XVI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Niedersachsen für die Jahre 2001 und 2002

Inhalt XVI. Tätigkeitsbericht

Abkürzungsverzeichnis

ABl. ..... Amtsblatt
Abs. ..... Absatz
ADV ..... Automatisierte Datenverarbeitung
AG ..... Aktiengesellschaft
AGB ..... Allgemeine Geschäftsbedingungen
AO ..... Abgabenordnung
AOK ..... Allgemeine Ortskrankenkasse
Art. ..... Artikel
AsylbLG ..... Asylbewerberleistungsgesetz
AsylVfG ..... Asylverfahrensgesetz
ATG ..... Aktionsforum Telematik im Gesundheitswesen
Aufl. ..... Auflage
AuslG ..... Ausländergesetz
AV ..... Allgemeine Verfügung
AWG ..... Außenwirtschaftsgesetz
AZRG ..... Gesetz über das Ausländerzentralregister
BAFl ..... Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAG ..... Bundesarbeitsgericht
BAMF ..... Bundesamt für Migration und Flüchtlinge
BDSG ..... Bundesdatenschutzgesetz
BfA ..... Bundesversicherungsanstalt für Angestellte
BfV ..... Bundesamt für Verfassungsschutz
BfD ..... Bundesbeauftragter für den Datenschutz
BGB ..... Bürgerliches Gesetzbuch
BGBl. ..... Bundesgesetzblatt
BGH ..... Bundesgerichtshof
BGS ..... Bundesgrenzschutz
BKA ..... Bundeskriminalamt
BKAG ..... Gesetz über das Bundeskriminalamt
BLK ..... Bund-Länder-Kommission
BNotO ..... Bundesnotarordnung
BND ..... Bundesnachrichtendienst
BRAO ..... Bundesrechtsanwaltsordnung
BR-Drs. ..... Bundesrats-Drucksache
BRRG ..... Beamtenrechtsrahmengesetz
BSHG ..... Bundessozialhilfegesetz
BSI ..... Bundesamt für Sicherheit in der Informationstechnik
BT-Drs. ..... Bundestags-Drucksache
Buchst. ..... Buchstabe
BVerfG ..... Bundesverfassungsgericht
BVerfGE ..... Amtliche Sammlung der Entscheidungen des BVerfG
BVerfSchG .. Bundesverfassungsschutzgesetz
BVerwG ..... Bundesverwaltungsgericht
BVerwGE .... Amtliche Sammlung der Entscheidungen des BVerwG
BW ..... Baden-Württemberg
bzgl. ..... bezüglich
CD-ROM ..... Compact Disc-Read Only Memory (nur lesbares Datenspeicherungsmedium)
CRM ..... Customer Relationship Management (Kundenbindungsverwaltung)
d.h. ..... das heißt
DENIC ..... Deutsches Network Information Center - „DE-NIC“
DNA ..... Deoxyribonucleic acid (Desoxyribonukleinsäure)
DSB ..... Datenschutzbeauftragter
DSRL ..... Datenschutzrichtlinie
EDV ..... Elektronische Datenverarbeitung
EFS ..... Encrypted File System (Verschlüsseltes Dateisystem)
EG ..... Europäische Gemeinschaft
EGG ..... Elektronischer Geschäftsverkehr-Gesetz
einschl. ..... einschließlich
EU ..... Europäische Union
EUROPOL .. Europäisches Polizeiamt
evtl. ..... eventuell
EWR ..... Europäischer Wirtschaftsraum
FAQ ..... Frequently asked questions (häufig gestellte Fragen)
f(f). ..... und folgende Seite(n)
ftp ..... File Transfer Protocol [Internetdienst]
GBO ..... Grundbuchordnung
GG ..... Grundgesetz
ggf. ..... gegebenenfalls
GDV ..... Gesamtverband der Deutschen Versicherungswirtschaft
GDW ..... Games Designer Workshop
GewO ..... Gewerbeordnung
GEZ ..... Gebühreneinzugszentrale
GMBl. ..... Gemeinsames Ministerialblatt
GPRS ..... General Packet Radio Services (allgemeiner Dienst zur Übermittlung von Daten per Funk) [Mobilfunkstandard]
GPS ..... Global Positioning System (weltweites Ortungssystem)
GSM ..... Global System for Mobile communication (weltweites System für mobile Kommunikation) [Mobilfunkstandard]
GVBl. ..... Gesetz- und Verordnungsblatt
GVG ..... Gerichtsverfassungsgesetz
G 10 ..... Gesetz zu Art. 10 GG
HAZ ..... Hannoversche Allgemeine Zeitung

HIV ..... Human Immuno-deficiency Virus (Immunschwächevirus)
HGB ..... Handelsgesetzbuch
HR ..... Human Ressources (Personalressourcen)
HTML ..... Hypertext Markup Language [Sprache zur Erstellung von Webseiten]
IDVS ..... Software der AOK
imA ..... interministerieller Arbeitskreis
IMSI ..... International Mobile Subscriber Identity (internationale mobile Teilnehmeridentität)
INPOL ..... [bundesweites Informationssystem der Polizei]
InsBVO ..... Insolvenz-Bekanntmachungs-Verordnung
InsO ..... Insolvenzordnung
IP ..... Internet protocol
ISDN ..... Integrated Services Digital Network [Telekommunikationsstandard]
IT ..... Informationstechnik
IuK ..... Informations- und Kommunikation
i.V.m. ..... in Verbindung mit
izn ..... Informatikzentrum Niedersachsen
JVA ..... Justizvollzugsanstalt
KBA ..... Kraftfahrt-Bundesamt
KFN ..... Kriminologisches Forschungsinstitut Niedersachsen
KLR ..... Kosten- und Leistungsrechnung
KWG ..... Gesetz über das Kreditwesen
LAN ..... Local Area Network (lokales Netzwerk)
LfD ..... Landesbeauftragter für den Datenschutz
LKA ..... Landeskriminalamt Niedersachsen
LoHN ..... Leistungsorientierte Haushaltswirtschaft Niedersachsen
LRH ..... Landesrechnungshof
LT-Drs. ..... Landtagsdrucksache
MAD ..... Militärischer Abschirmdienst
MDK ..... Medizinischer Dienst der Krankenversicherung
MDStV ..... Mediendienste-Staatsvertrag
MRRG ..... Melderechtsrahmengesetz
MPLS ..... Multiprotocol Label Switching [Routingstandard]
MoZART ..... Modellvorhaben zur Verbesserung der Zusammenarbeit zwischen Arbeitsämtern und Trägern der Sozialhilfe
MRRG ..... Melderechtsrahmengesetz
MV ..... Mecklenburg-Vorpommern
NAbfG ..... Niedersächsisches Abfallgesetz
NASA ..... National Aeronautics and Space Administration (Nationale Behörde für Luft- und Raumfahrt)
NBG ..... Niedersächsisches Beamtengesetz
NDR ..... Norddeutscher Rundfunk
Nds. ..... Niedersachsen, niedersächsische(r/s)
AGInSO ..... Gesetz zur Ausführung der Insolvenzordnung
NDSG ..... Niedersächsisches Datenschutzgesetz
Nds. MBl. ..... Niedersächsisches Ministerialblatt
NGDG ..... Niedersächsisches Gesundheitsdienstgesetz
NGefAG ..... Niedersächsisches Gefahrenabwehrgesetz
NGO ..... Niedersächsische Gemeindeordnung
Nieders. ..... Niedersächsische(r/s)
NIVADIS ..... Niedersächsisches Vorgangsbearbeitungs-, Analyse-, Dokumentations- und Informationssystem
NHG ..... Niedersächsisches Hochschulgesetz
NKAG ..... Nds. Kommunalabgabengesetz
NKWG ..... Niedersächsisches Kommunalwahlgesetz
NLfV ..... Niedersächsisches Landesamt für Verfassungsschutz
NLO ..... Niedersächsische Landkreisordnung
NMeldDÜV . Nds. Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
NMG ..... Niedersächsisches Meldegesetz
Nr. ..... Nummer(n)
NPersVG .... Niedersächsisches Personalvertretungsgesetz
NSchG ..... Niedersächsisches Schulgesetz
NVerfSchG . Niedersächsisches Verfassungsschutzgesetz
NWG ..... Niedersächsisches Wassergesetz
o.Ä. ..... oder Ähnliches
OFD ..... Oberfinanzdirektion
OT-Leit-ERV organisatorisch-technische Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften
OLG ..... Oberlandesgericht
OPTuM ..... Online Prüfung von Tele- und Mediendiensten
OWi ..... Ordnungswidrigkeiten
P53 ..... Projekt 53 (der Verwaltungsreform)
PersVG ..... Personalvertretungsgesetz
PC ..... Personal Computer

PMV ..... Personalmanagementverfahren
pp. ..... perge, perge (und so weiter),
PsychKG .... Gesetz über Hilfen für psychisch Kranke und Schutzmaßnahmen
RdErl. ..... Runderlass
Reg TP ..... Regulierungsbehörde für Telekommunikation und Post
RFTag ..... Radio Frequency Tag (Funkfrequenzauszeichner) [elektronisch mit eindeutigen Informationen programmierter Transponder]
S..... Seite
SAM ..... SAP AOK Master [Software der AOK]
SAP ..... [Deutsches Softwareunternehmen]
SCHUFA..... Schutzgemeinschaft für allgemeine Kreditsicherung
SGB..... Sozialgesetzbuch
SigG ..... Signaturgesetz
SiN ..... Studieninstitut Niedersachsen
SMS ..... Short Messaging System (Kurznachrichtensystem) [Standard zur Übermittlung kurzer Nachrichten]
Sten.Ber. .... Stenografische Berichte
StGB..... Strafgesetzbuch
StPO..... Strafprozessordnung
StrEG ..... Entschädigungsgesetz für Strafverfolgungsmaßnahmen
StV ..... Staatsvertrag
StVÄG ..... Strafverfahrensänderungsgesetz
StVG..... Straßenverkehrsgesetz
StVollzG ..... Strafvollzugsgesetz
TB ..... Tätigkeitsbericht
TCP/IP..... Transmission Control Protocol/ Internet Protol [Internetprotokolle]
TDDSG..... Teledienstedatenschutzgesetz
TDG..... Teledienstgesetz
TDSV..... Telekommunikations-Datenschutzverordnung
TierSchG .... Tierschutzgesetz
TKG..... Telekommunikationsgesetz
TKÜV..... Telekommunikations-Überwachungsverordnung
TOA..... Täter-Opfer-Ausgleich
u.a. ..... unter anderem
u.U. ..... unter Umständen
UDSV ..... Teledienstunternehmen-Datenschutzverordnung
UiG..... Umweltinformationsgesetz
ULD..... Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UMTS..... Universal Mobile Telecommunications System (universelles mobiles Telekommunikationssystem) [Mobilfunkstandard]
UNIX ..... Betriebssystem für Mehrplatzsysteme
URL..... Unique Ressource Locator [Internetadresse]
USA..... United States of America (Vereinigte Staaten von Amerika)
VGH ..... Verwaltungsgerichtshof
vgl. ..... vergleiche
VO..... Verordnung
VOB ..... Verdingungsordnung für Bauleistungen
VOF..... Verdingungsordnung für freiberufliche Leistungen
VOL..... Verdingungsordnung für Leistungen
VPN..... Virtual Private Network (virtuelles privates Netzwerk)
VwVfG..... Verwaltungsverfahrensgesetz
WWW..... World-Wide-Web [Internetdienst]
z.B..... zum Beispiel
ZDF ..... Zweites Deutsches Fernsehen
ZPO..... Zivilprozeßordnung
ZPO-E ..... Entwurf der Zivilprozessordnung
ZSchG..... Zeugenschutzgesetz
ZVG..... Zwangsversteigerungsgesetz

1 Einführung in den XVI. Tätigkeitsbericht

Der vorliegende XVI. Tätigkeitsbericht betrifft die Kalenderjahre 2001 und 2002. Redaktionsschluss war der 21. November 2002.

Veränderte Struktur

Dieser Tätigkeitsbericht folgt bei der Behandlung der einzelnen Sachthemen einer veränderten Struktur, die darauf ausgerichtet ist, für möglichst viele Themenfelder mit der Darstellung besonders bedeutsamer Einzelfragen eine Beschreibung der Ausgangssituation und der aus Datenschutzsicht wichtigen Zukunftsentwicklungen zu verbinden. Dadurch soll eine Ausrichtung verstärkt werden, die den Tätigkeitsbericht von einem reinen Rechenschaftsbericht mit einer dadurch geprägten Rückorientierung stärker zu einem die Zukunftssicht einbeziehenden Entwicklungsbericht werden lässt. Damit wird zugleich der Vorgabe in § 22 Abs. 3 Satz 3 NDSG Rechnung getragen, wonach der Landesbeauftragte den Landtag und die Öffentlichkeit auch über wesentliche Entwicklungen des Datenschutzes unterrichtet.

Die veränderte Struktur führt zu einer Änderung der aus den bisherigen Berichten gewohnten Kapitelüberschriften und ihrer Reihenfolge; durch das erweiterte Stichwortverzeichnis ist aber sichergestellt, dass alle Leser die für sie wichtigen Textstellen im Tätigkeitsbericht auffinden werden.

Gleichzeitig hat die veränderte Ausrichtung zur Folge, dass in den einzelnen Themenfeldern aus der großen Zahl der im Berichtszeitraum behandelten Einzelfragen und Einzelfälle nur noch die besonders bedeutsamen dargestellt werden. Dies führt aber nicht zu einer Verkürzung von Informationen, weil über die Ergebnisse der laufenden Arbeit schon jetzt kontinuierlich und aktuell im neu gestalteten Internet-Angebot des Landesbeauftragten für den Datenschutz informiert wird. Dieses Angebot soll künftig noch weiter ausgebaut werden.

Insgesamt wird, so hoffe ich, die neue Struktur den Anforderungen der Adressaten - gemäß § 22 Abs. 3 Satz 1 NDSG ist Adressat in erster Linie der Niedersächsische Landtag - noch besser gerecht werden und für die Diskussion des Tätigkeitsberichts und der Stellungnahme der Landesregierung in den Ausschüssen des Landtages Gewinn bringen.

Rückschau

Die im XV. Tätigkeitsbericht erstmalig enthaltenen Kapitel „Datenschutzpolitischer Handlungsbedarf“ und „Schwerpunkte“ werden auch in der neuen Struktur weitergeführt. Neu hinzu gekommen ist das Kapitel „Rückschau“, in dem in Kurzform dargestellt wird, ob und in welcher Weise die im letzten Tätigkeitsbericht erhobenen und im Kapitel „Datenschutzpolitischer Handlungsbedarf“ zusammengefassten Forderungen in der Zwischenzeit aufgenommen worden sind. Auch dies soll die Ausrichtung des Tätigkeitsberichtes zu einem Entwicklungsbericht unterstreichen und die Diskussion im Landtag und mit der Landesregierung beleben.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Der Vorsitz in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist im Jahre 2001 von Niedersachsen turnusgemäß auf die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Frau Bettina Sokol, übergegangen. Im Jahre 2002 liegt der Vorsitz beim Landesbeauftragten für den Datenschutz Rheinland-Pfalz, Herrn Prof. Dr. Walter Rudolf. Im Jahre 2003 wird der Sächsische Landesbeauftragte für den Datenschutz, Herr Dr. Thomas Giessen, den Vorsitz übernehmen.

Für Niedersachsen habe ich seit November 2001 den Vorsitz in der Arbeitsgruppe „Datenschutzgerechtes eGovernment“ der Konferenz inne. Über die Arbeit dieser Gruppe wird im Einzelnen in den Kapiteln 5.3.14 und 6.5 berichtet.

2 Datenschutzpolitischer Handlungsbedarf

In folgenden Bereichen besteht aus meiner Sicht kurzfristig Bedarf für ein Tätigwerden des Gesetzgebers, der Landesregierung bzw. des zuständigen Ressorts:

1. Parallel zu den Erörterungen im Bund sollte in Niedersachsen die Diskussion zur grundlegenden Modernisierung des Datenschutzrechts frühzeitig aufgenommen und so geführt werden, dass Niedersachsen im Bund-Länder-Abstimmungsverfahren und bei den Beratungen des Bundesrates eine aktive Mitgestaltungsrolle übernehmen kann (Kap. 4.2).

2. Nach dem Vorbild Schleswig-Holsteins sollten - zur Förderung von eGovernment in der niedersächsischen Verwaltung - baldmöglichst im NDSG Regelungen zur datenschutzrechtlichen Auditierung von Behörden oder Behördenteilen sowie zu einem Gütesiegel für IT-Produkte, die in der öffentlichen Verwaltung zum Einsatz kommen, verankert werden (Kap. 4.2 und 5.2.5).

3. Die Arbeiten zur Schaffung eines Informationszugangsgesetzes sollten in Niedersachsen möglichst zeitlich parallel zum Gesetzgebungsverfahren im Bund kurzfristig wieder aufgenommen werden (Kap. 4.7).

4. Um für die Verwaltungspraxis keine weiteren Verunsicherungen zu erzeugen, sollte in der Frage der Notwendigkeit einer gesetzlichen Grundlage für Videoüberwachungsmaßnahmen öffentlicher Stellen rasch ein Konsens zwischen Landesregierung und LfD gesucht werden, in dessen Rahmen auch geklärt werden muss, welche Bedeutung in diesem Zusammenhang dem so genannten Hausrecht zukommt (Kap. 6.2.1).

5. Im Rahmen der zentralen IT-Koordinierung des Landes sollten die Überlegungen forciert werden, zur Verbesserung der Datensicherheit modernere Chipkarten-Systeme einzusetzen, die auch eine hierarchische Struktur von Gruppenschlüsseln unterstützen (Kap. 7.5.2 und 7.5.3).

6. Bei der inhaltlichen Ausgestaltung der so genannten Neuen Medienordnung sollten die bewährten dezentralen Strukturen bei der Aufsicht über die Diensteanbie-

ter nur behutsam durch Instrumente der Selbstregulierung und einer zentralen Koordinierung ergänzt werden (Kap. 8.2).

7. Die Bedingungen für die datenschutzgerechte Nutzung von Internet und E-Mail an den Arbeitsplätzen in der öffentlichen Verwaltung sollten auf der Grundlage der von den Datenschutzbeauftragten entwickelten Orientierungshilfe in einer Vereinbarung mit den Spitzenorganisationen der Gewerkschaften nach § 81 Nds. PersVG festgeschrieben werden (Kap. 8.3).

8. Die Umsetzung der rahmenrechtlichen Vorgaben des novellierten Melderechtsrahmengesetzes in das niedersächsische Landesrecht sollte baldmöglichst erfolgen; dabei sollten zur Sicherstellung von Datenschutz und Datensicherheit bei Nutzung des elektronischen Weges zusätzliche Vorkehrungen geschaffen werden (Kap. 10.3).

9. Die Landesregierung sollte über den Bundesrat initiativ werden, um eine immissionsschutzrechtliche Rechtsgrundlage zum Anlegen eines Katasters über die Standorte von Mobilfunkanlagen und zu Regelungen über die Veröffentlichung von Standortdaten zu schaffen (Kap. 13.2).

10. Das Justizministerium sollte für Überweisungen von Geldauflagen an gemeinnützige Einrichtungen eine auch anderenorts praktizierte Verfahrensweise übernehmen, bei der den Empfängern der Geldauflage keine unnötigen personenbezogenen Daten übermittelt werden (Kap. 11.1.5).

11. Das Verfahren zur Übermittlung von personenbezogenen Informationen volljähriger Schüler von der Schule an die Eltern sollte überdacht und ggf. gesetzlich abgesichert werden (Kap. 14.4).

12. Auf der Grundlage der Ergebnisse der gemeinsamen Arbeitsgruppe Ministerium für Frauen, Arbeit und Soziales / LfD sollte gleich zu Beginn der nächsten Legislaturperiode das Gesetzgebungsverfahren zur Schaffung der erforderlichen Regelungen zum Schutz von Gesundheitsdaten eingeleitet werden (Kap. 16.1).

13. Die Landesregierung sollte alle Bemühungen, auf Bundesebene nunmehr rasch Regelungen für ein Arbeitnehmer-Datenschutzgesetz zu entwickeln und in das Gesetzgebungsverfahren einzubringen, nach Kräften unterstützen (Kap. 24).

3 Rückschau

Der XV. Tätigkeitsbericht enthielt erstmals ein Kapitel „Datenschutzpolitischer Handlungsbedarf“, in dem die Punkte in einer Übersicht zusammengestellt waren, bei denen Gesetzgebung oder Exekutive aus meiner Sicht aktuell tätig werden mussten. Natürlich haben diese Punkte auch für meine Arbeit in diesem Berichtszeitraum eine wichtige Rolle gespielt. Daher soll im Sinne einer resümierenden Rückschau an dieser Stelle in Kurzform dargestellt werden, ob und in welcher Weise meine Erwartungen und Forderungen zwischenzeitlich aufgenommen worden sind. Soweit einzelne

Punkte auch an anderer Stelle dieses Tätigkeitsberichts behandelt werden, wird darauf verwiesen.

1. Forderung: Die Datenschutzaufsicht über den nicht öffentlichen Bereich ist nach dem Vorbild anderer Länder im Sinne einer einstufigen Aufsicht durch den LfD zu organisieren, die die Befugnisse des Innenministeriums als oberster Landesbehörde unberührt lässt.
   Sachstand: Die Forderung besteht nach wie vor, nachdem es nicht gelungen ist, im Rahmen der NDSG-Novellierung eine Änderung des § 22 Abs. 6 Satz 2 zu erreichen. Hinsichtlich der Konformität dieser Regelung mit vorrangigem EU-Recht (Art. 28 EG-DSRL) ist die Prüfung der EU-Kommission noch nicht abgeschlossen.
2. Forderung: Es sollte auch in Niedersachsen ein Gesetz zur Regelung des Zugangs zu behördlichen Informationen (Informationszugangsgesetz) geschaffen werden, das zugleich die notwendigen Einschränkungen zum Schutz personenbezogener Daten und von Geschäftsgeheimnissen enthält.
   Sachstand: Die Haltung der Landesregierung und der beiden großen Landtagsfraktionen ist leider nach wie vor ablehnend (vgl. Kapitel 4.7). Meine Hoffnung richtet sich hier auf die XV. Legislaturperiode, insbesondere dann, wenn für den Bund die entsprechende Regelungsabsicht umgesetzt worden ist.
3. Forderung: Im NDSG bzw. NGefAG müssen gesetzliche Regelungen zur Videoüberwachung im öffentlichen Raum geschaffen werden.
   Sachstand: Die im Zusammenhang mit der Terrorismusbekämpfung erweiterten Regelungen in § 32 Abs. 3 NGefAG sind zur Lösung der Gesamtproblematik unzureichend (vgl. Kapitel 6.2.1). Insbesondere für die in großem Umfang in den Behörden zur Gebäudesicherung praktizierte Videoüberwachung gibt es keine ausreichende Rechtsgrundlage.
4. Forderung: Für die Verarbeitung von Gesundheitsdaten im Krankenhausbereich ist eine landesgesetzliche Regelung seit Jahren überfällig; durch die Vorgaben in Art. 8 der EG-DSRL wird der Handlungsbedarf noch einmal unterstrichen.
   Sachstand: In einer gemeinsamen Arbeitsgruppe mit dem Ministerium für Frauen, Arbeit und Soziales wird der Regelungsbedarf konkret und aktuell ermittelt, sodass die erforderlichen gesetzgeberischen Maßnahmen in der XV. Legislaturperiode rasch umgesetzt werden können (vgl. Kapitel 16.1).
5. Forderung: Die Landesregierung sollte Bemühungen zum datenschutzgerechten eGovernment nachhaltig unterstützen. Zur Sicherung der Authentizität bei einem elektronischen Dokumentenaustausch im Verwaltungsverfahrensrecht ist die elektronische Signatur als Surrogat der eigenhändigen Unterschrift einzuführen.
   Sachstand: Im Verwaltungsverfahrensgesetz des Bundes ist die elektronische Signatur inzwischen verankert; die dortigen Regelungen sollen in Kürze in das Niedersächsische Verwaltungsverfahrensgesetz übernommen werden. Insgesamt ist Niedersachsen beim eGovernment auf einem guten Weg. Durch die frühzeitige Einbindung des LfD bei der Entwicklung von eGovernment-Anwendungen ist sichergestellt, dass die Anforderungen an Datenschutz und Datensicherheit erfüllt werden.
6. Forderung: Beim Anschluss ans Internet müssen alle Dienststellen die Sicherheit der Daten von Bürgern durch technische und organisatorische Maßnahmen gewährleisten.

Sachstand: Über die Notwendigkeit entsprechender Maßnahmen besteht umfassende Einigkeit. Auf die Realisierung im Einzelfall wird der LfD sein verstärktes Augenmerk richten.

7. Forderung: Bei der anstehenden Weiterentwicklung des Systems der Rundfunkfinanzierung muss ein Modell zu Grunde gelegt werden, das sich stärker als das derzeitige Verfahren an den Prinzipien der Datenvermeidung und Datensparsamkeit orientiert.
   Sachstand: Die politische und rechtliche Grundsatzdiskussion zur künftigen Struktur der Rundfunkfinanzierung ist noch in vollem Gange. Unabhängig davon habe ich in Gesprächen mit dem NDR erreicht, dass das bisherige Verfahren zur Befreiung von der Rundfunkgebührenpflicht datenschutzgerechter ausgestaltet und der Umfang der über den Antragsteller zu erhebenden Daten reduziert worden ist; hierfür ist eine einjährige Erprobung mit nachfolgender Evaluierung vereinbart worden (vgl. Kapitel 8.6.7).
8. Forderung: Für in polizeilichen Kriminal- bzw. Sachakten gespeicherte Daten Dritter müssen Prüf- und Löschungsfristen eingeführt werden.
   Sachstand: Das Problem ist noch in der Diskussion mit dem Innenministerium.
9. Forderung: Es muss sorgfältig geprüft werden, ob der räumliche Anwendungsbereich der verdachtsunabhängigen Kontrollen gemäß § 12 Abs. 6 NGefAG vor dem Hintergrund des Urteils des Landesverfassungsgerichts Mecklenburg-Vorpommern zur sog. Schleierfahndung zu beschränken ist.
   Sachstand: Nachdem sichergestellt ist, dass die jeweilige Erkenntnislage, die Anlass zu einer verdachtsunabhängigen Kontrolle gegeben hat, nachvollziehbar dokumentiert wird, wird die Forderung nicht mehr aufrechterhalten.
10. Forderung: Für die Übernahme von Daten aus dem bestehenden System INPOL-aktuell in INPOL-neu müssen kurzfristig Auswahlkriterien entwickelt werden, damit die gesetzlichen Vorgaben für die Einspeicherung von Daten nach dem BKA-Gesetz nicht umgangen werden.
    Sachstand: Auch bei dem inzwischen veränderten technischen Ansatz eines einheitlichen Datenspeicherungssytems der Polizei (vgl. Kapitel 10.1.6) stellt sich das Problem in gleicher Weise. Ich werde die Einhaltung meiner Forderung bei der Migration der Daten aus dem bestehenden System im Auge behalten.
11. Forderung: Einzelne Vorschriften des NGefAG über die polizeiliche Datenerhebung und -verarbeitung entsprechen vor dem Hintergrund des sog. BND-Urteils des Bundesverfassungsgerichts nicht mehr den gesteigerten Anforderungen an die Zulässigkeit von Eingriffen in das allgemeine Persönlichkeitsrecht und müssen daher entsprechend ergänzt werden.
    Für das Niedersächsische Verfassungsschutzgesetz ergeben sich entsprechende Regelungsnotwendigkeiten.
    Sachstand: Das Innenministerium sieht sich für den Polizeibereich von dem BND-Urteil nicht betroffen und lehnt daher nach wie vor Änderungen des NGefAG zur Umsetzung der in dem Urteil entwickelten Grundsätze ab. Das Nds. Verfassungsschutzgesetz soll in Kürze novelliert werden; ein Entwurf liegt mir jedoch noch nicht vor, sodass auch noch nicht absehbar ist, in welchem Umfang dabei den Vorgaben aus dem BND-Urteil Rechnung getragen wird.

12. Forderung: Einer Ausweitung der Überwachungsbefugnisse des Verfassungsschutzes nach dem G 10-Gesetz auch auf extremistische Einzeltäter darf von Seiten der Landesregierung nicht zugestimmt werden.
    Sachstand: Der entsprechenden Regelung in § 3 Abs. 1 Ziff. 6 hat Niedersachsen in der Sitzung des Bundesrates vom 1. Juni 2001 zugestimmt.
13. Forderung: Das Niedersächsische Beamtengesetz sollte umgehend um Regelungen ergänzt werden, die die in der Praxis notwendige innerbehördliche oder ausnahmsweise auch nach außen gerichtete Weitergabe von Personalaktendaten rechtlich ermöglichen.
    Sachstand: Das Innenministerium weicht der Umsetzung der Forderung immer wieder aus, obwohl das NBG zwischenzeitlich aus verschiedenen Anlässen geändert worden ist. Nunmehr soll eine zeitlich überhaupt nicht eingrenzbare Novellierung des Beamtenrechtsrahmengesetzes abgewartet werden.
14. Forderung: Für die Teilnahme der Schwerbehindertenvertretung an Auswahlgesprächen bei der Personaleinstellung ist eine gesetzliche Grundlage zu schaffen.
    Sachstand: Die Forderung ist inzwischen durch Ergänzung des SGB IX in § 95 Abs. 2 Satz 3 umgesetzt.
15. Forderung: Im Zusammenwirken von LfD, Innenministerium und Kommunalen Spitzenverbänden sind Handreichungen für den Umgang mit personenbezogenen Daten im Bereich der kommunalen Mandatstätigkeit zu entwickeln und zu veröffentlichen.
    Sachstand: Nachdem das Innenministerium keine Notwendigkeit für die Herausgabe einer Handreichung gesehen hat, werde ich diese im Zusammenwirken mit den Kommunalen Spitzenverbänden, die das Vorhaben unterstützen, erarbeiten.
16. Forderung: Es ist dringend erforderlich, die seit mehr als zwei Jahren geforderte Anonymisierung des Abrechungsverfahrens bei Schwangerschaftsabbrüchen umzusetzen.
    Sachstand: Gemeinsam mit dem Ministerium für Frauen, Arbeit und Soziales ist es gelungen, den hinhaltenden Widerstand der Krankenkassen zu brechen, sodass ab dem 1. Januar 2003 das Abrechnungsverfahren datenschutzgerecht ausgestaltet sein wird.
17. Forderung: Soweit Massenreihenuntersuchungen, bei denen Unverdächtige freiwillig Speichelproben zum Zwecke der Abnahme eines sog. „genetischen Fingerabdrucks“ abgeben, als ultima ratio durchgeführt werden, um schwere Straftaten aufzuklären, ist durch die Ergänzung der DNA-Richtlinie und die Verwendung geeigneter polizeilicher Vordrucke dafür Sorge zu tragen, dass die Betroffnen umfassend und ordnungsgemäß belehrt werden.
    Sachstand: Als Ergebnis der Bemühungen einer gemeinsamen Arbeitsgruppe mit dem Innenministerium sind die Forderungen in der überarbeiteten Richtlinie umgesetzt worden.
18. Forderung: Um eine effektive parlamentarische Kontrolle des Einsatzes technischer Mittel zur akustischen Wohnraumüberwachung (sog. Großer Lauschangriff) zu gewährleisten, bedürfen die von der Bundesregierung gemäß Art. 13 Abs. 6 Satz 1 GG jährlich vorzulegenden Berichte ergänzender Angaben.
    Sachstand: Eine Arbeitsgruppe der Justizminister-Konferenz hat hierzu Vorschläge entwickelt, die aber kaum eine Verbesserung bedeuten, weil die meisten Forderungen der Datenschutzbeauftragten leider unberücksichtigt geblieben sind.

