen sind im Hessischen Datenschutzgesetz (HDSG) selbst zu finden: Vor der Einführung der Chipkarte ist hinsichtlich der mit ihrer Nutzung verbundenen Chancen und Risiken für die Studierenden die sogenannte Vorabkontrolle nach § 7 Abs. 6 HDSG durchzuführen.

§ 7 Abs. 6 HDSG

Wer für den Einsatz oder die wesentliche Änderung eines Verfahrens zur automatisierten Datenverarbeitung zuständig ist, hat vor dem Beginn der Verarbeitung zu untersuchen, ob damit Gefahren für die in § 1 Abs. 1 Nr. 1 geschützten Rechte verbunden sind; dies gilt in besonderem Maße für die in § 1 Abs. 4 genannten Daten. Das Verfahren darf nur eingesetzt werden, wenn sichergestellt ist, dass diese Gefahren nicht bestehen oder durch technische und organisatorische Maßnahmen verhindert wer-

den können. Das Ergebnis der Untersuchung und dessen Begründung sind aufzuzeichnen und dem behördlichen Datenschutzbeauftragten zur Prüfung zuzuleiten.

Für die Vorabkontrolle spielen die datenschutzrechtliche Verträglichkeit des einzuführenden Verfahrens und das gesetzlich vorgesehene Sicherheitskonzept eine wichtige Rolle. Die notwendige Transparenz ist durch die vorgeschriebene schriftliche Dokumentation gewährleistet. Schließlich verlangt § 8 Abs. 2 HDSG, dass die Studierenden über ihre datenschutzrechtlichen Ansprüche und die von ihnen bei Verlust des Datenträgers zu treffenden Maßnahmen aufgeklärt werden.

§ 8 Abs. 2 HDSB

Wenn eine in § 3 Abs. 1 genannte Stelle für die Gewährung einer Leistung, das Erkennen einer Person oder für einen anderen Zweck einen Datenträger herausgibt, auf dem personenbezogene Daten des Inhabers automatisiert, etwa in Form einer Chipkarte, verarbeitet werden, dann hat sie sicherzustellen, dass er dies erkennen und seine ihm nach Abs. 1 Nr. 1 bis 5 zustehenden Rechte ohne unvertretbaren Aufwand geltend machen kann. Der Inhaber ist bei Ausgabe des Datenträgers über die ihm nach Abs. 1 zustehenden Rechte sowie über die von ihm bei Verlust des Datenträgers zu treffenden Maßnahmen und über die Folgen aufzuklären.

23.1.1
Fachhochschule Frankfurt

Vorreiter ist die Fachhochschule Frankfurt, die bereits im Wintersemester 2001/2002 für Neueinschreiber den „Study-Chip“ eingeführt hat. Die Fachhochschule Frankfurt kooperiert mit der Frankfurter Sparkasse von 1822 und der Sparkassenorganisation und verwendet hierfür eine Geldkarte, die kein Konto bei der Sparkasse voraussetzt. Bei dem Entwurf der oben erwähnten Hochschulsatzung wurde ich beteiligt.
Die in Frankfurt durchgeführte Vorabkontrolle war lückenhaft und in folgenden Punkten zu ergänzen:
- darzustellen war der technische Ablauf der PIN-Vergabe und ihrer Änderung,
- zu beschreiben war die Geldkartenfunktion mit der damit einhergehenden Datenverarbeitung, verbunden mit dem Hinweis, welche Folgen der Verlust der Chipkarte hat
- hinzuweisen war auch auf die Rechtsgrundlage der Chipkarteneinführung.

Im Vordergrund stand bei dem eingesetzten Verfahren das Prinzip der Datensparsamkeit und Datenvermeidung.

Der Study-Chip erfüllt die folgenden Funktionen:
- Studentenausweis
- Berechtigungsnachweis für das Semesterticket
- Benutzerausweis für die Bibliothek
- Selbstbedienungsausweis im Bereich der Studierendenverwaltung (Studentenwerk, Studentensekretariat)
- Zahlungsmittel mit Geldkartenfunktion

An den Selbstbedienungsstationen werden bis Ende 2003, Zug um Zug in fünf Stufen, folgende Verwaltungsfunktionen ausgeführt werden können:

Stufe1
- Datenansicht und Adressenänderungen in der Studentenverwaltung
- Ausdruck von Studienbescheinigungen

Stufe 2
- Datenansicht in der Prüfungsverwaltung, sofern diese mit Hilfe der zentralen Prüfungsverwaltung erfolgt
- Ausdruck von Leistungsnachweisen, sofern die Prüfungsverwaltung mit Hilfe der zentralen Prüfungsverwaltung erfolgt
- Rückmeldung
- Beurlaubung
- Exmatrikulation

Stufe 3
- Anmeldung zu Prüfungen, sofern die Prüfungsverwaltung mit Hilfe der zentralen Prüfungsverwaltung erfolgt

Stufe 4
- Zugang zu Diensten, Geräten und Räumen in besonderen Fällen

Stufe 5
- Geldkarte kann in der Mensa, für Seminarbeiträge, für Semesterbeiträge und in der Bi-bliothek verwendet werden

Bis zum Redaktionsschluss waren die Funktionen der Stufe 1 für Neueinsteiger realisiert.

Auf der Studentenkarte werden äußerlich sichtbar durch die Hochschule
- Lichtbild
- Name, Vorname
- Barcode für die Bibliotheksnummer
- Bibliotheksnummer in Klarschrift

aufgebracht. Auf einen wiederbeschreibbaren Folienstreifen wird das gültige Semester , dessen Zeitraum sowie ein Text für den Rhein-Main-Verkehrsverbund gedruckt.
Im Chip selbst wird seitens der Hochschule nur die Matrikelnummer abgespeichert. Alle weiteren im Chip gespeicherten Daten ergeben sich aus dessen Technologie als Geldkarte und sind systemimmanent. Die Studierenden vergeben sich selbst eine fünfstellige PIN, die in verschlüsselter Form im Chip hinterlegt wird.

23.1.2
Justus-Liebig-Universität Gießen

Die Universität Gießen wählt einen anderen Ansatz im Vergleich zur Fachhochschule Frankfurt und führt eine multifunktionale Chip-Karte als fälschungssicheren Studentenausweis ein. Die Realisierung ist für das Sommersemester 2002 geplant. Die Chipkarte wird nur einmal für die gesamte Studienzeit an der Universität ausgestellt. Die Karte selbst hat die Größe einer EC-Karte und wird als Twin-Karte mit zwei unabhängigen Mikrochips ausgestattet.

Bei Redaktionsschluss lag mir erst der Entwurf einer Hochschulsatzung und der Vorabkontrolle vor.

Die Chipkarte soll verwendet werden als
- fälschungssicherer Studienausweis
- Bibliotheksausweis
- Elektronischer Türschlüssel
- Elektronischer Ausweis für den Zugriff auf persönliche oder administrative Daten in Datenbanken oder beim generellen Zugriff auf Server-Dienste der Hochschule über Datennetze einschließlich des Internets
- Elektronische Geldbörse

Der Entwurf der Vorabkontrolle war umfangreich. Eine abschließende datenschutzrechtliche Bewertung war aber leider noch nicht möglich, da die Konzeptionsphase bis zum Redaktionsschluss noch nicht abgeschlossen war.

Die Chipkarte selbst hat drei Bereiche:
- sichtbare Aufdrucke
- Kontakt-Chip zur Identifikation mit kryptographischem Identitätsschlüssel
- kontaktfreier Chip für die Funktionen Geldkarte und Zutrittskontrolle

Die sichtbare Fläche enthält:
- Lichtbild
- Name und Vorname
- Ident-Nummer (Kennung der Hochschule, Kartenfolgenummer, Prüfziffer, Kennung der Gruppe und Matrikelnummer)
- Barcode für die Bibliotheken
- RMV-Logo und Ablaufdatum des Semestertickets

Der Kontakt-Chip dient zur Identifikation und Authentifikation des Karteninhabers, unterstützt die digitale Signatur und beinhaltet folgende Daten:

- technische Prozessordaten (systemimanent)
- Name und Vorname des Studenten
- eindeutige Ident-Nummer
- den geheimen kryptografischen Schlüssel zur Ident-Nummer zur Absicherung der Kommunikation (kann nicht ausgelesen werden)
- öffentliches Zertifikat

Der kontaktfreie Chip kann sowohl zur Bezahlfunktion mit der internen Börse (Datensatz 1) als auch zur Zutrittskontrolle (Datensatz 2) verwendet werden und beinhaltet folgende Daten:
- technische Prozessordaten (systemimanent)
- Datensatz 1: elektronische Geldkarte
- Datensatz 2: die Ident-Nummer.

Das geplante Verfahren zum Einsatz der multifunktionalen Chipkarte ist sehr innovativ und wegweisend für andere Hochschulen. Aus juristischer Sicht muss die Freiwilligkeit der Nutzung der digitalen Signatur sichergestellt sein. Spätestens, wenn das Verfahren vom

Pilot- in den Produktionsbetrieb übergeht, muss hierfür eine technische Lösung vorliegen. Ob dies mit Hilfe einer PIN, die die entsprechende Funktion der Chipkarte frei schaltet oder auf eine andere Art geschieht, müssen die Systementwickler entscheiden.

23.2
Änderung der Immatrikulationsverordnung

Im Mittelpunkt der Änderung der Immatrikulationsverordnung steht die Chipkartenregelung.

Aus verschiedenen Anlässen sah das Hessische Ministerium für Wissenschaft und Kunst die Notwendigkeit, die Verordnung über die Verarbeitung von personenbezogener Daten und über das Verfahren der Immatrikulation an den Hochschulen des Landes Hessen vom 23. Januar 1995 (GVBl. 1995 I S. 79) zu ändern. Die Veröffentlichung erfolgte im GVBl. 2001 I S. 543. Überwiegend bestanden die Änderungen in der Anpassung an gewandelte Verwaltungsabläufe an den Hochschulen, sie waren datenschutzrechtlich unproblematisch.

Zu den datenschutzrechtlich wesentlichen Änderungen zählt § 18. Während früher die Aufbewahrungsfrist für bestimmte Prüfungsunterlagen durch Erlass festgelegt war, sind nunmehr alle Prüfungsunterlagen normativen Fristbestimmungen unterworfen. Dies erspart den Hochschulen allerdings nicht die bei Prüfbesuchen immer wieder angesprochene Notwendigkeit, für alle hochschulinternen Standard-Verwaltungsunterlagen Aufbewahrungsfristen generell festzulegen.

Die wesentliche Neuerung dieser Verordnung ist die in § 4 Abs. 2 vorgesehene Möglichkeit der Einführung des Studienausweises als Chipkarte. Zur Vorgeschichte sei erwähnt, dass seit 1999 hessische Hochschulen in konkrete Planungen zur Einführung einer Chipkarte für Studierende eintraten. Nun beabsichtigen die Fachhochschule Frankfurt und die Universität Gießen, die Chipkarte für Studenten einzuführen. Im Vorfeld war die Frage zu klären, welche allgemeine oder spezielle Rechtsgrundlage hierfür zu fordern ist.

§ 4 Abs. 2 der Verordnung über die Verarbeitung von personenbezogenen Daten und über das Verfahren der Immatrikulation an den Hochschulen des Landes Hessen

Die Hochschule kann den Studienausweis als Chipkarte ausstellen. Der Datenspeicher der Chipkarte enthält als einzige personenbezogene Daten Namen und Ident-/Matrikelnummer. Auf der Chipkartenoberfläche befinden sich die Angaben nach Absatz 1, die Bibliotheksbenutzernummern mit Barcode des/der Studierenden und ein Foto der Karteninhaberin oder des Karteninhabers. Die Einzelheiten des Nutzungsumfangs der Chipkarte bezüglich allgemeiner Serviceangebote der Hochschule wie etwa Einschreib- und Rückmeldeverfahren, Zugang zu Parkplätzen oder Nutzung von Hochschulrechenzentrum oder Bibliothek sowie der Einbeziehung von Angeboten des Studentenwerks und der Kosten regelt die Hochschule in einer Satzung.

§ 8 Abs. 2 HDSG enthält nur ergänzende Rahmenbedingungen für den Einsatz einer Chipkarte.

§ 8 Abs. 2 HDSG

Wenn eine in § 3 Abs. 1 genannte Stelle für die Gewährung einer Leistung, das Erkennen einer Person oder für einen anderen Zweck einen Datenträger herausgibt, auf dem personenbezogene Daten des Inhabers automatisiert verarbeitet werden, etwa in Form einer Chipkarte verarbeitet werden, dann hat sie sicherzustellen, dass er dies erkennen und seine ihm nach Abs. 1 Nr. 1 bis 5 zustehenden Rechte ohne unvertretbaren Aufwand geltend machen kann. Der Inhaber ist bei Ausgabe des Datenträgers über die ihm nach Abs. 1 zustehenden Rechte sowie über die von ihm bei Verlust des Datenträgers zu treffenden Maßnahmen und über die Folgen aufzuklären.

Für die darüber hinausgehenden Festlegungen für eine Chipkarte in den Hochschulen erweist sich nachrangiges Verordnungs- und Satzungsrecht als sachgerecht. Da die Chipkarte auch als Studentenausweis fungieren soll, war § 4 Abs. 2 der Verordnung neu zu fassen. Die Neuregelung wird der Überlegung gerecht, dass einerseits die zentralen Punkte einer Chipkartenregelung auf der Ebene der Immatrikulationsverordnung umrissen werden sollen, andererseits es der Hochschule, die die Studentenchipkarte einführen will, überlassen bleiben soll, die einzelnen Ausgestaltungsvarianten der Chipkarte in einer Hochschulsatzung normativ festzulegen. Es bleibt abzuwarten, wie die Hochschulen den rechtlichen Rahmen des § 4 Abs. 2 ausschöpfen. Ich werde die Schritte der Einführung der Chipkarte bei den Hochschulen weiterhin datenschutzrechtlich begleiten. Insbesondere ist sicher zu stellen, dass die Ausgestaltung Dienstleistungsaufgaben erfüllt und auf Verhaltensüberwachung verzichtet.

24. Rundfunk

Auskunftsverpflichtung von Gebührenzahlern - Beanstandung gegenüber dem Hessischen Rundfunk

Der Rundfunkgebührenstaatsvertrag verpflichtet Gebührenzahler nicht zur Auskunft über zum Empfang bereitgehaltene Rundfunk- und Fernsehgeräte, wenn keine Änderungen eingetreten sind, die Auswirkungen auf die Höhe der zu entrichtenden Gebühr haben. Anderslautende Anschreiben an Gebührenzahler durch die Gebühreneinzugszentrale sind unzulässig.

24.1
Mailing-Aktionen der GEZ

Die Gebühreneinzugszentrale (GEZ) in Köln, die als Körperschaft des öffentlichen Rechts im Auftrag der Landesrundfunkanstalten tätig wird, versucht u.a. mit sogenannten „Mailing-Aktionen“ eine Verbesserung des Gebührenaufkommens zu erreichen. Neben der „Anmietung“ von Adressen bestimmter Personengruppen bei kommerziellen Adresshandelsfirmen wird auch auf den eigenen Datenbestand zurückgegriffen. So werden beispielsweise gezielt Haushalte angeschrieben, die nur ein Rundfunkgerät bei der GEZ angemeldet haben. Die Anschreiben erwecken den Eindruck als habe der Betroffene die Pflicht, wiederkehrend Auskunft darüber zu geben, dass sich bei ihm nichts geändert habe. Mit jedem der drei Formschreiben der GEZ wird die Tonart massiver. Dabei wird der Eindruck vermittelt, als habe der Betroffene in jedem Fall zu antworten.

Die GEZ stützt sich auf die Vorschrift des § 4 Abs. 5 Rundfunkgebührenstaatsvertrag (RGebStV). Danach kann die zuständige Landesrundfunkanstalt vom Rundfunkteilnehmer oder von Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie ein Rundfunkempfangsgerät zum Empfang bereithalten und dies nicht oder nicht umfassend nach § 3 Abs. 1 und 2 angezeigt haben, Auskunft über diejenigen Tatsachen verlangen, die Grund, Höhe und Zeitraum ihrer Gebührenpflicht betreffen. Das Auskunftsverlangen kann im Verwaltungszwangsverfahren durchgesetzt werden.

24.2
Bewertung

Eine zunehmende Anzahl von Beschwerden hat mich veranlasst, eine rechtliche Bewertung des Sachverhaltes vorzunehmen. Dabei war streitig, ob die Vorschrift des § 4 Abs. 5 auch die Fälle erfasst, in denen sich beim Betroffenen seit seiner Anmeldung bei der GEZ keinerlei Änderungen im „Rundfunkverhalten“ ergeben haben. Die Landesrundfunkanstalten sind einmütig der Auffassung, dass auch in diesen Fällen eine sog. „negative“ Auskunftspflicht bestehe.

Dass der Betroffene zur Auskunft verpflichtet ist, wenn er bisher nicht angemeldete Geräte nutzt, ist unstrittig. Er hat die Tatsachen anzugeben, welche die Höhe der Rundfunkgebühren bestimmen. Die Vorschrift kann jedoch nicht herangezogen werden, wenn sich an dem Teilnehmerverhältnis nichts geändert hat. Das Verlangen, wiederkehrend Negativatteste abzugeben, ist unzumutbar, zumal die GEZ kein Rückporto beifügt.

24.3
Beanstandung

Auf die von mir ausgesprochene Beanstandung gemäß § 27 Abs. 1 HDSG hat der Intendant des Hessischen Rundfunks (HR) geantwortet, dass bei der heute üblichen Durchdringung der Haushalte mit Fernsehgeräten Einiges dafür spräche, dass bei einem nicht geringen Teil von Hörfunkteilnehmern auch ein Fernsehgerät zum Empfang bereitgehalten werde. Die Erfolge der Mailing-Aktionen bestätigten das. So sei von etwa 10 % aller angeschriebenen Hörfunkteilnehmer ein Fernsehgerät nachträglich angemeldet worden. Im Übrigen leite die GEZ bei Nichtbeantwortung der Anfragen keine weiteren Maßnahmen ein. Außerdem achte der HR den Wunsch von Teilnehmern, nicht mehr in entsprechende Mailing-Aktionen einbezogen zu werden (Einrichtung einer technischen Sperre).

Ungeachtet des konzertierten Vorgehens aller Rundfunkanstalten bleibe ich bei der Auffassung, dass es keine Verpflichtung zur Auskunft in den von mir geschilderten Fällen gibt. Bezeichnend ist in diesem Zusammenhang, dass der HR seinen vermeintlichen Auskunftsanspruch nicht im Verwaltungszwangsverfahren durchsetzt.

Der Intendant des HR hat mir gegenüber aber zugesagt, sich dafür einzusetzen, die Formulierungen im Zusammenhang mit den Anschreiben der GEZ abzumildern, um damit zusätzliche Irritationen zu reduzieren.

Ich habe inzwischen die Hessische Staatskanzlei auf das Problem aufmerksam gemacht und darum gebeten, bei der nächsten Novellierung des Rundfunkgebührenstaatsvertrages für eine Klarstellung in § 4 Abs. 5 zu sorgen.

25. Wahlrecht

Änderung des Landtags- und Kommunalwahlgesetzes

Der Wille, das hessische Wahlrecht mit dem im Frühjahr geänderten Bundeswahlrecht zu harmonisieren, führt zum Verzicht, Personen in das Wählerverzeichnis aufzunehmen, für die nach dem Melderecht eine Auskunftssperre wegen besonderer Gefahr für Leib oder Leben in das Melderegister eingetragen ist. Damit wird ein seit Jahren verfolgtes Anliegen der Datenschutzbeauftragten berücksichtigt.

Schon anlässlich der Wahlrechtsnovelle von 1997 hatte mein Amtsvorgänger vorgetragen, dass bei öffentlicher Auslegung der Wählerverzeichnisse die Gefahr bestehe, dass Personen, für die nach dem Meldegesetz, etwa zum Schutz der körperlichen Unversehrtheit, eine Auskunftssperre eingetragen ist, möglicherweise ausfindig gemacht werden können. Daraus folgte die Anregung gegenüber dem Gesetzgeber, die Wahlgesetze dahingehend zu ändern, dass diejenigen Wahlberechtigten, für die eine Auskunftssperre nach dem Meldegesetz eingetragen ist, nicht in das Wählerverzeichnis aufgenommen werden. Zunächst wurde die Möglichkeit der Einsichtnahme in Daten, die nicht die eigene Person betreffen, nur eingeschränkt, und zwar auf die Fälle, in denen Zweifel an der Richtigkeit des Eintrags vorgetragen wurden. Allerdings blieben die Namen der Personen, für die eine melderechtliche Auskunftssperre im Melderegister eingetragen war, nach wie vor im Wählerverzeichnis.

Mit Novelle vom 27. April 2001 ist das Bundeswahlgesetz dahingehend geändert worden, dass das Recht, die Richtigkeit des Wählerverzeichnisses zu überprüfen, nicht hinsichtlich der Daten von Wahlberechtigten besteht, für die im Melderegister eine Übermittlungssperre eingetragen ist. Zur Harmonisierung des Wahlrechts hatte der Hessische Minister des Innern im Sommer einen vergleichbaren Gesetzentwurf vorgelegt. Die nunmehr beabsichtigte Regelung entspricht aus den oben dargelegten Gründen meinen Vorstellungen an eine datenschutzkonforme Ausgestaltung der Erstellung und Einsichtnahme in das Wählerverzeichnis.

§ 12 Abs. 2 LWG-E

Jeder Wahlberechtigte hat das Recht, an den Werktagen vom zwanzigsten bis zum sechzehnten Tag vor der Wahl (Einsichtsfrist) während der allgemeinen Öffnungszeiten der Gemeindebehörde die Richtigkeit oder Vollständigkeit der zu seiner Person im Wählerverzeichnis eingetragenen Daten zu überprüfen. Zur Überprüfung der Richtigkeit oder Vollständigkeit der Daten der anderen im Wählerverzeichnis eingetragenen Personen haben Wahlberechtigte während der Einsichtsfrist nur dann ein Recht auf Einsicht in das Wählerverzeichnis, wenn sie Tatsachen glaubhaft machen, aus denen sich eine Unrichtigkeit oder Unvollständigkeit des Wählerverzeichnisses ergeben kann; die dabei gewonnenen Erkenntnisse dürfen nur für die Begründung eines Einspruchs gegen das Wählerverzeichnis und für Zwecke der Wahlprüfung verwendet werden. Das Recht zur Überprüfung nach Satz 2 besteht nicht hinsichtlich der Daten von Wahlberechtigten, für die im Melderegister eine Übermittlungssperre nach § 34 Abs. 5 des Hessischen Meldegesetzes eingetragen ist.

Datenschutzrechtlich bedeutsam ist auch die Neuregelung über die Rekrutierung der Mitglieder von Wahlvorständen für anstehende und zukünftige Wahlen. Die beabsichtigte Norm des § 17 Abs. 4 LWG (§ 6 Abs. 4 KWG) sieht vor, dass die Gemeindebehörden befugt sind, personenbezogene Daten von Wahlberechtigten (Name, Vorname, Geburtsdatum, Anschrift, Telefonnummern, Zahl der Berufungen zu Mitgliedern von Wahlvorständen und die dabei ausgeübte Funktion sowie die Art der Wahl, für die der Betroffene eingesetzt wurde) zum Zwecke ihrer Berufung zu Mitgliedern von Wahlvorständen zu erheben und zu verarbeiten. Die Neuregelung lässt dabei die Weiterverwendung für zukünftige Wahlen ausdrücklich zu, soweit die davon betroffenen Personen nicht widersprochen haben. Über das Widerspruchsrecht sind die Betroffenen zu informieren.

Ein weiterer Fragenkomplex betrifft öffentliche Bedienstete. Das Bundeswahlgesetz hatte die Möglichkeit geschaffen, dass öffentliche Stellen zur Sicherstellung der Wahldurchführung Daten ihrer Bediensteten auf Ersuchen der Gemeindebehörden an die Gemeinden übermitteln dürfen, wenn die Bediensteten ihren Wohnsitz im Gebiet der ersuchenden Gemeinde haben. Der hessische Entwurf sieht vor, dass diese nach Bundeswahlgesetz erhobenen Daten von den Gemeindebehörden auch für die Durchführung von Landtags- und Kommunalwahlen weiter verwenden dürfen (§§ 17 Abs. 5 LWG-E, 6 Abs. 5 KWG-E). Der Entwurf sieht vor, dass die übermittelnde Stelle die Betroffenen im Nachhinein informiert. Datenschutzrechtlich ist wünschenswert, dass die von der Übermittlung betroffenen Personen, vor der Herausgabe ihrer Daten über die beabsichtigte Übermittlung informiert werden (Transparenzgrundsatz).

Das Innenministerium verwies demgegenüber darauf, dass die Regelungen der §§ 17 Abs. 5 LWG-E und 6 Abs. 5 KWG-E keine eigene Datenerhebungsbefugnisse von Bedienstetendaten schaffen. Es handele sich hier lediglich um die Klarstellung, dass einmal übermittelte Bedienstetendaten nach Bundeswahlrecht auch für die Durchführung von Landtags- und Kommunalwahlen verwendet werden dürfen. Insofern sei es Sache des Bundesgesetzgebers, entsprechende Regelungen zu treffen.

26. Bilanz

26.1
Prüfung von Statistikstellen
(27. Tätigkeitsbericht, Ziff. 19; 28. Tätigkeitsbericht, Ziff. 19)

In den Jahren 1998 und 1999 fand eine Prüfserie von abgeschotteten Statistikstellen in größeren Städten des Landes statt. Lediglich bei den Statistikstellen Wiesbaden und Frankfurt gab es noch Klärungsbedarf hinsichtlich der technischen Anbindung an das jeweilige städtische Netz.
Die stringenten Abschottungskriterien, die sich aus dem Statistikgesetz ergeben, sind technisch nur mit Hilfe einer Firewall zu gewährleisten. Aber auch die von mir geforderten begleitenden organisatorischen Maßnahmen waren umfangreich.

Dieses Jahr wurden die beiden Statistikstellen auf die gewählten Lösungen geprüft. Sie entsprechen sowohl dem Stand der Technik als auch den von mir gemachten technischen und organisatorischen Vorgaben. In beiden Fällen wurde als Lösung ein Firewall-Modul im zen-tralen Gateway gewählt. Somit ist auch diese Prüfserie endgültig abgeschlossen.

26.2
Gesetzesinitiative für ein Informationszugangsgesetz
(29. Tätigkeitsbericht, Ziff. 3)

Die im letzten Jahr dargestellte parlamentarische Gesetzesinitiative der Fraktion Bündnis 90/Die Grünen für ein Informationsfreiheitsgesetz ist vom Parlament in seiner Sitzung vom 24. Oktober 2001 mit den Stimmen der Fraktionen der CDU und FDP gegen die Stimmen der Fraktion Bündnis 90/Die Grünen bei Enthaltung der SPD-Fraktion abgelehnt worden.

Vorausgegangen waren eine schriftliche und mündliche Anhörung im Hauptausschuss und eine auf dieser Grundlage geführte Diskussion der Positionen. Die Fraktion Bündnis 90/Die Grünen brachte auf Basis der Anregungen aus der Anhörung einen Änderungsantrag ein. Der Hauptausschuss fasste mehrheitlich den Beschluss, dem Plenum die Ablehnung des Gesetzesantrags sowie des Änderungsantrags zu empfehlen.

Bemerkenswert erscheint mir Folgendes: Bereits bei der Einbringung des Gesetzes am 19. September 2000 hatte der Hessische Minister des Innern und für Sport klar gegen ein solches Gesetz Position bezogen. Gleichwohl hat er meiner befürwortenden Stellungnahme im 29. Tätigkeitsbericht nicht widersprochen und bei der Behandlung des Tätigkeitsberichts im Ausschuss sogar ausdrücklich erklärt, das Schweigen der Landesregierung in ihrer Stellungnahme zu einem Beitrag im Tätigkeitsbericht sei stets so zu verstehen, dass die Landesregierung meine Ansicht vollständig teile. Dies traf auf meine positive Einschätzung eines Informationszugangsgesetzes offensichtlich zu keinem Zeitpunkt zu. Die ablehnende Haltung der Koalitionsmehrheit wird die gewünschten Fortschritte beim Ausbau elektronischer Verwaltung behindern und diesem Modernisierungsansatz nicht förderlich sein.

26.3
Verkehrsüberwachung durch Videoaufzeichnungen
(29. Tätigkeitsbericht, Ziff. 4.2)

In meinem 29. Tätigkeitsbericht hatte ich ausführlich dargelegt, dass eine dauerhafte Verkehrsüberwachung durch ununterbrochen laufende Videokameras, bei denen auch ordnungsgemäß fahrende Verkehrsteilnehmer aufgezeichnet werden, nicht zulässig ist.
Beamte der Hessischen Polizeischule haben in ausgiebigen Vorführungen dargelegt, dass eine zwischenzeitliche Unterbrechung technisch weder durchführbar noch sinnvoll ist. Diese Information war zu Beginn des Jahres nicht widerlegbar.

Inzwischen wurden jedoch Aufzeichnungsverfahren entwickelt, bei denen das Gesamtgeschehen scharf erkennbar, die Gesichter jedoch grundsätzlich gerastert werden. Wird im Rahmen der Auswertung der Videoaufzeichnungen ein strafrechtlich erhebliches Verhalten festgestellt, können besonders berechtigte Personen der Strafverfolgungsbehörden mit Hilfe eines bestimmten Entschlüsselungsverfahrens aus den verschlüsselten Bildern Klarbilder erstellen. Für diejenigen, die nicht im Besitz der Verschlüsselungsverfahren sind, bleiben die Bilder unscharf. Das neue entwickelte Verfahren verteuert Videokameras um ca. 100 €. Die erforderliche Technik wird derzeit von einem bekannten deutschen Unternehmen hergestellt. Der Einsatz verschlüsselnder Aufzeichnungstechniken kommt den datenschutzrechtlichen Forderungen nahe, personenbezogene Daten nur dort zu speichern, wo das zur Strafverfolgung oder Gefahrenabwehr erforderlich ist. Die Verwendung des neuen Aufzeichnungsverfahrens zur Überwachung des öffentlichen Raums und der Einsatz bei der Verkehrsüberwachung ist daher künftig datenschutzrechtlich geboten; bestehende Anlagen sind möglichst bald umzustellen.

26.4
Späte aber richtige Einsicht
(29. Tätigkeitsbericht, Ziff 6.1.1)

Nachdem die Staatsanwaltschaft in ihrer Einstellungsverfügung zu einem Ermittlungsverfahren den Wegfall des Tatverdachtes bestätigt hatte, bemühte sich die betroffene Frau um die Löschung ihrer Daten bei der Polizeidirektion des Wetteraukreises in Friedberg. Entgegen der klaren Rechtslage (§ 20 Abs. 4 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung) lehnte die Polizei die Löschung ab. Gegen diese Entscheidung legte sie Widerspruch ein. In kaum verständlicher Weise bestätigte das Regierungspräsidium Darmstadt in seinem Widerspruchsbescheid die falsche Entscheidung der Polizeidirektion Friedberg. Die Betroffene erhob Klage beim Verwaltungsgericht Gießen. In der Zwischenzeit trat das Hessische Polizeiumorganisationsgesetz in Kraft und die Zuständigkeit ging seitens der Polizei auf das neue Polizeipräsidium

Mittelhessen über. Dieses erkannte sofort den Fehler, hob die Bescheide des Wetteraukreises und des Regierungspräsidiums auf und veranlasste die Löschung der Daten über die Betroffene.