19. Forderung: Gleiches gilt auch für die von der Landesregierung durch Art. 13 Abs. 6 Satz 3 GG vorgeschriebene Unterrichtung des Niedersächsischen Landtages über die präventiven und repressiven Maßnahmen zur akustischen Wohnraumüberwachung. Die Umsetzung dieser Berichtspflicht bedarf noch einer gesetzlichen Regelung, die zudem sicherstellt, dass die Maßnahmen im Plenum des Niedersächsischen Landtages öffentlich beraten und erörtert werden.
Sachstand: Durch die Einfügung eines § 13 in das Nds. Ausführungsgesetz zum Gerichtsverfassungsgesetz zum 6. Juli 2001 ist die Berichtspflicht in das Landesrecht umgesetzt worden. Ein erster Bericht für das Jahr 2002 wird in Kürze vorgelegt werden. Auf der Grundlage dieser Berichte wird die Landesregierung künftig den Landtag jährlich unterrichten. Es wäre wünschenswert, wenn diese Unterrichtung ähnlich aussagekräftig gestaltet wird, wie dies etwa in Baden-Württemberg erfolgt (vgl. LT-Drs. BW 13/1312 vom 12. September 2002).

4 Zur Situation des Datenschutzes

4.1 Rechtlicher Rahmen - Bundesdatenschutzgesetz

Mit Wirkung vom 23. Mai 2001 sind das novellierte Bundesdatenschutzgesetz und mit Wirkung vom 6. Juli 2001 das novellierte Niedersächsische Datenschutzgesetz in Kraft getreten. In beiden Fällen war damit die von der EG-Datenschutz-Richtlinie vom 24. Oktober 1995 eingeräumte Umsetzungsfrist von drei Jahren weit überschritten. Ein von der EU-Kommission zunächst eingeleitetes Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland ist dann aber nicht weiter verfolgt, sondern eingestellt worden. Unabhängig davon ist die Überprüfung der EU-Kommission hinsichtlich einer inhaltlich sachgerechten Umsetzung der Vorgaben der Richtlinie aber noch nicht abgeschlossen.

Bei den Novellierungen sind die Forderungen und Erwartungen der Datenschutzbeauftragten, die insbesondere auf eine stärkere Einbeziehung der neuen technischen Entwicklungen und auf die Zusammenführung oder zumindest Harmonisierung mit den Datenschutzregelungen im Tele- und Medienrecht gerichtet waren, nur teilweise berücksichtigt worden. Dem fortbestehenden grundsätzlichen Modernisierungsbedarf ist beim BDSG dadurch Rechnung getragen worden, dass parallel zum Gesetzgebungsverfahren ein Gutachten über grundsätzliche Problemstellungen einer umfassenden Neuordnung des Datenschutzrechts im Rahmen einer zweiten Stufe der BDSG-Novellierung eingeholt worden ist. Das Gutachten der Professoren Roßnagel, Pfitzmann und Garstka ist im Herbst 2001 der Bundesregierung übergeben und unter dem Titel „Modernisierung des Datenschutzrechts“ als Broschüre vom Bundesinnenministerium veröffentlicht worden.

Die von den Gutachtern vorgeschlagenen Zielsetzungen und Lösungsansätze für eine grundlegende Modernisierung des Datenschutzrechts sind in thesenartiger Zuspitzung:

- Die allgemeinen Datenschutzgrundsätze müssen für den öffentlichen wie für den nicht öffentlichen Bereich in gleicher Weise gelten und ein gleiches Datenschutzniveau gewährleisten.
- Das Telekommunikations-, Tele- und Mediendienstedatenschutzrecht soll in das BDSG so integriert werden, dass eine Vereinheitlichung auf hohem Niveau erreicht wird.
- Das neue Datenschutzrecht muss darauf ausgerichtet sein, für alle Beteiligten eine möglichst hohe Transparenz über die Verarbeitung ihrer personenbezogenen Daten zu erreichen. Dazu gehören die Erhebung der Daten grundsätzlich beim Betroffenen, seine Unterrichtung bei einer sonstigen Erhebung sowie die Verpflichtung der Daten verarbeitenden Stelle, eine Datenschutzerklärung und Angaben über die Struktur der Datenverarbeitung zu veröffentlichen.
- Der Grundsatz der Datenvermeidung und Datensparsamkeit, mit dem nicht Daten, sondern deren Personenbezug vermieden werden sollen, muss als grundlegendes Prinzip für die Gestaltung technisch-organisatorischer Verfahren umfassend umgesetzt werden. Daraus ergibt sich auch eine zeitliche Beschränkung in der Weise, dass personenbezogen erhobene Daten zum frühestmöglichen Zeitpunkt zu löschen, zu anonymisieren oder zu pseudonymisieren sind.
- Zur Verstärkung des Prinzips der informationellen Selbstbestimmung sollte die Zulässigkeit der Datenverarbeitung grundsätzlich an die informierte Einwilligung der Betroffenen geknüpft werden; dadurch kann eine deutliche Eindämmung der Vielzahl der bereichsspezifischen Regelungen im Datenschutzrecht erreicht werden.
- Bei den Anforderungen an die Erforderlichkeit als Begrenzung der Verarbeitung personenbezogener Daten kann zwischen Verarbeitungen mit gezieltem Personenbezug, wo strengere Vorgaben gelten müssen, und Datenverarbeitungen ohne gezielten Personenbezug (z.B. bei Kommunikationsdienstleistungen, Suchprozessen oder technischen Dienstleistungen) differenziert werden.
- Der Grundsatz der Zweckbindung bleibt ein unverzichtbarer Verarbeitungsgrundsatz. Zu diskutieren bleibt der Spielraum, den Art. 6 Abs. 1 b EG-DSRL dadurch gewährt, dass die Datenverarbeitung nicht allein auf den ursprünglichen Zweck beschränkt, sondern (nur) mit ihm „vereinbar“ sein muss.
- Datenschutz muss künftig durch, nicht gegen Technik erreicht werden. Datenschutz sollte daher so weit wie möglich in Produkte, Dienste und Verfahren integriert und durch eine dem praktischen Einsatz vorhergehende Vorabkontrolle effektiviert werden. Durch ein integriertes Datenschutzmanagementsystem ist eine datenschutzfreundliche Betriebsorganisation und Verfahrensgestaltung sicherzustellen.
- Den Betroffenen muss es ermöglicht werden, den Schutz ihrer Daten durch entsprechende verfahrensmäßige und technische Lösungen selbst in die Hand zu nehmen. Hierzu gehört auch die Stärkung der Betroffenenrechte gegenüber den Daten verarbeitenden Stellen.
- Ein modernes Datenschutzrecht muss Anreize für einen effektiven Schutz durch gesellschaftliche oder unternehmensspezifische Selbstregulierung sowie durch Auditierungs- und Zertifizierungsverfahren enthalten.

Die Gutachter plädieren weiter dafür, dass

- als Ausdruck des Kommunikationsgehalts aller Grundrechte das Grundrecht auf informationelle Selbstbestimmung explizit als Grundgesetzartikel ausgestaltet werden sollte,
- als Bestandteil der informationellen Selbstbestimmung der freie Zugang zu Informationen im öffentlichen Bereich durch ein Informationsfreiheitsgesetz rechtlich abzusichern ist,
- die vollständige Unabhängigkeit der Datenschutz-Kontrollstellen gemäß Art. 28 EG-DSRL für den nicht öffentlichen Bereich überall sicherzustellen ist.

Ursprünglich war beabsichtigt, die Ergebnisse des Gutachtens zur Grundlage einer zweiten Stufe der Novellierung des BDSG noch in der XIV. Legislaturperiode des Deutschen Bundestages zu machen. Diese Absicht ist aus Zeitgründen fallen gelassen worden, sodass dies eine wichtige Aufgabe des im Herbst 2002 neu gewählten Bundestages und der neuen Bundesregierung sein wird. In einem Antrag vom 3. Juli 2002 sind dazu die aus Sicht der Fraktionen der SPD und von BÜNDNIS 90/DIE GRÜNEN bedeutsamen Punkte zusammen gestellt (BT-Drs. 14/9709); der Bundestag hat diesem Antrag in seiner Sitzung am 4. Juli 2002 mehrheitlich zugestimmt.

4.2 Rechtlicher Rahmen - Niedersächsisches Datenschutzgesetz

Für das Niedersächsische Datenschutzgesetz sind bei der Novellierung im Jahre 2001 nur Mindest-Anpassungen an die Vorgaben der EG-Datenschutz-Richtlinie vorgenommen und die Möglichkeiten zu einer darüber hinausgehenden Modernisierung nicht genutzt worden (vgl. dazu die Anmerkungen in der im Dezember 2001 veröffentlichten Broschüre des LfD mit Erläuterungen zur Anwendung des neuen NDSG). Hier wäre zu wünschen, dass die Diskussion über die notwendigen Weiterentwicklungen frühzeitig aufgenommen wird. Das bedeutet, dass nicht erst nach Abschluss, sondern parallel zu den Erörterungen im Bund eine vertiefte und nachhaltige Auseinandersetzung mit den Ergebnissen des Gutachtens auch in Niedersachsen und besonders auch im Niedersächsischen Landtag geführt werden sollte. Nur dann ist sichergestellt, dass Niedersachsen im Bund-Länder-Abstimmungsverfahren und bei den Beratungen des Bundesrates eine aktive Rolle bei der Modernisierung des deutschen Datenschutzrechts übernehmen kann. Ich bin gerne bereit, dabei jede nur denkbare Hilfe zu leisten.

Unabhängig von der anstehenden grundlegenden Modernisierung sollten im Niedersächsischen Datenschutzgesetz baldmöglichst in einer weiteren Novelle Regelungen zur datenschutzrechtlichen Auditierung von Behörden oder Behördenteilen sowie zu einem Gütesiegel für IT-Produkte, die in der öffentlichen Verwaltung zum Einsatz kommen, verankert werden. Entsprechende Regelungen im Schleswig-Holsteinischen Datenschutzgesetz werden dort mit großem Erfolg praktiziert. Die gute Position, die Niedersachsen beim Weg ins eGovernment einnimmt, verlangt aus meiner Sicht zwingend nach diesen neuen Instrumenten eines nutzerorientierten und akzeptanzfördernden Datenschutzes. Nur dann, wenn die Bürger das absolute Vertrauen haben, dass ihre personenbezogenen Daten bei der Verwaltung in jeder Hinsicht datenschutzgerecht behandelt werden und dass dort alle notwendigen Vorkehrungen zur

Datensicherheit getroffen worden sind, werden sie die Angebote zur elektronischen Kommunikation mit der Verwaltung beim eGovernment annehmen. Durch Einführung eines Gütesiegels und eines Datenschutz-Audits für Behörden würde dieses Vertrauen ganz wesentlich gestärkt werden und auf eine verlässliche Grundlage gestützt werden können.

Bei Gelegenheit dieser Novellierung könnte dann endlich auch die immer wieder kritisierte und gegen EU-Recht verstoßende Regelung des § 22 Abs. 6 Satz 2 NDSG zur Fachaufsicht über den LfD im nicht öffentlichen Bereich beseitigt werden.

4.3 Terrorismusbekämpfungsgesetze - wie viel Sicherheit verträgt die Freiheit?

Die Diskussion über die rechtlichen Rahmenbedingungen des Datenschutzes wird seit dem 11. September 2001 bei vielen Akteuren leider von einer Sichtweise dominiert, die wir Datenschützer eigentlich überwunden glaubten. „Datenschutz ist Täterschutz“, „Deutschland hat beim Datenschutz übertrieben“, „Wir müssen den Datenschutz tiefer hängen“, „hinderliche Vorschriften des Datenschutzes müssen beseitigt werden“, so und ähnlich lauteten die Äußerungen, leider gerade auch von maßgeblichen Vertretern der Politik und der Regierungen, die für das Datenschutzrecht Verantwortung tragen. Dabei weiß jeder, dass Anschläge wie die vom 11. September auch bei einem Datenschutz auf Null-Niveau nicht zu verhindern gewesen wären. Wer gleichwohl die Fahne des Datenschutzes hochhielt, lief - zumindest in den ersten Wochen nach den Anschlägen - Gefahr, in die Nähe der Terroristen gerückt oder öffentlich diffamiert zu werden. Ein Beispiel dafür waren die Äußerungen des Pressesprechers des Niedersächsischen Innenministeriums, die er auf eine kritische Feststellung des LfD zu den rechtlichen Grundlagen für die im September und Oktober 2001 - also vor dem In-Kraft-Treten des neuen § 45a NGefAG - in Niedersachsen von Ausländerbehörden unter Mithilfe der Universitäten durchgeführten Datenerhebungen vor der Landespressekonferenz machte (vgl. HAZ vom 3. November 2001). Ich bin dankbar, dass auf Initiative der Landtagsfraktion BÜNDNIS 90/DIE GRÜNEN (Entschließungsantrag vom 7. November 2001, LT-Drs. 14/2857) die Angelegenheit im Landtag zur Sprache gekommen ist und dass dabei über die Unangemessenheit der Äußerungen des Pressesprechers fraktionsübergreifend Konsens bestand.

Zu den insbesondere im Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 9. Januar 2002 neu geschaffenen Datenerhebungs- und Datenübermittlungsbefugnissen der Sicherheitsbehörden habe ich mich wie die meisten meiner Kolleginnen und Kollegen wiederholt kritisch geäußert. Ich sehe zentrale Prinzipen, über deren Bedeutung für unsere demokratische Bürgergesellschaft bisher ein breiter Konsens bestand, durch diese Regelungen in bedenklicher Weise tangiert, wie etwa

- den Grundsatz der freien und unbeobachteten Aktion, Bewegung und Kommunikation der Bürger,
- das Recht auf Anonymität in der Öffentlichkeit,

- die Aufnahme von personenbezogenen Ermittlungshandlungen nur bei einem konkreten Anfangsverdacht auf eine Straftat oder bei einer konkreten Gefahrenlage,
- das Verbot der Datensammlung auf Vorrat,
- die umfassende Geltung der Unschuldsvermutung,
- die strikte Trennung zwischen Polizei und Verfassungsschutz.

Ich bin nach wie vor der Auffassung, dass nur ein Teil der Neuregelungen überhaupt geeignet ist, den so genannten „Schläfern“ auf die Spur zu kommen, und fühle mich in dieser Einschätzung durch die bisherigen Abläufe und die Erkenntnisse bei der Fahndung bestätigt. Das konkrete Verfahren der Rasterfahndung nach Terroristen in den Ländern und der zentrale Datenabgleich beim BKA sind im Kapitel 10.1.2 gesondert unter datenschutzrechtlichen Gesichtspunkten dargestellt und bewertet.

Im Übrigen stand den Sicherheitsbehörden aufgrund ihrer in den letzten Jahren immer weiter ausgedehnten Befugnisse schon vor den Terroranschlägen des 11. September 2001 ein breites Arsenal an Eingriffsmöglichkeiten zur Verfügung. Die jetzt vorgenommenen Erweiterungen werfen die Frage auf, wie viel Sicherheit die Freiheit verträgt und wo für unseren Rechtsstaat die Mutation zum Überwachungsstaat beginnt bzw. bereits begonnen hat.

Die politische Diskussion läuft leider überwiegend in eine entgegengesetzte Richtung. Da wird von vielen mit Nachdruck gefordert, als weitere Option die technischen Möglichkeiten der restlosen Ausleuchtung der bei der Nutzung des Internets anfallenden Kommunikationsdaten zu nutzen und deren langfristige Vorratsspeicherung den Providern als gesetzliche Pflicht aufzuerlegen. Auch manche Äußerungen niedersächsischer Politiker in der letzten Zeit mit der Ankündigung neuer und noch schärferer „Anti-Terror-Pakete“ oder von Novellierungsabsichten zur Schaffung des „härtesten Polizeigesetzes der Bundesrepublik“ zeigen, dass an der Spirale der Eingriffsbefugnisse weiter gedreht wird. Aus meiner Sicht ist es unerlässlich und überfällig, eine offene Diskussion darüber zu führen, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und den individuellen Freiheitsrechten wieder neu hergestellt werden kann. Dazu ist eine umfassende und systematische Evaluierung aller Eingriffsbefugnisse der Sicherheitsbehörden, auch der schon vor dem 11. September 2001 bestehenden, durch unabhängige Stellen und an Hand objektiver Kriterien erforderlich. Sie muss aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Ich hoffe sehr, dass diese Evaluierung nicht durch den immer wieder zu beobachtenden Wettbewerb vieler Politiker um die härtesten und konsequentesten Sicherheitslösungen und die darauf gegründeten vollmundigen - gleichwohl aber niemals erfüllbaren - Sicherheitsversprechungen verhindert wird.

4.4 Stellenwert des Datenschutzes in der niedersächsischen Politik und in der Verwaltung

Der Stellenwert von Datenschutz und Datensicherheit in den Behörden der Landesverwaltung und der kommunalen Gebietskörperschaften sowie die Sensibilität gegenüber den Anforderungen an datenschutzgerechte Lösungen, hat sich, so ist mein

Eindruck, insgesamt im Berichtszeitraum verbessert. Dazu hat sicherlich auch beigetragen, dass der LfD und seine Mitarbeiter ihr Aufgabenverständnis von Datenschutzkontrolle so praktizieren, wie es in Nr. 6 des XV. TB LfD Nds. 1999/2000 dargestellt und im Leitbild der Geschäftsstelle (Nr. 4.2 des XV. TB LfD Nds. 1999/2000) niedergelegt worden ist. Es wird erfreulich rege Gebrauch von dem Angebot gemacht, schon frühzeitig bei der Ausformung von organisatorischen oder technischen Lösungen die sachkundige Beratung des LfD und seiner Mitarbeiter nachzufragen und sie in Arbeits- und Projektgruppen eng einzubinden. Dadurch ist es möglich gewesen, die vorsorgende aktive Beratung und Mitgestaltung bei der Entwicklung datenschutzgerechter Lösungen so voranzubringen, wie es meinem Verständnis von Datenschutzkontrolle im Internet-Zeitalter entspricht. Bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften mit Regelungen zum Recht auf informationelle Selbstbestimmung ist die Beteiligung des LfD nunmehr auch im NDSG selbst (§ 22 Abs. 1 Satz 4) festgeschrieben. In der Konsequenz dieser Entwicklung liegt es auch, dass die Verbindungen zu den behördlichen Datenschutzbeauftragten in der Landesverwaltung wie in der Kommunalverwaltung deutlich intensiviert worden sind (vgl. dazu unter 4.5).

Ich bin zuversichtlich, dass die in einzelnen Bereichen noch immer wahrnehmbare Zurückhaltung und Skepsis gegenüber den Beratungs- und Unterstützungsangeboten des LfD - etwa in den Leitungsebenen der Polizei oder der Steuerverwaltung - sich künftig werden vollständig überwinden lassen. Eine besonders hilfreiche Rolle dabei spielen schon jetzt die an meine Geschäftsstelle abgeordneten Beamten aus der Vollzugspolizei bzw. aus der Steuerverwaltung (vgl. dazu unter 5.1).

Diesem durchweg positiven Befund zum Stellenwert des Datenschutzes im Bereich der Verwaltung entspricht leider nicht das Maß der Beachtung, das nach meiner Wahrnehmung der Datenschutz im Berichtszeitraum in der Landespolitik und im Niedersächsischen Landtag gefunden hat. Auch wenn die Ereignisse des 11. September 2001 die politische Werteskala verändert haben und ich akzeptieren muss, dass seitdem der Datenschutz eine zusätzliche Begründungslast zu tragen hat, würde ich mir wünschen, dass der Kontakt und der Austausch zu datenschutzrechtlichen Fragen mit der Landespolitik und mit dem Parlament wieder die Intensität aus dem Anfang meiner Amtszeit erreicht. Vor allem die sehr enge und der Ausschussarbeit vorangehende Abstimmung von Ergebnissen zwischen der Mehrheitsfraktion einerseits und der Landesregierung bzw. den Ressorts andererseits hat es oft sehr erschwert, in den Beratungen der Ausschüsse datenschutzrechtliche Fragen eingehender zur Sprache zu bringen. Diese Verfahrensweise hat verständlicherweise auch die Bereitschaft der anderen Fraktionen, datenschutzrechtliche Aspekte in den Ausschüssen intensiver zu erörtern, nicht gefördert. Die Beratungsfunktion des LfD gegenüber dem Parlament (§ 22 Abs. 1 Satz 3 NDSG) und seine Funktion als Gesprächspartner des Landtages bei wesentlichen Entwicklungen des Datenschutzes oder bei Angelegenheiten von besonderer datenschutzrechtlicher Bedeutung (§ 22 Abs. 3 Sätze 3 und 4 NDSG) ist insofern im Berichtszeitraum nur unzureichend genutzt worden.

Demgegenüber haben die Landtagsverwaltung und insbesondere der Gesetzgebungs- und Beratungsdienst stets engen Kontakt zum LfD und seiner Geschäftsstelle gehalten. So hat der Gesetzgebungs- und Beratungsdienst bei der Vorbereitung der Ausschuss-Beratungen zur Novellierung des NDSG die Regelungsvorschläge und ihre konkrete Ausformulierung vorab jeweils intensiv mit dem LfD und seinen Mitarbeitern erörtert, sodass auf dieser Ebene ein Defizit nicht zu beklagen ist. Erfreulich ist auch, dass der Landtag meiner Empfehlung (vgl. Nr. 7 des XV. TB LfD Nds. 1999/2000) gefolgt ist und sich nunmehr als eines der letzten Landesparlamente in einem breiten Konsens aller im Landtag vertretenen Parteien eine eigenständige Datenschutzordnung gegeben hat. In dieser Datenschutzordnung vom 14. November 2001 (Nds. GVBl. S. 727) ist nunmehr normenklar geregelt, unter welchen Vorraussetzungen die einzelnen Gremien des Landtags, die Abgeordneten und Fraktionen und deren Beschäftigte personenbezogene Daten für parlamentarische Zwecke verarbeiten dürfen. Obwohl ich mir gewünscht hätte, dass der Landtag in Teilbereichen meinen weitergehenden Vorstellungen gefolgt wäre und etwa künftig auf die namentliche Benennung der Petenten in den Sammelübersichten verzichten würde, denke ich doch, dass es in der Gesamtheit gelungen ist, Regelungen zu treffen, die sowohl der besonderen verfassungsrechtlichen Stellung des Parlaments Rechnung tragen als auch den Schutz des informationellen Selbstbestimmungsrecht der betroffenen Bürger hinreichend gewährleisten.

Die parlamentarische Behandlung des vorliegenden Tätigkeitsberichts mit seiner gerade auch im Hinblick auf den Adressaten Landtag weiterentwickelten Struktur (vgl. unter 1) bietet, so hoffe ich, Gelegenheit, die Kommunikation zum und mit dem Landtag insgesamt wieder enger werden zu lassen. Unabhängig davon bleibt für mich die Frage, ob die Inanspruchnahme der gesetzlich vorgesehenen Beratungsdienstleistungen des LfD gegenüber dem Parlament für alle Beteiligten nicht leichter wäre, wenn die Geschäftsstelle des LfD, so wie es in neun anderen Bundesländern festgelegt ist, organisatorisch an den Landtag angebunden werden würde. Auch bei Beanstandungen des LfD im Rahmen seiner Kontrolltätigkeit, bei der Unterrichtung der Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes oder bei öffentlich geäußerter Kritik des LfD an bestimmten Vorfällen oder Vorgehensweisen der Verwaltung fällt es bei der derzeitigen Anbindung der Geschäftsstelle an das Innenministerium offensichtlich manchen Akteuren schwer, eigenständige Wertungen des LfD und konträre Positionen zu Auffassungen der Landesregierung richtig einzuordnen und zu akzeptieren. Bei einer Anbindung an den Landtag würden sich im Übrigen auch andere Fragen, wie das schon angesprochene Problem der Fachaufsicht über den LfD im nicht öffentlichen Bereich (§ 22 Abs. 6 Satz 2 NDSG) sicher leichter lösen lassen.

4.5 Die behördlichen Datenschutzbeauftragten

Den behördlicher Datenschutzbeauftragten sind durch die Novelle des Niedersächsischen Datenschutzgesetzes neue und veränderte Aufgaben zugewachsen. Auch der mit der Modernisierung der Verwaltung einhergehende verstärkte Einsatz automatisierter Verfahren, von Internet und E-Mail und fachspezifischer eGovernment-Anwendungen stellt erhöhte Anforderungen an die Kompetenz und Sachkunde der behördlichen Datenschutzbeauftragten, und zwar sowohl im Bereich des Daten-

schutzrechts als auch hinsichtlich der notwendigen technischen und organisatorischen Vorkehrungen zur Gewährleistung der Datensicherheit. Nur beispielhaft sei darauf verwiesen, dass die behördlichen Datenschutzbeauftragten im Sinne einer effizienten Datenschutzkontrolle nunmehr bereits im Vorfeld über geplante Verfahren der automatisierten Verarbeitung personenbezogener Daten zu unterrichten und für die Vorabprüfung von Verfahren, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien besondere Risiken mit sich bringen, zuständig sind (sog. Vorabkontrolle nach § 7 Abs. 3 NDSG).

Ich habe die gesetzlichen Änderungen zum Anlass genommen, die behördlichen Datenschutzbeauftragten in besonderen Veranstaltungen über die datenschutzrechtlichen Neuregelungen zu informieren und mir dabei gleichzeitig im persönlichen Austausch Erkenntnisse über die Situation und Arbeitsbedingungen der behördlichen Datenschutzbeauftragten vor Ort verschafft. Für die behördlichen Datenschutzbeauftragten der Gemeinden und Landkreise habe ich in allen Regierungsbezirken in enger Kooperation mit den kommunalen Spitzenverbänden Informationsveranstaltungen durchgeführt.

Die gute Resonanz auf die Veranstaltungen ist für mich Indiz dafür, dass die behördlichen Datenschutzbeauftragten sich ihrer besonderen datenschutzrechtlichen Verantwortung bewusst und in einem hohem Maße an praxisorientierten Informationen und Hinweisen zu datenschutzrechtlichen Fragestellungen interessiert sind. Die zwischenzeitlich in meinem Internetangebot eingerichtete Netzwerkplattform, in dem die in ihren Dienststellen oftmals als „Einzelkämpfer“ agierenden Datenschutzbeauftragten sich über besondere datenschutzrechtliche Problemstellungen ihrer Tätigkeit vor Ort austauschen und darüber hinaus Informationen über aktuelle Themen und Entwicklungen aus dem Bereich des Datenschutzes aufnehmen können, stellt nach Auffassung der Datenschutzbeauftragten eine wertvolle Unterstützung ihrer Arbeit dar (siehe auch unter Kapitel 5.3.4). Auch die Einrichtung des Datenschutzforums Niedersachsen geht auf Wünsche und Anregungen aus dem Kreis der behördlichen Datenschutzbeauftragten zurück, die mir gegenüber ihr großes Interesse an einer Ergänzung des datenschutzrechtlichen Fortbildungsangebots geäußert haben (siehe auch unter Kapitel 5.3.3).

Den Rückmeldungen der behördlichen Datenschutzbeauftragten konnte ich allerdings auch entnehmen, dass sich ihre Arbeitsbedingungen in den Dienststellen sehr unterschiedlich darstellen, in weiten Teilen verbesserungsbedürftig sind und maßgeblich davon abhängen, ob die jeweilige Dienststellenleitung datenschutzrechtlichen Fragen aufgeschlossen gegenübersteht.