26.5
Das Finanzamt im Firmennetz
(29. Tätigkeitsbericht, Ziff. 8.2)

Im 29. Tätigkeitsbericht hatte ich über die Einführung neuer Prüfungsmethoden in die Abgabenordnung (AO) im Rahmen der Außenprüfung berichtet. Mit ihnen soll der technischen Entwicklung moderner Buchführungstechniken Rechnung getragen werden. Nach § 147 Abs. 6 AO erhalten Betriebsprüfer ab Januar 2002 unter anderem das Recht, im Rahmen einer Außenprüfung unmittelbar auf die gesamte EDV-Buchhaltung eines Unternehmens zuzugreifen und sich diese Daten zur weiteren Auswertung im Finanzamt auf einem Datenträger aushändigen zu lassen.

§ 147 Abs. 6 AO

Sind die Unterlagen nach Absatz 1 mit Hilfe eines Datenverarbeitungssystems erstellt worden, hat die Finanzbehörde im Rahmen einer Außenprüfung das Recht, Einsicht in die gespeicherten Daten zu nehmen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen. Sie kann im Rahmen einer Außenprüfung auch verlangen, dass die Daten nach ihren Vorgaben maschinell ausgewertet oder ihr die gespeicherten Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden. Die Kosten trägt der Steuerpflichtige.

Mit einem Durchführungsschreiben (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen, GDBdU) grenzt das Bundesfinanzministerium den weitreichenden Anwendungsbereich dieser gesetzlichen Vorschrift ein. Ich hatte mich bereits im Vorfeld entschieden gegen die im Gesetzestext sehr pauschal gehaltene Formulierung gewandt und gefordert, diese erweiterten Befugnisse der Betriebsprüfer zumindest in einem Anwendungserlass zu begrenzen (Grenzen der Übermittlung und Verwertbarkeit, Aufbewahrung und Löschungsmodalitäten). In einem persönlichen Gespräch mit dem Hessischen Minister der Finanzen, Vertretern des Ministeriums und der Oberfinanzdirektion Frankfurt konnte ich meine Vorbehalte erläutern und die beabsichtigten Maßnahmen diskutieren. Der zwischenzeitlich im Bundessteuerblatt (BStBl. 2001 I S. 415) und im Internet (http://www.bundesfinanzministerium.de) veröffentlichte Erlass (BMF-Schreiben vom 16. Juli 2001 - IV D2 - S 0316 - 136/01) berücksichtigt die datenschutzrechtlichen Forderungen weithin.

Zum Beispiel wird klargestellt, dass

- ein DV-Zugriff nur auf steuerlich relevante Daten zulässig ist,
- eine Fernabfrage (Online-Zugriff) durch die Finanzbehörde ausdrücklich ausgeschlossen ist,
- beim Nur-Lesezugriff keine betriebsfremde Software benutzt wird; die Prüfer greifen unter Verwendung der im Datenverarbeitungssystem des Steuerpflichtigen oder des Beauftragten Dritten vorhandenen Auswertungsmöglichkeiten zu,
- der zur Auswertung überlassene Datenträger spätestens nach Bestandkraft der aufgrund der Außenprüfung ergangenen Bescheide an den Steuerpflichtigen zurück zu geben oder zu löschen ist.

Eine besondere Protokollierungspflicht bezüglich der Zugriffe ist nicht geregelt, sie ergibt sich aber auch nach Auffassung des Bundesministeriums der Finanzen aus dem Bundesdatenschutzgesetz und den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS; BStBl. 1995 I S. 741). Einer ergänzenden Regelung bedarf der Umgang mit den Daten, die dem Betriebsprüfer auf einem maschinell verwertbaren Datenträger ausgehändigt werden. Hier fehlt in dem Durchführungserlass insbesondere der Hinweis, dass die überlassenen Daten nur zur Prüfung der steuerlichen Angaben des betroffenen Steuerpflichtigen selbst, nicht aber zum systematischen Vergleich mit Datenverarbeitungsunterlagen anderer Steuerpflichtigen verwendet werden dürfen. Ein routinemäßiger Abgleich der Daten unterschiedlicher Steuerpflichtiger ist auszuschließen.

Das Hessische Finanzministerium hat meine dahingehende Anfrage dem für Fragen der Betriebsprüfung zuständigen Referatsleiter der obersten Finanzbehörden des Bundes und der Länder vorgelegt. Diese sind übereinstimmend zu der Auffassung gelangt, dass ein solcher routinemäßiger Abgleich nicht vorgesehen sei und dass die nachgeordneten Behörden entsprechend angewiesen werden.

26.6
Medizinische Forschungsnetze
(29. Tätigkeitsbericht, Ziff. 9.2)

In den Jahren 2000 und 2001 sind die datenschutzrechtlichen Rahmenbedingungen für den Aufbau des Kompetenznetzes Parkinson - teilweise auch gemeinsam mit dem Fraunhofer-Institut Software- und Systemschutz (ISST), anderen Forschungsverbünden sowie dem Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder - intensiv diskutiert worden. Die grundsätzlichen datenschutzrechtlichen Anforderungen habe ich in meinem letzten Tätigkeitsbericht

eingehend dargelegt. Das Kompetenznetz Parkinson e.V. hat diese Anforderungen bei der Entwicklung seines Konzepts berücksichtigt und auch teilweise bereits umgesetzt. Gegen das jetzt vorliegende Datenschutzkonzept einschließlich der überarbeiteten Merkblätter/Formulare für die Einwilligungserklärungen der Patienten, dem Vertrag zwischen dem Kompetenznetz und dem Treuhänder sowie dem Vertragsformular für den zwischen den Prüfärzten und dem Kompetenznetz Parkinson zu schließenden Vertrag bestehen aus meiner Sicht keine datenschutzrechtlichen Bedenken.

Im Kompetenznetz Parkinson werden auf dem zentralen Server langfristig pseudonymisierte Patientendaten für Forschungszwecke gespeichert. Es ist zentraler Bestandteil des Datenschutzkonzepts, dass auf dem zentralen Server ausschließlich pseudonymisierte - d.h. keine personenbezogenen - Patientendaten gespeichert werden. Die Daten dürfen nur in den durch die Verträge und Einwilligungserklärungen verbindlich festgelegten Fällen und nur durch den Treuhänder über die bei ihm vorhandene Zuordnungsregel identifiziert werden.

Pseudonymisieren ist das Verändern von personenbezogenen Daten in der Weise, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (vgl. z. B. § 3 Abs. 6a Bundesdatenschutzgesetz). Nur wenn eine Aufdeckung der Pseudonyme durch einen Nichtinhaber der Zuordnungsregel praktisch ausgeschlossen ist, handelt es sich bei den auf dem zentralen Server gespeicherten Daten um pseudonymisierte Daten. Das Kompetenznetz Parkinson muss dauerhaft sicherstellen, dass ein Identifizierungsrisiko für die Patienten nicht besteht und auch künftig nicht entsteht - etwa im Zusammenhang mit einer Ergänzung der zu einem Pseudonym gespeicherten Datensätze oder einer Weitergabe der pseudonymisierten Daten an Dritte.

Gegen das vom Verein vorgeschlagene Verfahren der Generierung der Pseudonyme bestehen keine datenschutzrechtlichen Bedenken:

- Das Verfahren ist geeignet, die Aufdeckung des Pseudonyms durch Administratoren des Servers zu verhindern. Der Ablauf sieht vor, dass zu einem Patienten, der erstmalig einen Arzt aufsucht, ein neuer Datensatz angelegt wird. Als Pseudonym wird eine Zufallszahl erstellt, die auf dem zentralen Server generiert wird und noch nicht vergeben wurde. Unter diesem Pseudonym werden die medizinischen Daten an den Server verschlüsselt übertragen. Gleichzeitig wird eine verschlüsselte E-Mail an den Treuhänder geschickt, in der die zum Pseudonym zugehörenden identifizierenden Daten mitgeteilt werden. Der Treuhänder prüft nun, ob zu den identifizierenden Daten bereits ein Pseudonym bekannt ist. Wenn ja, wird dem Betreiber des Server mitgeteilt, welche Pseudonyme zu einer Person gehören und die Daten werden zusammengefasst. Das Verfahren geht von der Prämisse aus, dass Patienten selten den Arzt wechseln und beim erneuten Arztbesuch das Pseudonym bekannt ist, nur dann kann es mit vertretbarem Aufwand umgesetzt werden.

- Die Frage, inwieweit sich unabhängig davon ein Reidentifizierungsrisiko für die betroffenen Patienten dadurch ergeben kann, dass auf dem zentralen Server sehr detaillierte medizinische (möglicherweise auch soziale) Daten zu den einzelnen Pseudonymen gespeichert werden, konnte bisher nicht abschließend geklärt werden. Das Kompetenznetz Parkinson befindet sich noch im Aufbau, so dass der Umfang des Datensatzes nicht abschließend geklärt werden konnte. Diese Frage muss in regelmäßigen Zeitabständen überprüft werden. Soweit ein Reidentifizierungsrisiko erkennbar wird, müssen geeignete Maßnahmen zur Reduktion des Reidentifizierungsrisikos getroffen werden wie z. B. eine Reduktion des Datensatzes, eine Veränderung der Datenfelder etc.

Die pseudonymisierten Patientendaten sollen auf Antrag an Forscher zur Durchführung von Forschungsprojekten im Rahmen des Kompetenznetzes Parkinson sowie an ähnlich ausgerichtete Forschungsnetze weitergegeben werden. Voraus geht eine Entscheidung der zuständigen Zentralen Konsensuskonferenz des Vereins. Sie prüft, ob ein Reidentifizierungsrisiko für die Patienten durch die Weitergabe der Daten entsteht. Zur Vermeidung von Reidentifizierungsrisiken sollte das Pseudonym, unter dem der Patient auf dem zentralen Server des Kompetenznetzes Parkinson gespeichert wird, nicht an die Forscher weitergegeben werden. Im Übrigen muss vor jeder Weitergabe im Einzelfall geprüft werden, ob durch das bei dem Datenempfänger vorhandene Wissen oder die geplante Weiterverarbeitung der Daten ein Re-identifizierungsrisiko entstehen kann. In diesem Fall sind zusätzlich geeignete Maßnahmen zu treffen, die dieses Risiko vermeiden, z. B. eine Reduktion des Datensatzes, der übermittelt wird etc.

Das Verfahren der Prüfung, Genehmigung und Weitergabe von Datensätzen des Kompetenznetzes Parkinson an Dritte muss dokumentiert werden.

Einige Datensicherheitsmaßnahmen müssen noch entsprechend dem vorgestellten Konzept umgesetzt werden. Der Schutz der dem Kompetenznetzwerk angeschlossenen Rechner gegen unberechtigte Zugriffe muss selbstverständlich gewährleistet sein.

Bei Recherchen zu Forschungszwecken ist es nicht erforderlich, das Pseudonym selbst zu kennen. Die Patienten könnten durch eine datenbankinterne „laufende Nummer“ gegenüber Forschern ausgewiesen werden, so dass eine zweite Pseudonymisierung stattfindet. Hierdurch würde das Risiko einer Reidentifizierung zusätzlich verringert.

Dem Verein Parkinsonnetz e.V. habe ich meine Bewertung mitgeteilt. Die vollständige Umsetzung des Konzepts werde ich im Jahr 2002 vor Ort überprüfen.

27. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

27.1
Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Novellierung des G 10-Gesetzes

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

- die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G 10-Daten an Strafverfolgungsbehörden gegenüber dem Gesetzentwurf noch deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste u.a. zur Strafverfolgung weit über die Schwerkriminalität hinaus genutzt werden dürften,

- der Verzicht auf die Kennzeichnung von G 10-Daten sogar ohne vorherige Zustimmung der G 10-Kommission zulässig sein und

- die Schwelle dafür, endgültig von der Benachrichtigung Betroffener abzusehen, deutlich herabgesetzt werden soll.

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

- Die Anforderungen an die halbjährlichen Berichte des zuständigen Bundesministers an die PKG müssen so gefasst werden, dass eine wirksame parlamentarische Kontrolle erreicht wird. Dies ist derzeit nicht gewährleistet. Deshalb muss über Anlass, Umfang, Dauer, Ergebnis und Kosten aller Maßnahmen nach dem G 10-Gesetz sowie über die Benachrichtigung der Beteiligten berichtet werden. Die gleichen Anforderungen müssen auch für die Berichte der PKG an den Bundestag gelten.

- Die Neuregelung, nach der auch außerhalb der Staatsschutzdelikte mutmaßliche Einzeltäter und lose Gruppierungen den Maßnahmen nach dem G 10-Gesetz unterliegen sollen, stellt das Trennungsgebot nach Art. 87 Abs. 1 Satz 2 GG weiter infrage. Ermittlungen von der Eingriffsschwelle eines konkreten Anfangsverdachts zu lösen und nach nachrichtendienstlicher Art schon im Vorfeld zur Verdachtsgewinnung durchzuführen, weitet die Gefahr unverhältnismäßig aus, dass auch gegen Unbescholtene strafrechtlich ermittelt wird.

- Alle Neuregelungen wie z. B. zum Parteienverbotsverfahren, zur Verwendung von G 10-Erkenntnissen bei Gefahren für Leib oder Leben einer Person im Ausland und zu Spontanübermittlungen an den BND müssen befristet und einer effizienten Erfolgskontrolle unterzogen worden.

- Bei der internen Datenverarbeitung durch die Nachrichtendienste ist die Zweckbindung so zu formulieren, dass die erhobenen Daten nicht zur Erforschung und Verfolgung anderer als der in § 3 und § 5 G 10-E genannten Straftaten genutzt werden dürfen.

- Die vorgesehenen Ausnahmen von der vom BVerfG geforderten Kennzeichnungspflicht bei der Übermittlung von Daten, die aus G 10-Maßnahmen stammen, begegnen schwerwiegenden datenschutzrechtlichen Bedenken.

- Im Gesetzentwurf fehlt die Regelung, dass eine Weiterübermittlung an andere Stellen und Dritte nicht zulässig ist. Sie darf nur durch die erhebende Stelle erfolgen. Die Weitergabe von G 10-Daten an andere Dienststellen ist bei der übermittelnden Stelle stets zu dokumentieren und zu kennzeichnen.

- Eine dauerhafte Ausnahme von der Benachrichtigungspflicht ist abzulehnen. Sie würde für die Betroffenen zu einem Ausschluss des Rechtsweges führen.
- Dem BND wird nicht mehr nur die „strategische Überwachung“ des nicht-leitungs-gebundenen, sondern künftig des gesamten internationalen Telekommunikationsverkehrs ermöglicht. Dies setzt den Zugriff deutscher Stellen auf Telekommunikationssysteme in fremden Hoheitsbereichen voraus. Dabei muss sichergestellt werden, dass die Anforderungen des Völkerrechts eingehalten werden.