Obwohl sich die Aufgaben und Befugnisse mit In-Kraft-Treten der Neuregelungen im NDSG am 6. Juli 2001 erheblich ausgeweitet haben, nehmen die Datenschutzbeauftragten ihre Funktion weiterhin zusätzlich zu ihren Aufgaben im Hauptamt wahr („zur Erledigung nebenbei“). Dieser Aufgabenzuwachs muss jedoch bei der Bemessung der Arbeitskapazitäten für den Datenschutzbereich angemessen berücksichtigt werden. Entgegen der eindeutigen gesetzlichen Regelung werden die Datenschutzbeauftragten bei der Einführung automatisierter Verfahren offenbar nicht selten erst kurz-

fristig oder gar erst dann beteiligt, wenn die Entscheidungen über die Einführung der Verfahren bereits getroffen wurden und somit kaum noch Veränderungen möglich sind. Hinweise und Änderungswünsche der Datenschutzbeauftragten werden dann oftmals als lästig und verfahrenshemmend abgetan. Eine auch unter Kostenaspekten effiziente und bereits im Vorfeld greifende Datenschutzkontrolle lässt sich auf diese Weise natürlich nicht realisieren. Dienstanweisungen oder Zielvereinbarungen mit der Behördenleitung, in denen die in durch den Datenschutzbeauftragten wahrzunehmenden Aufgaben und Befugnisse konkretisiert und für alle Beteiligten verbindlich festgelegt werden, sind oft veraltet oder liegen in vielen Fällen nicht vor. Es verwundert daher nicht, dass nach meinen Feststellungen den Beschäftigten oftmals überhaupt nicht bekannt ist, wer die Funktion des Datenschutzbeauftragten in der Dienststelle wahrnimmt und welche Rechte und Pflichten sich daran knüpfen. Da die Funktion des Datenschutzbeauftragten nur selten in den Behördenübersichten und Geschäftsverteilungsplänen dargestellt wird, haben darüber hinaus auch Bürger, die sich gemäß § 8a Abs. 3 NDSG in einer datenschutzrechtlichen Eingabe vertrauensvoll an den Datenschutzbeauftragten vor Ort wenden wollen, Schwierigkeiten, den richtigen Ansprechpartner zu ermitteln.

Die mir von vielen Datenschutzbeauftragten geschilderten Probleme in der Aufgabenerledigung, die durch die Erfahrungen aus der Arbeit meiner Geschäftsstelle immer wieder bestätigt werden, lassen vermuten, dass viele Dienststellen ihrer gesetzlichen Unterstützungspflicht noch nicht hinreichend nachkommen. Ich beabsichtige daher, im Rahmen einer zunächst auf den Bereich der Kommunalverwaltung beschränkten Befragung genauere Erkenntnisse und Informationen darüber zu gewinnen, wie sich die Arbeitssituation der behördlichen Datenschutzbeauftragten tatsächlich darstellt. Ziel ist es, den Dienststellen und behördlichen Datenschutzbeauftragten konkrete Lösungsansätze zur Verbesserung ihrer Arbeitsbedingungen aufzuzeigen.

4.6 Neuordnung der IT-Struktur des Landes

Die Landesregierung hat sich zum Ziel gesetzt, die IT-Struktur des Landes neu auszurichten und ein gesamtverantwortliches Informationstechnik-Management aufzubauen, das über zentrale Koordinierungs-, Steuerungs- und Controllingkompetenzen verfügt; außerdem soll das Informatikzentrum Niedersachsen zu einem leistungsfähigen zentralen Dienstleister für den IT-Bereich entwickelt werden. Diese Zielsetzungen werden vom LfD gerade auch angesichts der notwendigen Fortschritte im Bereich des eGovernment nachhaltig unterstützt. Seine Forderung, in dem zentralen Begleitgremium der neuen Struktur (IT-Board) als Mitglied vertreten zu sein, ist erfreulicherweise aufgenommen worden. Die Mitgliedschaft entspricht der auch sonst praktizierten engen und frühzeitigen Einbindung des LfD in die Entscheidungs- und Entscheidungsvorbereitungsprozesse in der Landesverwaltung zum Aufbau und zum Betrieb automatisierter Informations- und Kommunikationssysteme, wie sie auch durch die Regelungen im NDSG (§ 22 Abs. 1 Satz 3 und Satz 4, Abs. 2) für die vom LfD wahrgenommene Querschnittsaufgabe Datenschutz und Datensicherheit vorgegeben ist. Der LfD wird in dem neuen Gremium seinen Ansatz der konstruktiven, auf die Lösung (und nicht auf die Verfestigung) von Problemen ausgerichteten Mitarbeit fortsetzen und die mit der Schaffung der neuen Organisationsstrukturen verfolgten Zielsetzungen nach Kräften fördern.

4.7 Informationszugangsgesetz

Es besteht mittlerweile in weiten Teilen der Politik und Wirtschaft Konsens darüber, dass es in einer modernen Informationsgesellschaft notwendig ist, die Transparenz des Verwaltungshandelns und damit gleichzeitig auch die demokratischen Mitwirkungs- und Beteiligungsrechte durch einen verfahrensunabhängigen Anspruch auf Zugang zu den amtlichen Informationen und Dokumenten zu verbessern. Der Anspruch auf Informationszugang ist mittlerweile Standard in fast allen Mitgliedstaaten der EU. Auf Länderebene hat nach Brandenburg, Berlin und Schleswig-Holstein auch das Land Nordrhein-Westfalen im November 2001 ein Informationszugangsgesetz verabschiedet, übrigens mit Zustimmung aller im Landtag vertretenen Parteien.

Bereits in Nr. 3.4 des XV. TB LfD Nds. 1999/2000 habe ich an die politischen Entscheidungsträger in Niedersachsen appelliert, die Diskussion über die Verabschiedung eines vor dem Hintergrund der Rechtsentwicklung in anderen Ländern längst überfälligen Akteneinsichts- und Informationszugangsgesetzes rasch aufzunehmen und unvoreingenommen zu führen. Ich war daher sehr erfreut, dass ich in der öffentlichen Anhörung zum Entschließungsantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN „Stärkung der Demokratie und mehr Verwaltungstransparenz in Niedersachsen - Landtag macht sich stark für ein Informationsfreiheitsgesetz“ (LT-Drs. 14/2191) Gelegenheit hatte, dem Rechts- und Verfassungsausschuss meine Position darzustellen. Bei dieser Gelegenheit konnte ich auch mit Hinweis auf die Erfahrungen aus anderen Ländern deutlich machen, dass der vielbeschworene Zielkonflikt mit den datenschutzrechtlichen Belangen der Betroffenen und den Interessen der Unternehmen an der Wahrung ihrer Betriebs- und Geschäftsgeheimnisse durchaus praktikabel und sachgerecht zu lösen ist.

Leider haben sich die großen Fraktionen des Landtages, zum Teil wohl auch unter dem Eindruck der ablehnenden Haltung der Landesregierung, nicht entschließen können, das an eine subjektive Betroffenheit anknüpfende Prinzip der nur beschränkten Aktenöffentlichkeit umzukehren und nun endlich auch den niedersächsischen Bürgern den in anderen Ländern längst selbstverständlichen Anspruch auf einen geregelten Zugang zu den Informationen ihrer Verwaltung zuzubilligen. Neben allgemeinen Zweifeln am Bedarf und an der praktischen Durchführbarkeit einer gesetzlichen Regelung wurde im Wesentlichen auf den vornehmlich bei den Kommunen entstehenden Verwaltungsaufwand und auf die damit einhergehenden Kostenbelastungen abgestellt. Diese Argumente werden aber durch die praktischen Erfahrungen in den Ländern, die bereits über ein Informationszugangsgesetz verfügen, widerlegt (vgl. zuletzt die Erhebung aus Schleswig-Holstein, siehe http://www.datenschutzzentrum.de/informationsfreiheit).

Nachdem die neue Bundesregierung in der Koalitionsvereinbarung (Seite 67) ihre Absicht bekräftigt hat, ein für den Bereich der Bundesbehörden geltendes Informationsfreiheitsgesetz zu schaffen, hoffe ich, dass auch in Niedersachen die Diskussion bald wieder aufgenommen wird.

5 Der Landesbeauftragte

5.1 Geschäftsstelle

Angesichts der Vielfalt der wahrzunehmenden Aufgaben und der begrenzten Stellenausstattung der Geschäftsstelle ist es weiterhin erforderlich, einen Großteil der Kapazitäten durch Schwerpunktsetzung und Prioritätenbildung auf die Bereiche zu konzentrieren, die für die weitere Entwicklung aus Datenschutzsicht von besonderer Bedeutung sind. Die Darstellungen in diesem Tätigkeitsbericht machen diese Schwerpunktsetzungen und Prioritätenbildungen deutlich und transparent.

Durch Abordnungen aus Fachverwaltungen hat die Geschäftsstelle ihre Personalkapazitäten über die zugewiesenen Planstellen hinaus erweitern können. Die schon bewährten Abordnungen aus dem Bereich der Vollzugspolizei und der Steuerverwaltung (vgl. Nr. 4.1 des XV. TB LfD Nds. 1999/2000) sind ergänzt worden durch die Abordnung eines Kollegen aus dem Bereich der gesetzlichen Krankenversicherung. Sein Sachverstand ist gerade bei den aktuellen Reformdiskussionen im Gesundheitswesen und deren Auswirkungen auf den Schutz von Gesundheitsdaten außerordentlich wertvoll.

Für den Aufgabenbereich einer Kollegin mit Teilzeitarbeit ist eine Lösung für einen Telearbeitsplatz entwickelt und erprobt worden, bei der sowohl die technischen als auch die organisatorischen und sozialen Gesichtspunkte umfassend und musterhaft eingearbeitet worden sind. Es ist beabsichtigt, diese Lösung über den Ansatz der Telearbeit hinaus zu einem Referenzmodell für mobile working weiter zu entwickeln, einer Arbeitsform, bei der von wechselnden Einsatz- oder Aufenthaltsorten aus die sichere elektronische Kommunikation mit der Dienststelle und der direkte geschützte elektronische Zugriff auf deren Datenbestände gewährleistet sein muss. Diese Arbeitsform wird in der Zukunft auch in der öffentlichen Verwaltung vermehrt nachgefragt werden und muss die elektronische Kommunikation und den Datenzugriff vom Konferenz- oder Besprechungsort, vom Übernachtungsort bei Dienstreisen oder an den Abenden, an Wochenenden oder im sonstigen Bedarfsfall von zu Hause aus ermöglichen können. Voraussetzung ist aber, dass die Vertraulichkeit der Kommunikation und die Datensicherheit beim Zugriff auf dienstliche Datenbestände ohne Einschränkung sichergestellt ist. Hierzu soll eine Muster-Lösung entwickelt werden (vgl. Kapitel 7.6.3).

5.2 Neue Prüfstrategien und Handlungsansätze

Übergreifendes Ziel bei der Wahrnehmung aller Aufgaben des LfD und seiner Geschäftsstelle ist weiterhin nicht das nachsorgende Herausfinden von Datenschutzverstößen, sondern die vorsorgende aktive Beratung und die Mitgestaltung bei der Entwicklung von datenschutzgerechten und datenschutzfreundlichen Lösungen und Leistungsangeboten in Wirtschaft und Verwaltung sowie die Aufklärung der Bürger über Gefährdungen ihres Rechts auf informationelle Selbstbestimmung. Hierzu sind im Berichtszeitraum neue Strategien und Handlungsansätze sowie eine Reihe neuer Instrumente, Angebote und Produkte entwickelt worden.

Das neue Bundesdatenschutzgesetz hat mein Aufgabenfeld der Datenschutzaufsicht in der Wirtschaft wesentlich erweitert. Die Aufsichtsbehörden nach dem BDSG können die Einhaltung der Datenschutzbestimmungen nun auch ohne Anlass überprüfen. Damit unterfallen Tausende von Wirtschaftsunternehmen, Handwerksbetrieben, Arztpraxen und Anwaltskanzleien meiner Kontrolle. Auch durch verstärkten IuK-Technikeinsatz und durch zunehmende Internet-Präsenz der öffentlichen Verwaltung steigt deren Beratungs- und Kontrollbedarf gewaltig. Doch ohne Personalvermehrung wird dieses neue Aufgabenspektrum selbst unter Ausnutzen von Synergieeffekten nicht zu meistern sein. Da keine neuen Stellen in Aussicht sind, müssen neue Strategien und Handlungsansätze einer angemessenen Beratung und Aufsicht entwickelt werden. Diese bestehen im Wesentlichen aus fünf Elementen:

- Thematische Gruppenprüfungen,
- Online-Prüfungen,
- Kooperationen mit unseren Prüflingen,
- Beratung der Bürger sowie
- Verstärken marktwirtschaftlicher Anreize.

5.2.1 Gruppenprüfungen

Meine Aufgabenwahrnehmung im Bereich der Datenschutzaufsicht stützt sich - neben der Bearbeitung von Eingaben und der Begleitung von einschlägigen Regelungsvorhaben - derzeit im Wesentlichen auf drei Säulen:

- Allgemeine Fortbildungsveranstaltungen,
- Einzelberatungen von Stellen im öffentlichen Bereich und Unternehmen der Wirtschaft sowie
- formelle Prüfungen.

Ergänzend zu den bisherigen drei Säulen wurde in einem ersten Versuch anstelle formaler Einzelprüfungen eine Gruppenprüfung bei mehreren Stellen im öffentlichen Bereich durchgeführt. Die Gruppenprüfungen erfolgen in Absprache und enger Zusammenarbeit mit den geprüften Stellen. Sie enthalten sowohl Elemente der klassischen formalen Einzelprüfung als auch der Einzelberatung. Konkret werden in den Gruppenprüfungen jeweils Themen aufgegriffen, die erfahrungsgemäß in ähnlicher Weise bei einer größeren Anzahl von öffentlichen Stellen auftreten. Im weiteren Verlauf der Prüfung werden möglichst umfassende Lösungsmodelle für die Problemfelder in Form von Workshops unter aktiver Mitarbeit der Geprüften erarbeitet. Dabei wird angestrebt, dass die Lösungsmodelle auch über den Kreis der Geprüften hinaus als eine Art Leitfaden nutzbar sind. Die Gruppenprüfung werden in weiten Strecken als formale Prüfung nach § 22 NDSG abgewickelt; dabei werden neben den speziell ausgewählten Problemfeldern auch die übrigen technischen und organisatorischen Maßnahmen bei den zu Prüfenden untersucht.

Darüber hinaus bieten auch die Gruppenprüfungen wie derzeit die Einzelberatung oder -prüfung Möglichkeiten, offene Fragen zur Sprache zu bringen und an einer datenschutzgerechten und praktikablen Lösung mitzuarbeiten. Hierzu werden speziel-

le Fragestellungen zu Beginn der Gruppenprüfung abgefragt und bei der Festlegung der Prüfungsschwerpunkte berücksichtigt. Der Versuch wurde durch die kommunalen Spitzenverbände unterstützt und aktiv begleitet. Die ersten Ergebnisse sind vielversprechend und machen Mut auf mehr.

5.2.2 Online-Prüfungen

In Niedersachsen präsentieren sich immer mehr Unternehmen und Behörden mit eigenen Homepages. Dabei können einfache Informationen über den Anbieter abgerufen werden, Software-Downloads gestartet und Supportanfragen übermittelt werden. Darüber hinaus entstehen immer mehr automatisierte Anwendungen im eCommerce und eGovernment. Bei allen Internet-Auftritten ist von mir als Aufsichtsbehörden zu überprüfen, ob die Angebote den Vorschriften des Multimediarechts und des allgemeinen Datenschutzrechts entsprechen. Dabei sind auch die in den Webangeboten verankerten technischen Lösungen, die zum einen Gefahren für den Besucher der Website beinhalten können (z.B. ActiveX, Java-Skript) oder die Rückschlüsse auf das Nutzerverhalten erlauben (z.B. Cookies, Web Bugs) zu überprüfen. Mir war es bisher aus Kapazitätsgründen nicht möglich, die Vielzahl von Online-Angeboten in Niedersachsen umfassend zu prüfen.

Wirkungsvolle Hilfe in der Zukunft verspreche ich mir vom Einsatz geeigneter automatisierter Prüfwerkzeuge. Prüftools können zwar nicht das rechtliche und technische „know-how“ eines Prüfers ersetzen, sie können ihn aber bei seiner Aufgabe wesentlich unterstützen. Bekannte Online-Tools untersuchen den inhaltliche Teil und den technischen Teil des Internet-Angebots getrennt. Die inhaltliche Prüfung erfolgt durch Recherche bestimmter Stichworte (z.B. Impressum zum Auffinden der Anbieterkennzeichnung) oder einer automatisierten Anfrage bei der DENIC. Die daraus resultierenden Ergebnisse müssen vom Prüfer bewertet werden, sie erleichtern ihm die Erstellung des Prüfberichtes. Gerade in technischer Hinsicht kann ein Prüftool jedoch eine große Hilfe bringen. Die automatisierte Prüfung kann die Quelltexte einer Internet-Seite analysieren und nach bestimmten Codes suchen, die zum Beispiel auf den Einsatz von Skriptsprachen wie Java-Skript oder auf Cookies hinweisen. Durch die automatisierte Suche erspart sich der Prüfer das manuelle Lesen der Quelltexte, er kann stattdessen die vom Prüfwerkzeug gefundenen Ergebnisse verifizieren.

Ich habe mich für den Einsatz des Prüfwerkzeugs OPTuM der datenschutz nord GmbH entschieden. Mit OPTuM wird eine Kopie des zu prüfenden Online-Angebotes auf dem Prüfserver abgelegt und dann eingehend analysiert. Weiter unterstützt OPTuM die Abfassung eines Prüfberichts und eines Anschreiben an das geprüfte Unternehmen oder die Behörde. Gegenwärtig wird OPTuM zusammen mit ausgewählten niedersächsischen Unternehmen getestet. Die Prüfergebnisse sollen den Unternehmen zur Verbesserung ihrer Online-Angebote dienen und gleichzeitig zur Weiterentwicklung und Anpassung des Prüfwerkzeuges herangezogen werden.

5.2.3 Kooperationen mit meinen „Prüflingen“

Die Informations- und Wissensgesellschaft bietet neben Chancen viele Gefahren und Risiken für die geschäftsmäßige und private Nutzung des Internet. Ein durchdachtes

und schlüssiges Datenschutz- und Datensicherungskonzept ist Voraussetzung für den Erfolg von eCommerce und eGovernment. Ich bin bereit, gemeinsam mit Partnern aus Wirtschaft und Verwaltung datenschutzgerechte Lösungen in Kooperationen zu entwickeln. Meine Projektpartner erhalten aktuelle Informationen rund um ihr Projekt, Antworten auf ihre Fragen und eine Plattform für Zusammenarbeit mit anderen Projektteilnehmern. Durch Transparenz der Projekte können die Schutz- und Sicherheitskonzepte verbessert sowie Entwicklungen datenschutzfreundlicher Technologien an Beispielen verfolgt werden. Ein erfolgreiches Beispiel ist das Projekt „Datenschutzgerechte Internet-Angebote der Wirtschaft“, das ich mit vier Großfirmen der niedersächsischen Wirtschaft betreibe (vgl. Kapitel 19).

5.2.4 Beratung

Meine Beratungsaktivitäten im Internet und per Telefon richten sich schwerpunktmäßig an die Verbraucher. Ich kläre sie über ihre Rechte nach den Datenschutzgesetzen auf und zeige ihnen den Weg zur Durchsetzung ihrer Rechte. Im folgenden Abschnitt „Angebote und Produkte des LfD“ unter 5.3 sind dazu Einzelheiten beschrieben.

5.2.5 Marktwirtschaftlicher Anreiz - Datenschutz-Audit

Datenschutz und angemessene Datensicherung im Internet sind die Akzeptanzvoraussetzungen für erfolgreiches eCommerce und eGovernment. Dies belegen nicht zuletzt Umfragen unter Nutzern. Sie verlangen einen hinreichenden Schutz ihrer personenbezogenen Daten. Anbieter von Datenverarbeitungssystemen oder -programmen sowie Daten verarbeitende Stellen können ihre Datenschutzkonzepte sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen, um den Nachweis für ihre Sicherungen führen zu können. Dies sehen § 17 Mediendienste-Staatsvertrag, § 9a Bundesdatenschutzgesetz und mehrere Landesdatenschutzgesetze vor. Leider stehen die erforderlichen Ausführungsvorschriften zu der Regelung des § 9a BDSG noch aus, sodass sich die praktische Umsetzung bundesweit verzögert. Ausführungsvorschriften sind bisher nur für ein Behördenaudit nach § 43 Abs. 2 des Landesdatenschutzgesetzes Schleswig-Holstein vorhanden. Ich werde mich aus den im Kapitel 4.2 dargestellten Gründen dafür einsetzen, dass möglichst bald entsprechende Regelungen auch in das Niedersächsische Datenschutzgesetz eingefügt werden.

Ein Gutachten für eine bundesgesetzliche Regelung ist in Arbeit und wird voraussichtlich Ende 2002 vorliegen. Zielsetzung des Datenschutz-Audits ist die freiwillige Überprüfung der datenschutzrechtlichen Eignung von Produkten und Verfahren. Damit soll zugleich eine kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit erreicht werden. Das Audit fördert Eigenverantwortung durch Selbstkontrolle und Selbstregulierung. Es belohnt die Teilnehmer mit der Möglichkeit, mit dem Datenschutz-Audit zu werben und das Vertrauen von Nutzern zu gewinnen.

Bisher fehlen bundesweit anerkannte Kriterien für ein Datenschutz-Audit nach dem Bundesdatenschutzgesetz, mit denen die datenschutzrechtliche Qualität von Produkten, Dienstleistungen und Datenverarbeitungsverfahren für den Einsatz in Wirtschaft und Verwaltung gemessen werden kann. Eine gute Grundlage für deren Ausgestal-

tung ist zum einen das Prüfschema des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD). Das ULD begutachtet schon jetzt IT-Produkte, die durch öffentliche Stellen des Landes Schleswig-Holstein eingesetzt werden sollen, auf Geeignetheit und Vereinbarkeit mit den Rechtsvorschriften über den Datenschutz und die Datensicherheit. Darüber hinaus können auch öffentliche Stellen ihr Datenschutzkonzept durch das ULD prüfen und beurteilen lassen. Auch wenn IT-Produkte und Datenverarbeitungsverfahren in privatwirtschaftlichen Unternehmen oder in der öffentlichen Verwaltung anderer Bundesländer davon nicht erfasst werden, sind die Anforderungen und die Prüfergebnisse auf sie übertragbar. Sie werden von mir bei Prüfungen in Niedersachsen entsprechend gewürdigt.

Erfahrungen mit Auditierungen liegen auch bei der aus einem Forschungsprojekt der Fachhochschule Frankfurt in Zusammenarbeit mit der Gewerkschaft ver.di entstandenen Gütesiegels der quid!GmbH vor. Erklärte Ziele des quid!-Gütesiegels sind der betriebliche und produktbezogene Datenschutz, Stärkung der Persönlichkeitsrechte von Arbeitnehmern sowie Kunden- und Anwenderfreundlichkeit. Vorleistungen zur Erstellung von Bewertungskriterien hat auch die datenschutz nord GmbH - eine Landesgesellschaft der Freien Hansestadt Bremen mit den Geschäftsbereichen Datenschutz und Datensicherheit - erbracht. In einem ersten Entwurf von "protection profiles" wurde ein allgemein gültiger Anforderungskatalog für online abwickelbare Dienstleistungen erstellt und mit den Datenschutzaufsichtsbehörden der norddeutschen Länder abgestimmt. Auch ich arbeite daran mit. Der Katalog soll künftigen Datenschutz-Gutachten zugrunde gelegt werden und ein Zertifikat "Datenschutzgerecht" ermöglichen. Dem zertifizierten Unternehmen winken Marktvorteile, wenn sie nachweisen können, dass sie fair und verabredungsgemäß mit den Daten der Kunden umgehen.

5.3 Angebote & Produkte des LfD

Ich informiere stets aktuell Bürger, Verwaltung und Wirtschaft sowie die Medien über meine Erfahrungen, Forderungen und Empfehlungen zum Datenschutz und zur Datensicherung. Ich bin insbesondere bemüht, durch meine Veröffentlichungen und durch aktive Präsenz im Internet mit allen Datenschutzinteressierten ins Gespräch zu kommen.

5.3.1 Neues Internetangebot

Seit dem 12. August 2002 präsentiere ich mich in einer optisch und inhaltlich neu gestalteten Homepage im Internet unter der bekannten Adresse:

http://www.lfd.niedersachsen.de

im neuen Niedersachsen-Portal. Bereits seit 1998 betreibe ich meine Internet-Plattform für Bürger, Medienvertreter, Stellen der öffentlichen Verwaltung und Unternehmen der Wirtschaft. Neu sind in dem dynamisch aufgebauten Angebot ein optisch gefälligeres Layout, die übersichtlichere Navigation, eine neue Themenreihe mit aktuellen Informationen zum Datenschutz und zur Datensicherheit in Deutschland und eine leistungsstarke Suchmaschine. Diese Neuerungen erleichtern den Zugang zu

den Informationen. Sie sollen zur verstärkten Interaktion sowie zur direkten Kommunikation anregen. Ich möchte Fachkräften aus Verwaltung und Wirtschaft Hilfen zum datenschutzgerechten Umgang mit personenbezogenen Daten anbieten; sie finden dafür 200 Download-Dokumente. Betroffenen Bürgern zeige ich auf, welche Rechte sie haben, wenn Verwaltung und Wirtschaft ihre personenbezogenen Daten verarbeiten. Ich unterrichte ferner über eigene Gestaltungs- und Wahlmöglichkeiten.

Zugegeben, die ersten Wochen des Auftritts des neuen Niedersachsen-Portal waren für alle Nutzer, aber auch für mich sehr nervig und erforderten viel Geduld und Verständnis, weil das Antwort-Zeit-Verhalten auf Grund von Perfomanceproblemen auf der zentralen Systemebene nicht akzeptabel war. Das hat mir unberechtigt viel kritische Bemerkungen gebracht. Ungeachtet dessen bin ich sehr an einem lebhaften und konstruktiven Meinungsaustausch interessiert. Mit Zustimmung der Betroffenen weisen alle Internet-Artikel die jeweiligen Ansprechpartner meiner Dienststelle aus. Die eingeblendeten E-Mail-Adressen sollen die erwünschte Kommunikation mit unseren Nutzern erleichtern. Lassen auch Sie sich als Leserin oder Leser dieses Tätigkeitsberichtes einladen und besuchen Sie das Informationsangebot auf unserer neuen Webpage.

5.3.2 Virtuelles Datenschutzbüro

Das virtuelle Datenschutzbüro ist eine Kooperation nationaler und internationaler Datenschutzbeauftragter, die durch ihre Kompetenz und ihre Unabhängigkeit für ausgewogene Bewertungen und Hilfen sorgen. Der internationale Charakter ist in dem weltweiten Internet von großer Bedeutung. Dies kommt durch die Mehrsprachigkeit der Angebote, insbesondere durch die englische Sprache, zum Ausdruck. Der gemeinsame Rechtsrahmen innerhalb der Europäischen Union erleichtert zudem die europäische Kooperation. Darüber hinaus werden externe Fachleute an den Themen im virtuellen Datenschutzbüro beteiligt. Ich bin seit Beginn Kooperationspartner im virtuellen Datenschutzbüro.

Nutzer erhalten durch das Portal des virtuellen Datenschutzbüros einen komfortablen Zugang zu den für sie relevanten Informationen. Das virtuelle Datenschutzbüro dient also auch als Orientierungshilfe, die dezentrale Strukturen transparent macht. Es ist geplant, das virtuelle Datenschutzbüro auch Anbietern von Datenschutz- und Datensicherheitsprodukten aus der Wirtschaft, für Projekte aus der Wissenschaft und Selbsthilfeorganisationen für Bürger zu öffnen und ihnen eigene Beiträge zu ermöglichen.

5.3.3 Datenschutzforum Niedersachsen

Das Datenschutzforum Niedersachsen ist ein neues Schulungsangebot für aktuelle Themen des Datenschutzes und der Datensicherung. Ich verfolge damit das Ziel, die Erkenntnisse aus Datenschutz-Prüfungen sowie Erfahrungen aus Datenverarbeitungs-Projekten in die Praxis zu transferieren. Datenschutz-Kurse sollen fundierte Kenntnisse vermitteln. In Seminaren wird die Verknüpfung von Theorie und Praxis im Vordergrund stehen. In Workshops mit Experten aus Verwaltung und Wirtschaft sol-

len Empfehlungen für behördliche und betriebliche Datenschutzbeauftragte gemeinsam erarbeitet werden. Das Programm startet im Frühjahr 2003.

Das Schulungsangebot richtet sich an Mitarbeiter aus Verwaltung und Wirtschaft sowie an Bürger des Landes Niedersachsen. Das Schulungsangebot soll zeitnah Wissen, beispielhafte Lösungen und Werkzeuge zum Thema Datenschutz und Datensicherheit vermitteln. Das Schulungsangebot will nicht in Konkurrenz zu Angeboten anderer Fortbildungsträger treten, sondern vorhandene Kurse um spezielles Wissen und Erfahrungen des Landesbeauftragten für den Datenschutz ergänzen.

5.3.4 Netzwerk der behördlichen Datenschutzbeauftragten

Den behördlichen Datenschutzbeauftragten sind durch die Novelle des Niedersächsischen Datenschutzgesetzes neue und veränderte Aufgaben zugewachsen. Auch technischer Wandel stellt sie vor neue Herausforderungen, wenn es darum geht, in ihren Dienststellen auf einen datenschutzgerechten Einsatz der modernen Informations- und Kommunikationstechnologien hinzuwirken. Meine Kontakte mit behördlichen Datenschutzbeauftragten und die Erfahrungen aus der Tätigkeit meiner Geschäftsstelle zeigen sehr deutlich, dass es notwendig ist, die in ihren Dienststellen oftmals als „Einzelkämpfer“ agierenden behördlichen Datenschutzbeauftragten bei der Wahrnehmung ihres Amtes zu unterstützen. Darüber hinaus möchte ich alle Mitarbeiter ermutigen, sich für den Datenschutz zu engagieren und die Einhaltung der Datenschutzpflichten ihrer Organisationen selbst zu kontrollieren. Ich möchte zur partnerschaftlichen Problemlösung beitragen und als Dienstleister und Kompetenzzentrum überzeugen.

Dazu habe ich ein Netzwerk behördlicher Datenschutzbeauftragter aus dem Bereich der Landes- und Kommunalverwaltung initiiert, die über das Internet in einer geschlossenen Benutzergruppe Erfahrungen austauschen sowie gemeinsam datenschutzgerechte Lösungen erarbeiten. Hier können besondere Problemstellungen aus der Tätigkeit vor Ort und aktuelle Themen sowie Entwicklungen aus dem Bereich des Datenschutzes erörtert und zugleich ein regelmäßiger Erfahrungsaustausch gepflegt werden. Weitere Interessierte sind herzlich willkommen.

5.3.5 Netzwerk der behördlichen Datenschutzbeauftragten der Polizei

Auch für behördliche Datenschutzbeauftragte und Datenschutz-Interessierte der niedersächsischen Polizei habe ich ein solches Netzwerk angeregt. Alle Benutzer des Datenschutzforums Polizei werden aktuell über unsere Erfahrungen aus der Prüfpraxis sowie über unsere Empfehlungen und Forderungen in allen Fragen der personenbezogenen Datenverarbeitung informiert. In diesem Netzwerk diskutiert eine geschlossene Benutzergruppe über Probleme und Fragen des Datenschutzes im Bereich der Polizei und erarbeitet gemeinsam Lösungen. Da das Netzwerk Belebung braucht, ermutige ich auf diese Weise weitere Interessierte zum Mitmachen.

5.3.6 Angebot an Datenschutzbeauftragte der Träger der freien Jugendhilfe und der freien Wohlfahrtspflege

Die Träger der freien Jugendhilfe und der freien Wohlfahrtspflege sind wichtige "Mitspieler" im sozialen Netz der Bundesrepublik Deutschland. Bei ihrer Betreuungsaufgabe haben sie Umgang mit sensiblen personenbezogenen Daten. Dabei haben sie die Vorschriften des Sozialgesetzbuches zu beachten. Dieses Regelwerk ist nicht nur umfangreich, sondern auch sehr kompliziert.

Als Orientierungshilfe für Mitarbeiter der freien Träger biete ich eine Vortragsreihe zum datenschutzgerechten Umgang mit Sozialdaten an. Dabei sollen die erforderliche Kenntnisse vermittelt und Gelegenheit gegeben werden, über alle erkannten Probleme zu diskutieren. Zugleich dienen die angebotenen Veranstaltungen als „Türöffner“ für auszubauende Kontakte mit den Freien Trägern.

5.3.7 CeBIT - Der besondere Datenschutz-Tag

Das Datenschutz-Forum der CeBIT habe ich auch in den Jahren 2001 und 2002 erfolgreich veranstalten können. „Vorgaben und Werkzeuge für datenschutzgerechtes eCommerce und eGovernment“ war die jüngste Veranstaltung überschrieben. Renommierte Experten aus Wirtschaft und Wissenschaft diskutierten über die Akzeptanz-Voraussetzung Datenschutz. Sie stellten datenschutzgerechte Werkzeuge für einen erfolgreichen Einsatz vor. Ohne einen besseren Schutz der Privatsphäre wird es keine demokratisch verantwortbare Informationsgesellschaft geben, darüber war man sich schnell einig. Die anwesenden Datenschutzbeauftragten des Bundes und der Länder erklärten ihre Bereitschaft, solche Entwicklungen konstruktiv zu begleiten.

Die CeBIT-Veranstaltung 2003 am 17. März 2003 wird ein neues Gesicht erhalten. Sie wird Datenschutz-Tag heißen und ganztägig in einem größeren Saal veranstaltet werden. Dort werden neben dem Plenum Marktstände mit vielfältigen Informationen unterschiedlicher Aussteller und Organisationen aufgebaut sein. Detaillierte Informationen und Praxistipps von IT- und Datenschutzfachleuten sollen angeboten werden.

5.3.8 Datenschutz-Workshop für behördliche Datenschutzbeauftragte

Vorhaben des eGovernment, der digitale Zugang zu behördlichen Informationen und die elektronische Teilhabe am politischen Willensbildungsprozess, digitale Personalverwaltungssysteme und mobile working sind die Datenschutz-Herausforderungen der Gegenwart. Für Bedienstete der öffentlichen Verwaltung, die für die IuK-Technik verantwortlich sind, sowie für behördliche Datenschutzbeauftragte biete ich jährlich einen zweitägigen Workshop an, in dem aktuelle Informationen zum Datenschutz und zur Datensicherung gegeben werden. Meine Mitarbeiter und ich stehen dabei für eine offene Diskussion zur Verfügung. In kleinen Arbeitskreisen werden Erfahrungen ausgetauscht und Konzepte für Teilaufgaben erarbeitet.

Der Datenschutz-Workshop findet in Zusammenarbeit mit dem SiN in Bad Münder statt. Er hat eine erfreuliche Resonanz gefunden; die offene Diskussion über alle aktuellen Datenschutzthemen der öffentlichen Verwaltung wird besonders hervorgehoben.

5.3.9 eBusiness-Tag der Industrie- und Handelskammer

Auf Einladung habe ich mich am eBusiness-Tag der Industrie- und Handelskammer Hannover beteiligt und einen Informationsstand betrieben. Dessen Angebote wurden in erfreulichem Maße angenommen; die begonnenen Fachgespräche werden in mehreren Kooperationen fortgesetzt.

5.3.10 PC-Selbsttest

Über meine Homepage www.lfd.niedersachsen.de stelle ich einen Selbst-Test zur Verfügung. Der Test ist für Privatanwender gedacht ist und soll helfen, unsichere Systemkonfigurationen aufzudecken. Nur wenn bekannt ist, welche Lücken ein System aufweist, kann qualifiziert Abhilfe geschaffen werden. Daher überprüft der Test in einem mehrstufigen Verfahren nicht nur die Einstellungen des Browsers, sondern führt auf Wunsch des Nutzers auch einen sog. Port-Scan durch. Die Ergebnisse werden dem Tester vertraulich zur Verfügung gestellt und ermöglichen, die notwendigen Maßnahmen zur Absicherung des Systems zu treffen. Nachdem der Selbst-Test zwischenzeitlich überarbeitet und für diese Zeit vom Netz genommen werden musste, steht er allen Nutzern wieder zur Verfügung.

5.3.11 OPTuM - Online-Prüfung von Tele- und Mediendiensten

Mit OPTuM - Online-Prüfung von Tele- und Mediendiensten - lassen sich Internetangebote privater oder öffentlicher Stellen automatisiert überprüfen. Dazu werden sämtliche Seiten des zu prüfenden Angebots auf datenschutzrechtlich relevante Aspekte untersucht. Die Ergebnisse werden dem Prüfer übersichtlich präsentiert, der daraus einen Prüfbericht erstellt. Zurzeit werden folgende Aspekte berücksichtigt:

- Anbieterkennzeichnung,
- Datenschutzerklärung,
- Verwendung von Cookies,
- Unterrichtung des Nutzers,
- Automatische Weitervermittlungen auf Angebote Dritter und
- Web-Bugs.

OPTuM ist für mich ein strategisches Werkzeug, mit dem ich meinen Prüf- und Beratungsauftrag gegenüber den vielen Tele- und Mediendiensteanbietern angemessen und zeitgerecht erfüllen möchte. Ich habe eine Nutzungslizenz erworben. In einer ersten Testanwendung habe ich mehrere große Tele- und Mediendienste überprüft. Weitere Prüfungen und Auswertungen sind in Vorbereitung. Meine Prüferfahrungen bringe ich in die geplante Weiterentwicklung des Prüfwerkzeugs ein. Es ist erklärte Absicht, das Prüf-Tool zu einem späteren Zeitpunkt nach ausreichenden Tests allen Diensteanbietern zur Selbstkontrolle anzubieten.

5.3.12 Hinweise und Erläuterungen zum NDSG

Unmittelbar nach In-Kraft-Treten des novellierten Niedersächsischen Datenschutzgesetzes habe ich Hinweise und Erläuterungen zu den Einzelvorschriften des NDSG veröffentlicht. Die Erläuterungen - ein Gemeinschaftswerk meiner Mitarbeiter - sind als gedruckte Broschüre erschienen, sie sind auch als elektronisches Dokument im

Internet abrufbar. Sie sollen allen, die nicht tagtäglich mit datenschutzrechtlichen Fragestellungen befasst sind, das Verständnis für die recht komplizierten Vorschriften erleichtern. Für behördliche Datenschutzbeauftragte sind die Hinweise und Erläuterungen zum NDSG „Pflichtlektüre“ am Arbeitsplatz, wie viele positive Kommentare zur Veröffentlichung belegen. Die gedruckte Broschüre wurde großflächig an alle Landesdienststellen und an Stellen der Kommunalverwaltung verteilt. Die Auflage ist inzwischen weitgehend vergriffen, nur ein kleiner Restbestand steht noch zur Verfügung. Eine stets aktuelle Fassung ist über das Internet im Download abrufbar.

5.3.13 Schulen ans Netz - mit Sicherheit

„Wir sind schon drin“, das sagen heute bereits viele niedersächsische Schulen. Fast alle Schulen haben einen Internetzugang, viele Schulen betreiben eigene Internet-Angebote. Beim Gang ins Internet ergeben sich neben vielen handwerklichen Problemen auch Fragen zum sicheren Umgang mit dem weltweiten Web. Ausführliche Hinweise und Empfehlungen für Schulleitungen, Lehrer, Schüler sowie Eltern sind in meiner Broschüre „Schulen ans Netz - mit Sicherheit“ zusammengefasst. Sie will die nötige Sensibilität für Sicherheits- und Datenschutzprobleme vermitteln, praktische Lösungen für weitere Fragestellungen vorstellen und soll helfen, mit den Herausforderungen des Internet konstruktiv und sachgerecht umzugehen.

Ganz allgemein wird berufliches und privates Handeln immer ausgeprägter in der "Computerwelt" stattfinden. Sicherheitskompetenz muss deshalb als Bestandteil schulischer Bildung verstanden und als Schwerpunkt im Bereich der Aus- und Weiterbildung gesetzt werden. Hierzu will eine medienpädagogisch aufbereitete CD-ROM die wichtige Zielgruppe der 14- bis 21-jährigen Schüler sowie der Auszubildenden an allgemein- und berufsbildenden Schulen hinsichtlich informationstechnischer Sicherheitskompetenz und Sicherheitskultur sensibilisieren. Die CD-ROM wurde von Fachleuten der IT-Sicherheit und des Datenschutzes im Auftrag des Bundesministerium für Bildung und Forschung erstellt. Ich empfehle ihren breiten und intensiven Einsatz.

5.3.14 Handreichung „Datenschutzgerechtes eGovernment“

Die Datenschutzbeauftragten des Bundes und der Länder arbeiten unter meinem Vorsitz an der Fortschreibung und Konkretisierung ihrer Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Sie werden dabei durch das BSI sowie die Professoren Dr. Alexander Roßnagel und Dr. Klaus Lenk unterstützt. Die im Frühjahr 2003 erscheinende Handreichung wird neben der Darstellung rechtlicher Rahmenbedingungen praktische Handlungsempfehlungen für eGovernment enthalten. Umfangreich und sicherlich sehr interessant wird die Sammlung gelungener eGovernment-Anwendungen und fachkundiger Ansprechpartner sein.

Die Datenschutzbeauftragten wollen dem eGovernment in Deutschland zu einem raschen datenschutzgerechten Durchbruch verhelfen. Adressat dieser geplanten Veröffentlichung sollen die Verwaltungschefs, die Organisatoren, Verfahrensentwickler, IT-Verantwortliche, interne Datenschutzbeauftragte sowie Personalräte sein, die den Weg ins eGovernment vorzubereiten und umzusetzen haben. Im Focus sind auch Bürger, Vertreter der Wirtschaft und andere Kunden der Verwaltung, die die

neuen Angebote im eGovernment nutzen werden. Für sie finden sich Hinweise und Empfehlungen zum Selbstdatenschutz; denn ein wesentlicher Teil der Verantwortung für Sicherheit und Vertraulichkeit ihrer Daten verbleibt auch weiterhin bei ihnen selbst.

5.3.15 Weitere Neuerscheinungen

Mit meinen Broschüren und Merkblättern möchte ich Datenschutzinteressierte in die Lage versetzen, ihre Anforderungen und Aufgaben im Umgang mit personenbezogenen Daten datenschutzgerecht zu lösen. Mit meinen Checklisten kann das vorhandene Sicherheitskonzept der eingesetzten Informations- und Kommunikationstechnik geprüft und verbessert werden. Neu sind meine Broschüren:

- Datenschutz im Verein,
- Handels- und Wirtschaftsauskunfteien,
- UNIX & LINUX,
- Datenschutz im Strafvollzug,
- Orientierungshilfe Telearbeit,
- Datenschutzbriefe für sozialtherapeutische Einrichtungen.

Meine Veröffentlichungen werden in kleiner Auflage gedruckt. Sie werden nach individuellen Verteilern verteilt und können von Interessierten bei mir auch direkt angefordert werden, soweit der Vorrat reicht. Alle Veröffentlichungen werden komplett im Internet veröffentlicht; sie sind so im Download jederzeit und schnell erhältlich.

6 Schwerpunkte

6.1 Die Erweiterung der „Vorfeldbefugnisse“ der Sicherheitsbehörden und die Legitimierung der Vorratsdatenhaltung - eine Entwicklung ohne Ende

Bereits in Nr. 12.4 des XI. TB LfD Nds. 1991/1992 habe ich zu dem seinerzeitigen Gesetzentwurf zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung kritisiert, dass die Aufgabenfelder der Polizei gegenüber dem damals geltenden Gesetz erheblich ausgeweitet werden sollten. Bis zu diesem Zeitpunkt war es Aufgabe der Polizei, konkrete Gefahren abzuwehren und nach den Vorschriften der Strafprozessordnung Straftaten zu verfolgen. Neu eingeführt werden sollten das Treffen von Vorbereitungen, um künftige Gefahren abzuwehren, das Verhüten von Straftaten und die Vorsorge für die Verfolgung von Straftaten. Diesen neuen Aufgaben war gemeinsam, dass die polizeiliche Tätigkeit nun im „Vorfeld“ von Gefahren und Straftaten einsetzen konnte, während die Polizei bislang auf ein Tätigwerden ab der Grenze „konkrete Gefahr/Anfangsverdacht“ beschränkt war. Die hieraus folgende Datenverarbeitung im Vorfeld gerät in eine gefährliche Nähe zu der im Volkszählungsurteil des Bundesverfassungsgerichts als unzulässig erachteten Vorratshaltung von Daten. Der Aufgabenzuwachs bedeutete zwingend auch einen Ausbau der polizeilichen Eingriffsnormen (Befugnisse). Die Polizei erhielt nun den Zugriff auf die bisher nur den Verfassungsschutzbehörden vorbehaltenen heimlichen Ermittlungsmethoden. Zu nennen sind u.a. der verdeckte Einsatz von Videokameras bei nicht dem Versammlungsgesetz unterliegenden Veranstaltungen, die längerfristige Beobachtung, die Verwendung von optischen, akustischen und technischen Mitteln,

z.B. in Wohnungen, der Einsatz von Vertrauenspersonen und die beobachtende Fahndung. Im Ergebnis entfernten sich die neuen Vorfeldaufgaben von der bisherigen Eingriffsschwelle „konkrete Gefahr“. Genauso wurde im Bereich der Strafverfolgung die Schwelle des „Tatverdachts“ verlassen. Das neue Gefahrenabwehrgesetz wurde vom Niedersächsischen Landtag am 19. Januar 1994 beschlossen. Die Ausweitungen der Befugnisse der Polizei in der Vorfeldarbeit habe ich in Nr. 12.1 des XII. TB LfD Nds. ausführlich dargestellt.

In Nr. 11.2 des folgenden XIII. TB LfD Nds. 1995/1996 musste ich über eine erneute Änderung des Gefahrenabwehrgesetzes berichten, die zu einem weiteren Abbau von Bürgerrechten führte. So wurde beispielsweise die erste Einschränkung zur Begrenzung der weitreichenden Vorfeldbefugnisse, der begrenzende Straftatenkatalog, aufgeweicht. Seitdem dürfen besondere Mittel heimlich zur Verhütung auch solcher Straftaten eingesetzt werden, die bezogen auf das zu schützende Rechtsgut und der Strafandrohung den bereits aufgezählten Vergehen vergleichbar waren. Im Dunkeln bleibt, welche Vergehen damit gemeint sind, denn die Strafandrohungen bei den schon bisher genannten Vergehen sind sehr unterschiedlich. Als Folge dieser Öffnung des Katalogs ging die Einschätzung, ob eine Straftat von erheblicher Bedeutung vorliegt, auf den jeweiligen Dienststellenleiter über und wurde nicht mehr vom Gesetzgeber vorgegeben. Die noch während der ersten Gesetzesberatungen überwiegende Meinung, der Katalog stelle eine wesentliche Leitentscheidung dar und nur das Parlament solle den möglichen Rahmen heimlicher Ermittlungen im Vorfeldbereich bestimmen, war damit nur noch Geschichte.

In Nr. 10.1 des XIV. TB LfD Nds. 1997/1998 berichtete ich erneut über eine Änderung des Gefahrenabwehrgesetzes zu Beginn des Jahres 1998. Bis dahin war das heimliche Abhören von Wohnungen bereits vor einem Anfangsverdacht auf eine Straftat grundsätzlich möglich. Diese Zulässigkeit wurde jedoch massiv erweitert, da nunmehr das Lauschen in Wohnungen auch zur Abwehr der Gefahr, jemand könne eine Straftat von erheblicher Bedeutung begehen, ausgeweitet wurde. Im Klartext bedeutet dies, dass es ausreichend ist, wenn sich zwei Jugendliche zusammentun, um Fahrräder zu stehlen. Neu war auch die Erlaubnis, verdeckte Ermittler einzusetzen. Dies war bis dahin nur in Ermittlungsverfahren nach der Strafprozessordnung möglich. Diese verdeckten Ermittler, die unter falscher Identität in die Szene gehen, sollten die Frühentstehungsphase bei Straftaten von erheblicher Bedeutung ergründen. Ich habe dieses damals als einen nicht mehr vertretbaren Schritt in Richtung Geheimpolizei bezeichnet. Weiterhin wurden etwa zwei Drittel aller Bestimmungen, die den Grundrechtsschutz durch Verfahren sichern sollen, gestrichen. Dieses waren z.B. externe Anordnungskompetenzen (Richtervorbehalte) bei bestimmten besonderen Mitteln und die Unterrichtung Betroffener nach verdeckten Datenerhebungen. Auch die öffentliche Berichtspflicht der Landesregierung gegenüber dem Landtag zu Entwicklungen polizeilicher Vorfeldaktivitäten wurde durch eine Berichtspflicht gegenüber einem in nicht öffentlicher Sitzung tagenden parlamentarischen Ausschuss ersetzt.

Im XV. TB LfD Nds. 1999/2000 war nicht über weitere Ausdehnungen sicherheitsbehördlicher Befugnisse im Vorfeld zu berichten. Ich habe jedoch unter der Nr. 11.2 die Befugnis der Polizei zu verdachtsunabhängigen Kontrollen, der sog. Schleierfahn-

dung, vor dem Hintergrund eines Urteils des Landesverfassungsgerichts Mecklenburg-Vorpommern problematisiert. Hierbei ging es aus meiner Sicht insbesondere um die Frage, ob es geboten sei, den bisherigen Anwendungsbereich (nämlich den gesamten öffentlichen Verkehrsraum des Landes) zu beschränken. In Gesprächen mit dem Innenministerium habe ich diese Forderung nicht mehr aufrechterhalten, nachdem sichergestellt wurde, dass die jeweilige Erkenntnislage, die Anlass zu einer verdachtsunabhängigen Kontrolle gegeben hat, nachvollziehbar dokumentiert wird.

Für den Berichtszeitraum dieses Tätigkeitsberichts habe ich in den Kapiteln 10.1.3 ff. die Änderungen der niedersächsischen Sicherheitsgesetze im Einzelnen dargestellt. Sowohl durch die Ausweitung der Befugnisse der Polizei im Bereich der Videoüberwachung als auch durch die Einführung der sog. Rasterfahndung werden zwar die Befugnisse der Polizei nicht direkt noch weiter ins Vorfeld verlagert, jedoch werden immer mehr unbeteiligte und völlig gesetzestreue Bürger von polizeilichen Maßnahmen betroffen. Die Polizei darf nunmehr ohne Differenzierung der Personen an öffentlichen Orten Videoaufzeichnungen vornehmen, wenn lediglich angenommen wird, dass dort künftig Straftaten von erheblicher Bedeutung begangen werden, ohne dass man weiß, von welchen Personen. Es handelt sich somit um den typischen Fall einer Datenhaltung auf Vorrat. Gleiches gilt für die sog. Rasterfahndung. Hier werden durch die Polizei Daten von Personen erhoben, völlig unabhängig davon, ob diese eine persönliche „Nähe“ zu der abzuwehrenden Gefahr oder zu den erwarteten Straftaten haben. Inwieweit mit der Novellierung des Niedersächsischen Verfassungsschutzgesetzes Ausweitungen in den Aufgaben und Befugnissen des Landesamtes für Verfassungsschutz geplant sind, ist zzt. noch nicht abzusehen.

Anders sieht es auf der Bundesebene aus. Ich habe dieses im Kapitel 10.1.1 ausführlich dargestellt. So wurden die Befugnisse des Bundesamtes für Verfassungsschutz erheblich ausgeweitet, da es nunmehr zur Erfüllung seiner Aufgaben in der Vorfeldbeobachtung bei Finanzdienstleistungsunternehmen, Postdienstleistungsunternehmen und Luftverkehrsunternehmen personenbezogene Daten erheben darf. Die Aufgaben und Befugnisse des Bundesamtes für Verfassungsschutz bewegen sich also in den Bereich der Verfolgung konkreter Straftaten, denn die Einholung von Auskünften bei Banken, Post und Fluggesellschaften dürfte sich in der Regel nur dann als sinnvoll darstellen, wenn man hierdurch konkreten Personen (Straf-)taten nachweisen will. Auf der anderen Seite darf das Bundeskriminalamt nunmehr auch ohne das Vorliegen eines konkreten Anfangsverdachtes eigene Ermittlungen durchführen. Die Aufgaben des Bundeskriminalamtes wurden also weit in das Vorfeld einer Straftat verlagert, indem man ihm die Befugnis gegeben hat, nach „Anhaltspunkten für eine Straftat“ zu suchen. Das verfassungsrechtliche Trennungsgebot zwischen Polizei und Verfassungsschutz ist hierdurch durchlöchert worden: Der Verfassungsschutz arbeitet wie die Polizei und die Polizei wie der Verfassungsschutz. Dieses Trennungsgebot ist bisher ein tragendes Prinzip unseres freiheitlichen Rechtsstaats gewesen.

Schon im XII. TB LfD Nds. 1993/1994 habe ich hierzu ausgeführt, dass eine staatliche Sicherheitsphilosophie, nach der mehr staatliche Eingriffsmöglichkeiten und präventive Vorzeichen zu einem „Mehr“ an innerer Sicherheit führen sollen, fast zwangsläufig zu weiteren konkreten Einschränkungen für die Bürger führe. Jedes neue Sze-

narium und jede neue Qualität von Bedrohung hat selbstverständlich neue Gegenmittel zur Folge. Eine Schraube ohne Ende! Letztlich bleibt, bei allem Verständnis für die Absicht der Sicherheitsbehörden, uns allen ein sicheres Leben zu gewährleisten, die persönliche Freiheit eines jeden Einzelnen Stück für Stück auf der Strecke.

6.2 Videoüberwachung

6.2.1 Öffentlicher Bereich

Bereits im XV. TB LfD Nds. 1999/2000 habe ich die Videoüberwachung durch öffentliche Stellen im so genannten öffentlich zugänglichen Raum genauer beleuchtet. Entsprechend meinem gesetzlichen Auftrag, die Einhaltung der Vorschriften über den Datenschutz bei den Behörden und sonstigen öffentlichen Stellen des Landes zu kontrollieren und unter dem Eindruck der Diskussion im Innenausschuss des Nds. Landtages am 22. August 2001 zu dem Antrag der CDU-Fraktion „Bessere Videoüberwachung von gefährlichen Plätzen in Niedersachsen“ (vgl. LT-Drs. 14/2553) habe ich Ende 2001 alle Behörden und sonstigen öffentlichen Stellen der Landes- und Kommunalverwaltung in Niedersachsen gebeten, mir unter Verwendung eines Vordrucks die derzeit von ihnen im öffentlich zugänglichen Raum praktizierten Maßnahmen der Videoüberwachung zu benennen.

Die rechtlichen Rahmenbedingungen für Videoüberwachungsmaßnahmen öffentlicher Stellen im öffentlich zugänglichen Raum stellen sich in Niedersachsen derzeit wie folgt dar:

Bei der grundlegenden Novellierung des NDSG zur Anpassung an die Vorgaben des Bundesverfassungsgerichts im so genannten Volkszählungsurteil hatte der Gesetzgeber 1993 Fragen des Videoeinsatzes nicht erörtert. Bei der Anpassung des Landesdatenschutzrechts an die EG-Datenschutz-Richtlinie (am 13. Juni 2001 hat der Niedersächsische Landtag die Novelle zum Niedersächsischen Datenschutzgesetz verabschiedet) ist meine Anregung, auch für diesen Bereich geeignete, das Recht auf informationelle Selbstbestimmung beachtende Regelungen zu schaffen, leider nicht aufgegriffen worden. Die Landesregierung hat stattdessen darauf verwiesen, dass die derzeitigen Regelungen des NGefAG zur Videoüberwachung ausreichten. In der parlamentarischen Diskussion habe ich auf die Unzulänglichkeit der niedersächsischen Regelungen nachdrücklich hingewiesen. Als Grundlage für einen Einsatz von Videotechnik durch Behörden der Landes- und Kommunalverwaltung zur Überwachung öffentlich zugänglicher Räume kommt derzeit neben der speziellen Regelung im Niedersächsischen Spielbankgesetz allein § 32 Abs. 3 NGefAG (mit Ausnahme strafprozessualer Ermächtigungen und der sonstigen Regelungen in § 32 NGefAG) in Betracht. Die Vorschrift erlaubt nur eine Videobeobachtung zu Zwecken der Gefahrenabwehr. Im Gegensatz zur Polizei dürfen allerdings Gefahrenabwehrbehörden beobachtete Vorgänge nicht aufzeichnen, zulässig ist lediglich eine simultane Beobachtung am Bildschirm. Eine Datenerhebung durch Videobeobachtung stellt schon wegen der hohen Informationsdichte, die Bildinformationen aufweisen, und wegen der daraus zwangsläufig folgenden Erhebung nicht erforderlicher Daten (z.B. über Körperhaltung, Bekleidung) einen besonders tiefen Eingriff in die Persönlichkeitsrechte dar. Ein solcher Eingriff bedarf einer (bereichsspezifischen) Regelung, welche die Voraussetzungen dieser besonderen Form der Datenverarbeitung im

Voraussetzungen dieser besonderen Form der Datenverarbeitung im Einzelnen festlegt. Deshalb kann aus meiner Sicht die Videobeobachtung nicht auf die allgemeine Datenerhebungsvorschrift des § 9 NDSG gestützt werden.

Im Übrigen ist diese Bestimmung auf diese besondere Form der Datenverarbeitung auch nicht zugeschnitten. So lassen sich z.B. dem Gesetz keine Aussagen darüber entnehmen, dass eine Videobeobachtung wegen überwiegender schutzwürdiger Belange der Betroffenen (z.B. Beobachtung von Umkleideräumen und Toilettenanlagen) unterbleiben muss. Ein Hinweis auf die Videobeobachtung und die dafür verantwortliche Stelle ist nicht vorgesehen. Auch die Pflicht zur Aufklärung über den Zweck der Erhebung und die zugrunde liegende Rechtsgrundlage (§ 9 Abs. 2 NDSG) wird den tatsächlichen Verhältnissen bei einer Videobeobachtung nicht gerecht.

Schließlich ergäbe sich bei Zulassung einer Videoüberwachung nach den allgemeinen Datenverarbeitungsbestimmungen des NDSG ein eklatanter Wertungswiderspruch zum Gefahrenabwehrrecht. Nach § 32 Abs. 3 NGefAG dürfen öffentlich zugängliche Orte zwar von Gefahrenabwehrbehörden mit einer Videokamera offen beobachtet werden, eine Aufzeichnung darf nach dieser Vorschrift aber nicht erfolgen (lediglich die Polizei darf aufzeichnen, wenn Tatsachen die Annahme rechtfertigen, dass an diesem Ort Straftaten von erheblicher Bedeutung begangen werden). Würde man eine Videoüberwachung nach § 9 NDSG für möglich halten, wäre eine Aufzeichnung dagegen nach § 10 NDSG zulässig. Dies würde bedeuten, dass der Gesetzgeber einen konkreten Rechtseingriff in einem Spezialgesetz ablehnt, den selben Eingriff aber in einem Querschnittsgesetz zulässt, das die allgemeine Tätigkeit öffentlicher Stellen regelt, die nicht durch besondere verwaltungsspezifische Aspekte bestimmt wird. Dies zeigt die innere Unstimmigkeit dieser Argumentation. Hierauf hatte bei den Beratungen zur Novellierung des NDSG auch der Gesetzgebungs- und Beratungsdienst hingewiesen.

In der rechtlichen Bewertung dieser Frage besteht leider nach wie vor kein Konsens mit dem Innenministerium. Dieses hat in den Verwaltungsvorschriften zu § 9 NDSG eine Videoüberwachung im Rahmen des Hausrechts für zulässig erklärt, setzt sich mit den dann ergebenden und von mir wiederholt vorgetragenen gesetzlichen Wertungswidersprüchen zum NGefAG und meinen übrigen Einwänden aber nicht auseinander.

Entsprechend der Definition im neugeschaffenen § 6b BDSG verstehe ich unter Videoüberwachung „die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen“. Unter öffentlich zugänglichen Räumen sind die Bereiche zu verstehen, die von einer unbestimmten bzw. unbestimmbaren Anzahl betriebsfremder Personen betreten werden dürfen. Hierbei ist es unerheblich, wenn z.B. ein Entgelt für den Zutritt erhoben wird. Dazu gehören insbesondere dem Gemeingebrauch gewidmete Straßen, Wege und Plätze, aber auch tatsächlich für jedermann zugängliche Bereiche wie z.B. Eingangs- und Flurbereiche von Behördengebäuden, Schulen, Abfallsammelstellen und Schwimmbäder. Auch die Fälle einer nur teilweisen Einbeziehung öffentlich zugänglicher Räume (z.B. wird bei der Überwachung eines nicht für die Öffentlichkeit zugänglichen Behördengebäudes der vor dem Eingang

liegende Fußweg- oder Straßenbereich von der Kameraeinstellung mit erfasst) unterfallen der o. a. Definition. Nicht erfasst werden von der Definition optisch-elektronische Einrichtungen, bei denen durch unveränderbare Einstellung oder Ausstattung Bildaufnahmen entstehen, bei denen ein Personenbezug oder eine Personenbeziehbarkeit definitiv nicht, auch nicht durch ggf. nachfolgende Bildbearbeitung, hergestellt werden kann. Ich habe ausdrücklich darauf hingewiesen, dass Videokameras, bei denen nach ihrer technischen Ausstattung die Möglichkeit der Veränderung der Bildeinstellung (Zoomfunktion) oder des Aufnahmefeldes sowie der Bildaufzeichnung besteht, von der Definition erfasst werden.