- Die Überwachung internationaler Telekommunikationsbeziehungen im Falle einer Gefahr für Leib oder Leben einer Person im Ausland (§ 8 G 10-E) ermöglicht sehr intensive Grundrechtseingriffe in großer Zahl und mit einer hohen Dichte, die höher sein kann als bei „strategischer Überwachung“ nach § 5 G 10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

27.2
Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Datenschutz bei der Bekämpfung von Datennetzkriminalität

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

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

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

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

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

- Maßnahmen zur Identifikation von Internet-Nutzenden, zur Registrierung des Nutzungsverhaltens und Übermittlung der dabei gewonnenen Daten für Zwecke der Strafverfolgung erst dann erfolgen dürfen, wenn ein konkreter Verdacht besteht,

- der Datenschutz und das Fernmeldegeheimnis gewährleistet und Grundrechtseingriffe auf das unabdingbare Maß begrenzt werden,

- der Zugriff und die Nutzung personenbezogener Daten einer strikten und eindeutigen Zweckbindung unterworfen werden,

- Daten von Internet-Nutzenden nur in Länder übermittelt werden dürfen, in denen ein angemessenes Niveau des Datenschutzes, des Fernmeldegeheimnisses und der Informationsfreiheit gewährleistet ist sowie verfahrensmäßige Garantien bei entsprechenden Eingriffen bestehen.

27.3
Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Äußerungsrecht der Datenschutzbeauftragten

Die Datenschutzbeauftragten des Bundes und der Länder sind verpflichtet, Einzelne - wie es die Rechtsprechung des Bundesverfassungsgerichts und die Richtlinie der Europäischen Gemeinschaft zum Datenschutz von 1995 vorsehen - vor rechtswidrigem Umgang mit ihren personenbezogenen Daten wirksam zu schützen. Die damit verbundenen Beratungs- und Kontrollaufgaben verleihen den Datenschutzbeauftragten ein öffentliches Wächteramt, das die Befugnis einschließt, Behörden-

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

[2] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 26.01.2001 – KOM (2000) 890 endgültig

verhalten auch im Detail und, soweit der Bedeutung der Sache angemessen, auch unter Bezeichnung der Amtsträgerinnen und Amtsträger öffentlich zu rügen.

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

27.4
Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Informationszugangsgesetze

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

27.5
Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Novellierung des Melderechtsrahmengesetzes

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

1. Allerdings sind aus dem vorliegenden Gesetzentwurf Tendenzen zu erkennen, dass durch den Zusammenschluss mehrerer Melderegister übergreifende Dateien entstehen können, die letztlich sogar zu einem zentralen Melderegister führen würden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil damit das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger unverhältnismäßig eingeschränkt werden würde.

2. Bereits die bisherige Rechtslage, nach der nahezu jedermann eine einfache Melderegisterauskunft von der Meldebehörde erhalten kann, ist äußerst unbefriedigend. Dies wird dadurch verschärft, dass der Gesetzentwurf - wie in seiner Begründung ausdrücklich betont wird – nunmehr vorsieht, einfache Melderegisterauskünfte mit Hilfe des Internet durch jedermann auch elektronisch abrufen zu können. Um sich gegen eine unkontrollierte Weitergabe solcher über das Internet zum Abruf bereitgehaltener Daten schützen zu können und weil beim Internet-gestützten Abruf die gesetzlich vorgeschriebene Berücksichtigung der schutzwürdigen Belange Betroffener nicht möglich ist, sollte für die Bürgerin oder den Bürger in diesen Fällen ein ausdrückliches Einwilligungsrecht oder mindestens ein Widerspruchsrecht geschaffen werden. Es handelt sich hier um personenbezogene Daten, die auf der Grundlage einer gesetzlichen Auskunftspflicht erhoben wurden.

3. Auch für öffentliche Stellen sollte in das Gesetz eine Bestimmung aufgenommen werden, wonach bei elektronischen Abrufverfahren über das Internet zur Wahrung der schutzwürdigen Interessen der Betroffenen zumindest Verfahren der fortgeschrittenen elektronischen Signatur gemäß den Regelungen des Signaturgesetzes einzusetzen sind.

4. Nach geltendem Recht ist jede Melderegisterauskunft unzulässig, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange glaubhaft gemacht wird. Diese Regelung hat sich bewährt. Die Datenschutzbeauftragten treten angesichts des in diesen Fällen bestehenden hohen Schutzbedarfs dem Vorhaben entschieden entgegen, diese Regelung durch eine Risikoabwägung im Einzelfall aufzuweichen.

5. Bislang dürfen Meldebehörden an Parteien, Wählergruppen und andere Träger von Wahl-vorschlägen Auskunft über Daten von Gruppen von Wahlberechtigten erteilen, sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Datenschutzbeauftragten bekräftigen ihre bereits in der Vergangenheit erhobene Forderung, gesetzlich zu regeln, dass eine Einwilligung der Betroffenen Voraussetzung für solche Datenweitergaben sein muss. Die bisherige Widerspruchslösung ist in weiten Kreisen der Bevölkerung unbekannt.

6. Außerdem fordern die Datenschutzbeauftragten, die Hotelmeldepflicht abzuschaffen, da die hiermit verbundene millionenfache Datenerhebung auf Vorrat unverhältnismäßig ist.

Bei Enthaltung Thüringens zu Ziff. 6.

27.6
Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Überlegungen des BMG für ein Gesetz zur Verbesserung der Datentransparenz

Beschluss der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Arbeitsentwurf aus dem BMG für ein Gesetz zur Verbesserung der Datentransparenz und des Datenschutzes in der gesetzlichen Krankenversicherung (Transparenzgesetz – GKV - TG)

Die Datenschutzkonferenz begrüßt es, dass mit dem Arbeitsentwurf die Forderung der Konferenz wieder aufgegriffen wird, durch Pseudonymisierung des Abrechnungsverfahrens die Belange des Patientengeheimnisses und des Datenschutzes zu wahren. Ziel muss sein den „gläsernen Patienten“ bei den gesetzlichen Krankenkassen zu vermeiden. Mit Pseudonymisierungsverfahren lässt sich dieses Ziel erreichen, ohne dass beispielsweise die Kostenkontrolle oder Qualitätssicherung durch eine Krankenkasse beeinträchtigt wäre. Der Deutsche Bundestag hat die Realisierbarkeit dieses Ansatzes mit seinem Beschluss eines Gesundheitsreformgesetzes vom 4. November 1999, der nach einem Vermittlungsverfahren aus anderen als datenschutzrechtlichen Gründen nicht in vollem Umfang in Kraft getreten ist, bereits bejaht.

Die Datenschutzkonferenz begrüßt es weiterhin, dass in dem Arbeitsentwurf im Rahmen einer Klausel „Modellvorhaben Telematik“ die Weiterentwicklung des Datenschutzes als Ziel vorgegeben und dazu gefordert wird, die Modellvorhaben im Benehmen mit den Datenschutzbehörden durchzuführen. Die Konferenz geht dabei davon aus, dass unter „Weiterentwicklung“ die Sicherung der Patientenrechte auf Wahrung des Arztgeheimnisses und des Datenschutzes auch unter den Randbedingungen der Telematikanwendungen im medizinischen Bereich zu verstehen ist. Sie weist dazu besonders auf ihre Beschlüsse von der 47. und der 50. Konferenz zu Chipkarten im Gesundheitswesen hin, mit denen die Sicherung von Patientenautonomie und Transparenz sowie die Sicherheit der Datenverarbeitung gefordert wurde.

Die Konferenz nimmt auch zustimmend zur Kenntnis, dass durch die Begrenzung auf die Verarbeitung von höchstens 20% der Versichertendaten in den Datenannahme- und -weiter-leitungsstellen der Gefahr der Bildung mehr oder weniger bundesweiter Dateien mit sensiblen medizinischen Daten der Krankenversicherten begegnet werden soll.
Die Konferenz hält zu nachstehenden Punkten ergänzende Regelungen bzw. nähere Darlegungen für erforderlich:

- Die Effektivität eines Pseudonymisierungsverfahrens zum Schutz der sensiblen Versichertendaten steht und fällt mit sicheren Pseudonymen, mit der klaren Begrenzung von Reidentifikationen auf im überwiegenden öffentlichen Interesse absolut notwendige Fälle und der Vermeidung des Abgleichs mit identifizierenden Klardaten.

- Unter diesen Aspekten hält die Datenschutzkonferenz den Katalog der Reidentifikationsfälle für bedenklich: So ist nicht ersichtlich, in wieweit die Krankenkassen zur Durchführung des Risikostrukturausgleichs versichertenbezogene Detailangaben über Diagnosen und Leistungen benötigen. Das gilt auch im Hinblick auf in jüngsten Pressemeldungen berichtete Absichten, im Rahmen des Risikostrukturausgleichs einen sogenannten Risikopool einzuführen, über den Kassen mit sog. schlechten Risiken verstärkte Ausgleichsmittel erhalten sollen. Die Feststellung derartiger „schlechter Risiken“ kann auch über Pseudonyme und die ihnen zugeordneten Leistungszahlen erfolgen. Im Falle der Unterstützung der Versicherten bei Verdacht auf Behandlungsfehler sollte die Einwilligung der Versicherten in die Reidentifikation, die durch die Vertrauensstelle eingeholt werden könnte, angestrebt werden. Auch weitere Katalogfälle von Reidentifikationen sind kritisch zu hinterfragen, so insbesondere die Reidentifikation von Versicherten unter Bekanntgabe des Pseudonyms gegenüber den Kassen(zahn)ärztlichen Vereinigungen.

- Es muss verhindert werden, dass über einen zu weit gefassten Katalog von Reidentifikationsfällen ohne Zustimmung der Versicherten das Ziel der Pseudonymisierung praktisch verfehlt wird. Es ist zu gewährleisten, dass keine personenbezogenen Krankheitsdatenkonten bei den gesetzlichen Krankenversicherungen, oder kurz gesagt, dass keine gläsernen Patienten entstehen.

- In gleicher Weise ist zuverlässig zu vermeiden, dass durch Abgleich mit zeitweilig vorhandenen Klardaten Pseudonyme aufgelöst werden. Hierfür ist eine gesetzliche Sicherstellung erforderlich.

- Schließlich ist die Begrenzung der Speicherung und die Zweckbindung aufgelöster Pseudonyme nicht ausreichend klar. Über eine Verweisung in § 284 SGB V würden die dortigen erweiterten Zweckänderungs- und Verarbeitungsregelungen auch auf die Speicherungen von aufgelösten Pseudonymen angewandt und damit die anscheinend strengen Speicherungs-

und Zweckbindungsregelungen des Arbeitsentwurfs für die genannten Daten ausgehöhlt. Es müsste klargestellt werden, dass die speziellen Speicher- und Zweckbindungsregelungen der allgemeinen Regel des § 284 SGB V vorgehen.

- Die oben erwähnte, nicht in Kraft getretene Fassung der GKV-Gesundheitsreform 2000 sah die alsbaldige Pseudonymisierung der Versichertendaten in allen Abrechnungen der Leistungserbringer vor, und zwar vor Kenntnisnahme durch die Krankenkassen. Der jetzige Arbeitsentwurf sieht die Pseudonymisierung der Versichertendaten in den Abrechnungen aller nicht-vertragsärztlichen Leistungserbringer erst nach Überprüfung durch die Krankenkassen vor. Dies wäre ein datenschutzrechtlicher Rückschritt gegenüber dem Gesetzesbeschluss vom 4. November 1999. Die fachliche Erforderlichkeit dieses Rückschritts sollte, nicht zuletzt auch angesichts des o.g. Bundestagsbeschlusses, näher begründet werden. Zumindest sollte über eine Weiterentwicklungsklausel die Nutzung von Pseudonymen auch für diese Leistungsabrechnungen angestrebt werden. Dazu sollte auch geprüft werden, in wieweit die Krankenversichertenkarte als Mittel zur Pseudonymisierung verwendet werden kann.

- Die Konferenz fordert im Sinn von Lösungen, die dem Datensparsamkeitsprinzip genügen, auch eine Pseudonymisierung der Daten der Vertragsärztinnen und -ärzte. Angesichts der Deckelung der vertragsärztlichen Leistungen und der Verordnungen ist nicht ersichtlich, inwiefern für die GKV personenbezogene Daten dieser Leistungserbringer erforderlich sind. Es müsste ausreichen, wie bei den Versicherten die Reidentifikation nur in gesetzlich festgelegten Ausnahmefällen vorzusehen. Die regionalen Datenauswertungsstellen sollen die Daten auch der sonstigen Leistungserbringer nur pseudonymisiert erhalten.

- Die Konferenz würde es generell begrüßen, wenn im Rahmen der Reformüberlegungen zur Gesundheitsversorgung nach Systemen gesucht würde, die mit möglichst wenig personenbezogenen Daten auskommen. Dies würde dem Gebot der Datensparsamkeit entsprechen.

- Wesentliche Grundlage eines sicheren Pseudonymisierungskonzepts ist die Trennung der die Pseudonymisierung durchführenden Vertrauensstellen von den übrigen Datenverarbeitungsstellen des Systems. Für die Trennung von Datenaufbereitungs- und Vertrauensstellen ist das explizit im Arbeitsentwurf festgelegt, es fehlt aber eine entsprechende Regelung für das Verhältnis Vertrauensstellen zu den übrigen Verarbeitungsstellen. Ungeachtet, dass diese Trennung selbstverständlich sein sollte, wird angeregt, das auch gesetzlich sicherzustellen. Das Gleiche gilt für die Trennung der übrigen Stellen voneinander. Für die datenverarbeitenden Stellen ist der Schutz des Sozialgeheimnisses zu gewährleisten.

- Die vorgesehene „Arbeitsgemeinschaft auf Bundesebene“, deren Mitglieder und das BMG dürfen keine personenbezogenen Versicherten- und Leistungserbringerdaten erhalten. Es ist kein zureichender Grund ersichtlich, warum diese auf Bundesebene angesiedelte Arbeitsgemeinschaft, deren Aufgabe die Festlegung einheitlicher Standards für die Datenverarbeitung bei den Datenaufbereitungsstellen sein soll, derartige Daten benötigt. Das Gleiche gilt für die Vertragspartner auf Bundesebene und das Bundesministerium für Gesundheit. Die Datenschutzkonferenz geht davon aus, dass die Übermittlung personenbezogener Daten an diese Stellen nicht beabsichtigt ist. Die Entwurfsformulierung ist insoweit aber unklar. Ebenso ist sicherzustellen, dass die Arbeitsgemeinschaften auf Landesebene über ihren Sicherstellungsauftrag für die Vertrauensstellen keine Pseudonymisierungsparameter erhalten.

- Die Konferenz sieht keinen zureichenden Grund dafür, dass das datenschutzrechtlich begründete Verbot einer personenbezogenen Datei beim MDK mit medizinischen Daten aufgehoben wird. Die dann entstehende landesweite, einzelne Versicherte aller GKV umfassende Datei mit medizinischen Angaben birgt wegen der einfachen Auswertbarkeit in Bezug auf einzelne Personen ein hohes datenschutzrechtliches Risiko, dessen Eingehung damals wie heute nicht durch die „Medienbruchfreiheit“ zu rechtfertigen ist.

- Die Konferenz hat Bedenken gegen weitgehende Richtlinienermächtigungen zu Gunsten der Spitzenverbände der Krankenkassen. Der Gesetzgeber müsste die wesentlichen Inhalte eingreifender Regelungen selbst bestimmen.

Die Konferenz begrüßt nochmals die in dem Arbeitsentwurf zum Ausdruck kommende Bereitschaft zur Zusammenarbeit mit den Datenschutzstellen und bietet ihrerseits eine enge Zusammenarbeit für die zukünftigen Verhandlungen an, in denen diverse weitere Unklarheiten und Widersprüchlichkeiten des Entwurf auszuräumen sein werden. Sie richtet zu diesem Zweck eine Ad-hoc-Arbeitsgruppe des AK Gesundheit und Soziales ein, die auch vom BfD jeweils für die Verhandlungen einberufen werden kann.

27.7
Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Datenschutz in der Abgabenordnung

Die Datenschutzbeauftragten des Bundes und der Länder sind sich einig, dass zur Umsetzung des Grundrechtes auf informationelle Selbstbestimmung in die Abgabenordnung insbesondere folgende Punkte aufgenommen werden müssen:

1. Die datenschutzrechtlichte Absicherung der Datenverarbeitung.

2. Die gesetzliche Festschreibung eines Rechtes auf Auskunft und Akteneinsicht.

3. Die Gewährung von Rechtsansprüchen auf Berichtigung oder Löschung personenbezogener Daten: Festlegung von Löschungsfristen.

4. Gesetzliche Regelungen zum Outsourcing und der Datenverarbeitung im Auftrag.

5. Gesetzliche Regelungen zur Zulässigkeit und dem Gegenstand von Kontrollmitteilungen innerhalb der Finanzverwaltung, insbesondere unter dem Gesichtspunkt der Erforderlichkeit und des Übermaßverbotes.

6. Die Aufnahme einer eigenständigen Regelung über die Schadensersatzpflicht für Datenschutzverstöße.

7. Die Harmonisierung oder einzelstaatliche Abstimmung der Auskunftserteilung an ausländische Behörden, Anpassung an die §§ 4b, 4c E-BDSG.

Außerdem sind die Zugriffsrechte auf Unternehmensdaten bei Betriebsprüfungen durch § 147 VI AO angemessen zu begrenzen,

a) insbesondere durch ein Verbot einer Parallelbuchführung durch die Finanzämter und
b) eines generellen automatisierten Datenabgleichs zwischen Buchhaltungen verschiedener Unternehmen/Selbständiger.

27.8
Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001

Datenschutz beim elektronischen Geschäftsverkehr

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

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

27.9
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12. März 2001

Anlasslose DNA-Analyse aller Männer verfassungswidrig

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

27.10
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. April 2001

Veröffentlichungen von Insolvenzinformationen im Internet

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (BTDrucks. 14/5680) vor, wonach künftig zur Ersparnis der Bekanntmachungs-kosten in Printmedien gerichtliche Entscheidungen vor allem in Verbraucherinsolvenzverfahren auch über das Internet veröffentlicht werden können. Die Datenschutzbeauftragten des Bun-

des und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt werden, durch die Justiz weder räumlich begrenzt noch deren Speicherung zeitlich beherrscht werden können und vielfältigen Auswertungen zugänglich sind. Dies kann dazu führen, dass die Daten auch lange nach Abschluss eines Insolvenzverfahrens durch Speicherungen Dritter, etwa Auskunfteien oder Wirtschaftsinformationsdienste jederzeit im Internet verfügbar sind und so die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn letztlich auf Dauer beeinträchtigt wird. Es besteht somit die Gefahr, dass Insolvenzschuldner zeitlebens weltweit abrufbar am Schulden-Pranger stehen.

Der Gesetzgeber muss das Risiko für die betroffenen Verbraucher, aufgrund einer möglichen Auswertung justizieller Internetveröffentlichungen dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der beabsichtigten Senkung von Bekanntmachungskosten abwägen. Hierbei muss auch die gesetzgeberische Wertung berücksichtigt werden, dass Personen, für die ein Insolvenzverfahren eröffnet wurde, gerade nicht in das Schuldnerverzeichnis beim Amtsgericht aufgenommen werden. Das Internet bietet im Gegensatz zu einem gerichtlichen Verzeichnis letztlich keine Gewähr, die ordnungsgemäße Pflege und die Löschung personenbezogener Daten sicherzustellen, die für die Betroffenen von entscheidender wirtschaftlicher Bedeutung sein können. Die Datenschutzbeauftragten appellieren daher an den Gesetzgeber und an die Justizverwaltungen der Länder, die aufgezeigten Risiken insbesondere für Verbraucherinsolvenzen neu zu bewerten. Die vorgenannten Überlegungen sind im Gesetzgebungsverfahren bisher nicht in ausreichendem Maße berücksichtigt worden.

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

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

Auch in anderen Bereichen der Bereitstellung justizieller Informationen, z. B. der Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckungsverfahren, wird das Internet bereits genutzt bzw. seine Nutzung erprobt oder erwogen. Inwieweit das Internet als Medium der im Ergebnis unbegrenzbaren Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil ins Internet eingestellt werden darf, muss differenziert in Übereinstimmung mit dem gesetzlich bezweckten Grad der Publizität der jeweiligen Daten entschieden werden. Jede gesetzgeberische Entscheidung für eine Veröffentlichung über das Internet sollte aber im Hinblick auf deren besondere Risiken Regelungen treffen, durch die eine Befristung der Veröffentlichung sowie besondere Vorkehrungen zur Sicherung von Identität und Authentizität und zur Verhinderung einer automatischen Übernahme der Daten (Kopierschutz) sichergestellt werden.

27.11
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10. Mai 2001

Zum Entwurf der Telekommunikations-Überwachungsverordnung

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

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

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

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

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

27.12
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. Oktober 2001

Zur Terrorismusbekämpfung

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

Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungsbehörden zur Terrorismusbekämpfung bereits über weitreichende Befugnisse zur Datenverarbeitung verfügen. So ist z. B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenabwehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den Verfassungsschutz und die Polizei übermitteln. Auch ist eine effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch die geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.
Die Datenschutzbeauftragten sind zu einem offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Datenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffsbefugnisse zu befristen und tiefgreifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

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

27.13
Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober 2001

Datenschutzrechtliche Anforderungen an den "Arzneimittelpass" (Medikamentenchipkarte)

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

Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen eine Medikamentenchipkarte als **Pflichtkarte**. Die Datenschutzbeauftragten begrüßen es daher ausdrücklich, dass der Gedanke einer Pflichtkarte fallen gelassen wurde. Die Patientinnen und Patienten würden sonst rechtlich oder faktisch gezwungen, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- und/oder Apothekenbesuch ohne ihren Willen zu offenbaren. Dies würde eine wesentliche Einschränkung des Arztgeheimnisses bewirken, das auch gegenüber anderen Ärztinnen und Ärzten gilt. Zudem

würde sich dadurch das Vertrauensverhältnis, das für die Behandlung und für eine funktionierende Gesundheitsfürsorge insgesamt unabdingbar ist, grundlegend verändern. Darüber hinaus wäre das Einholen einer unbeeinflussten Zweitmeinung nahezu ausgeschlossen.

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

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

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

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

Der Chipkarteneinsatz darf nicht zur Entstehung neuer zentraler Datensammlungen über Pa-tientinnen und Patienten führen.

Datenschutzrechtlich problematisch wäre es, den "Arzneimittelpass" auf der **Krankenversichertenkarte** gemäß § 291 SGB V zu implementieren. Eine solche Erweiterung wäre allenfalls vertretbar, wenn die "Funktion Krankenversichertenkarte" von der "Funktion Arzneimittelpass" informationstechnisch getrennt würde, so dass die Patientinnen oder Patienten bei einem Arzt- oder Apothekenbesuch nicht gezwungen werden, ihre gesamten Gesundheitsdaten ungewollt zu offenbaren. Ihre Entscheidungsfreiheit, wem gegenüber sie welche Gesundheitsdaten offen legen, müsste also durch die technische Ausgestaltung der Karte gewährleistet sein.

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

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

27.14
Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober 2001

Zur gesetzlichen Regelung von genetischen Untersuchungen

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

- Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;

- Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;

- Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;

- Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;

- Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;
- Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt in ärztlicher Praxis oder Labor;
- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegen zu nehmen;
- Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;
- Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänderschaft;
- Hilfe für die Betroffenen durch die Pflicht, im Rahmen der Forschung, individuell bedeutsame Untersuchungsergebnisse mitzuteilen;
- Absicherung der Regelungen durch die Einführung von Straftatbeständen.

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

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

Anlage zu der Entschließung

Vorschläge zur Sicherung der Selbstbestimmung bei genetischen Untersuchungen

Allgemeines

Gegenstand

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

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

zu treffen.

Ziel, Benachteiligungsverbot

(1) Ziel der Regelungen ist der Schutz der Menschenwürde, der Persönlichkeit und der informationellen Selbstbestimmung der Betroffenen bei genetischen Untersuchungen.
(2) Niemand darf wegen seiner Erbanlagen oder wegen der Weigerung, eine genetische Untersuchung bei sich durchführen zu lassen, benachteiligt werden.

Begriffe

1. *Genetische Untersuchungen:* Untersuchungen auf Chromosomen-, Genprodukt- oder molekularer DNS / RNS-Ebene, die darauf abzielen, Informationen über das Erbgut zu erhalten;
2. *Prädiktive Untersuchungen:* vor- oder nachgeburtliche genetische Untersuchungen mit dem Ziel, Erbanlagen einer Person, insbesondere Krankheitsanlagen vor dem Auftreten von Symptomen oder einen Überträgerstatus, zu erkennen;
3. *Überträgerstatus:* Erbablagen, die erst in Verbindung mit entsprechenden Erbanlagen eines Partners oder einer Partnerin eine Krankheitsanlage bei den gemeinsamen Nachkommen ausbilden.
4. *Pränatale Untersuchungen:* vorgeburtliche genetische Untersuchungen mit dem Ziel, während der Schwangerschaft Informationen über das Erbgut des Embryos oder des Fötus zu gewinnen;

5. *Reihenuntersuchung:* genetische Untersuchungen, die systematisch der gesamten Bevölkerung oder bestimmten Gruppen der Bevölkerung angeboten werden, ohne dass bei den Betroffenen Anhaltspunkte dafür bestehen, dass die gesuchten Erbanlagen bei ihnen vorhanden sind;
6. *Diagnostische genetische Untersuchungen:* genetische Untersuchungen zur Abklärung der Diagnose einer manifesten Erkrankung oder zur Vorbereitung oder Verlaufskontrolle einer Behandlung;
7. *Probe:* die für eine genetische Untersuchung vorgesehene oder genutzte biologische Substanz;
8. *Genetische Daten:* im Zusammenhang mit genetischen Untersuchungen erlangte Informationen über eine Person;
9. *Betroffene Person:* die Person, von der eine Probe vorliegt oder deren genetische Daten erhoben, verarbeitet oder genutzt werden; bei pränatalen Untersuchungen auch die schwangere Frau.
10. *Verarbeiten:* das Speichern, Verändern, Übermitteln, Sperren und Löschen erhobener personenbezogener genetischer Daten.

Zulässigkeit genetischer Untersuchungen

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

Zulassung zur Durchführung genetischer Untersuchungen

(1) Wer genetische Untersuchungen durchführen will, bedarf hierfür der Zulassung durch die zuständige Aufsichtsbehörde des Landes.
(2) Die Zulassung wird erteilt, wenn Gewähr dafür besteht, dass
- die Untersuchungen und ihre Auswertungen sorgfältig und nach dem Stand von Wissenschaft und Technik durchgeführt werden,
- die Regelungen gemäß diesen Vorschlägen eingehalten, insbesondere Information und Beratung der betroffenen Person und die Datensicherheit gewährleistet werden und
- in der antragstellenden Person die berufsrechtlichen und gewerberechtlichen Voraussetzungen vorliegen.

(3) Das Nähere regelt die Bundesregierung durch Rechtsverordnung.

Inverkehrbringen genetischer Tests und Angebote von genetischen Untersuchungen

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

Zweckbindung

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

Datensicherheit

(1) Proben und genetische Daten sind vor dem Zugriff unbefugter Dritter wirksam zu schützen. Dies gilt auch in Bezug auf Mitarbeiterinnen und Mitarbeiter der untersuchenden und datenverarbeitenden Stelle, die an der genetischen Untersuchung, Aufklärung und Beratung nicht beteiligt sind oder waren.
(2) Genetische Daten sind von anderen Datenarten gesondert zu speichern.
(3) Im Übrigen gilt hinsichtlich der genetischen Daten die Bestimmung des Bundesdatenschutzgesetzes über die technischen und organisatorischen Maßnahmen der Datensicherheit in der jeweils geltenden Fassung.

Einsichts- und Auskunftsrecht

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

Genetische Untersuchungen zu medizinischen Zwecken

Grundsatz

(1) Zu medizinischen Zwecken dürfen prädiktive Untersuchungen nur durchgeführt werden, wenn sie nach ärztlicher Indikation der Vorsorge, der Behandlung oder der Familienplanung der betroffenen Person dienen.
(2) Eine genetische Untersuchung zum Erkennen eines Überträgerstatus ist nur zu Zwecken der konkreten Familienplanung zulässig.
(3) Für diagnostische genetische Untersuchungen gelten nur die Anforderungen gemäß dem Arztvorbehalt (siehe unten) und an diagnostische genetische Untersuchungen bei behinderten Personen (siehe am Ende dieses Abschnitts).

Pränatale Untersuchungen

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

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

Genetische Untersuchungen bei Minderjährigen und nicht einsichtsfähigen Erwachsenen

(1) Genetische Untersuchungen bei Minderjährigen sind nur zulässig, wenn ihre Durchführung vor Erreichen der Volljährigkeit erforderlich ist, um den Ausbruch einer Krankheit zu vermeiden oder zu verzögern, eine Heilung oder Verlaufsmilderung zu erreichen oder spätere besonders belastende Untersuchungen zu vermeiden. Bei Aufklärung, Beratung und Einwilligung (siehe unten) ist die Einsichtsfähigkeit der betroffenen minderjährigen Person zu berücksichtigen.
(2) Prädiktive Untersuchungen bei nicht einsichtsfähigen Erwachsenen dürfen sich nur auf das Erkennen von Krankheiten richten, deren Ausbruch vermieden oder verzögert oder bei denen eine Heilung oder Verlaufsmilderung erreicht werden kann. Die Einwilligung obliegt dem gesetzlichen Vertreter.

Reihenuntersuchungen

(1) Genetische Reihenuntersuchungen bedürfen der Zulassung durch die zuständige Landesbehörde.
(2) Voraussetzung für die Zulassung ist, dass
- die Reihenuntersuchung gerichtet ist auf das Erkennen von verbreiteten oder schweren Krankheiten, die unverzüglich nach dem Untersuchungsergebnis behandelt werden können, oder von Krankheiten, deren Ausbruch verhindert werden kann,
- die Untersuchungsmethode eindeutige Ergebnisse liefert,
- die Freiwilligkeit der Teilnahme und die genetische Beratung gewährleistet und
- der Datenschutz gesichert ist.

Arztvorbehalt

(1) Prädiktive Untersuchungen dürfen nur von Fachärztinnen und Fachärzten für Humangenetik veranlasst werden. Diagnostische genetische Untersuchungen dürfen auch von anderen zur Berufsausübung zugelassenen Ärztinnen und Ärzten veranlasst werden.
(2) Die veranlassende Ärztin oder der veranlassende Arzt hat die Aufklärung und Beratung (siehe nachstehend) und die Einholung und Dokumentation der Einwilligung (siehe unten) sicherzustellen.

Aufklärung und Beratung

(1) Vor und nach einer prädiktiven genetischen Untersuchung ist die betroffene Person umfassend aufzuklären und zu beraten, um ihr eine selbstbestimmte Entscheidung gemäß den Anforderungen an die Einwilligung (siehe unten) zu ermöglichen.
(2) Die betroffene Person und gegebenenfalls ihr gesetzlicher Vertreter muss insbesondere aufgeklärt werden über
- Ziel, Art, Aussagekraft und Risiko der Untersuchung und die Folgen ihrer Unterlassung;
- mögliche, auch unerwartete Ergebnisse der Untersuchung;

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

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

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

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

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

Einwilligung

(1) Nach der Aufklärung und Beratung entscheidet die betroffene Person nach angemessener Bedenkzeit in freier Selbstbestimmung darüber,
- ob die genetische Untersuchung durchgeführt werden soll,
- welches Ziel die genetische Untersuchung hat,
- ob sie auch unvermeidbare weitere Untersuchungsergebnisse zur Kenntnis nehmen will,
- wie gegebenenfalls mit der Probe und den genetischen Daten weiter verfahren werden soll.