Meine Erhebung bei den Behörden und sonstigen Stellen der Landes- und Kommunalverwaltung über den Einsatz solcher Einrichtungen ist mittlerweile abgeschlossen. Insgesamt wurden 159 Videoüberwachungsmaßnahmen durch Behörden der Landesverwaltung in Niedersachsen (enthalten sind 83 Meldungen für die Polizei) unter den genannten Voraussetzungen gemeldet. Durch die Kommunalverwaltung wurden 142 Videoüberwachungsmaßnahmen angezeigt. Es lässt sich abschätzen, dass ca. 425 einzelne Kameras durch Landesbehörden und ca. 325 Kameras durch die kommunalen Gebietskörperschaften eingesetzt werden. Eine erste Auswertung hat ergeben, dass die eingesetzten Anlagen der Polizei auf der Grundlage des § 32 Abs. 3 NGefAG rechtmäßig genutzt werden. Die Polizeidirektion Hannover hat zusätzlich die Möglichkeit, sich auf ca. 152 Kameras der Üstra und ca. 24 Kameras der „Move"-GmbH aufschalten zu lassen. Dieses kommt jedoch nur bei konkreten Anlässen zur Strafverfolgung oder Gefahrenabwehr in Betracht. Insgesamt werden nur in wenigen Einzelfällen der polizeilichen Videoüberwachung Nachfragen durch mich nötig sein. Aus diesem Grund habe ich die Anlagen der Polizei nicht in die weitere Darstellung einbezogen.

Die übrigen gemeldeten Überwachungsmaßnahmen lassen sich insgesamt grob nach folgenden Unterscheidungsmerkmalen klassifizieren:

- Überwachung „rein" technischer Vorgänge wie z.B. die gefahrenträchtige Schleusung eines Schiffes oder die Öffnung einer Hebebrücke,
- „Automatische Klingelanlagen" (der Besucher nutzt eine Klingel zum Einlass und im betroffenen Gebäude öffnet sich das Bild der Person auf einem Monitor),
- Überwachung im Rahmen des so genannten Hausrechts zur Gebäude- bzw. Liegenschaftssicherung innerhalb des öffentlich zugänglichen Gebäudes bzw. mit Bezug in den öffentlich zugänglichen Bereich außerhalb des Gebäudes (z.B. Gehwege und Straßenteile),
- Überwachung an oder in Gebäuden zum Schutz dritter Personen oder der von ihnen eingebrachten Sachen (z.B. der öffentlich zugängliche Wartebereich für Patienten in der Notaufnahme eines Krankenhauses; Überwachung des Fahrradständers einer Schule).

Die Überwachung der technischen Vorgänge ist aus meiner Sicht datenschutzrechtlich unproblematisch, weil regelmäßig keine personenbezogenen Daten erhoben werden. Es soll lediglich sichergestellt werden, dass gefahrenträchtige Situationen im Ansatz vermieden werden, ohne einen Personenbezug herzustellen. Die mir gemel-

deten Videoüberwachungsmaßnahmen technischer Vorgänge ergeben einen Anteil von weniger als 10 Prozent.

Auch die „automatischen Klingelanlagen“ unterziehe ich keiner weiteren Überprüfung, weil der Einlassbegehrende regelmäßig Kenntnis von der Übertragung seiner Bilddaten erhält und somit von seiner Einwilligung ausgegangen werden kann, wenn er die Klingelanlage nutzt. Es ist ausgeschlossen, die Anlage für ständige Überwachungen größerer (öffentlicher) Bereiche einzusetzen. Der Anteil dieser Maßnahmen ist ebenfalls unterhalb von 10 Prozent angesiedelt.

Der größte Teil der Überwachungsmaßnahmen wurde mir unter dem Oberbegriff „Hausrecht“ gemeldet; er nimmt einen Anteil von mehr als 80 Prozent der Meldungen ein. Hier besteht das oben bereits angesprochene Problem, dass eine Rechtsgrundlage für einen Grundrechtseingriff durch eine Videoüberwachung nicht vorhanden ist. Das Hausrecht muss nach seiner Entstehungsgeschichte und nach seinem im Wege der Auslegung herausgebildeten Rechtsgehalt als ein notwehrähnliches Recht gesehen werden. Im Einzelfall dürfen konkrete Verstöße gegen und Eingriffe in das befriedete Besitztum abgewehrt werden; das Hausrecht gibt jedoch generell nicht die Berechtigung zur Vornahme präventiver (d.h. vorbeugender) Maßnahmen. Die Videoüberwachung ist dagegen zunächst eine reine Präventionsmaßnahme. Eine Notwehrsituation erfordert immer das Vorliegen einer gegenwärtigen Gefahr für das entsprechende Rechtsgut. Allein die Möglichkeit, dass sich eine entsprechende Gefahr entwickeln könnte, genügt dem Erfordernis der Gegenwärtigkeit nicht. Ein Eingriff in das Recht auf informationelle Selbstbestimmung in Form einer Videoüberwachung kann deshalb nach meiner Auffassung nicht auf das Hausrecht gestützt werden. Die Tatsache, dass sowohl der Bundes- als auch einige Landesgesetzgeber außerhalb Niedersachsens den Begriff des Hausrechts in den jeweiligen Datenschutzgesetzen genutzt und in Verbindung mit dem Hausrecht eine Ermächtigungsgrundlage für eine Videoüberwachung (abhängig vom Vorliegen weiterer Voraussetzungen) geschaffen haben, lässt insofern nur den Schluss zu, dass im Kontext des Datenschutzrechts offensichtlich ein von der obigen Auffassung abweichendes Verständnis des Terminus „Hausrecht“ gegeben ist. Zielsetzung der Gesetzgeber war es offenbar, die bereits bestehenden Videoüberwachungen zu legalisieren und diese in einen gesetzlichen Rahmen zu bringen. Sie wollten jedoch keine „Generalermächtigung“ schaffen, sondern formulierten weitere einschränkende Voraussetzungen, wie z.B. die Erforderlichkeit der Maßnahme. Auch im Gesetzgebungsverfahren des Bundes wurde der Begriff soweit ersichtlich nicht näher hinterfragt oder erläutert (vgl. BT-Drs. 14/4329, 14/4458, 14/4571, 14/5793; BR-Drs. 461/00).

Meine Auffassung zum Inhalt des überkommenen Begriffs des Hausrechts und zu der insoweit problematischen Verknüpfung dieses Begriffs mit einer Befugnisnorm zur präventiven Überwachung durch optisch-elektronische Einrichtungen in den Datenschutzgesetzen habe ich dem Bundesbeauftragten für den Datenschutz und den von einer entsprechenden Ländergesetzgebung betroffenen Landesbeauftragten für den Datenschutz übermittelt, um auf diesem Wege eine breite Diskussion und Klärung des Problems zu ermöglichen. Neben der Frage der grundsätzlichen Geeignetheit des Hausrechts als Ermächtigungsgrundlage für den Einsatz von Videotechnik ist

insbesondere auch der Umfang dieses „Rechts“ klärungsbedürftig. Umfasst das Hausrecht neben dem Schutz des Eigentums und der Sicherheit der dort Beschäftigten auch den Schutz von Eigentum und Sicherheit von z.B. Besuchern, Schülern usw.? Diese aus datenschutzrechtlicher Sicht grundsätzlichen Fragestellungen zur Videoüberwachung unter dem Oberbegriff „Hausrecht“ habe ich auch den betroffenen öffentlichen Stellen in Niedersachsen mitgeteilt. Bis zu einer endgültigen Klärung werde ich den bislang praktizierten Videoeinsatz unter diesem Gesichtspunkt zunächst unbeanstandet lassen.

In fünf Fällen habe ich kommunale Stellen um eine ergänzende Stellungnahme gebeten, weil die durchgeführten Überwachungsmaßnahmen in den intimen Bereich der Bürger hineinreichen könnten (Maßnahmen zur Überwachung in einer Sauna bzw. Überwachung eines Toilettenvorraumes). In solchen sensiblen Bereichen sehe ich neben dem Aspekt des Hausrechts auch die Verhältnismäßigkeit einer Videoüberwachung als Problem. Die Antworten stehen derzeit noch aus.

6.2.2 Nicht öffentlicher Bereich

In der Vergangenheit habe ich mich wiederholt mit Anfragen und Beschwerden zum Thema Videoüberwachung durch nicht öffentliche Stellen befasst. In meinem letzten Tätigkeitsbericht habe ich darauf hingewiesen, dass die Videoüberwachung weder grundsätzlich verdammt noch als ein Allheilmittel gepriesen werden kann. Es ist daran festzuhalten, dass eine sachgerechte datenschutzrechtliche Bewertung immer auf den konkreten Zweck der Maßnahme abzustellen hat und die anlassgebenden Umstände zu berücksichtigen sind. Die anhaltende Diskussion über diese spezielle Überwachungstechnik hat den Gesetzgeber veranlasst, mit § 6b eine Regelung für diesen Bereich in das BDSG einzufügen. Es bleibt abzuwarten, ob das gesetzgeberische Ziel, den immer weiter zunehmenden Einsatz dieser Überwachungstechnik einzudämmen, erreicht werden kann.

Die neue Regelung

Die neue Regelung ist im nicht öffentlichen Bereich anwendbar, wenn Private öffentlich zugänglich Räume mit optisch-elektronischen Einrichtungen beobachten und die Beobachtung nicht ausschließlich persönlichen oder familiären Zwecken dient. Auf die eingesetzte Kameratechnik kommt es nicht mehr an. Es ist somit unerheblich, ob für die Beobachtung digitale oder analoge Kameratechnik eingesetzt wird, denn die Regelung setzt nicht voraus, dass die gewonnenen (Bild-)Daten unter Einsatz von oder für Datenverarbeitungsanlagen erhoben werden. Die datenschutzrechtliche Relevanz der Beobachtungsmaßnahme ist unabhängig von der Frage, ob das Bildmaterial nur betrachtet oder auch gespeichert wird.

Öffentlich zugängliche Räume

In Anfragen wird oft die Frage aufgeworfen, was denn „öffentlich zugängliche Räume“ seien. Ein öffentlich zugänglicher Raum ist jeder Bereich, der ohne besondere Voraussetzungen betreten werden kann. In der Gesetzesbegründung werden beispielhaft Bahnsteige, Ausstellungsräume eines Museums, Verkaufsräume oder Schalterhallen aufgeführt. Hierunter sind alle Räume zu fassen, die nach dem Willen des oder der Berechtigten für jedermann zugänglich sind beziehungsweise von jedermann

- gegebenenfalls nach dem Kauf einer Eintrittskarte - betreten werden können. Der zu beobachtende Bereich kann innerhalb oder außerhalb von Gebäuden liegen. In diesem Zusammenhang kommt es auch nicht auf die Eigentumsverhältnisse an, es kann sich also um öffentliche oder private Grundstücke handeln.

Die Erforderlichkeit der Videoüberwachung

Bei der Konzeption von Überwachungsmaßnahmen ist als gesetzliche Voraussetzung für den rechtmäßigen Einsatz von Videotechnik die Erforderlichkeit zu prüfen. Sie ist dann gegeben, wenn der verfolgte beabsichtigte Zweck nicht mit einem anderen zumutbaren Mittel, das weniger in die Rechte der Betroffenen eingreift, erreicht werden kann. In diesem Zusammenhang ist auch zu prüfen, ob eine flächendeckende Einführung der Überwachungstechnik erforderlich ist oder ob ein Einsatz an Schwerpunkten oder zu bestimmten Zeiten ausreicht. Unter den Gesichtspunkt der Datenvermeidung und Datensparsamkeit ist weiterhin zu prüfen, ob durch den Einsatz von inzwischen verfügbarer Technik bestimmte Bereiche des Aufnahmefeldes komplett ausgeblendet oder die Gesichter der sich in diesen Bereichen aufhaltenden Personen „verschleiert“ werden können.

Die zulässigen Zwecke

Die Videoüberwachung durch nicht öffentliche Stellen ist nach § 6b Abs. 1 Nr. 2 und 3 BDSG nur zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen des Betroffenen bestehen.

Nach § 6b Abs. 1 Nr. 2 BDSG ist eine Videoüberwachung zur Wahrnehmung des Hausrechts zulässig, durch diese Bestimmung wird der Umfang der aus dem Hausrecht abzuleitenden Überwachungsbefugnisse aber nicht konkret festgelegt. Zivilrechtlich gesehen ist das Hausrecht die Befugnis, über die Benutzung eines geschützten Raums zu verfügen und gegebenenfalls ein Hausverbot aussprechen zu können. Ob daraus allein allerdings eine Berechtigung zu einer umfassenden präventiven Überwachung abgeleitet werden kann, erscheint mir zweifelhaft; auf die vorstehenden Ausführungen zur Videoüberwachung durch öffentliche Stellen weise ich insoweit hin. Von Seiten der Praxis werden vom Hausrecht die Maßnahmen als gedeckt angesehen, die die ordnungsgemäße Nutzung der überwachten Räume sicherstellen sollen, um bei einer nicht bestimmungsgemäßen Nutzung einschreiten zu können. Auch die Überwachung ausgesprochener Hausverbote wird davon erfasst.

Maßnahmen, die zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke bestimmt sind, fallen unter § 6b Abs. 1 Nr. 3 BDSG. Diese Regelung wurde erst im Gesetzgebungsverfahren in das Gesetz aufgenommen und führte gegenüber dem Regierungsentwurf zu einer Einschränkung der Videoüberwachung, da sie eine engere Zweckbindung beinhaltet. Berechtigt ist jedes Interesse, das nach vernünftiger Erwägung durch die Sachlage gerechtfertigt ist, also ein tatsächliches Interesse, das wirtschaftlicher oder ideeller Natur sein kann. Nach diesen Kriterien kann sich beispielsweise aus dem Schutz des Eigentums ein berechtigtes Interesse ergeben. Das Motiv einer allgemeinen abstrakten Gefahrenvorsorge für den Schutz des Eigentums

reicht dabei aber nicht. Vielmehr müssen belegbare Tatsache die Annahme rechtfertigen, dass schwerwiegende Beeinträchtigungen des Eigentums drohen und es diese abzuwehren gilt.

Die Dokumentation der Zwecke

Die Zwecke der Videoüberwachung sind schriftlich vor der Inbetriebnahme der Überwachungsanlage zu dokumentieren. Hierbei ist zu bedenken, dass in einem Objekt gegebenenfalls mehrere unterschiedliche Zwecke bestehen können. So kann beispielsweise die Überwachung der Frauenparkplätze im kaufhauseigenen Parkhaus nicht mit dem Schutz vor Diebstählen, der aber für die Verkaufsräume zutreffend ist, begründet werden. Die Festlegung der Zwecke ist sehr sorgfältig vorzunehmen, da mittels der Videoüberwachung gewonnene Erkenntnisse für andere als die festgelegte Zwecke nicht verwendet werden dürfen.

Weiterverarbeitung von Bildaufnahmen

In den Fällen, in denen die Videoaufnahmen auch aufgezeichnet werden sollen, ist gemäß § 6b Abs. 3 Satz 1 BDSG sowohl die Erforderlichkeit erneut zu prüfen als auch eine erneute Abwägung der schutzwürdigen Interessen der Betroffenen vorzunehmen. Auch ist die beabsichtigte Weiterverarbeitung zu dokumentieren. Die Übermittlung der gewonnenen Aufnahmen an Strafverfolgungsbehörden beziehungsweise deren Nutzung als Beweismittel zur Erlangung von Schadensersatz kann zum Erreichen eines dokumentierten Zwecks erforderlich sein. Bei Personen, die einer Straftat verdächtigt werden, dürften in der Regel keine Anhaltspunkte überwiegender schutzwürdiger Interessen am Ausschluss der Nutzung der Aufnahmen als Beweismittel bestehen. Für einen anderen als den dokumentierten Zweck dürfen die aufgezeichneten Videoaufnahmen gemäß § 6b Abs. 3 Satz 2 BDSG nur benutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

Die Unterrichtungspflicht

Zur Transparenz der Verarbeitung und Nutzung von durch Videoüberwachungsmaßnahmen gewonnenen personenbezogenen Daten soll § 6b Abs. 4 BDSG beitragen. Durch organisatorische Maßnahmen hat die verantwortliche Stelle sicherzustellen, dass identifizierte Personen gemäß § 33 BDSG benachrichtigt werden. Darunter fällt immer die verdächtigte Person, aber auch das Opfer eines Zwischenfalls oder sonstige namentlich bekannte Personen.

Die schutzwürdigen Interessen der Betroffenen

Vor dem Beginn der Überwachungsmaßnahme ist auch zu prüfen, ob Anhaltspunkte für überwiegende schutzwürdige Interessen der Betroffenen bestehen. In Bereichen, in denen die freie Entfaltung der Persönlichkeit oder die Wahrnehmung von Freiheitsrechten eher untypisch ist, werden die schutzwürdigen Interessen der Betroffenen in der Regel nicht betroffen. Als derartige Bereiche sind zum Beispiel Kaufhäuser, Bankgebäude oder Tankstellen anzusehen. Werden aber Stätten der Begegnung, zum Beispiel Freizeiteinrichtungen, Restaurants, Fußgängerzonen und zum Verweilen einladende Freiflächen beobachtet, ist genauer zu prüfen, ob schutzwürdige Interessen dem Einsatz von Überwachungstechnik entgegenstehen. Wenn Personen so videoüberwacht werden, wie ein aufmerksamer Beobachter dies mit bloßem Auge

auch tun könnte, und ist nicht zu erwarten, dass die Beobachtung zu einem übersteigert angepassten Verhalten der Beobachteten führt, so wird man im Regelfall keine Verletzung eines schutzwürdigen Interesses feststellen können. Geht die Videoüberwachung jedoch über die „normale“ Beobachtung hinaus, wird beispielsweise durch eine beabsichtigte Beobachtung auch Einblick in Situationen oder Handlungsabläufe ermöglicht, die der Privat- und Intimsphäre der Betroffenen zuzurechnen sind, so werden deren schutzwürdige Interessen verletzt und die Maßnahme ist unzulässig.

Da bei einem Einsatz von Videotechnik im gewerblichen Bereich gegebenenfalls auch die Beschäftigten von der Videoüberwachung betroffen werden, sind auch deren schutzwürdige Interessen zu berücksichtigen.

Die Hinweispflicht

Meine Beratungs- und Kontrolltätigkeit zeigt, dass die in § 6b Abs. 2 BDSG vorgeschriebene Hinweispflicht noch nicht überall beachtet wird bzw. bekannt ist. Durch Hinweisschilder ist sowohl auf die Tatsache der Videobeobachtung als auch auf die dafür verantwortliche Stelle deutlich hinzuweisen. Die im „Düsseldorfer Kreis“ kooperierenden Aufsichtsbehörden entwickeln zurzeit ein Piktogramm für die Videoüberwachung, um eine Vereinheitlichung der optischen Gestaltung der Hinweisschilder zu erreichen.

Ein Hinweis auf die verantwortliche Stelle ist bei jeder Darstellungsform zu geben. Es liegt zwar nahe, dass die Überwachung eines Kaufhauses durch das Kaufhaus selbst, im Auftrag durch ein Sicherheitsunternehmen durchgeführt wird, der Gesetzgeber verlangt aber ausdrücklich die Benennung der verantwortlichen Stelle, damit der Betroffene bei dieser seine Rechte geltend machen kann. Der Kunde kennt meist die konkrete Rechtsform des Unternehmens und die für sie handelnden Personen nicht. Beispielsweise ist in einem Filialunternehmen die verantwortliche Stelle aus Sicht des Kunden nicht selbsterklärend. Er weiß nicht, bei wem er seine Rechte geltend machen kann, in der Filiale vor Ort oder in der Konzernzentrale. Er weiß auch nicht, ob die Überwachung durch das Kaufhaus selbst oder im Wege der Funktionsübertragung von einem Dritten durchgeführt wird. Diese Unsicherheit besteht auch in so genannten Einkaufsmärkten mit verschiedenen Einzelhandelsgeschäften - Shop in Shop - in einem Gebäude.

Der Hinweis ist deutlich sichtbar anzubringen. Was deutlich sichtbar ist, hängt von der Größe und Gestaltung des Hinweises, aber auch vom Umfeld und dem Hintergrund ab. So habe ich ein Verkehrunternehmen darauf hingewiesen, dass ein mit weißen Buchstaben bedrucktes Hinweisschild, welches sich nicht von dem silberfarbenen Fahrzeug erkennbar absetzt, seine Funktion nicht erfüllt. Die optische Gestaltung und räumliche Anordnung des Hinweises ist so vorzunehmen, dass der Kunde den Hinweis vor dem Eintritt in den überwachten Bereich im normalen Blickwinkel hat. Die Hinweisfunktion ist nur erfüllt, wenn sie für den Kunden ohne weiteres wahrnehmbar ist und von ihm nicht erst gesucht werden muss. Durch den deutlich wahrnehmbaren Hinweis auf die Videoüberwachung wird der „demnächst“ von ihr Betroffene gewarnt und kann sich dann entscheiden, ob er diesen überwachten Bereich überhaupt betreten möchte.

Die Löschung

Das durch die Videobeobachtung gewonnene Bildmaterial darf gemäß § 6b Abs. 5 BDSG nur so lange gespeichert werden, wie es zur Erreichung des verfolgten Zweckes erforderlich ist. Aber auch Aufnahmen, die für den Beobachtungszweck noch benötigt werden, etwa weil aufklärungsbedürftige Vorkommnisse aufgezeichnet wurden, dürfen nur gespeichert bleiben, wenn schutzwürdige Interessen des Betroffenen nicht entgegenstehen und solange sie zur Erreichung des Beobachtungszwecks erforderlich sind. Die verantwortliche Stelle hat daher die angefallenen Aufnahmen unverzüglich einer Bedarfsprüfung zu unterziehen. In den Fällen, in denen die Aufnahmen nicht mehr für die Erreichung des dokumentierten Aufnahmezwecks benötigt werden, sind diese unverzüglich, d.h. in der Regel innerhalb von ein bis zwei Arbeitstagen, zu löschen. Bei der Konzeption von Überwachungsmaßnahmen sind die hierzu erforderlichen organisatorischen Maßnahmen zu regeln. Am wirksamsten wird dem Löschungsgebot durch eine automatisierte periodische Löschung, etwa durch Selbstüberschreiben zurückliegender Aufnahmen entsprochen.

Der Handlungsbedarf

Meine bisherigen Erfahrungen mit der in vielen Bereichen des täglichen Lebens eingesetzten Videoüberwachung veranlassen mich, diesem Bereich auch zukünftig erhöhte Beachtung zu schenken. Die für die Videobeobachtung verantwortlichen Stellen werde ich zur datenschutzgerechten Ausgestaltung der Überwachungsmaßnahmen anhalten, wenn andere geeignete Maßnahmen nicht ausreichen, die mit dem Einsatz der Videotechnik angestrebten Zwecke zu erreichen. Insbesondere werde ich auf die Durchführung der erforderlichen Vorabkontrolle und die notwendigen organisatorischen Maßnahmen achten.

6.3 Datenschutz im Gesundheitswesen

Die Reform der gesetzlichen Krankenversicherung ist längst ein datenschutzrechtliches Dauerthema, man denke nur an die Debatten um die Einführung der Versichertenkarte und der ICD-10-Verschlüsselungen in den Arztpraxen vor knapp zehn Jahren. Im Rahmen der jüngsten Bemühungen, Einsparpotentiale im Gesundheitssystem aufzudecken und zu nutzen, rücken zunehmend Vorhaben in den Mittelpunkt, die darauf angelegt sind, Kosten- und Mittelverteilungen transparent zu machen. Zu diesem Zweck richtet sich das Hauptaugenmerk auf zentrale Datensammlungen über die Patienten als Leistungsempfänger und über die Leistungserbringer - die Schlüsselworte heißen Disease-Management-Programme und Datentransparenzgesetz.

Darüber hinaus werden große Hoffnungen darauf gesetzt, durch telematische Anwendungen Synergieeffekte zu erzielen, die dazu beitragen die Kosten im Gesundheitswesen zu senken. Hier ging es im Berichtszeitraum insbesondere um die Weiterentwicklung der Krankenversichertenkarte zur „intelligenten“ Chipkarte.

Alle Projekte haben unmittelbare Auswirkungen auf Umfang, Zweck sowie Art und Weise der Verarbeitung zum Teil höchst sensibler Gesundheitsdaten. Betroffen hiervon sind ca. 90% der Bevölkerung als gesetzlich Krankenversicherte.

Eine kritische datenschutzrechtliche Begleitung aller Vorhaben ist daher unerlässlich.

6.3.1 Chancen und Risiken zentraler Datenbestände

Derzeit werden jährlich 140 Mrd. Euro für Gesundheitsleistungen durch die Krankenkassen ausgegeben. Die Abrechnung der Leistungen erfolgt durch eine Vielzahl von Leistungserbringern auf örtlicher und damit dezentraler Ebene. Abrechnungs- und Leistungsdaten sind bei ca. 350 verschiedenen Krankenkassen und über 40 Kassen(zahn)ärztlichen Vereinigungen gespeichert, ohne dass es zu einer kassenartübergreifenden, das gesamte Leistungsgeschehen wiedergebenden Zusammenführung kommt.

Warum nun eine Zusammenführung von Leistungsdaten?

Nicht nur in den letzten Jahren haben die stark gestiegenen Gesundheitskosten den Krankenkassen und der Politik Kopfzerbrechen bereitet. Durch verschiedene gesetzliche Maßnahmen (Eigenbeteiligungen bei Arznei-, Verband- und Heilmitteln, Krankenhausaufenthalten und Kuren, Budgets bei Arzneien und ärztlicher Behandlung) wurden kurzfristig wirkende Kostendämpfungsbemühungen umgesetzt. Langfristig jedoch konnte das Ziel der Beitragsstabilität in der gesetzlichen Krankenversicherung nicht erreicht werden.

Ziel der Zusammenführung aller im System vorhandenen Gesundheitsdaten ist es daher, diese in einer geeigneten Form zu erfassen, aufzubereiten, zusammenzuführen und auszuwerten. Dieser aggregierte Datenbestand soll Grundlage von Planungen zum Zwecke der Steuerung und Sicherstellung von Qualität und Wirtschaftlichkeit in der medizinischen Versorgung und Forschung sein. Nicht zuletzt dient der Datenpool der Politik und den Verbänden zur Gesundheitsberichterstattung.

Das von der Bundesregierung vorgelegte Konzept eines Datentransparenzgesetzes kann unter datenschutzrechtlichen Gesichtspunkten nur dann erfolgreich sein, wenn die vorhandenen sensiblen Abrechnungs- und Leistungsdaten der Versicherten und Leistungserbringer weiterhin dem Schutz des informationellen Selbstbestimmungsrechts unterliegen. Die Schaffung von Datentransparenz für das GKV-System muss daher den durch das Sozialgesetzbuch vorgesehenen Schutz der Sozialdaten der Versicherten und Leistungserbringer wahren.

Um eine nicht kontrollierbare Verwendung der versichertenbezogenen Daten der Krankenkassen und Leistungserbringer zu verhindern, muss der Versicherten- und Leistungserbringerbezug pseudonymisiert werden.

Hierzu bedarf es der bundesweiten Errichtung von Vertrauens- und Datenaufbereitungsstellen. Diese müssen räumlich, organisatorisch und personell von den Krankenkassen und deren Verbänden, den Kassen(zahn)ärztlichen Vereinigungen, deren Bundesvereinigungen und anderen abrufberechtigten Stellen getrennt sein.

Diese bisher noch nicht vorhandenen Vertrauens- und Datenaufbereitungsstellen sollen als Körperschaften des öffentlichen Rechts mit Selbstverwaltungsbefugnis fungieren. Der Verwaltungsrat dieser Stellen soll sich aus Vertretern der Spitzenverbände der Krankenkassen, der Kassen(zahn)ärztlichen Vereinigungen, den Spitzen-

organisationen der Leistungserbringer, den Vertretern von Bund und Ländern, der Wissenschaft und Patientenvertretern zusammensetzen.

Die Datenaufbereitungsstellen auf Landesebene führen die Daten kassenartübergreifend zusammen. Damit wird erstmalig eine Datengrundlage geschaffen, die unter Beteiligung aller am Leistungsgeschehen in der gesetzlichen Krankenversicherung Teilnehmenden zu mehr Qualität und Effizienz in der gesundheitlichen Versorgung führen soll.

Wer ist Nutzer des Datenpools?

Für die abrufberechtigten Krankenkassen und Leistungserbringer bilden die Daten eine verbesserte Grundlage für die vom Gesetzgeber vorgeschriebenen Aufgaben wie Wirtschaftlichkeits-, Abrechnungs-, Plausiblilitätsprüfung und Qualitätssicherung. Darüber hinaus dienen sie der Information und Beratung der Versicherten und Vertrags(zahn)ärzte sowie dem Abschluss von Verträgen auf Landesebene. Für die Notwendigkeit der politischen Steuerung des Gesundheitswesens stehen erstmalig aggregierte Daten zur Verfügung. Die Politik wird in die Lage versetzt, Entwicklungen besser nachvollziehen, analysieren und ggf. Elemente zur Steuerung erarbeiten zu können. Das Ziel der langfristigen Beitragsstabilität und damit die Vermeidung einer weiteren Erhöhung der Personalnebenkosten in den Betrieben und öffentlichen Verwaltungen kann durch Erkenntnisse und Folgerungen aus der Datenzusammenführung eher erreicht werden.

Der Wissenschaft und Gesundheitsberichterstattung wird durch das Datentransparenzgesetz der Zugriff für systematische epidemiologische Fragestellungen umfassend und flächendeckend ermöglicht. Die Ergebnisse dienen der Beseitigung bestehender Defizite und Fehlversorgung, unterstützen den effizienten Ressourceneinsatz und dienen einer zielgerichteten Gesundheitsversorgung, -förderung und -vorsorge.

Bevor ein derart umfangreicher zentraler Datenpool entsteht, sollte der Gesetzgeber prüfen, ob das Ziel der Kostentransparenz auch mit einer Stichprobenerhebung erreichbar ist. Sofern Stichprobenerhebungen für den vorgesehenen Zweck repräsentativ und hinreichend aussagefähig sind, wird aus Sicht des Datenschutzes diese Möglichkeit zur Schaffung notwendiger Transparenz favorisiert. Das Vorhalten von Daten ohne zusätzlichen Nutzen ist unzulässig. Das Bundesministerium für Gesundheit und Soziale Sicherung hat in diesem Punkt Gesprächsbereitschaft signalisiert.

Es bleibt zu hoffen, dass die von den Datenschutzbeauftragten des Bundes und der Länder erhobenen Anforderungen tatsächlich in das Gesetz einfließen und somit das Recht auf informationelle Selbstbestimmung für die Versicherten und Leistungserbringer erhalten bleibt.

6.3.2 Chipkarte

Ausgelöst durch die sog. Lipobay-Affäre hatte plötzlich das bereits 1994/95 umfassend unter den Datenschutzbeauftragten diskutierte Thema „Chipkarten und Telematik im Gesundheitswesen“ wieder Konjunktur.

Zwar hatten seit 1999 das bei der Gesellschaft für Versicherungswissenschaft und -gestaltung e.V. (GVG) mit dem Bundesministerium für Gesundheit und Soziale Sicherung und dem Bundesministerium für Bildung und Forschung gegründete „Aktionsforum Telematik im Gesundheitswesen“ (ATG) zu den Themen „Elektronisches Rezept“, „Elektronischer Arztbrief“, „Sicherheitsinfrastruktur“ und „Europäische und internationale Dimensionen von Telematik im Gesundheitswesen“ Handlungsempfehlungen für die Selbstverwaltungen und die Gesetzgebung erarbeitet (http://atg.gvg-koeln.de) und der Arbeitskreis Gesundheit und Soziales der Datenschutzkonferenz insbesondere zum elektronischen Arztbrief Stellung genommen, konkrete Umsetzungsschritte waren aber ausgeblieben. Ab August 2001 gewann die Diskussion um telematische Anwendungen im Gesundheitswesen zunehmend an Fahrt.

Anfangs stand unter dem Eindruck der durch Wechselwirkungen des Medikamentes Lipobay mit anderen Präparaten verursachten Todesfälle die Einführung einer Arzneimittelchipkarte zur Debatte, auf der alle den Patienten verordneten Medikamente verpflichtend gespeichert werden sollten.

Ob die Einführung einer Pflichtkarte überhaupt ein geeignetes Mittel wäre, um das Ziel - schädigende Wechselwirkungen sicher auszuschließen - zu erreichen, war dabei durchaus fraglich und wurde von den Datenschutzbeauftragten auch sofort problematisiert. Denn nicht verschreibungspflichtige Medikamente sowie über das Ausland bzw. über das Internet bezogene Arzneien würden auch mit Hilfe einer Pflichtkarte nicht erfasst werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Entschließung „Datenschutzrechtliche Anforderungen an den Arzneimittelpass" (Anlage 14) erhebliche Bedenken gegen die Einführung eines Pflicht-Arzneimittelpasses geäußert, weil hierdurch Patienten faktisch bei jedem Arzt- oder Apothekenbesuch gezwungen wären, alle Erkrankungen zu offenbaren. Dieses widerspricht den Grundsätzen des Arztgeheimnisses, das auch gegenüber anderen Ärzten gilt. Die Datenschutzkonferenz hat daher nachdrücklich auf den Grundsatz der Freiwilligkeit hingewiesen. Sie hat in diesem Zusammenhang noch einmal auf die im Rahmen der 47. Konferenz (Frühjahr 1994) und der 50. Konferenz (Herbst 1995) zum Schutz des Persönlichkeitsrechts der Patienten formulierten Bedingungen zum Einsatz von Chipkarten im Gesundheitswesen verwiesen. Danach müssen die Patienten die Möglichkeit haben zu entscheiden,

- ob überhaupt Daten auf einer Chipkarte gespeichert werden sollen,
- welche Gesundheitsdaten auf die Karte aufgenommen werden,
- welche Daten auf der Karte wieder gelöscht werden,
- ob sie die Karte beim Arzt- oder Apothekenbesuch vorlegen und
- welche Daten im Einzelfall zugänglich gemacht werden (die Technik muss eine partielle Freigabe ermöglichen).

Die Datenschutzkonferenz hat es als problematisch angesehen, den Arzneimittelpass mit der Krankenversichertenkarte gem. § 291 SGB V zu verbinden. In diese Richtung

steuerte jedoch die weitere Entwicklung, denn Anfang Dezember 2001 wandte sich die Gesundheitsministerin mit Plänen für einen elektronischen Gesundheitspass an die Öffentlichkeit, die eine Projektgruppe erarbeitet hatte.

„Telematik im Gesundheitswesen bringt den Patienten einen Zugewinn an Information und Transparenz bei gleichzeitig garantiertem Datenschutz“, hieß es dazu in der Pressemitteilung des Bundesgesundheitsministeriums. Trotz des erklärten Willens der Projektverantwortlichen, datenschutzrechtliche Sicherungsmaßnahmen im Konzept zu verankern, hat der Arbeitskreis Gesundheit und Soziales der Datenschutzkonferenz anhand der Projektunterlagen erhebliche Datenschutzdefizite festgestellt und in seiner Stellungnahme gegenüber den Beteiligten im Januar 2002 eine entsprechende Überarbeitung gefordert.

Noch bevor eine weitergehende Erörterung des Konzepts erfolgen konnte, hat das Bundesgesundheitsministerium im Februar einen Gesetzentwurf zur Änderung des § 63 SGB V vorgelegt, mit dem Modellvorhaben zur Einführung einer freiwilligen elektronischen Gesundheitskarte ermöglicht werden sollten. Der Entwurf sah eine Öffnungsklausel vor, die ein Abweichen von den datenschutzrechtlichen Bestimmungen des SGB V erlauben sollte. Er stieß deshalb bei den Datenschutzbeauftragten auf nachdrückliche Kritik. Aus Datenschutzsicht ist es eine zentrale Forderung, den Patienten die Entscheidung darüber zu ermöglichen, wem sie in welchem Umfang ihre personenbezogenen Daten zugänglich machen. Noch bevor diese Problematik mit dem Ministerium eingehend erörtert werden konnte, hat das Fachressort im März 2002 ein Eckpunktepapier zur Einführung einer elektronischen Gesundheitskarte vorgelegt. Die „multifunktionale“ Karte soll danach eine Kommunikationsschnittstelle zwischen den Trägern des Gesundheitswesens darstellen. Das Projekt wird in seiner überarbeiteten Form aufgrund seines Umfanges und seiner datenschutzrechtlichen Tragweite die Datenschutzbeauftragten auch in der Zukunft noch ausgiebig beschäftigen.

Die Gesundheitskarte soll jetzt ein freiwilliges Angebot an die Versicherten sein. Dieser Ansatz ist aus datenschutzrechtlicher Sicht zu begrüßen. Damit wird eine Forderung der Datenschutzkonferenz erfüllt. Geplant ist eine Chipkarte mit Mikroprozessor auf der Basis der bisherigen Krankenversichertenkarte mit folgenden Anwendungsmöglichkeiten (Fächern):

- Dokumentation der eingenommenen Arzneimittel,
- Fach für zusätzliche Gesundheitsinformationen/ -karten / -pässe des Versicherten,
- elektronisches Rezept,
- elektronischer Arztbrief,
- patientenbezogene Verweis-/Pointerfunktion (z.B. Spezialdaten auf Servern wie etwa Röntgenaufnahmen o.Ä.),
- Versicherungsangaben,
- Patientenaufzeichnungen (z.B. Patientenverfügung, Organspendeausweis),
- Notfallinformationen (europäischer Notfallausweis),
- Tresorfach für besonders sensible Daten (z.B. HIV-Erkrankung, Methadonsubstitution).

Für den Zugriff auf die Fächer soll eine Reihe von Sicherheitsmaßnahmen vorgesehen werden. Es handelt sich um ein sehr anspruchsvolles Projekt, das Zweifel aufkommen lässt, ob die für die neun Fächer geplanten Funktionen und zu speichernden Datensätze nicht die Leistungsfähigkeit der Chipkarte übersteigen. Am 3. Mai 2002 haben das BMG und die Spitzenorganisationen im Gesundheitswesen in Abstimmung mit dem Bundesbeauftragten für den Datenschutz zu dem Vorhaben ein Eckpunktepapier als gemeinsame Erklärung veröffentlicht.

In dem Erklärungstext wird nicht nur die datenschutzrechtliche Kernforderung der Freiwilligkeit berücksichtigt, sondern es ist auch vorgesehen, dass die Patienten selbst entscheiden können, welche ihrer Daten aufgenommen und wem die Daten zugänglich gemacht werden sollen. Im August wurde mit der „Gesundheitskarte Schleswig-Holstein“ im Raum Flensburg ein Modellversuch für die Einführung der neuen Kartengeneration gestartet. Die bundesweite Umsetzung soll nach dem Abschluss dieses und weiterer Modellversuche in der XV. Legislaturperiode erfolgen.

Trotz der Prämisse der Freiwilligkeit, den bereits bestehenden Sicherungsüberlegungen und dem erklärten Willen, die Datenhoheit in die Hand des Patienten zu geben, ist aus datenschutzrechtlicher Sicht eine kritische Begleitung der konkreten Ausgestaltung des Vorhabens unerlässlich, um die bisher geltenden Datenschutzstandards für Gesundheitsdaten zu wahren. Die datenschutzrechtliche Zielsetzung muss dahin gehen, die Möglichkeit, mit Hilfe der Gesundheitskarte individuelle „Gesundheitsprofile“ zu erstellen, deren Missbrauch nicht ausgeschlossen werden kann, wirksam zu verhindern.

6.3.3 Disease-Management-Programme

Mit Einführung der Wahlfreiheit der gesetzlich Krankenversicherten im Jahre 1996 hat der Gesetzgeber die Voraussetzungen für mehr Wettbewerb unter den ehemals 960 Krankenkassen geschaffen. Zeitgleich wurde der Risikostrukturausgleich (RSA) unter den Kassen eingeführt. Der RSA verfolgt den Zweck, im Rahmen einer solidarischen Wettbewerbsordnung dafür zu sorgen, dass Krankenkassen nicht aufgrund ihrer Mitgliederstruktur finanziell benachteiligt werden. Unterschiedliche Versichertenstrukturen, etwa durch den Altersaufbau oder die Anzahl der kostenlos mitversicherten Familienangehörigen einer Krankenkasse, sollen ausgeglichen werden. Durch den RSA wird sichergestellt, dass die so genannten „Versorgerkassen“ (AOK, BEK, DAK) mit ihrem hohen Anteil älterer Versicherter und überdurchschnittlich vorhandenen Familienangehörigen finanziell durch die anderen Krankenkassenarten unterstützt werden.

In den vergangenen Jahren hat sich der Wettbewerb unter den jetzt noch 350 Kassen als ein Wettbewerb um die guten Risiken entwickelt. Dies führte dazu, dass jüngere gesunde Mitglieder der Versorgerkassen von anderen Krankenkassen umworben wurden. In erheblichem Umfang wechselten die Umworbenen wegen der günstigeren Beitragssätze die Krankenkasse. Kranke und alte Mitglieder wurden jedoch wegen des erhöhten Kostenfaktors nicht umworben und verblieben bei den Versorgerkassen.

Da diese politisch nicht gewollte Fehlentwicklung jedes weitere Wahljahr an Dynamik zunahm und sich gleichzeitig weitere Defizite in der Gesundheitsversorgung chronisch Kranker aufbauten, entstand die Idee, Disease-Management-Programme (DMP) für chronisch kranke Versicherte zu entwickeln.

Die dahinterstehende Grundidee ist, dass diese Programme die Chance bieten, die medizinische Versorgung systematisch, integriert, multiprofessionell und patientenorientiert zu organisieren. Mit der Einführung der DMP wurde auch der RSA novelliert. Durch den novellierten RSA und den neu eingeführten DMP wurden für die Krankenkassen deutliche finanzielle Anreize geschaffen, die Versorgungssituation für chronisch Kranke zu verbessern. Für den Fall, dass eine Krankenkasse über einen überdurchschnittlich hohen Anteil von DMP-Teilnehmern verfügt, werden die dadurch entstehenden Gesundheitskosten von den anderen Krankenkassen ausgeglichen.

Datenschutzrechtlich wären die DMP unproblematisch, wenn da nicht die vom Gesetzgeber gewollte Datenübermittlung des behandelnden Arztes an die zuständige Krankenkasse wäre. Das erste Mal im bundesdeutschen Gesundheitswesen soll die ärztliche Schweigepflicht durch die Datenweitergabe an die Krankenkasse eingeschränkt werden. Zwar soll ausschließlich der Versicherte über seine Teilnahme an einem DMP entscheiden und damit in die Datenübermittlung einwilligen, faktisch bedeutet die Einwilligung aber die Einschränkung der ärztlichen Schweigepflicht.

Der Gesetzgeber hat den Krankenkassen jedoch die Steuerungsfunktion der DMP übertragen. Steuern kann nur, wer über die notwendigen Informationen verfügt. Bisher wurden den Krankenkassen die Gesundheitsdaten der ärztlichen Behandlung ihrer Versicherten nur sehr eingeschränkt bekannt. Die Leistungen der ärztlichen Behandlung wurden ohne Namensbezug im Rahmen einer Fallpauschale über die Kassenärztlichen Vereinigungen abgerechnet. Die Datenhoheit verblieb also beim Arzt.

Nunmehr sollen diese bisher nur dem behandelnden Arzt bekannten Gesundheitsdaten der DMP-Teilnehmer der Krankenkasse offenbart werden. Aus der Sicht der Krankenkasse werden die Daten zur Steuerung der DMP benötigt, da sie vom Gesetzgeber zu ihrer Durchführung verpflichtet wurden. Die jeweilige Krankenkasse hat natürlich auch ein starkes Interesse an der Steuerung, da jeder DMP-Teilnehmer über den RSA zum Defizitausgleich beiträgt.

Die Datenschutzbeauftragten des Bundes und der Länder halten an ihrer Forderung fest, dass es keinen gläsernen DMP-Patienten geben darf. Zwar wurde im § 137f Abs. 3 SGB V die Übermittlungsbefugnis der Daten an die Krankenkasse geregelt, es stellt sich aber die Frage, ob die versichertenbezogene Erhebung und Weitergabe von DMP-Daten auf ein Mindestmaß beschränkt werden kann. Es wird daher auch im Hinblick auf das Gebot zur Datenvermeidung, Datensparsamkeit und Pseudonymisierung gefordert, die patienten- und leistungserbringerbezogene Dokumentation bei den Krankenkassen möglichst zu unterlassen.

Sofern aber eine lückenlose Erhebung und Weitergabe von DMP-Daten notwendig ist, muss über die Schaffung von Vertrauens- und Datenaufbereitungsstellen außerhalb der Krankenkassen nachgedacht werden. Diese bei dem Entwurf zum Datentransparenzgesetz bereits diskutierten Einrichtungen könnten dann auch die Verwaltung und Steuerung der DMP-Daten übernehmen. Auch wären so genannte Datentreuhandstellen z.B. bei den kassenärztlichen Vereinigungen denkbar. Hier liegen ohnehin die Abrechnungsdaten der behandelnden Ärzte vor.

Obwohl seit dem 01.07.2002 die rechtlichen Voraussetzungen vorliegen, ist noch kein DMP in Kraft getreten. Strittig ist nach wie vor die Übermittlungsnotwendigkeit der Gesundheitsdaten an die Krankenkassen. Zurzeit prüft das Bundesversicherungsamt als Akkreditierungsstelle das bisher einzig vorgelegte DMP für an Brustkrebs erkrankte Versicherte. Sollte die Genehmigung scheitern, so kann nur eine Novellierung der Risikostrukturausgleichsverordnung mit einer veränderten Datenübermittlungspraxis zum Durchbruch der Programme verhelfen.

6.4 Anonymität im Internet

Das Recht auf Anonymität ist an sich so selbstverständlich, dass man darüber nicht schreiben oder sprechen müsste. Anonymität wird von uns als selbstverständlicher Bestandteil unserer Lebensqualität angesehen. Doch unser Recht auf Anonymität ist inzwischen so massiv gefährdet, dass Aufklärung über Gefährdung und mögliche Sicherung erforderlich erscheint.

Die heutige Informations- und Kommunikations-Technik ermöglicht es, Menschen in vielen Lebenslagen unbemerkt und ohne Berücksichtigung ihres Willens zu identifizieren und ihre Bewegungen zu registrieren. Wer ein Handy benutzt, kann geortet werden, sobald es eingeschaltet ist. Videokameras oder gar Satelliten aus dem Weltall zeichnen auf, wer was wann wo gemacht hat. Auch im Internet lauern überall Schnüffler. Über die eindeutige Adressierung des Rechners im Internet (IP-Adresse) ist eine Identifizierung des einzelnen Nutzers grundsätzlich möglich. Bedrohungen unseres Rechts auf Anonymität gehen sowohl von staatlichen Sicherheitsbehörden als auch von der privaten Wirtschaft und von versteckten und gewieften Hackern aus.

Die wirksamste Sicherung gegen diese Gefahren ist Anonymität an der Quelle, beim Entstehen von Daten. Das hat auch der Gesetzgeber erkannt, der im Teledienstedatenschutzgesetz jedem das Recht eingeräumt hat, sich anonym durch das Netz zu bewegen. § 4 Abs. 6 Teledienstedatenschutzgesetz (TDDSG) schreibt vor: „Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren“. § 18 Abs. 6 Mediendienstestaatsvertrag (MDStV) enthält eine gleich lautende Vorschrift für die Anbieter von Mediendiensten. Kein Provider darf aufzeichnen, wer was wann im Netz getan hat, wenn dies nicht ausnahmsweise für Abrechnungszwecke erforderlich ist. Und dann dürfen die Daten auch nur für diesen Zweck verwendet werden.

Leider halten sich viele Mitspieler im Internet nicht an diese Spielregel. Das Recht auf Anonymität, das der Gesetzgeber den Internetnutzern ausdrücklich zugebilligt hat, muss in Wirklichkeit immer erst erkämpft werden. Dem Internetnutzer bieten sich hierfür technische Verfahren, mit denen er sein Recht auf Anonymität tatsächlich in Anspruch nehmen kann. Das Projekt AN.ON, das die Technische Universität Dresden, die Freie Universität Berlin und das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein gemeinsam betreiben, stellt zum Beispiel allen Internetnutzern kostenlos eine Software zur Verfügung, mit deren Hilfe sie sich anonym im Internet bewegen können. Eine sehr gute Dokumentation und Gebrauchsanweisung ist im Internet unter http://www.datenschutzzentrum.de/projekte/anon/index.htm#pub zu finden.

Doch das Recht auf Anonymität im Internet ist, obwohl noch gar nicht konsequent umgesetzt, auch schon wieder bedroht. Internet- und Telekommunikations-Provider sollen nach einer Gesetzesinitiative des Bundesrates zur zwangsweisen Vorratsspeicherung sämtlicher Schritte und aller Aktivitäten der Nutzer verpflichtet werden. Ich hoffe sehr, dass die neue Bundesregierung bei der bisherigen Ablehnung einer solchen Gedankenpolizei (vgl. BT-Drs. 14/9801) und auch bei den Festlegungen zur staatlichen Kryptopolitik bleibt und keine Kehrt- und Rückwendung stattfindet. Deutschland darf nicht dem Beispiel anderer Länder folgen, die entweder den Einsatz kryptografischer Verfahren gänzlich verbieten (Australien) oder die Anbieter solcher Verfahren verpflichten, den Schlüssel bei einer staatlichen Stelle zu hinterlegen (Frankreich). Damit würde das Recht auf Anonymität ad absurdum geführt und die jederzeitige Entschlüsselung durch staatliche (Sicherheits-)Stellen ermöglicht. Nicht anonym, sondern allenfalls vertraulich wird die Internet-Kommunikation per E-Mail betrieben. Leider wird die Empfehlung der Datenschutzbeauftragten des Bundes und der Länder, die Inhalte der elektronischen Post zu verschlüsseln, bisher wenig genutzt. Auch meine Kommunikationspartner machen von meinem Angebot zur gesicherten Kommunikation kaum Gebrauch. Dabei stehen mehrere benutzerfreundliche Werkzeuge im Internet zur kostenfreien Verfügung bereit (zum Beispiel:

- http://www.pgp.de,
- http://www.steganos.de,
- http://www.gnupp.org/aegypten/index.de.html,
- http://www.gnupp.de,).

Der Prozess der Bewußtseinsbildung der Nutzer scheint nicht immer im gleichen Takt der technischen Entwicklung des Internet zu schlagen.

6.5 Herausforderung eGovernment

Das Thema eGovernment bleibt eine zentrale Herausforderung beim Übergang in die Informations- und Wissensgesellschaft. Bereits in meinem letzten Tätigkeitsbericht hatte ich diesem Thema ein eigenes Schwerpunkt-Kapitel (vgl. Nr. 5.4 des XV. TB LfD Nds. 1999/2000) gewidmet. Die neuen Informations- und Kommunikationstechniken ermöglichen ganz neue Formen von Dienstleistungs- und Bürgerorientierung. Entsprechend muss dem Begriff eGovernment, orientiert an den speziellen Verwaltungsanforderungen und Aufgaben der Behörde, auch ein eigener Bedeutungsinhalt gegeben werden.

eGovernment bezeichnet die Durchführung von Prozessen der öffentlichen Willensbildung, der Entscheidung sowie der Leistungserstellung und -abwicklung in Politik, Regierung und Verwaltung unter Nutzung der modernen Informations- und Kommunikationstechniken. Einbezogen sind der gesamte öffentliche Sektor, bestehend aus Legislative, Exekutive und Judikative, sowie die öffentlichen Unternehmen.

eGovernment bedeutet andererseits aber auch, dass die Gefahrenpotentiale für die informationelle Selbstbestimmung der Betroffenen größer werden. Die Verarbeitung von personenbezogenen Informationen erfolgt beim eGovernment nicht mehr nur in einer eindeutig lokalisierbaren und einem bestimmten Verantwortlichen fest zuordenbaren Datenverarbeitungsanlage, sondern in behördenübergreifenden Netzen oder sogar im weltweiten Verbund des Internet mit einer unübersehbaren Zahl von Beteiligten und Nutzern. Wie kann hier noch sichergestellt werden, dass - wie das Bundesverfassungsgericht es im Volkszählungsurteil als Grundlage des informationellen Selbstbestimmungsrechts gefordert hat - jeder selbst bestimmen kann, wer was wann bei welcher Gelegenheit über ihn weiß? Das Gericht hat ferner den Grundsatz der Datenvermeidung durch Technik im Hinblick auf die sich drastisch ändernde Informations- und Kommunikationstechnik unterstrichen. Danach ist bei der Erhebung von personenbezogenen Daten zu prüfen, „ob das Ziel der Erhebung nicht auch durch anonymisierte Ermittlung erreicht werden kann“. Der Nutzer muss auch in einer Online-Welt eGovernment-Angebote ebenso spurenlos beanspruchen können wie jemand, der persönlich die Verwaltung aufsucht. Wenn dem Bürger neben der Möglichkeit des konventionellen Verwaltungsverfahrens die Online-Variante angeboten wird, sind die folgenden allgemeinen, schon häufiger hervorgehobenen Anforderungen zu beachten:

- Personenbezogene Daten dürfen nur im erforderlichen Umfang erhoben und verarbeitet werden. Dies gilt auch für die mit der Protokollierung entstehenden Sammlungen personenbezogener Daten der Nutzer (Erforderlichkeit).
- Soweit möglich, ist die Verarbeitung personenbezogener Daten zu vermeiden (Datenvermeidung und Datensparsamkeit).
- Personenbezogene Daten dürfen nur für die in den Erlaubnistatbeständen (Zulässigkeit) und in Einwilligungen genannten Zwecken verarbeitet werden. Diese Zweckbindung ist sicherzustellen.
- Die personenbezogenen Daten müssen sicher, vertraulich und verfügbar verarbeitet werden (Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit).
- Der Nutzer muss wissen, wie die Datenverarbeitungsvorgänge ablaufen (Transparenz).
- Die Kontroll- und Korrekturrechte der Betroffenen sind zu gewährleisten.

Das Vertrauen in die Online-Welt kann aber nicht allein durch rechtliche Vorgaben gewährleistet werden. Vielmehr muss Datenschutz bei eGovernment auch durch Technik garantiert werden. Die Anforderungen an den Datenschutz durch Technik hat der Gesetzgeber im Teledienstedatenschutzgesetz (TDDSG) festgehalten. Das TDDSG hat zum einen bewährte Grundsätze des Datenschutzes an die neuen technischen Entwicklungen angepasst und zum anderen erstmals neue Ansätze des

Selbst- und Systemdatenschutzes umgesetzt. Wesentliche technische und organisatorische Werkzeuge dabei sind Kryptographie, Firewalls, Nutzungsbedingungen und Selbsttest für Nutzer, Zugriffskonzepte etc.

Die Datenschutzbeauftragten stellen sich der Verpflichtung, zu konstruktiven Lösungen für die Nutzung der Online-Verwaltung beizutragen. Aspekte des Datenschutzes müssen von vornherein in den Reformprozess selbst integriert werden, weil dieses zur Kundenorientierung der umstrukturierten Verwaltungen gehört und zugleich einen Beitrag zur technischen Modernisierung darstellt. Datenschutz ist der entscheidende Akzeptanzfaktor für alle Formen des elektronischen Handelns in einer elektronischen Verwaltung. Er kann Vertrauen in die elektronische Kommunikation schaffen und verbreiteten Befürchtungen über den Missbrauch personenbezogener Daten entgegenwirken. Ein moderner und den neuen Technikanwendungen adäquater Datenschutz ist damit ein bedeutender Wettbewerbsfaktor und Standortvorteil.

Die Datenschutzbeauftragten des Bundes und der Länder haben die Entwicklungsprozesse beim eGovernment von Anfang an offensiv und konstruktiv begleitet und dabei bewiesen, dass Datenschutz kein Hemmnis für eine moderne Verwaltung ist. Die in Kürze erscheinende Handreichung „Datenschutzgerechtes eGovernment“, die eine Arbeitsgruppe unter meiner Leitung erarbeitet hat, wird eine Vielzahl sehr konkreter, praxisbezogener Handlungsempfehlungen zur Gewährleistung von Datenschutz und Datensicherheit geben und einen Baukasten für technische und organisatorische Werkzeuge enthalten. Durch die Darstellung von zahlreichen datenschutzgerechten Referenzanwendungen, die bereits praktisch eingesetzt werden und von der zuständigen Datenschutzaufsicht als datenschutzgerecht bewertet worden sind, soll darüber hinaus die Herausbildung von Musterlösungen und standardisierten Anwendungen gefördert und zugleich Doppelaufwand bei der Entwicklung erspart werden.

„Anwendungen, Anwendungen, Anwendungen...!“ war die Marschrichtung der eGovernment-Entwicklung der letzten Jahre. Viele Verwaltungen bieten bereits heute Informationen, Downloads und Interaktionen als eService an. Für einen breiten Einsatz von eGovernment ist jedoch eine frühzeitige Vereinheitlichung und Standardisierung der Verfahrenslösungen und der eingesetzten Werkzeuge unverzichtbar. Dazu gehört auch die Interoperabilität zwischen Systemen unterschiedlicher Hersteller und Dienstleister sowie die Entwicklung von Basiskomponenten für die Bereiche Vorgangsbearbeitung, Datensicherheit, Content-Management-System, secure E-Mail, Payment-Funktionen inkl. der elektronischen Rechnungsübermittlung und von Formularservern. Datenschutz und Datensicherheit sind für die Ausprägung der Standardisierungen ein wesentlicher Baustein. Sie sind mitentscheidender Vertrauensfaktor für eine breite Akzeptanz bei Bürgern, Wirtschaft und Verwaltung. Die neue Marschrichtung sollte daher lauten: „Infrastruktur, Infrastruktur, Infrastruktur...!“ Ich bin bereit, auch hier meinen Beitrag zu leisten.