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

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

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

Unterrichtung über das Untersuchungsergebnis

(1) Die veranlassende Ärztin oder der veranlassende Arzt teilt das Ergebnis der genetischen Untersuchung nur der betroffenen Person, bei Minderjährigen auch oder nur ihrem gesetzlichen Vertreter mit und berät über die möglichen Folgen und Entscheidungsalternativen.

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

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

Diagnostische genetische Untersuchung bei behinderten Personen

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

Genetische Untersuchungen im Zusammenhang mit Arbeits- und Versicherungsverhältnissen

Grundsatz

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

Arbeitsverhältnis

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

Ausnahmen für das Versicherungsverhältnis

(1) Strebt die betroffene Person eine Versicherung mit einer Leistungssumme über 250.000 € an, ist der Versicherer berechtigt zu fragen, ob und gegebenenfalls wann bei der betroffenen Person eine prädiktive genetische Untersuchung durchgeführt wurde. Bei arglistigem Verschweigen kann der Versicherer den Versicherungsvertrag kündigen.
(2) Bestehen konkrete Anhaltspunkte, insbesondere aufgrund des Zeitabstandes zwischen genetischer Untersuchung und Versicherungsantrag, dafür, dass die Höhe der gewünschten Versicherungsleistung mit dem Ergebnis der genetischen Untersuchung zusammenhängt, kann der Versicherer das Ergebnis der genetischen Untersuchung verlangen. Dies gilt nicht für eine genetische Untersuchung, die bei der betroffenen Person pränatal oder während der Minderjährigkeit oder einer Einsichtsunfähigkeit durchgeführt wurde. In diesen Fällen darf der Versicherer das Ergebnis der genetischen Untersuchung von der betroffenen Person entgegennehmen.

Genetische Untersuchungen zur Abstammungsklärung und zur Identifizierung außerhalb der Strafverfolgung

Grundsatz

(1) Zu Zwecken der Abstammungsklärung und der Identifizierung dürfen nur die dazu geeigneten und erforderlichen genetischen Untersuchungen (DNA-Identifizierungsmuster) durchgeführt werden. Diagnostische oder prädiktive Untersuchungen nach Krankheitsanlagen oder Merkmalen der betroffenen Person sind unzulässig. Abgesehen vom Merkmal Geschlecht sind unvermeidliche Überschussinformationen so früh wie möglich zu vernichten.
(2) Die untersuchende Stelle hat selbst die Proben bei der betroffenen Person zu entnehmen und dies zu dokumentieren.
(3) Die Proben sind zu vernichten, wenn die betroffene Person dies wünscht oder ein Gericht die Vernichtung anordnet, im Übrigen wenn die genetische Untersuchung durchgeführt ist. Die Dokumentation ist 10 Jahre aufzubewahren.

Einwilligung

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

Anordnung genetischer Untersuchungen zu Identifizierungszwecken

(1) In gerichtlichen und Verwaltungsverfahren kann das Gericht bzw. die Verwaltungsbehörde eine genetische Untersuchung zu Identifizierungszwecken anordnen, wenn die Identität einer Partei, eines Beteiligten oder einer für das Verfahren wichtigen dritten Person oder Leiche in Zweifel steht und nicht auf andere Weise geklärt werden kann. Ist die Identitätsfeststellung Voraussetzung für die Gewährung von behördlichen Genehmigungen oder Leistungen an die betroffene Person, ist die genetische Untersuchung nur mit ihrer Einwilligung zulässig.
(2) Die Anordnung hat die Art der Probe, das Ziel der Untersuchung sowie den Zeitpunkt der Vernichtung der Probe und der Löschung der genetischen Daten festzulegen. Bei lebenden Personen ist die Probe ohne Eingriff in die körperliche Unversehrtheit zu entnehmen, es sei denn, die betroffene Person willigt in einen Eingriff ein.

Genetische Untersuchungen zu Forschungszwecken

Konkrete, zeitlich befristete Forschungsvorhaben

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

(2) In den Fällen der Ziffer (1) Nr. 2 und 3 sind bei Proben vor der Untersuchung, bei genetischen Daten vor der Verarbeitung oder Nutzung die Merkmale, mit denen ein Personenbezug hergestellt werden kann, gesondert zu speichern. Die Zuordnungsmöglichkeit ist aufzuheben, sobald der Forschungszweck es erlaubt und schutzwürdige Interessen der betroffenen Person gemäß der Regelung über deren Rechte (siehe unten) nicht entgegenstehen.
(3) Die Proben dürfen nur im Rahmen des Forschungsvorhabens untersucht, die genetischen Daten dürfen nur zu den Zwecken verarbeitet oder genutzt werden, für die sie im Rahmen des Forschungsvorhabens erhoben wurden.
(4) Mit Beendigung des Forschungsvorhabens sind die Proben zu vernichten und die genetischen Daten zu löschen. Ist ihre Aufbewahrung oder Speicherung zum Zwecke der Selbstkontrolle der Wissenschaft erforderlich, ist dies in pseudonymisierter Form für einen Zeitraum von längstens 10 Jahren zulässig.
(5) Konkrete, zeitlich befristete Forschungsvorhaben nach Ziffer (1) bedürfen der vorherigen Zustimmung der zuständigen Ethikkommission.

Sammlungen von Proben und genetischen Daten

(1) Das Sammeln von Proben einschließlich isolierter DNS oder RNS oder von genetischen Daten zu allgemeinen Forschungszwecken ist nur zulässig, wenn die betroffenen Personen über Zweck und Nutzungsmöglichkeiten der Sammlung aufgeklärt wurden und in die Entnahme der Probe sowie die Aufnahme von Probe und Daten in die Sammlung eingewilligt haben (siehe unten) Satz 1 gilt entsprechend für die Übernahme bereits vorhandener Proben oder genetischer Daten.
(2) Die Zuordnung der Probe und der genetischen Daten zur betroffenen Person ist vor der Aufnahme in die Sammlung aufzuheben. Erfordert der Zweck der Sammlung die Möglichkeit einer Zuordnung, sind die Proben und die genetischen Daten vor der Aufnahme in die Sammlung bei Treuhändern zu pseudonymisieren.
(3) Vor einer Weitergabe von Proben und einer Übermittlung genetischer Daten für konkrete Forschungsvorhaben ist die Möglichkeit der Zuordnung zur betroffenen Person aufzuheben oder, wenn der Forschungszweck dem entgegensteht, eine weitere Pseudonymisierung gemäß den Regelungen bei Treuhändern (siehe unten) vorzunehmen.
(4) Der Träger einer Sammlung hat eine kontinuierliche interne Datenschutzkontrolle sicher zu stellen. Bei Trägerwechsel gehen alle Verpflichtungen aus diesem Gesetz auf den neuen Träger über. Soll eine Sammlung beendet werden, sind die Proben zu vernichten und die genetischen Daten sowie die beim Treuhänder (siehe unten) gespeicherten Daten zu löschen.
(5) Die Einrichtung einer neuen und die Übernahme einer bestehenden Sammlung nach Ziffer (1) bedürfen der Zustimmung durch die zuständige Ethikkommission. Die Einrichtung ist mit dem Votum der Ethikkommission und unter Darlegung der in den Vorschlägen zur Sammlung von Proben und genetischen Daten, zur Aufklärung und Einwilligung, über die Rechte der betroffenen Person und über die Treuhänder geforderten Maßnahmen bei der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen. Betriebs- und Geschäftsgeheimnisse sind kenntlich zu machen. Die Anzeige ist jeweils nach 5 Jahren mit einer Begründung der weiteren Speicherung zu erneuern. Ebenso sind die Vernichtung oder Löschung von Sammlungen nach Ziffer (1), die Löschung der Zuordnungsmerkmale bei Treuhändern und Trägerwechsel nach Ziffer (4) anzuzeigen.

Aufklärung und Einwilligung

(1) Die betroffene Person ist vor ihrer Einwilligung im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert (siehe oben), oder bei Sammlungen von Proben oder genetischen Daten (siehe oben) insbesondere aufzuklären über
- den verantwortlichen Träger des Forschungsvorhabens oder der Sammlung,
- das Ziel der Forschung oder bei Sammlungen die möglichen Forschungsrichtungen,
- ihre Rechte bei Patentanmeldungen und gewerblichen Nutzungen,
- die Dauer der Aufbewahrung von Proben und der Speicherung der genetischen Daten,
- Zeitpunkt und Art der Pseudonymisierung von Proben und genetischen Daten, sowie über die mögliche Wiederherstellung der Zuordnung zur betroffenen Person,
- ihr Recht - vorbehaltlich der pseudonymisierten Verarbeitung nach Beendigung des Forschungsvorhabens (siehe oben) - die Vernichtung der Probe und die Löschung der genetischen Daten oder die Aufhebung der Zuordnungsmöglichkeit zu verlangen, wenn sie die Einwilligung widerruft,
- ihr Recht, Ergebnisse von Untersuchungen nicht zur Kenntnis zu nehmen oder unter Nutzung eines darzustellenden Ent-Pseudonymisierungsverfahrens zu erfahren,
- ihr Recht, Auskunft über die zu ihr gespeicherten genetischen Daten zu verlangen.

Die Aufklärung hat schriftlich und mündlich zu erfolgen.
(2) Die Einwilligung soll die Entscheidung darüber umfassen, ob die betroffene Person vom Ergebnis der Untersuchung Kenntnis nehmen will oder nicht.
(3) Die Einwilligung kann eine Schweigepflichtentbindung für zu benennende behandelnde Ärzte einschließen, wenn die betroffene Person über Art und Umfang der Patientendaten informiert wird, die der Arzt für das Forschungsvorhaben (siehe oben) oder die Sammlung von Proben oder genetischen Daten (siehe oben) übermittelt.

Rechte der betroffenen Person

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

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

Treuhänder

(1) Die Pseudonymisierung von Proben und genetischen Daten erfolgt durch einen Treuhänder. Er vergibt die Pseudonyme unverzüglich, verwahrt und verwaltet die Zuordnungsmerkmale und sichert die Rechte der betroffenen Person (siehe oben). Soweit erforderlich, kann er für diese Zwecke Kontakt mit der betroffenen Person aufnehmen. Er hat keinen Zugriff auf genetische Daten.
(2) Treuhänder kann eine natürliche Person sein, die von Berufs wegen einer besonderen Schweigepflicht unterliegt und vom Träger des Forschungsprojekts oder der Sammlung von Proben oder genetischen Daten unabhängig ist. Im Vertrag zwischen dem Treuhänder und dem Träger des Forschungsvorhabens oder der Sammlung von Proben oder genetischen Daten sind insbesondere die Anlässe und das Verfahren zur Wiederherstellung des Personenbezuges, die Nutzungsformen durch die Selbstkontrollgremien der Wissenschaft sowie die technischen und organisatorischen Maßnahmen zur Datensicherheit festzulegen. Der Vertrag ist vorab der für die Datenschutzkontrolle zuständigen Behörde vorzulegen.

Schlussvorschläge

Ordnungswidrigkeit

Ordnungswidrig handelt, wer
- eine Reihenuntersuchung ohne die erforderliche Zulassung durchführt oder
- den Anzeigepflichten bei der Einrichtung einer neuen oder der Übernahme einer bestehenden Sammlung von Proben oder genetischen Daten oder bei bestehenden Proben- oder genetischen Datensammlungen nicht fristgemäß nachkommt.

Straftaten

(1) Wer genetische Testverfahren unter Verstoß gegen die Anforderungen an das Inverkehr-bringen genetischer Tests und Angebote von genetischen Untersuchungen einführt oder in Verkehr bringt oder genetische Untersuchungen ohne eine individuelle Beratung öffentlich anbietet, wird mit ... ...bestraft. Handelt die Täterin oder der Täter gewerbsmäßig, ist die Strafe ... .
(2) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu medizinischen Zwecken durchführt, ohne
- Arzt oder Ärztin zu sein,
- die für die genetischen Untersuchungen zu medizinischen Zwecken festgelegten Beschränkungen der Untersuchungszwecke einzuhalten,
- die geforderte Aufklärung und Beratung unternommen bzw. sichergestellt zu haben oder
- die Einwilligung der betroffenen Person eingeholt zu haben, wird mit ... ... bestraft.

(3) Wer als Arbeitgeber oder als Versicherer gegen das Verbot genetischer Untersuchungen verstößt, ohne dass die vorgesehene Ausnahmeregelung eingreift, wird mit ... ... bestraft.
(4) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu Zwecken der Abstammungsklärung oder Identifizierung in unzulässiger Weise auf prädiktive oder diagnostische Ziele ausrichtet oder ohne die geforderte Einwilligung durchführt, wird mit ... ... bestraft.
(5) Wer vorsätzlich oder fahrlässig personenbeziehbare Proben, DNS-/RNS-Teile oder genetische Daten entgegen den Regelungen für genetische Untersuchungen zu Forschungszwecken
- ohne Einwilligung oder Aufklärung zu Forschungszwecken nutzt oder
- in Sammlungen für Forschungszwecke zur Verfügung stellt,

wird mit ... ... bestraft.

Antrag

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

Befristung

Die Regelungen sind auf zehn Jahre zu befristen. Acht Jahre nach In-Kraft-Treten haben die für die Datenschutzkontrolle zuständigen Behörden unter Federführung des Bundesbeauftragten für den Datenschutz dem Gesetzgeber einen Bericht über die Wirksamkeit der

vorgeschlagenen Regelungen und über neue Gefährdungen für das Persönlichkeitsrecht sowie zu möglichen Rechtsvereinfachungen vorzulegen. Diesem Bericht sind Stellungnahmen des Ethikrates und der Deutschen Forschungsgemeinschaft beizufügen.

Übergangsvorschrift

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

27.15
Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober 2001

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

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, bei der technischen Realisierung und bei der anstehenden internationalen Normierung elektronischer Mautsysteme datenschutzrechtliche Anforderungen durchzusetzen.
Das Bundeskabinett hat am 15. August 2001 den Gesetzentwurf für die Einführung eines solchen Mautsystems beschlossen. Ab 2003 ist neben der manuellen Erfassung der Gebühren ein automatisches System geplant, mit dem eine streckenbezogene Autobahnbenutzungsgebühr (Maut) für Lastkraftwagen erhoben werden soll. Das Bundesministerium für Verkehr, Bau- und Wohnungswesen prüft zurzeit Angebote, die im Ergebnis einer europaweiten Ausschreibung eingegangen sind.

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

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

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

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

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

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Identität der Mautpflichtigen darf nur dann aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht entrichtet worden sind.

- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Mautpflichtigen durchschaubar sein. Sie müssen sich jederzeit über den Abrechnungsvorgang informieren sowie den eventuellen Kontrollvorgang erkennen können.

- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, dass sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

- Es ist sicherzustellen, dass anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen.

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

27.16
Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober 2001

Zur "neuen Medienordnung"

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

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

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

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

27.17
Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober 2001

Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

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

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

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

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

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

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

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

Der Verfassungsschutz soll künftig zur Erfüllung aller seiner Aufgaben von den Banken die Kontenbewegungen, von den Luftverkehrsunternehmen alle Reisedaten und von den Post- und Telekommunikationsunternehmen alle Informationen darüber erhalten können, wer von wem Post erhalten und wann mit wem telefoniert hat. All dies soll ohne Wissen der Betroffenen erfolgen und bis zu 15 Jahren gespeichert werden.
Die geplante Befugnis des BKA, Vorermittlungen ohne Anfangsverdacht im Sinne der StPO zu ergreifen, führt zu Eingriffen in das Persönlichkeitsrecht, die weit über das verfassungsrechtlich Zulässige hinausreichen und das tradierte System der Strafverfolgung sprengen. Dies verschiebt die bisher klaren Grenzen zwischen BKA und Verfassungsschutz sowie zwischen Gefahrenabwehr und Strafverfolgung. Ohne jeden Anfangsverdacht soll das BKA künftig Daten über nicht näher eingegrenzte Personenkreise erheben dürfen. Dies kann im Prinzip jede Bürgerin und jeden Bürger betreffen, ohne dass sie sich auf die Schutzmechanismen der Strafprozessordnung verlassen können.

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

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

27.18
Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober 2001

Biometrische Merkmale in Personalausweisen und Pässen

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

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

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

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

27.19
Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober 2001

EUROJUST - Vorläufer einer künftigen europäischen Staatsanwaltschaft?

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

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

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

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

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

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

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

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

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

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

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

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

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

Rechtsetzungsbedarf

Zur Erfüllung seiner Aufgaben muss EUROJUST Auskünfte über strafrechtliche Ermittlungsverfahren einholen. Nach geltendem Recht (§ 474 StPO) können die Ermittlungsbehörden der Bundesrepublik Deutschland derartigen Ersuchen nicht stattgeben. Darüber hinaus bedarf der Zugriff des deutschen EUROJUST-Mitglieds auf das Bundeszentralregister und auf das Zentrale Staatsanwaltschaftliche Verfahrensregister einer eindeutigen gesetzlichen Grundlage.

28. Materialien

28.1
Dienstliche und private Nutzung von E-Mail und www
(Stand: 17. Oktober 2001)

Bei der Nutzung der Internetdienste E-Mail und www entstehen eine Reihe datenschutzrechtlicher Fragen, die in nachfolgendem Papier diskutiert sind. Die Zulassung privater Nutzung wirft rechtliche Probleme auf, die nur mit technischen und organisatorischen Maßnahmen und bei Einwilligung jedes Bediensteten in die Verarbeitung seiner Daten zu lösen sind.
Bei E-Mail werden auf dem E-Mail-Server Verbindungsdaten zu jeder E-Mail aufgezeichnet, d.h. wer wohin wann und in welcher Größe eine E-Mail versendet. Diese Daten können mit dem Ende der Verbindung gelöscht oder auch längerfristig gespeichert werden (programmabhängig). Eine Speicherung der Verbindungsdaten der E-Mail-Verbindung kann z. B. Nachweis der Absendung, zum Zwecke der Fehlersuche oder der Missbrauchskontrolle erforderlich sein oder werden. Außerdem wird die eigentliche E-Mail zwischengespeichert. Die rechtlichen Bedingungen, welche Daten unter welchen Voraussetzungen, zu welchem Zweck und wie lange gespeichert werden dürfen und wer wann darauf zugreifen darf, sind nachfolgend dargelegt. Dabei sind die Fälle der ausschließlich dienstlichen und der ausschließlich privaten Nutzung rechtlich unproblematisch; schwierige Rechtsfragen entstehen dagegen, wenn diese beiden Nutzungsarten vermischt werden.

1. Dienstliche Nutzung von E-Mail

Gegen eine *Speicherung von Verbindungsdaten* dienstlicher E-Mail bestehen keine Bedenken. Die Zwecke der Protokollierung richten sich nach den Bedürfnissen der Dienststelle (z. B. Missbrauchskontrolle, Fehlersuche, Nachweis von Posteinund -ausgängen). Jede Dienststelle hat aufgrund der konkret bei ihr gegebenen Situation über die Zwecke und die Erforderlichkeit der Protokollierung sowie über die Dauer der Speicherung der Protokolldaten zu entscheiden. Die Protokolle dürfen nur zu dem festgelegten Zweck ausgewertet werden und nur solange gespeichert bleiben, wie es für diesen Zweck notwendig ist (§§ 13 Abs. 5, 34 Abs. 6 HDSG).
Die *Speicherung des Inhalts* der E-Mail ist - wie das Aufheben von herkömmlicher ein- und ausgehender Dienstpost - für den Dienstbetrieb notwendig. Die Inhalte dienstlicher E-Mails unterliegen im Verhältnis zur Dienststellenleitung nicht dem Fernmeldegeheimnis. Ebenso wie vom sonstigen dienstlichen Schriftverkehr dürfen außer dem Adressaten auch sonstige zuständige Bedienstete und die Leitung der Dienststelle von Inhalten der E-Mails Kenntnis nehmen. Ausgenommen davon sind E-Mails, die an Funktionsträger gerichtet sind, für die eine besondere Vertrauensstellung besteht (z. B. Personalrat). Es empfiehlt sich für diesen Personenkreis, eigene E-Mail-Adressen einzurichten und zumindest organisatorisch (z. B. durch ausdrückliche Anweisung an die Administratoren) sicherzustellen, dass die Inhalte von Dritten in der Dienststelle nicht erschlossen werden.

2. Rechtsfragen bei vom Dienstherrn zugelassener privater Nutzung von E-Mail

Keine Dienststelle ist verpflichtet, private E-Mail- oder Internet-Nutzung zuzulassen. Wenn die private Nutzung zugelassen wird, sollten Dienststellen sich vorher über die technischen und organisatorischen Rahmenbedingungen und über deren Rechtsfolgen im Klaren sein. Die nachfolgenden Ausführungen sollen Orientierung und Hilfestellung für die erforderlichen Abwägungen und Festlegungen bieten.

Wird auch die private Nutzung von E-Mail erlaubt, ergeben sich zahlreiche Rechtsprobleme. Insbesondere sind das Fernmeldegeheimnis (§ 85 Telekommunikationsgesetz) und die Regelungen des Teledienstedatenschutzgesetzes (TDDSG) zu beachten. Der Arbeitgeber wird mit der Zulassung der privaten Nutzung Diensteanbieter im Sinne des TDDSG.

Die **Inhalte** privater E-Mails dürfen grundsätzlich von der Dienststelle nicht zur Kenntnis genommen werden, denn diese werden vom Fernmeldegeheimnis erfasst. Lässt die Dienststelle die Nutzung von E-Mail auch zu privaten Zwecken zu, so muss sie Maßnahmen wählen, um dieses sicherzustellen.

Auch die **Verbindungsdaten** unterliegen dem Fernmeldegeheimnis. Der Diensteanbieter muss die personenbezogenen Daten des privaten Nutzers löschen, und zwar unmittelbar nach Beendigung des Abrufs oder Zugriffs (§ 4 Abs. 2 Ziff. 2 TDDSG). Abweichend davon erlaubt das TDDSG eine Speicherung, soweit und solange sie erfolgt, um dem Nutzer die Inanspruchnahme des Dienstes zu ermöglichen oder zu Abrechnungszwecken. Wenn die Nutzung des Dienstes generell unentgeltlich zugelassen wird, kann die Speicherung der Verbindungsdaten nicht mit Abrechnungszwecken gerechtfertigt werden. Soweit die Protokollierung von Verbindungsdaten allerdings für die Fehlersuche und -behebung erforderlich ist, und damit der Aufrechterhaltung des Dienstes dient, darf sie kurzfristig auch erfolgen (§ 6 Abs. 1 Nr. 1 TDDSG). Auch bei privaten E-Mails gilt, dass Speicherung und Zugriff auf diese Daten nur für Zwecke der Fehlerbehebung und zur Aufrechterhaltung des E-Mail-Betriebes zulässig sind.

Gibt es nur eine **einheitliche E-Mail-Adresse** für dienstliche und private E-Mails, so müssen aus technischen Gründen private und dienstliche E-Mails gleich behandelt werden. Deshalb müssten auch dienstliche E-Mails rechtlich zwingend nach den für private E-Mail geltenden Rechtsvorschriften behandelt werden. Unter dieser Voraussetzung kann der ordnungsgemäße Dienstbetrieb nicht aufrechterhalten werden. Bei dienstlichen E-Mails besteht das Interesse der Dienststelle, Verbindungsdaten z. B. zum Nachweis des Postein- und -ausgangs längerfristig zu speichern, was bei privater E-Mail nicht zulässig wäre. Die Einhaltung des Fernmeldegeheimnisses bei privaten Nutzungen ist indes nur möglich, wenn von den Inhalten aller E-Mails keine anderen Personen als die Adressaten Kenntnis erhalten. Dies bringt eine erhebliche Erschwerung für die Verarbeitung dienstlicher E-Mails mit sich, weil die Dienststelle dann auf die für sie bestimmten Speicherungen nicht zugreifen und auch eine Weiterleitung der E-Mails an die Vertretung und Kontrollen nicht vorsehen kann. Darin liegen aber legitime Interessen der Dienststelle. Da es keine technische Möglichkeit gibt, zwischen dienstlichen und privaten Verbindungsdaten zu unterscheiden, wenn für private und dienstliche E-Mails über denselben Server laufen, müssten auch die Verbindungsdaten dienstlicher E-Mails nach kurzer Zeit gelöscht werden. Sollen Verbindungsdaten gespeichert werden, etwa weil dies für parallel laufende dienstliche E-Mail erforderlich ist (z. B. zum Nachweis des Postein- und -ausgangs) und eine Trennung von dienstlicher und privater E-Mail technisch nicht geleistet werden kann, kann den Anforderungen des § 4 Abs. 2 Nr. 2 TDDSG nicht genügt werden.

Das gilt noch mehr für die Inhaltsdaten der E-Mails. Eine Einwilligung der Nutzer in die Kenntnisnahme der Inhalte aller privaten E-Mails durch die Dienststelle, die eine einheitliche Behandlung nach den für dienstliche E-Mails geltenden Regeln ermöglichen würde, stellt sich als völlige Aufhebung des Fernmeldegeheimnisses dar, was einer Einwilligung nicht zugänglich ist.

Ein technisch einfacher Ausweg ist die Einrichtung einer **separaten E-Mail-Adresse für private Nutzungen**. Durch die Einrichtung einer dienstlichen und einer zusätzlichen privaten E-Mail-Adresse kann eine Kenntnisnahme des Inhalts privater E-Mails durch Dritte weitgehend, wenn auch nicht vollständig, ausgeschlossen werden. Für den Dienstbetrieb ist es grundsätzlich nicht erforderlich, auf die Inhalte von E-Mails in der privaten Adresse zuzugreifen. Durch die separate Adresse kann die Einhaltung dieser Schranke auch weitgehend technisch sichergestellt werden. Allerdings ist der Administrator in jedem Fall technisch in der Lage, den Inhalt privater E-Mails zur Kenntnis zu nehmen.

Soweit die Speicherungen von Verbindungsdaten privater E-Mails nicht für Abrechnungszwecke oder zur Aufrechterhaltung des Dienstes erforderlich sind, dürfen sie nur mit ausdrücklicher Einwilligung der Betroffenen geschehen. Die Einwilligung ist außerdem erforderlich, wenn bereits bei der Zulassung der privaten Nutzung Einschränkungen gemacht worden sind (z. B. im Umfang oder zur Vermeidung von Störungen des Dienstbetriebes), und die Prüfung der Einhaltung dieser Einschränkungen möglich sein soll (Missbrauchskontrolle). Mitarbeiter, die die Einwilligung verweigern, müssen von der privaten Nutzung ausgeschlossen werden. Die Einwilligung kann weder kollektivrechtlich (sprich: durch Vereinbarung mit dem Personalrat) noch durch die konkludente Anerkennung einer Nutzungsordnung erfolgen. Mit jedem Mitarbeiter und jeder Mitarbeiterin muss eine schriftliche Vereinbarung über die genauen Bedingungen der Nutzung der E-Mail für private Zwecke geschlossen werden, in der aber auf die Bedingungen einer Nutzungsordnung verwiesen werden kann. In der Nutzungsordnung muss die Dienststellenleitung insbesondere auch festlegen, welche Überprüfungen vom Administrator oder von der Dienststellenleitung wahrgenommen werden. Die Vereinbarung muss (ggf. durch Verweis auf die Nutzungs-

ordnung) den Umfang des Verzichts auf die Rechte beschreiben - z. B. die mögliche Kenntnisnahme der privaten Verbindungen durch den Administrator und im Einzelfall auch der Inhalte, soweit dies zur Missbrauchskontrolle notwendig ist. Das TDDSG verbietet dem Diensteanbieter zwar, die Erbringung des Teledienstes von der Einwilligung des Nutzers in zusätzliche Datenverarbeitung abhängig zu machen, das gilt jedoch nur, soweit der Diensteanbieter eine Monopolstellung inne hat (§ 3 Abs. 3 TDDSG). Letzteres trifft auf den Arbeitgeber nicht zu, denn er ist nicht verpflichtet, den Bediensteten die Nutzung des Internets überhaupt zu ermöglichen.

Eine weitere - bessere - Möglichkeit ist die Gestattung der privaten Nutzung des www zum **Abruf von E-Mails vom externen** (z. B. häuslichen) **Web-Mail-Anschluss**. Auch hierbei ist der Zugriff von Personen in der Dienststelle, an die die E-Mail nicht adressiert ist, auf die Inhalte nicht völlig ausgeschlossen, allerdings kann der Nutzer das weitgehend selbst ausschließen, z. B. in dem er den Cache-Speicher nach Abruf der E-Mail löscht. Hinsichtlich der Verbindungsdaten gilt das oben Gesagte auch für diese Lösung, d.h. die Nutzer müssen ihre ausdrückliche Einwilligung unter den von der Dienststelle zu setzenden Rahmenbedingungen erklären.

3. Dienstliche und private Nutzung des www:
Verarbeitung von Verbindungsdaten/Kenntnisnahme des Inhalts aufgerufener Internetseiten durch die Dienststelle

Für die Protokollierung des Aufrufs von Internet-Seiten gilt Entsprechendes. Eine Protokollierung des Aufrufs von Internet-Seiten kann in der Dienststelle u.U. an mehreren Orten erfolgen. Nicht nur auf Servern oder Firewalls, sondern auch am Arbeitsplatz werden Daten über aufgerufene Internetseiten - je nach Einstellung der Browser - gespeichert. Bei der Protokollierung ist eine Trennung nach dienstlicher und privater Nutzung des Internet technisch nicht möglich. Für jede Protokollierung müssen insbesondere der Zweck (Datensicherheit, Fehlersuche, Missbrauchskontrolle), der Umfang und die Dauer der Speicherung festgelegt werden.
Die Nutzung der Protokollierung von Internetzugriffen der Mitarbeiter zur laufenden Verhaltens- und Leistungskontrolle ist unverhältnismäßig und daher unzulässig.
Sofern eine private Nutzung des Internet zugelassen wird, bedarf es hierfür individueller Nutzungsvereinbarungen. Insofern gelten die Ausführungen zu 2. entsprechend.

28.2
Datenschutz in der Justiz

I. Grundnorm: HDSG

Maßgebend für die datenschutzrechtlichen Pflichten ist das Hessische Datenschutzgesetz, im Rahmen verfassungskonformer Eingrenzungen ergänzend das Grundrecht auf informationelle Selbstbestimmung. Das HDSG legt die folgenden Grundsätze für die Richterschaft fest:

- Die materiell-rechtliche Geltung des HDSG für alle richterlichen Handlungen, einschließlich der Entscheidungsfindung und der vorausgehenden Schritte (§ 3 Abs. 1 Satz 1 HDSG).

- Die Einrichtung eines - weisungsfreien - gerichtlichen Datenschutzbeauftragten zur gerichtsinternen Sicherstellung des Datenschutzes (§ 5 Abs. 1 HDSG). Ihm stehen allerdings keine Befugnisse zu, die die richterliche Unabhängigkeit einschränken können (Art. 97 Abs. 1 GG). Im Grundsatz ist das HDSG zu vollziehen, verfassungsrechtliche Einwendungen unterliegen dem Verwerfungsmonopol des Bundesverfassungsgerichts.