7 Informations- und Kommunikationstechnologie

7.1 Gegenwart und Zukunft

Der sichere Übergang in die Informations- und Wissensgesellschaft ist noch immer ein zentrales Thema. Leistungsfähigkeit und Miniaturisierung von Prozessoren und Speicherbausteinen steigen ungebremst. Die gewaltigen Steigerungsraten bei den Rechner- und Übertragungskapazitäten ermöglichen es, ganz neue Anwendungen zu erschließen und für jedermann über alle nur denkbaren Übertragungswege verfügbar zu machen. Der schnell laufende Prozess der Digitalisierung lässt Informations-, Kommunikations- und Mediendienste zusammenwachsen. Mit dem digitalen Rundfunk und Fernsehen werden auch Multimediadienste übertragen, mit denen Programme in Bouquets zusammengestellt und durch programmbegleitende Zusatzdienste erweitert werden können. Elektronische Programmführer und das interaktive Mitgestalten der Programme durch die Zuschauer werden möglich. Folgende Trends werden von Analysten vorausgesagt:

- Die Übertragungsraten in drahtgebundenen Telekommunikationsnetzen haben heute den Terrabit-Bereich erreicht. Veranschaulicht bedeutet dies zum Beispiel, dass die Informationen eines 20-bändigen Lexikons binnen 5 Sekunden über 1000 Kilometer übertragen werden können. Die schon jetzt erkennbaren Steigerungen der nächsten beiden Jahre führen in den Betabit-Bereich.
- Auch die drahtlose Übertragung macht erhebliche Fortschritte. Der GSM-Standard ist vom GPRS-Standard mit 100 Kilobit/Sekunde und dem UMTS-Standard mit bis zu zwei Megabit/Sekunde abgelöst. Neue Leistungen - wie Bildübertragung, Internet und Ortungsdienste - sollen uns neue Handy-Dienste schmackhaft machen. Die weltweite Vernetzung im Internet, Intranet und Extranet wird immer leichter möglich und zudem immer attraktiver.
- Personal Computer werden durch spezialisierte Miniatursysteme verdrängt. Dies führt zum allgegenwärtigen Computereinsatz, deren Systemteile sich spontan vernetzen und selbstständig miteinander kommunizieren.
- Neue elektronische Materialien wie organische Halbleiter, flexible Plastikdisplays und smartes Papier zur Darstellung von digitalen Informationen ermöglichen Datenverarbeitung in der Westentasche.
- Siliziumchips in der Größe von Staubkörnern werden gegen den Terror eingesetzt. Sie werden in die Luft geblasen, um giftige Chemikalien und biologisches Material zu identifizieren und zu warnen. Milzbrandsporen sollen mit dieser Technik aus einem Kilometer Entfernung erkannt werden können.
- Chips zur Mustererkennung mit Selbstlernfähigkeiten sind im Test („Der Nutzer ist in einem Meeting…“). Sprechererkennung und sprachgesteuerte Geräte, Fingerabdrucksensoren in mobilen Objekten sind dem Forschungsstadium inzwischen entwachsen; sie sind vielfach bereits im Echteinsatz.
- Kleinste Kameras, integrierte GPS-Ortung und Mikrophone in Kinderkleidung eingenäht ermöglichen eine ständige Beobachtung der Kinder auch vom Arbeitsplatz der Eltern aus.
- Auf die Entführung und Ermordung zweier Mädchen in Großbritannien folgte prompt der Vorschlag, allen Kindern Ortungschips einzupflanzen, um sie jederzeit

aufspüren zu können. Ein solcher Eingriff Orwellscher Ausmaße könnte zwar zum schnelleren Auffinden führen, wäre jedoch keine Garantie der Verhinderung von schlimmen Taten. Dem könnte schnell der Vorschlag folgen, allen Menschen einen Personalausweis-Chip zu implantieren und so die jederzeitige Identifikation und Ortung aller Bürger zu ermöglichen.

- Ortungschips als elektronische Diebstahlsicherung für Autos erscheinen dagegen erfolgreicher im Einsatz. Sie dienen primär zur Abschreckung durch deutlichen Hinweis auf ihre Sicherungsfunktion, erst in zweiter Linie sollen sie das Wiederauffinden des gestohlenen Autos ermöglichen.
- Nach Kühlschränken, die selbstständig über das Internet einkaufen, und elektronisch gesteuerten Heizungen und Waschmaschinen übernimmt nun der elektronische Kleiderschrank die allmorgendliche Kleiderwahl. Er stellt ein Outfit gemäß Wettervorhersage und Vorgaben wie „leger“ oder „elegant“ zusammen.
- Sensoren in Kleidungsstoffen integriert, zum Beispiel zum Messen von Körper- sowie Außentemperatur, ermöglichen angepasste Schutzeigenschaften der Kleidung.
- Implantierte medizinische Sensoren zum Messen von Pulsfrequenz, Blutdruck und Zuckerwert bei Diabetes übermitteln ihre Messwerte schnell und allzeit dem behandelnden Arzt und ermöglichen eine 24-Stunden-Betreuung. Die Ortungsfunktion des Mobiltelefons lässt zusätzlich die nächstgelegene Hilfestation ermitteln.
- Die US-Weltraumbehörde NASA arbeitet an neuroelektrischen Sensoren, die beim Begehen von Sicherheitsschleusen auf Flughäfen berührungslos Gehirnströme und Herzschlag von Passagieren messen und so ergänzt durch Zusatzwissen Gedanken und Absichten „lesen“ können sollen.

7.2 Die Datenjagd ist im vollen Gange

Bei aller Begeisterung über viele neue und nützliche Anwendungen muss an dieser Stelle die Frage nach der Sicherung des informationellen Selbstbestimmungsrechtes und nach datenschutzgerechter Technikgestaltung gestellt werden. Jeder von uns ist sich klar, dass Leistungssteigerung und Miniaturisierung der Technik auch neue Überwachungspotenziale freisetzt. Dies erleichtern insbesondere die neuen allgegenwärtigen Computersysteme; denn sie erzeugen eine Vielzahl personenbeziehbarer Daten, ohne dass dies der Besitzer bemerkt oder nachvollziehen kann. Jeder von uns gibt Tag für Tag viele Daten über sich weiter, ahnungs- oder bedenkenlos. Jeder Bundesbürger über 18 Jahre ist durchschnittlich in 52 kommerziellen Datenbanken erfasst, hinzu kommen die Datensammlungen der öffentlichen Verwaltung. Es besteht die Gefahr, dass sich daraus omnipräsente Überwachungsinfrastrukturen entwickeln.

An der Jagd nach personenbeziehbaren Spuren in unserer Informationsgesellschaft beteiligen sich neben Freizeitjägern und Kriminellen auch Staat und Wirtschaft. Sie suchen nach Informationen, die Nutzer beim Surfen im Netz oder bei sonstiger elektronischer Kommunikation hinterlassen haben. Für Beobachtung, Überwachung und Ausforschung stehen inzwischen mächtige Ausspähtechnologien zur Verfügung. Das für eine demokratische Informationsgesellschaft unerlässliche Recht auf unbeobachtete Kommunikation gerät so in größte Gefahr. Das Grundrecht des Einzelnen, grundsätzlich selbst darüber zu entscheiden, wer was und bei welcher Gelegenheit

über ihn weiß, geht verloren; er selbst kann nicht mehr verfolgen, wann Daten über ihn erhoben, verarbeitet und genutzt werden. So verwundert es nicht, dass bei einer repräsentativen Befragung 78% meinten, sie hätten die Kontrolle über ihre persönlichen Daten bereits verloren.

7.3 Besondere Problembereiche

7.3.1 Internet

Weiterhin im Mittelpunkt der schnellen technischen Entwicklungen und Anwendungen steht das Internet; Angebote wie Telefonie, Rundfunk und Video werden schon heute zunehmend über das Internet-Protokoll TCP/IP übertragen. Das Internet ist zu einem Kommunikationsmedium für jedermann geworden; eCommerce, eBusiness und eGovernment beherrschen die Szene, eCrime sowie Cyber-Terrorismus sind gefährliche, ungewollte Nebenerscheinungen. Das Internet ging in seinen Anfängen vom Prinzip der Kontrollfreiheit aus. Anonymität, für die heute Datenschützer und Cyberrechtler kämpfen, war selbstverständlich. Jeder Versuch einer korrigierenden oder steuernden Funktion wurde entschieden zurückgewiesen und leidenschaftlich bekämpft. Das Prinzip des freien Flusses der Information (free flow of information) war fast noch mehr verwurzelt als das Prinzip der Informationsfreiheit (freedom of information).

Die vielfachen Nutzungsmöglichkeiten des Internets sind inzwischen Bestandteil unseres Alltags geworden, sowohl am Arbeitsplatz als auch Zuhause. Das Internet wird nicht nur zur Abfrage von Informationen genutzt, sondern zunehmend auch zur Abwicklung von Rechtsgeschäften und zur interaktiven Beantragung und Bearbeitung von Verwaltungsentscheidungen. Das öffentliche Kommunikationsnetz Internet offenbart dabei systembedingt viele Informationen über seine Nutzer. So werden Name und Adresse beim Absenden der E-Mail beigestellt. Beginn, Ende und Dauer einer Verbindung, Datenmenge, das verwendete Protokoll sowie die eingesetzte Software sind erkennbar. Das alles sind personenbeziehbare Informationen, die viel über die handelnden Personen aussagen. An den Kommunikationsschnittstellen zwischen Netzen und Nutzern (Knotenpunkte im Internet, Internet-Portal und virtuelle Poststelle) laufen alle Kommunikationsvorgänge zusammen. Dabei entstehen umfangreiche Datensammlungen und damit neuartige Bedrohungen für die Privatsphäre der Bürger. Einige dieser Überwachungsmöglichkeiten sollen hier aufgezeigt werden:

- Auf die Terroranschläge vom 11. September 2001 haben die USA unter anderem mit weitgehenden Überwachungsmaßnahmen und Eingriffen im Internet reagiert (Patriot Act). Wer durch Selbstschutz sein Recht auf unbeobachtete Kommunikation wahrnehmen will und Spuren zu verwischen sucht, wird als Eindringling eingestuft, der keinen Anspruch auf Achtung seines „right to privacy“ hat.
- Das deutsche Terrorismusbekämpfungsgesetz vom 14. Dezember 2001 enthält weitgehende Befugnisse zur Überwachung der Konten und Geldbewegungen bei Kreditinstituten, der Postbewegungen bei allen Postdienstleistern, der Transport- und Reisebewegungen bei Lufttransporteuren und der Telekommunikationsdienstleistungen bei entsprechenden Anbietern. Eine zentrale Rolle bei der Bekämpfung des internationalen Terrorismus wird dem Bundesverfassungsschutz zugewiesen. Diese Befugnisse ermöglichen es, umfassende Verhaltens- und Bewegungsprofile

zu erstellen. Im Einzelnen wird dazu auf die Darstellung in Kapitel 10.1.1 verwiesen.

- Auf Initiative des Bundesrates sollen durch Änderung der StPO alle Telekommunikationsunternehmen und sämtliche Internetprovider verpflichtet werden, alle Daten über Kunden und ihre Nutzungen ausnahmslos zu speichern und für Polizei- und Sicherheitsbehörden bereithalten. Dies stellt eine Vorratsspeicherung dar, die das Bundesverfassungsgericht im Volkszählungsurteil als unzulässig angesehen hat.
- Suchmaschinen liefern Infopartikel und Fakten über ihre Nutzer. So kann der Betreiber der Suchmaschine rückverfolgen, welche Seiten mit welchen Suchbegriffen von einem Nutzer gefunden und in welcher Reihenfolge abgerufen worden sind. Auch die Verweildauer ist erkennbar.
- Cookies werden auf fremden Rechnern gespeichert. Sie machen Nutzer beim nächsten Besuch erkennbar; Online-Händler identifizieren über Sammelfilter ihre Kunden.
- Customer Relation Management (CRM) hat Konjunktur. Durch Verknüpfung (Data Warehouse) und Auswertung (Data Mining) systematisch zusammengeführter Kundendaten versuchen Handelsunternehmen personenbezogene Erkenntnisse für erfolgreiches Direktmarketing oder kommerziellen Datenhandel zu gewinnen. Die betroffenen Kunden sind vielfach weder unterrichtet noch um Einwilligung gebeten worden (vgl. Kapitel 20).
- Arbeitgeber haben zwar das Recht, die Erfüllung dienstlicher Aufgaben auch bei der Internetnutzung angemessen zu kontrollieren, unzulässig dagegen ist eine Totalüberwachung der Mitarbeiter (vgl. dazu Kapitel 8.3). Das Überwachungsprogramm mit dem sinnigen Namen „Little Brother“ bietet dazu die Möglichkeit; Verhalten und Leistung der Mitarbeiter können so detailliert offengelegt werden. So kann die dringend benötigte Kommunikationskultur in Unternehmen und Behörden zerstört werden. Damit wird mehr Schaden angerichtet als dies je nützen könnte.

Diese mächtigen Überwachungsmöglichkeiten drohen das zarte Pflänzchen der beginnenden Informationsgesellschaft zu ersticken. Besonders seit dem 11. September 2001 verschiebt sich die Balance zwischen Schutz der Privatsphäre einerseits und sicherheitstechnischen und kommerziellen Interessen andererseits. Zum wiederholten Mal wurde der Versuch gestartet, den Datenschutz bei der Nutzung von Internet und Telekommunikation auszuhebeln. Internet- und Telekommunikations-Provider sollten zur zwangsweisen Vorratsspeicherung sämtlicher Daten ihrer Kunden zu verpflichten werden (vgl. Kapitel 8.6.3). Eine entsprechende Initiative des Bundesrates ist zwar durch den Ablauf der Legislaturperiode des Bundestages vorerst gegenstandslos geworden. Es ist aber sicher davon auszugehen, dass es neue Vorstöße in dieser Richtung geben wird, zumal auch die dänische Ratspräsidentschaft auf europäischer Ebene entsprechende Initiativen eingeleitet hat. Dies darf nicht geschehen!

7.3.2 Audiovisuelle Systeme

Videokameras suggerieren Sicherheit. In ganz Deutschland gibt es über 500 000 davon, auf öffentlichen Straßen, Wegen und Plätzen, in Kaufhäusern, Ladenpassagen, Verkaufsräumen, Tankstellen und Bahnhöfen. Allein im Hauptbahnhof Hannover sind 180 Videokameras installiert, „gut“ getarnt, zoom- und schwenkbar, in neuester Technologie. Mit UMTS erlangt die Videoüberwachung eine ganz neue Dimension.

Das UMTS-Handy mit einer Videokamera ausgestattet ermöglicht dem Besitzer jederzeit auf Sendung zu gehen - nach Hause, zur Stammkneipe, zur nächsten Polizeistation oder zu einem Fernsehsender. UMTS und Nachfolgetechnologien können leicht zur Massenüberwachung eingesetzt werden. Sie unterlaufen alle Transparenzgebote des Datenschutzrechts.

Beim Videoeinsatz wird häufig vergessen, dass jede Form der Beobachtung persönlichen Verhaltens durch Kameras einen Eingriff in das verfassungsmäßig geschützte allgemeine Persönlichkeitsrecht darstellt. Eines sei klar gestellt, Videoüberwachung ist weder grundsätzlich zu verdammen noch als Allheilmittel der Sicherheit zu preisen. Es kommt immer auf den Zweck und die Umstände des Einsatzes an. Während die Beobachtung durch Behörden einer gesetzlichen Grundlage bedarf, ist der Einsatz audiovisueller Systeme durch Privatpersonen derzeit kaum geregelt. Mit Videobeobachtung wird die Tatsache, dass sich eine Person zu einer bestimmten Zeit an einem bestimmten Ort in einem bestimmten Zustand aufhält, möglicherweise in Begleitung einer bestimmten Person, von Kameras erfasst und auswertbar. Es ist für Betroffene nicht erkennbar, wer alles Kenntnis nimmt, wer die Bilder zu welchem Zweck betrachtet und weiterverarbeitet. Die bloße Vermutung, man könnte gerade in diesem Augenblick von einer Kamera beobachtet werden, führt zu einem permanenten Anpassungsdruck. Wer nicht weiß, ob und von wem und zu welchem Zweck er beobachtet wird, verliert seine Unbefangenheit und wird sich im Zweifel vorsorglich auf diese Überwachungssituation einstellen. Deshalb bedarf es über den neuen § 6b BDSG hinaus weiterer Regelungen für den Einsatz audio-visueller Systeme, die die bislang allein einschlägigen, von der technischen Entwicklung aber längst überholten Vorschriften im Kunsturhebergesetz aus dem Jahre 1907 ablösen.

7.3.3 Biometrie

Biometrische Verfahren nutzen physische Merkmale (Fingerabdruck, Gesicht, Muster der Iris) oder verhaltensbedingte Merkmale (Schreibverhalten, Lippenbewegung, Stimme) zur Identifikation einer Person. Bekannteste Anwendungsfälle sind die Zugangssicherungen von Rechenzentren, Haustüren, Autos, Bankautomaten oder auch der Zugang zum eBanking. Bei erstmaliger Nutzung werden ausgewählte Merkmale der betroffenen Person vermessen und mathematisch beschrieben (komprimiert). Bei Kontrollen werden die aktuellen Messwerte mit den komprimierten Werten verglichen. Der Vorteil biometrischer Merkmale ist, dass sie an die jeweilige Person gebunden sind. Sie können von Unbefugten nur schwer kopiert und entwendet werden und gehen auch kaum verloren. Die Verfahren arbeiten jedoch nicht fehlerfrei und können überlistet werden. Darüber hinaus sind biometrische Merkmale, allein schon durch die natürlichen Alterungsprozesse, Veränderungen unterworfen. Datenschutzrechtlich problematisch ist, dass sich aus den biometrischen Rohdaten über den eigentlichen Verwendungszweck hinaus weitere Rückschlüsse auf die Person ziehen lassen. Zum Beispiel kann aus einem Bild das Geschlecht, das ungefähre Alter, die Hautfarbe erkannt werden. Aus dem Augenhintergrund soll auf Krankheiten wie Diabetes oder Bluthochdruck und vom Fingerabdruck auf den Beruf geschlossen werden können.

Durch die Terroranschläge vom 11. September 2001 haben biometrische Merkmale eine unerwartete Aufwertung erfahren. In Pässen und Personalausweisen dürfen

neuerdings neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern, Händen oder Gesicht des Inhabers aufgenommen werden. Alle Merkmale und Angaben über die Person dürfen auf den Ausweispapieren verschlüsselt gespeichert werden. Die Datenschutzbeauftragten des Bundes und der Länder haben untersucht, ob diese Maßnahmen geeignet und angemessen sind. In einem Positionspapier haben sie Zweifel angemeldet sowie datenschutzrechtliche Eckpunkte für eine erforderlich erscheinende Erprobung genannt (siehe Anlage 19).

Biometrische Kontrollen, die zuvor oft als nicht ausgereifte Nischenprodukte angesehen wurden, hat man nach den Terroranschlägen als Zugangskontrollen in sicherheitsempfindlichen Bereichen einzuführen versucht. Doch kaum begonnen, wurden einschlägige Vorhaben auf Flughäfen und bei Banken wegen der großen Fehleranfälligkeit schon wieder eingestellt. Damit ist allerdings noch kein endgültiges Urteil über die Biometrie gesprochen. Datenschutzfreundlich und förderwürdig erscheinen besonders biometrische Verfahren, die eine Überprüfung zulassen, ohne die Identität des Betroffenen zu offenbaren. Denkbare Einsatzfelder wären eBanking, eCommerce und eGovernment. Auch biometrische Verschlüsselungs- und Signaturverfahren sind denkbar. Erfolg und Einsatz der Biometrie hängt wesentlich davon ab, ob Fehler des fälschlichen Akzeptierens oder des fälschlichen Abweisens minimiert werden können. Hierzu sind noch vielfältige Forschungsarbeiten erforderlich.

7.3.4 Mobile Datenverarbeitung

An unsere Chipkarten im Portemonnaie haben wir uns inzwischen gewöhnt, sie gehören zu unserem Alltag. Unsere Sammlung enthält zum Teil kontaktbehaftete Chipkarten, die Spuren hinterlassen, wenn sie in ein Lesegerät gesteckt werden, etwa beim Arzt oder beim Händler zur Bezahlung, und kontaktlose Chipkarten, die gelesen werden können, wenn der Besitzer sie bei sich führt und in die Nähe einer Lesestation kommt. Für manche Anwendungen ist dies verlockend bequem, zum Beispiel bei der Zugangskontrolle gesicherter Räume, beim Einsteigen in öffentliche Verkehrsmittel oder bei der elektronischen Kurkarte, weil sich damit Türen automatisch öffnen und zeitaufwendige Prüf- und Bezahlverfahren entfallen.

Neu sind so genannte RFTags, kleinste Spulen (deutlich kleiner und leichter als ein Konfetti), die, wenn sie mit einem Hochfrequenzsignal angeregt werden, eine sie identifizierende eindeutige Kennung zurücksenden. Sie werden künftig für wenige Cent produzierbar und in viele Gegenstände des täglichen Gebrauchs integriert sein. Die Anwendung der RFTags wird ganz harmlos damit beginnen, dass im Supermarkt alle Produkte statt mit Preisaufklebern mit solchen Tags versehen werden. Dann braucht man den Einkaufswagen nur noch an einer Lesestation vorbeizuschieben - und schon wird die Rechnung erstellt und ausgedruckt. Die gleiche Technik der Preisauszeichnung wird auch bei Kleidung angewendet werden - und damit tragen wir bald alle leicht verfolgbare Personenkennzeichen mit uns herum. RFTags werden in Gegenstände integriert ohne von uns ausdrücklich gewollt zu sein; sie werden nicht gesondert ausgegeben. Auf ihnen findet keine weitergehende Speicherung und erst recht keine Verarbeitung personenbezogener Daten statt. Betroffene können den Gebrauch des Mediums nicht beeinflussen. RFTags sind universell verwendbar, isoliert für sich betrachtet sind sie vollkommen harmlos. Gleichwohl kann von ihnen

eine unüberschaubare Folgewirkung mit vielfacher Datenspeicherung und -verarbeitung ausgehen. Es gibt keine verantwortliche Stelle, die das Medium ausgibt oder verkauft und somit auch keine Stelle, die mögliche Anwendungen verantwortet. Das Transparenzgebot, das eine vorzeitige Unterrichtung über alle Vorgänge (egal wo sie ablaufen) fordert, wird faktisch unerfüllbar.

„Datenschutz wird in Zukunft nur möglich sein, wenn versucht wird, die technische Entwicklung in der Weise zu beeinflussen, dass Datenschutzaspekte von Anfang an berücksichtigt werden oder sogar als Ziel die Entwicklung der Informations- und Kommunikationstechnik anleiten“, mahnen Roßnagel/Pfitzmann/Garstka im Gutachten „Modernisierung des Datenschutzrechts.

7.4 Selbstdatenschutz

Da Staat und Recht in globalen Netzen und einer Welt allgegenwärtiger Datenverarbeitung nur begrenzt in der Lage sind, die informationelle Selbstbestimmung ihrer Bürger zu schützen, ist es erforderlich, dass nach Ausschöpfen aller bereits genannten Möglichkeiten zum Schutz der Selbstbestimmung den Bürgern ermöglicht wird, Mittel zu ergreifen, um ihre informationelle Selbstbestimmung selbst zu schützen.

Für einen umfassenden Persönlichkeitsschutz sollten dem Nutzer die technischen Instrumente sowie notwendige Infrastrukturleistungen zur Verfügung gestellt werden. Ein wichtiges Mittel des Selbstdatenschutzes ist die selbstbestimmte Wahl von anonymen Nutzungen, von Pseudonymen oder von Verschlüsselungstechniken. Ein weiteres Instrument des Selbstdatenschutzes ist die Möglichkeit, sich durch Zugriff auf die Datenschutzerklärung der Daten verarbeitenden Stelle jederzeit ausreichende Gewissheit über die Bedingungen der Datenverarbeitung zu verschaffen. Durch Offenlegen der Datenverarbeitungspraxis kann dem Nutzer ein Teil seiner Besorgnis genommen werden.

Schutz und Hilfestellung gegen Bedrohungen bei der Nutzung von E-Mail und Internet werden in vielfacher Hinsicht geboten. Die Möglichkeiten reichen von umfassenden Informationen zur datenschutzgerechten Auswahl und Konfiguration des Web-Browsers oder des Mail-Clients bis hin zum Einsatz von Hard- und Softwareprodukten, die es dem Nutzer erlauben, die Verbindungen seines Rechnersystems zum Netz wirksam zu kontrollieren. Eine zentrale Rolle bei allen Bemühungen muss aber stets der Benutzer einnehmen; er muss sich über mögliche Gefahren informieren und Abwehrstrategien entwickeln. Geeignete Hilfsmittel zur Entwicklung und Umsetzung solcher Strategien sind teils kostenlos, teil zu durchaus erschwinglichen Preisen am Markt verfügbar. Entsprechende Informationen finden sich unter anderem auf unserer Homepage http://www.lfd.niedersachsen.de, unter http://www.datenschutz.de oder in den einschlägigen Veröffentlichungen der Fachpresse.

PC-Selbsttest

Über unsere Homepage www.lfd.niedersachsen.de stellen wir einen Selbsttest zur Verfügung. Der Test ist für Privatanwender gedacht und soll helfen, unsichere Systemkonfigurationen aufzudecken. Nur wenn bekannt ist, welche Lücken ein System aufweist, kann qualifiziert Abhilfe geschaffen werden. Daher überprüft der Test in

einem mehrstufigen Verfahren nicht nur die Einstellungen des Browsers, sondern führt auf Wunsch des Nutzers auch einen sog. Port-Scann durch. Die Ergebnisse werden dem Tester vertraulich zur Verfügung gestellt und ermöglichen, die notwendigen Maßnahmen zur Absicherung des Systems zu treffen.

7.5 Strategische Neuausrichtung des Systemdatenschutzes

7.5.1 Sichere E-Mail

Der E-Mail-Dienst hat in den letzten Jahren immens an Bedeutung gewonnen. Mit dem umfassenden Einsatz von vernetzten Rechnersystemen in Verwaltung und Wirtschaft hat sich dieses Kommunikationsmedium in der modernen Arbeitswelt etabliert. Aber auch im Privatbereich ist die E-Mail heute überaus beliebt. Eine Vielzahl von Providern bieten kostenlose E-Mail-Postfächer für Privatkunden an. Die schnelle und preiswerte Kommunikation ist der große Vorteil, der zu dieser starken Verbreitung geführt hat.

Mit dem Einsatz von E-Mail treten aber auch eine Reihe neuer Gefahren auf. Ungesichert übertragene E-Mails können abgefangen, gelesen und verfälscht werden. Zudem ist nicht sichergestellt, dass die E-Mail wirklich den Empfänger erreicht. E-Mails können Viren oder andere Schadprogramme enthalten, die Datenbestände auf Arbeitsplatz-PCs und in Netzwerken gefährden. Verbreitungsszenarien wie beim „Loveletter“-Mailvirus haben dies deutlich gezeigt. Während jedoch Virenscanner in großen Teilen von Verwaltung und Wirtschaft heute obligatorisch sind und so auch die Mailserver und Mailclients sichern, gilt dies nicht für Lösungen, die die Inhalte der Mailkommunikation sichern sollen.

Die Niedersächsische Landesverwaltung hat im Jahr 1996 mit der Einführung von Electronic Mail begonnen. Seit diesem Zeitpunkt wurden etwa 50 000 Mitarbeiter der Landesverwaltung an den Telekommunikationsdienst Electronic Mail angeschlossen, weitere Anschlüsse und der Verbund mit der niedersächsischen Kommunalverwaltung sind geplant. Der E-Mail-Dienst ist zu einem wichtigen und unverzichtbaren Arbeitsmittel in der öffentlichen Verwaltung geworden. Er bildet darüber hinaus die Basis für die Realisierung verschiedener eGovernment-Projekte.

Der sich über einen längeren Zeitraum hinziehende Anschluss der Dienststellen an den landesweiten Mailverbund hatte zur Folge, dass einheitliche Festlegungen zur technischen Ausgestaltung und zur Nutzung des komplexen Dienstes fehlten. Leider erst nach fast abgeschlossener Einführung erarbeitet eine Arbeitsgruppe des IMA-IuK eine Rahmendienstanweisung zur Nutzung des E-Mail-Dienstes sowie eine Dienstanweisung für Administratoren. An den Entwurfsarbeiten habe ich mich aktiv beteiligt. Kernpunkte der Dienstanweisung sind:

- Personenbezogenen Daten und Informationen, die besonders schutzbedürftig sind, dürfen nicht ohne zusätzliche Sicherungen (elektronische Signatur, Verschlüsselung) versandt werden.
- Bei Einsatz der Verschlüsselung ist die elektronische Signatur obligatorisch.
- Der E-Mail-Dienst ist nur für den dienstlichen Gebrauch zugelassen.

- Eine Kontrolle der Nutzung des E-Mail-Dienstes erfolgt nur im erforderlichen Umfang (gelegentliche Stichproben und Anlasskontrollen).
- Die auf Grund der elektronischen Verarbeitung entstehenden Nachweisdaten dürfen nicht für Zwecke der Leistungs- und Verhaltenskontrolle von Mitarbeitern verwendet werden.
- E-Mails dürfen nicht länger gespeichert werden, als dies für die Aufgabenerfüllung erforderlich ist.

Eine Strategie-Entscheidung der niedersächsischen Landesverwaltung sieht vor, künftig in verstärktem Maße die elektronische Signatur und Verschlüsselungstechniken einzusetzen. Hierfür ist eine geeignete Infrastruktur zur Signatur und Verschlüsselung von E-Mails aufzubauen. Verbleibende Restrisiken der Vertraulichkeit sind durch organisatorische Maßnahmen wirksam abzusichern. Hierzu gehört auch eine angemessene Sensibilisierung der Mitarbeiter im Umgang mit personenbezogenen Daten und anderen vertraulichen Informationen.

7.5.2 Verschlüsselung bei Speicherung und Übermittlung

Der technisch-organisatorische Datenschutz umfasst die Maßnahmen, die nach § 7 des Niedersächsischen Datenschutzgesetzes bzw. nach der Anlage zu § 9 des Bundesdatenschutzgesetzes zu treffen sind, um die dort niedergelegten Ziele zu erreichen und einen datenschutzgerechten Umgang mit personenbezogenen Daten sicherzustellen. Die technische Umsetzung dieser Anforderungen war in der Vergangenheit im Wesentlichen darauf abgestellt, Unbefugten den Zugang zu den Räumen, Maschinen und Netzwerken, in denen Datenverarbeitung stattfindet, zu verwehren und die befugte Nutzung von Räumen, Maschinen und Kommunikationswegen nachvollziehbar zu protokollieren.