- Die Beschränkung der Kontrollbefugnisse des HDSB auf Tätigkeiten, die außerhalb richterlicher Unabhängigkeit liegen (§ 24 Abs. 1 Satz 3 HDSG).

II. Abweichungen vom allgemeinen Datenschutzrecht

Divergenzen gegenüber den allgemeinen datenschutzrechtlichen Pflichten ergeben sich für Richter vor allem aus:

- der institutionellen Garantie richterlicher Unabhängigkeit,
- den verfahrensrechtlichen Regelungen der Prozessordnungen, insbesondere den dort begründeten Übermittlungs- und Benachrichtigungspflichten,
- bundesrechtlichen Sondervorschriften der Strafprozessordnung und des Strafvollzugsgesetzes, des HGB (Handelsregister), der Insolvenzordnung (Veröffentlichung), des BGB (Vereins- und Güterrechtsregister).

III. Einzelne Problembereiche:

1. Arbeit am PC - Dienstausübung ohne Grundrechtsschutz

Richterliche Tätigkeiten am PC oder im gerichtseigenen Netz (Serverbetrieb) erfolgen in Dienstausübung und unterstehen daher keinen grundrechtlichen Beschränkungen. Richterliche Unabhängigkeit stellt keine Individualrechtsgewährleistung dar, so dass keine persönlichen informationellen Abwehrrechte daraus herzuleiten sind. Die dienstlich bedingten Zugriffsrechte der einzelnen Richter sind vom Präsidium bzw. Vorsitzenden Richter des Spruchkörpers genau und vorab festzulegen. Die Ein-

richtung der Zugriffsrechte erfolgt durch die Administratoren nach den Vorgaben des Präsidiums. Eigenständige Zugriffsrechte der Geschäftsstellen, des Präsidenten/Direktors oder des Pressesprechers dürfen nicht vorgesehen werden, soweit richterliche Tätigkeiten von sonstigen ununterschieden gespeichert sind.

2. Technische Sicherheitsmaßnahmen

Der richterliche Arbeitsplatz ist durch technische Sicherheitsmaßnahmen gegen unberechtigte Zugriffe zu sichern (§ 10 HDSG). Einzelarbeitsplätze, die am gerichtlichen Netz hängen, müssen nicht nur gegen externe, sondern auch gegen unberechtigte interne Zugriffe geschützt werden, da erfahrungsgemäß ca. 80 % der unberechtigten Zugriffe von innen kommen. Dies kann mit Firewalls am Arbeitsplatz, Intrusion Detection Systemen oder vergleichbaren Maßnahmen erreicht werden. Passwortschutz allein reicht nicht aus.

Der Rechtsgrund für die Sicherheitsmaßnahmen liegt im Amtsgeheimnis (§§ 203, 353b StGB) und im Datengeheimnis (§ 9 HDSG). Geschützt ist das Vertrauen in das amtliche Stillschweigen.

3. Vorabkontrolle

Da die Arbeit am PC oder Server „automatisierte“ Datenverarbeitung (Definition: § 3 Abs. 2 BDSG, enger § 2 Abs. 6 HDSG) darstellt, sind Vorabkontrollen durchzuführen und Verfahrensverzeichnisse zu erstellen (§§ 6, 7 Abs. 6 HSDG). In die Verfahrensverzeichnisse kann jedermann einsehen. Die bisherige Regelung in § 6 Abs. 2 Satz 2 Ziff. 2 HDSG wird durch § 491 Abs. 2 StPO überlagert.

4. Zuständigkeits- sind Zugriffsgrenzen

Zuständigkeitsübergreifende Zugriffe (bspw. des leitenden Richters oder des Dienstherrn) auf den Arbeitsplatz sind unzulässig. Nicht ausgeschlossen sind Zugriffe im Vertretungsfall, da der Vertreter den Richter uneingeschränkt ersetzt (zum Zugriff auf Entwürfe vgl. unten Ziff. 10). Ist der Vorsitzende des Spruchkörpers Vertreter, so steht auch ihm das Zugriffsrecht zu.

5. Dienstordnungs- und strafverfolgende Zugriffe

Zugriffsbefugnisse in Zuge von Ermittlungen gegen den Richter bestehen nur in Disziplinarverfahren oder zur Strafverfolgung (bspw. Vorwurf der Rechtsbeugung, Bestechlichkeit). Insofern gilt das Gleiche wie bei Papierakten. Problematisch ist, ob § 22a HDO auch gegenüber diesbezüglichen Speicherungen im richterlichen PC gilt. Soweit ein förmliches Verfahren eröffnet oder Vorermittlungen für die Verfügung eines Verweises angeordnet ist, sieht das HRiG keine Abweichung vom allgemeinen Dienstordnungsrecht vor. Sofern nicht besondere Gründe vorliegen, die dafür sprechen, dass der Zugriff auf Daten die richterliche Unabhängigkeit in Frage stellen kann und soll, ist § 22a auch bei richterlichen PC-Arbeitsplätzen anzuwenden.

6. Administration

Die alltäglichen Fehler am PC (Abstürze, Programmmängel, Zugriffsverweigerung, Passwortirrtümer) zwingen zur Vorhaltung einer professionellen Administration der PC oder der Server. Die Administration sollte weder durch staatliche Fernwartungsanbieter noch durch außenstehende Firmen erfolgen, da deren Verhalten im Netz nur schwer kontrollierbar ist (vgl. HDSB-Mustervertrag Fernwartung, unter www.datenschutz.hessen.de:Musterverträge). Es ist dringend zu empfehlen, dass gerichtsinterne Administratoren durch Dienstanweisung auf unerlässliche Datenzugriffe beschränkt und - ergänzend zu § 9 HDSG - zu besonderer Geheimhaltung verpflichtet werden.

7. Gerichtliche Datenschutzbeauftragte

Der - weisungsunabhängige und zur Geheimhaltung verpflichtete - gerichtliche Datenschutzbeauftragte muss ungeachtet der Schranken aus Art. 97 GG überall dort auf Erfüllung der datenschutzrechtlichen Pflichten durch die Richterschaft dringen, wo eine verfassungskonforme Reduktion den Auslegungsspielraum überschreiten würde. Das gilt insbesondere für die Prüfung, ob die institutionellen datenschutzrechtlichen Sicherungen auf den Richter-PC und Arbeitsplätzen eingehalten sind.

8. Elektronische Kommunikation innerhalb der Gerichte

Der Umfang elektronischer Kommunikation innerhalb der Gerichte hängt vom Willen der Teilnehmenden ab und stellt deswegen keine Gefahr für die richterliche Unabhängigkeit dar. Die Grenze liegt daher im Datenschutz: Soweit personenbezogene Daten Parteien/Beteiligte weitergegeben werden, handelt es sich um eine Übermittlung, die aufgrund des prozessualen Verfahrensrechts legitimiert ist und damit im Rahmen der Zweckbestimmung liegt. Diese darf nur ausnahmsweise durchbrochen werden (§§ 13 Abs. 2, 12 Abs. 2 HDSG). Regelmäßig darf innerhalb des Spruchkörpers und des Instanzenzuges übermittelt werden. Eine „Beiziehung“ zu anderen Verfahren muss über die jeweiligen Verfahrensordnungen oder § 12 Abs. 2 HDSG legitimiert werden.

Neben der technischen Absicherung des richterlichen Arbeitsplatzes muss auch die Kommunikation und der Datenaustausch unter Richtern und deren Hilfskräften sicher (verschlüsselt) ablaufen. Neue Betriebssysteme wie zum Beispiel Windows 2000 bieten die dazu nötigen Funktionen.

9. Elektronische Kommunikation mit Außenstehenden

Elektronische Kommunikation mit Parteien/Beteiligten/Angeklagten setzt deren ausdrückliche Zustimmung voraus. Sie wird durch die Angabe einer E-Mail-Adresse nicht erteilt. Zugangsfragen werden derzeit beraten. Alle Datenschützer fordern, auch hier die 3-Tages-Frist gelten zu lassen. Die Kommunikation bedarf aus datenschutzrechtlichen Gründen der Verschlüsselung. Außerdem ist bei verfahrensbestimmenden Verfügungen und Entscheidungen mit einer qualifizierten elektronischen Signatur (ggf. mit Anbieterakkreditierung) zu arbeiten. Einfacher ist allerdings die nachfolgende Versendung in Papierform.

10. Speicherungen vor Verkündung

Speicherungen vor Verkündung der Entscheidung berühren neben datenschutzrechtlichen Fragen auch die richterliche Unabhängigkeit. Eine Einsichtnahme durch Dritte erlaubt diesen möglicherweise, den Entscheidungsprozess nachzuvollziehen und ggf. anders zu beeinflussen, als das ohne die so erlangte Kenntnis stattfände.

Der Zugriff des Vertreters auf vorbereitende Überlegungen setzt die Einwilligung des eigentlich Zuständigen voraus, denn der Vertreter entscheidet aus eigener Beurteilung; im Übrigen kann er zugreifen.

11. Speicherungen nach Rechtskraft

Speicherungen nach Rechtskraft der Entscheidung berühren nur noch Datenschutz. Da gerichtliche Entscheidungen das Zivil- oder Verwaltungsrechtsverhältnis bestimmen, zuweilen sogar gestalten, sind sie zu dokumentieren. Das Gleiche gilt für Strafakten, deren lebensgestaltende Wirkung über den Tag der Entscheidung hinausreicht; auch sie sind zu dokumentieren. Aufbewahrungsort kann die traditionelle Papierakte oder ein grundsätzlich gleichwertiges elektronisches Aktenverwaltungssystem sein. Zugang zu dieser Dokumentation ist den Verfahrensbeteiligten zu gewähren und staatlichen Instanzen, denen eine Zugriffsbefugnis gesetzlich eingeräumt worden ist.

12. Nachweissystem – Anonymisierung

Für alle übrigen Nutzer ist grundsätzlich der Weg der Anonymisierung zu gehen. Die Wiederauffindung von Präjudizien wird durch Schlagworte oder Volltext-Suchfunk-tionen besser geleistet als durch Namen (Bsp. JURIS-Erschließung). Der Einwand zu hohen Arbeitsaufwands ist nicht begründet, da mit einfachen PC-Befehlen („Ersetzen“) Namen getilgt und durch A, B, C ersetzt werden können. Ausdrucke auf Papier sind nach Anonymisierung zu erstellen - das gilt auch für die gerichtsinterne Information und Bibliothek. Die personenbezogenen Daten sind zu löschen, sobald feststeht, dass sie nicht mehr benötigt werden (§ 19 Abs. 3 HDSG). Sofern neben dem Urteilsausdruck auf Papier elektronische Dokumente mit Personenbezug aufbewahrt werden sollen, ist die Verwendung von Disketten oder CD-ROM vorzuziehen, da diese der Akte beigefügt werden können.

13. Auswertung der Speicherungen durch die Dienststelle

Eine dienstaufsichtlich zu begründende oder organisationsrechtlich begründete Auswertung von Speicherungen in Einzel-PCs und Servern (bspw. durch das Präsidium) ist generell unzulässig, soweit die betreffenden Daten auf richterliche Tätigkeiten zurückgehen. Insoweit besteht hinsichtlich der Inhalte keine allgemeine dienstaufsichtliche Zuständigkeit. Eine „Erledigungskontrolle“ im Sinne eines Pensenschlüssels darf nicht durch Zugriffe auf den PC oder Server stattfinden; sie muss - soweit sie dienst- und personalvertretungsrechtlich zulässig ist - offen und mit Kenntnis der betroffenen Richterinnen und Richter über Art und Umfang der dabei verwendeten Daten erfolgen. Überprüft werden kann allerdings auch von der Dienstaufsicht, ob die in § 10 vorgeschriebenen informationstechnischen Sicherheitsbestimmungen eingehalten werden, ob ausreichende Verfahrensverzeichnisse erstellt worden sind, insbesondere, ob die Übermittlungsschranken aus § 13 Abs. 1 HDSG beachtet sind. Insofern sind keine Probleme richterlicher Unabhängigkeit berührt.

14. Missbrauch des Internetzugangs

Vermutete Straftaten oder vermuteter Missbrauch des Internetzugangs dürfen nur straf- oder disziplinarrechtlich verfolgt werden, nicht durch formlose Einsichtnahme. Im Straf- oder Disziplinarverfahren sind nur solche Zugriffe als „erforderlich“ i. S. v. § 11 Abs. 1 HDSG anzusehen, mit denen Dienstvergehen bewiesen werden sollen, die sich aus dem Vorgang der Entscheidungsfindung, aus anderen dienstlichen Verrichtungen oder aus allgemeinen Straftaten herleiten.

15. Internet-Nutzung und E-Mails

Hier entstehen wiederkehrende Gefahren, da unberechtigte Zugriffe auf dienstliche PC oder Server von außen nicht mit Sicherheit abgewehrt werden können. Nicht einmal der Einsatz von Firewalls und Intrusion Detection Systemen bietet eine 100 %-Sicherheit. Um eine höchstmögliche Sicherheit zu erreichen, ist der Einsatz besonderer PCs zweckmäßig, die vom Gerichtsnetz physikalisch getrennt sind und auf denen sich keine zu schützenden Daten befinden. Besondere Gefahren entstehen bei der Öffnung von „Anhängen“ zu E-Mails, da sie Schadprogramme enthalten können. Auch sie sollten nur auf PCs geöffnet werden, die keine Verbindung zum inneren Netz haben.

16. Private Mitnutzung

Die persönliche Inanspruchnahme dienstlicher Internet-Anschlüsse führt zu kaum überwindbaren Telekommunikationsproblemen, denn die Dienststelle wird damit Diensteanbieter (Provider) und darf nach TDDSG und TKG nur auf die Verbindungsdaten (zur Abrechnung und Funktionssicherung) zugreifen, die Inhalte hingegen nicht zur Kenntnis nehmen. Das aber ist für dienstliche E-Mails unerlässlich (vgl. dazu das Papier: Dienstliche und private

Nutzung von E-Mail und www, Stand 24.10.2001, unter www.datenschutz.hessen.de). Private Mitnutzung sollte deswegen nicht gestattet werden, allenfalls der Abruf von der privaten Mailbox über dienstliche Anschlüsse.

17. Bereichsspezifische strafprozessuale Datenschutzvorschriften

Die neu gefasste StPO (§§ 474 bis 495) enthält erstmals eigenständiges Datenschutzrecht für das Strafverfahren. Außerdem werden die Übermittlungsbefugnisse zwischen StA und Polizei und die (gelockerte) Zweckbindung bei repressiven und präventiven Zwecken geregelt. Die §§ 479, 481 StPO regeln, inwieweit die Staatsanwaltschaften andere Strafverfolgungs- und Polizeibehörden aktiv informieren dürfen. Die §§ 474 bis 495 StPO sind als bereichsspezifische Regelung auf die Strafverfolgung beschränkt. Eine entsprechende Anwendung in anderen Bereichen der Gerichtsbarkeit scheidet aus.

18. Übermittlungen außerhalb der StPO

Die Übermittlungsbefugnisse der anderen Gerichtsbarkeiten richten sich nach den Verfahrensordnungen bzw. § 13 HDSG. Nach § 13 Abs. 1 können Übermittlungen im Rahmen der jeweiligen Zweckbestimmung erfolgen, bspw. an die Vollstreckungsinstanzen. Nach § 13 Abs. 2 i. V. m. § 12 Abs. 2 darf übermittelt werden, wenn antragsbegründende Angaben des Betroffenen überprüft werden müssen oder wenn die Abwehr erheblicher Nachteile für das Gemeinwohl oder für Leben, Gesundheit und persönliche Freiheit das gebietet, oder in Fällen, in denen sich Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben haben.