Der Aufwand, auf diesem Wege ein hohes Maß an Sicherheit zu erreichen, hat in verschiedenen Bereichen wie z.B. der Netzwerkabsicherung eine Größenordnung erreicht, die von kleineren Organisationen nur noch bedingt zu leisten ist. Im Gegensatz zu klassischen Maßnahmen der baulichen Absicherung von technischen Betriebsräumen und Kommunikationswegen, die sich in den letzten Jahren im Kern nur in bescheidenem Umfang verändert haben, ist der Bereich der Netzwerkabsicherung förmlich explodiert. In dem Maße, wie die öffentlichen Stellen sich verstärkt offener, technisch nicht kontrollierbarer Kommunikationswege bedienen, sind die Aufwendungen für die Absicherung der internen Netze in die Höhe geklettert. Um die Kosten in einigermaßen erträglichen Grenzen zu halten, sind häufig zentrale Übergangsstellen zwischen internen und externen Netzen gebildet worden. Diese Firewalls sind meist in gesicherten Räumen ordnungsgemäß untergebracht. An diesen Übergangsstellen wird mit einem immer größer werdenden technischen Aufwand versucht, die möglichen Bedrohungen aus dem externen Netz soweit möglich zu begrenzen. Dennoch bieten die in dieser Weise abgesicherten zentralen Übergangspunkte oftmals nur einen trügerischen Schutz, da technisch nicht hinreichend sichergestellt werden kann, dass es wirklich keine „Nebenstrecken“ zu Fremdnetzen gibt.

Dies zeigt, dass die herkömmlichen Maßnahmen im Grunde vordringlich auf eine Absicherung der „Datenumgebung“ gerichtet sind; es werden räumliche Sicherungen

installiert, Zutrittskontrollen durchgeführt, Zugangskontrollen installiert usw. Zur Sicherung der Daten selbst stehen bislang außer der Zuordnung von Zugriffsrechten unterschiedlicher Qualität kaum praktisch relevante Verfahren zur Verfügung. Die theoretisch denkbare Verwendung vom kryptografischen Methoden zur Absicherung der Daten während der Speicherung und Übermittlung scheitert bislang an organisatorischen, technischen und rechtlichen Problemen bei der Vergabe und Verwaltung geeigneter Schlüsselpaare. Erst wenn es gelingt, hierarchisch strukturierte Gruppenschlüssel in ausreichender Anzahl in geeigneter Weise bereitzustellen, wären die technischen Grundlagen geschaffen, um den technischen Datenschutz im engeren Sinne voranzutreiben. Die bei der flächendeckenden Ausstattung der niedersächsischen Landesverwaltung anfallenden Kosten für Crypto-Cards, Lesegeräte und Software wären durch den Zuwachs an Sicherheit für personenbezogene Daten in allen Stufen der Verarbeitung gerechtfertigt. Ob Einsparpotentiale entstehen, wenn innerhalb der Landesverwaltung alle schützenswerten Daten nur noch in verschlüsselter Form gespeichert oder übermittelt werden, wäre gesondert zu betrachten. Dabei muss jedoch bedacht werden, dass die Zugangssicherungen einen wesentlichen Beitrag zur Verfügbarkeit der Daten leisten, der ausschließlich über kryptografische Verfahren nicht sichergestellt werden kann.

7.5.3 Elektronische Signatur / Crypto-Card Niedersachsen

In den verschiedensten Bereichen des IuK-Technikeinsatzes und in der Kommunikation halten verstärkt kryptografische Methoden Einzug, um die Sicherungsziele Authentizität, Integrität und Verfügbarkeit bei der Verarbeitung von personenbezogenen Daten zu erreichen. Eine nachhaltige Nutzung dieser Methoden bedingt den Einsatz geeigneter Chipkartensysteme. In Niedersachsen findet für einen Teilbereich der Verwaltung eine Signatur-Karte der TeleSec Anwendung. Vor diesem Hintergrund erscheint es sinnvoll, Modelle für einen erweiterten Einsatz dieser Karten-Technologie zu entwickeln, die den weitergehenden Einsatz von Signatur und Verschlüsselung vorsehen und somit zu einer wesentlichen Verbesserung des Datenschutzniveaus in der niedersächsischen Landesverwaltung beitragen können.

Auf der in der niedersächsischen Landesverwaltung verwendeten Crypto-Card der TeleSec sind zwei Schlüsselpaare hinterlegt; ein Schlüsselpaar dient der gesetzeskonformen Signatur, das andere kann für die Verschlüsselung von Mailinhalten genutzt werden. Da der private Schlüsselteil für den persönlichen Verschlüsselungsschlüssel ausschließlich auf der Karte vorgehalten wird, ist der Zugriff auf verschlüsselte Dokumente nur mit der persönlichen Karte möglich. Ist der Inhaber der Karte längerfristig nicht verfügbar oder hat ein unberechtigter Nutzer die Karte durch Falscheingabe der PIN gesperrt, sind die verschlüsselten Dokumente endgültig verloren. Dieses hohe Risiko hat sicherlich mit dazu beigetragen, dass die Crypto-Card außerhalb der Kernfunktionalität der automatisierten Haushaltsbewirtschaftung (P53) derzeit nur begrenzte praktische Verwendung findet.

Durch hierarchische Gruppenschlüssel ließe sich dieses Risiko reduzieren und der erwünschte Mehrnutzen erreichen. Hierzu wäre es erforderlich, auf den eingesetzten Chips zusätzliche Speicherbereiche bereitzustellen, die vom Nutzer in eigener Verantwortung belegt werden können. Leider sieht diese Erweiterung die bei der TeleSec

ab Mitte 2003 verfügbare „neue“ Chipkarte noch nicht vor. Bis zur Realisierung derartiger Chipkarten muss für den Einsatz von organisationsgebundenen Schlüsseln auf reine Softwarelösungen ausgewichen werden. Unter Einbeziehung der weiterhin vorhandenen persönlichen Schlüssel für Signatur und Verschlüsselung könnten so mehrstufige Hierarchien aufgebaut werden. Die Generierung und Verwaltung dieser Organisationsschlüssel sollte zentral für die jeweilige Organisation erfolgen.

Die Crypto-Card des Landes Niedersachsen hat sich bei P53 und in Ansätzen bei der Mail-Verschlüsselung bewährt. Die einer Erweiterung ihrer Einsatzmöglichkeiten bislang entgegenstehenden technischen Probleme könnten durch Einführung einer verbesserten Chip-Karte befriedigend gelöst werden. Damit würden sich für Niedersachsen eine ganze Reihe neuer Anwendungsfelder erschließen, zum Beispiel im Bereich der Kommunikations- und Datensicherheit und beim verstärkten Einsatz der Signatur in der öffentlichen Verwaltung. Eine Arbeitsgruppe des IMA-IuK, an der ich aktiv mitarbeite, untersucht Einsatzmöglichkeiten und Möglichkeiten der technischen Realisierung.

7.5.4 Virtual Private Networking

Der Oberbegriff „Virtual Private Networking“ (VPN) fasst verschiedene Methoden zur sicheren Übertragung von elektronischen Informationen (Daten, Sprache und Video) über die gleichen physikalischen Übertragungswege zusammen. Der Netzteilnehmer eines VPN kann die Daten eines anderen VPN nicht „sehen“ und damit zu keiner Zeit darauf zugreifen. In seinem eigenen VPN ist der netzwerkseitig uneingeschränkte Zugriff auf die Daten möglich. Im Gegensatz zu einem physikalisch getrennten VPN, dass von einer Organisation exklusiv und mit eigenen Übertragungsmedien und -einrichtungen betrieben wird, sind die Betriebskosten durch Nutzung gemeinsamer physikalischer Ressourcen im Intranet und Internet deutlich geringer.

Das izn ist Netzwerkbetreiber des iznNet 2000 für Landesdienststellen und bietet dafür auch VPN-Dienste an. Das izn muss dabei sicherstellen, dass trotz der Nutzung gleicher Medien zu jeder Zeit an jedem Ort im Netzwerk die Daten der unterschiedlichen Benutzergruppen auf sichere Weise logisch entkoppelt werden. Durch den Einsatz von MPLS (Multiprotocol Label Switching) wird eine Trennung im iznNet 2000 wirksam vorgenommen. An den VPN-Übergängen wird die Sicherheit durch eine zentrale VPN-Firewall erreicht. Sie stellt auch die zentrale Verbindung zwischen den Landesintranet und dem Internet dar. Zusätzlich wird empfohlen und ermöglicht, durch dezentrale Firewalls die Sicherheit an den Schnittstellen der Dienststellen-VPN weiter zu erhöhen. Optional ist es zudem möglich, eine verschlüsselte Datenübertragung durch Einsatz von IPSec (Secure-VPN) zu erreichen. Aus meiner Sicht bietet die VPN-Konzeption des iznNet 2000 ein gut abgestuftes Sicherheitskonzept für die Übertragung von Daten zwischen den Dienststellen der niedersächsischen Landesverwaltung.

7.6 Unsere Projekte

7.6.1 Innovationsbündnis mit der Landeshauptstadt Hannover

In einem Pilotprojekt mit der Landeshauptstadt Hannover und der Universität Kassel wurden die rechtlichen und technischen Voraussetzungen für ein datenschutzgerechtes eGovernment untersucht und in einem Pilotfeld umgesetzt. Das Projekt hat die "Einfache Melderegisterauskunft" für Personen, Unternehmen oder andere Behörden, die regelmäßige Verwaltungskontakte unterhalten, auf Geeignetheit untersucht und benutzerfreundliche Verfahrenslösung erarbeitet. Das Verfahren unterscheidet drei Fallkonstellationen:

- Anonyme Auskunftsanfrage mit Bezahlung der Gebühren per Geldkarte.
- Auskunftsanfragen von Mitarbeitern registrierter privater Stellen (Firmen, Freiberufler usw.) mit Sammelabrechnung der Gebühren. Auskunftssuchende weisen sich durch eine elektronische Signatur aus; dies kann auch pseudonym erfolgen. Die Authentifizierung dient der Nachweisbarkeit der Kostenübernahmepflicht.
- Gebührenfreie Auskünfte auf Anfragen von Mitarbeitern von Behörden oder sonstigen öffentlichen Stellen. Auskunftssuchende weisen sich durch elektronische Signatur als berechtigt aus.

Rechtliche Rahmenbedingungen

Das Niedersächsische Meldegesetz (NMG) bietet noch keine Rechtsgrundlage, Melderegisterauskünfte online über das Internet zu erteilen. Eine entsprechende Anpassung des Niedersächsischen Meldegesetzes an das Rahmenrecht ist in Kürze zu erwarten. Andererseits ist die Online-Auskunft durch das geltende Recht nicht ausdrücklich untersagt; unter bestimmten Einschränkungen, die unter dem Begriff „Adressbuchlösung“ zusammengefasst werden, wird sie auch jetzt für zulässig gehalten. Zwar macht § 12 Abs. 1 des Niedersächsischen Datenschutzgesetzes (NDSG) die Zulässigkeit des automatisierten Datenabrufs von einer (ausdrücklichen) gesetzlichen Zulassung abhängig, und § 12 Abs. 4 NDSG untersagt sogar, personenbezogene Daten für Personen und Stellen außerhalb des öffentlichen Bereichs zum Abruf bereitzuhalten. Allerdings gelten die Einschränkungen der Absätze 1 bis 4 nicht für den Abruf aus solchen Datenbeständen, deren Inhalt veröffentlicht werden darf. Für Daten aus dem Melderegister kommt die Veröffentlichung in Adressbüchern in Frage; im Umfang der Datenweitergabe an Adressbuchverlage ist somit auch die Online-Melderegisterauskunft zulässig. Gegenüber der einfachen Melderegisterauskunft in anderer Form sind deshalb bei der Online-Auskunft zurzeit die Einschränkungen von § 34 Abs. 4 und 5 NMG zu beachten: Es dürfen lediglich Auskünfte über Einwohner erteilt werden, die das 18. Lebensjahr vollendet haben und der Weitergabe an Adressbuchverlage nicht widersprochen haben. Die Ankopplung an die Adressbuchregelung schließt auch Auskünfte über ehemalige Einwohner (Wegzugadressen) und Verstorbene aus.

Datenschutzgrundsätze

Professor Dr. Alexander Roßnagel hat für das Projekt ein Rechtsgutachten mit einer signaturrechtlichen Bewertung elektronischer Verwaltungsprozesse erstellt. Zusammen mit der Landeshauptstadt habe ich eine Gefahren- und Risikoanalyse und ein

Datensicherheitskonzept erarbeitet. Dabei wurden die erforderlichen technischen und organisatorischen Maßnahmen festgelegt und ein Vorschlag für den elektronischen Rechtsverkehr (Sicherungsinfrastruktur digitaler Signaturverfahren) erarbeitet. Im Projekt wurden folgende Datenschutzgrundsätze verwirklicht:

- es werden nur erforderliche Daten gespeichert,
- die Speicherung erfolgt nicht länger als nötig,
- personenbezogene Daten werden nicht für andere Zwecke genutzt,
- Cookies werden nur sparsam verwendet und nach Ende der Kommunikation gelöscht,
- es werden sichere Verbindungen aufgebaut,
- es wird eine anonyme Bezahlmöglichkeit mit der Geldkarte ermöglicht.

Das hannoversche Verfahren der einfachen Meldeauskunft hat sich im Echteinsatz bewährt.

7.6.2 Windows 2000

Windows 2000 ist mit einer Reihe technischer Neuerungen ausgestattet, die sowohl die Administration als auch die Sicherheit des Betriebssystems deutlich verändern. Neue Sicherheitsfunktionen sind die Authentisierung im Netzwerk mittels des Kerberos-Protokolls, die gesicherte Datenübermittlung mit IPSec und die verschlüsselte Datenspeicherung mit Encrypted File System (EFS). Die bisher aus Windows NT bekannten Benutzerrichtlinien wurden durch Gruppenrichtlinien ersetzt, die weitaus differenziertere und umfassendere Steuerungsmöglichkeiten erlauben. Zudem lässt Windows 2000 eine verbesserte Delegation von administrativen Rechten zu. Die für Administratoren auffälligste Neuerung in Windows 2000 Server ist der Active Directory Service (ADS). Hierbei handelt es sich um einen Verzeichnisdienst, der domänenübergreifend alle Benutzerkonten, Gruppenkonten und Ressourcen in einer Datenbank speichert. Diese Daten können dann unternehmens- bzw. behördenweit zur Verfügung gestellt werden. Das Active Directory (AD) stellt verschiedene Domänenmodelle bereit, die die unterschiedlichen Anforderungen der Unternehmen und Behörden berücksichtigen sollen. Dabei kann die Ausprägung eines AD von einem Einzeldomänenmodell, das mit der bisher von Windows NT bekannten Domäne gleichgesetzt werden kann, bis zu einem so genannten Forest mit hierarchisch strukturierten Domänenbäumen reichen. Entscheidend ist die Organisationsstruktur des Unternehmens oder der Behörde, die das AD einsetzen will.

Mit der Einführung von Windows 2000 in der niedersächsischen Landesverwaltung wurde auch die Planung eines landesweiten neuen Verzeichnisdienst begonnen. Eine Arbeitsgruppe des IMA-IuK, an der ich aktiv mitgearbeitet habe, hat die Auswirkungen untersucht und notwendigen technischen und organisatorischen Maßnahmen beschrieben. Durch Installation einer so genannten Stamm-Domäne (Root-Domäne) wurde ein zentraler Ausgangspunkt für ein ressortübergreifendes AD geschaffen. Unterhalb dieser Root-Domäne können dann die Ressorts sowie deren nachgeordneter Bereich in die Struktur eingefügt werden. Aus datenschutzrechtlicher Sicht wirft dieser Ansatz mehrere Probleme auf, die wirksam gelöst werden müssen.

In der Root-Domäne wird automatisch ein so genannter Organisations-Administrator (Enterprise-Administrator) eingerichtet. Der Enterprise-Administrator hat Zugriff auf alle Domänen-Controller des Forest und kann Besitz über alle Elemente des Forest übernehmen. Diese weitreichenden Befugnisse können durch verschiedene organisatorische oder technische Lösungen eingeschränkt werden. Eine organisatorische Möglichkeit besteht darin, einer möglichst kleinen Anzahl ausgewählter Administratoren den Zugriff auf das Konto des Enterprise-Administrators nach dem Vier-Augen-Prinzip (geteiltes Kennwort) zu erlauben. Technisch ist es zudem möglich, die Gruppe der Enterprise-Administratoren aus einer Mitgliedsdomäne in einem AD auszuschließen. Dies hat aber Funktionseinschränkungen zur Folge und sollte im Vorfeld unbedingt getestet werden. Zudem muss bei Änderungen am globalen Schema des AD der Ausschluss temporär rückgängig gemacht werden, was einen erhöhten administrativen Aufwand bedeutet. Inwieweit eine vollständige Abschottung von Domänen gegeneinander erforderlich und organisatorisch sinnvoll ist, liegt in der Entscheidung der Dienststelle. Bei Planung und Implementierung eines AD sollte jedoch beachtet werden, dass vollständig abgeschottete Bereiche nur durch die Einrichtung verschiedener Forests oder durch Domänen, die nicht in einer Baumstruktur zusammengefasst werden, gebildet werden können. Der technisch realisierte Ausschluss der Enterprise-Administratoren muss sich erst in langzeitigen Tests als praktikabel erweisen, um eine Alternative darzustellen.

7.6.3 Mobiles Arbeiten

Im Rahmen des Projektes „Mobiles Arbeiten“ habe ich einen datenschutzgerechten ortsfesten Arbeitsplatz Zuhause bei einer Mitarbeiterin eingerichtet. Dem Konzept dieses externen Arbeitsplatzes lagen die Empfehlungen für Telearbeitsplätze des Landes Niedersachsen zugrunde. Zur Verbesserung der Datensicherheit und des Bedienerkomforts wurde die Anbindung jedoch unter Zuhilfenahme der Terminal-Server-Technik realisiert. Dieses Konzept basiert auf der Überlegung, an dem externen Arbeitsplatz lediglich Technik für die Darstellung und Bedienung des Systems bereitszustellen, während die Verarbeitungskomponenten und damit auch die Daten im geschützten Umfeld der Geschäftsstelle verbleiben.

Zur Umsetzung dieses Konzepts wurde nach umfangreicher Recherche für den externen Arbeitsplatz ein Thin-Client der Fa. Igel beschafft, der sowohl die Darstellung übernimmt als auch die Eingabe der Bedienungsfunktionen realisiert. Daneben ist es möglich, über diesen Thin-Client lokale Druckausgaben zu erzeugen. Die Verarbeitungskomponenten befinden sich hingegen im geschützten Bereich des Geschäftsstelle auf einem speziellen Server, dem Terminal-Server.

Über diese Konstruktion ist es möglich, für die Mitarbeiterin an dem externen Arbeitsplatz identische Arbeitsbedingungen zu erzeugen, wie sie auch in der Geschäftsstelle an den lokalen Systemen herrschen. Aufgrund dieser Konstellation ist ein zusätzlicher Schulungsaufwand weitestgehend entbehrlich, und der Mitarbeiterin bleibt an ihren Präsenztagen eine ständige Umstellung erspart. Darüber hinaus stellt sich diese Konzeption aus datenschutzrechtlicher und organisatorischer Sicht als erhebliche Verbesserung heraus, da die Daten den geschützten Bereich der Geschäftsstelle nicht verlassen. Während einer Bearbeitung vom häuslichen Arbeitsplatz aus werden

lediglich Steuerungs- und Bildinformationen über öffentliche Netze übertragen; die Übertragung erfolgt generell verschlüsselt. Der Zugriff auf die im lokalen Netz verfügbaren Informationen wird über eine geeignete Firewall-Konfiguration geregelt; Restrisiken lassen sich auf diesem Wege erfolgreich beherrschen.

Die Erfahrungen aus diesem Projekt sind in unsere Orientierungshilfe „Datenschutzgerechte Telearbeit“ eingeflossen; als nächster Schritt in unserem Projekt „mobiles Arbeiten“ ist die datenschutzgerechte Anbindungen für örtlich ungebundene Arbeitsplätze vorgesehen, also für Zugriffe vom Besprechungszimmer, vom Konferenzort, von unterwegs auf Dienstreisen oder von zu Hause aus. Über Ergebnisse werden wir in Zukunft zeitnah informieren.

7.6.4 Automatisierte Personalverwaltung

Das Land Niedersachsen ist gegenwärtig dabei, ein automatisiertes Personalmanagementverfahren für seine annähernd 200 000 Landesbedienstete einzuführen. In der Arbeitsgruppe des Landes zur Pilotierung habe ich aktiv mitgearbeitet (vgl. Kapitel 9.2). Eine Vorabkontrolle der Grundfunktionen schreibt Datenschutzleitplanken für das Projekt fest. Die Pilotierung ist bis 2004 vorgesehen. Bis Ende 2006 soll der vollständige Roll-out erfolgen. Meine Beteiligung in der Koordinierungsgruppe bleibt auch in der Einführungsphase erhalten. Dabei werde ich auf Fortschreibung der Vorabkontrolle nach endgültiger Festlegung weitere Funktionen dringen.

8 Tele- und Mediendienste

8.1 Neue Rechtsvorschriften

Mit dem Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz - EGG - vom 14.12.2001; BGBl. I 3721) in Verbindung mit dem neuen Bundesdatenschutz vom 18.05.2001 (BGBl. I 904) wurde der Rechtsrahmen für die Verarbeitung personenbezogener Daten im Internet weiterentwickelt. Das EGG enthält wesentliche Änderungen des Teledienstgesetzes (TDG) und des Teledienstedatenschutzgesetzes (TDDSG). Einige Bestimmungen des alten TDDSG konnten gestrichen werden, da sie Eingang in das BDSG gefunden haben. Auch die Länder sind um Neuordnung bemüht; sie haben inzwischen die Datenschutzvorschriften des Mediendienste-Staatsvertrages angepasst. Die wichtigsten Änderungen des Rechtsrahmens sollen hier kurz vorgestellt werden:

- Bei geschäftsmäßigen Telediensten sind neben Name und Anschrift der Verantwortlichen auch Registernummer des Handels-, Vereins- oder Genossenschaftsregisters, bei freien Berufen Kammerzugehörigkeiten und Berufsbezeichnungen, ferner gegebenenfalls Umsatzsteueridentifikationsnummern anzugeben (§ 6 TDG). Damit soll eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation ermöglicht werden. Kommerzielle Angebote sind eindeutig als solche zu kennzeichnen. Damit sind die Informations- und Kennzeichnungspflichten für Diensteanbieter ausgeweitet worden.

- Die Verantwortlichkeiten für die angebotenen Informationen wurden neu geregelt (§§ 8 bis 11 TDG).
- Betroffene haben ein Widerspruchsrecht, wenn Nutzungsdaten zur Erstellung von Profilen verwendet werden sollen (§ 6 Abs. 3 TDDSG).
- Diensteanbietern ist es gestattet, Abrechnungsdaten auch für die Aufklärung missbräuchlicher Inanspruchnahme ihrer Dienste zu nutzen, wenn tatsächliche Anhaltspunkte für einen entsprechenden Missbrauchsfall vorliegen (§ 6 Abs. 8 TDDSG).
- Verstöße gegen das TDDSG können mit einer Geldbuße bis zu 50 000 € geahndet werden (§ 9 TDDSG).

Doch bei aller Zufriedenheit über die weiterentwickelten Rechtsvorschriften bleibt angesichts des weltweiten Internets die traurige Erkenntnis, dass diese länderspezifischen Regelungen nur bedingt dem Datenschutz nutzen. Es fehlen nach wie vor internationale Festlegungen über Mindeststandards, um die Interessen von wirtschaftlicher Nutzung und individuellem Schutz angemessen auszugleichen.

8.2 Eine harmonisierte Medienordnung tut Not

Datenschutzexperten sind sich einig, dass das Datenschutzrecht im Bereich der elektronischen Medien (Teledienste, Mediendienste, Rundfunk) in einer neuen Medienordnung zusammengeführt werden sollte, damit die materiell-rechtlichen Bestimmungen von Providern und ihren Kunden überhaupt gefunden, gelesen und verstanden werden können. Gefordert wird die Weiterentwicklung des Fernmeldegeheimnisses zu einem Mediennutzungsgeheimnis sowie eine Vereinfachung und Vereinheitlichung der datenschutzrechtlichen Anforderungen. Angesichts der schnellen 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 Mediennutzung ein angemessen hoher Schutz gewährleistet werden.

Auch die unterschiedlichen und für die Betroffenen verwirrenden Aufsichtsstrukturen stehen bei einer neuen Medienordnung auf dem Prüfstand. Während die Datenschutzaufsichtsbehörden der Länder für Beibehaltung bewährter Strukturen und die Dienste-Betreiber für Instrumente zur Selbstkontrolle eintreten, gab es Stimmen für eine Aufsichts-Bündelung, zum Beispiel beim Bundesbeauftragten für den Datenschutz. „Wie so oft im Leben“ liegt die richtige Lösung in der Mitte. Schon jetzt können Berufsverbände Verhaltensregeln zur Förderung datenschutzgerechter Lösungen entwickeln und mit den zuständigen Aufsichtsbehörden abstimmen. Solche selbst festgelegten Verhaltensregeln ersetzen aber nicht etwa die notwendige Aufsicht, sondern ergänzen und vereinfachen sie. Gegen den Vorschlag einer zentralen Aufsicht spricht, dass damit eine Aufspaltung der Aufsichtskompetenz für den Datenschutz bei Online- und Offline-Geschäften (etwa im Versandhandel) eintreten würde, die für die praktische Handhabung der Aufsicht erhebliche Umsetzungsprobleme mit sich bringen würde, und die fehlende Serviceorientierung einer weit entfernten Bundesaufsicht. Ich begrüße den Vorschlag zahlreicher Bundestagsabgeordneten im Antrag „Reform der Medien- und Kommunikationsordnung für die Wissens- und Informationsgesellschaft“ (BT-Drs. 14/8649), der die Aufforderung zur stärkeren Zu-

sammenarbeit der Länderaufsichtsbehörden mit den für den Bereich der Information und Kommunikation zuständigen Bundesbehörden enthält. „Es ist zu prüfen, ob und in welcher Form eine institutionalisierte Plattform zur Koordination eingerichtet werden kann“, steht im Koalitionsvertrag der neuen Bundesregierung unter den Vereinbarungen zur Medienpolitik.

Ein erster Arbeitsentwurf für ein „Gesetz über den Datenschutz bei der Nutzung elektronischer Medien“ (Elektronische-Medien-Datenschutzgesetz - EMDSG), der die Forderungen der Datenschutzbeauftragten zur Harmonisierung weitestgehend aufgreift, liegt inzwischen vor. Der Entwurf bestätigt ausdrücklich die Kontrollzuständigkeit der Aufsichtsbehörden im jeweiligen Niederlassungsland, enthält aber auch Regelungen zur Schaffung von Einrichtungen der freiwilligen Selbstkontrolle. Nach den Vorstellungen des Entwurfs soll die freiwillige Selbstkontrolle der staatlichen Aufsicht insoweit vorgehen, als die Aufsichtsbehörde eigene Maßnahmen gegenüber einem Anbieter, der einer Einrichtung der freiwilligen Selbstkontrolle angehört, nur noch durchführen darf, wenn die Einrichtung der freiwilligen Selbstkontrolle trotz ausdrücklicher Aufforderung untätig bleibt oder die von ihr getroffenen Maßnahmen von der Aufsichtsbehörde für rechtlich nicht vertretbar gehalten werden. Dieser Regelungsansatz geht aus meiner Sicht zu weit und überzeichnet die sinnvollen Möglichkeiten einer Selbstregulierung. Es muss gerade auch zum Schutz der Nutzerinteressen bei den massenhaften Anwendungen im Bereich der elektronischen Medien weiterhin die Möglichkeit schnell wirkender Interventionen einer unabhängigen staatlichen Aufsichtsinstanz geben und nicht nur deren nachgeschaltetes und ersatzweises Agieren gewissermaßen aus der zweiten Reihe. Auch bei anderen, in dem Entwurf vorgeschlagenen Regelungen, etwa zu der dem Bundesbeauftragten für den Datenschutz zugewiesenen neuen Aufgabe, im Benehmen mit den Datenschutzbehörden der Länder auf eine einheitliche Ausführung der Vorschriften des Gesetzes hinzuwirken, sehe ich noch erheblichen Diskussionsbedarf.

8.3 Internet am Arbeitsplatz

Neben den gängigen Kommunikationsverbindungen Telefon und Fax gehört ein eigener Internetanschluss mittlerweile in der privaten Wirtschaft und in der öffentlichen Verwaltung zur unverzichtbaren und fast schon selbstverständlichen Mindestausstattung eines Arbeitsplatzes. So verfügen in Niedersachsen über das iznNet mehr als 50 000 Bedienstete der unmittelbaren Landesverwaltung über einen eigenen Zugang zum Internet nebst persönlicher E-Mail-Adresse. Den Beschäftigten wird die Nutzung des Internet vielfach ausschließlich zu dienstlichen oder betrieblichen Zwecken, teils aber ausdrücklich oder im Rahmen einer so genannten „betrieblichen Übung“ auch zu privaten Zwecken gestattet.

Nach einer Umfrage der Zeitschrift Capital aus dem September 2001 war es den Beschäftigten großer Firmen, so etwa Siemens, Deutsche Post World Net oder Bertelsmann, untersagt, das Internet zu privaten Zwecken zu nutzen. Ausgehende E-Mails wurden grundsätzlich nur von 13 % der befragten Unternehmen kontrolliert. Veröffentlichungen in den Medien und die in meiner Geschäftsstelle aus dem Kreis der betroffenen Beschäftigten und Mitarbeitervertretungen eingehenden Anfragen

lassen jedoch vermuten, dass die Betriebe und Dienststellen vermehrt dazu übergehen, die Surfgewohnheiten der Beschäftigten zu kontrollieren.

Die Motive der Arbeitgeber und Dienststellen für eine Überprüfung sind vielfältig. Sie erfolgen teils gezielt auf entsprechende Hinweise der Systemadministration, aus Anlass von Beschwerden einzelner Beschäftigter über die Zusendung „unerwünschter“ E-Mails oder flächendeckend allein aus dem Interesse, Erkenntnisse über die Art und Weise sowie den Umfang der Internutzung zu gewinnen und unnötige Kosten zu sparen. Auf die in der Öffentlichkeit und im politischen Raum kontrovers erörterten Ergebnisse der Prüfung des Niedersächsischen Landesrechnungshofs, der auf der Grundlage einer Auswertung der beim Informatikzentrum Niedersachsen gespeicherten Protokolldaten davon ausgeht, dass der Umfang der privaten Internetrecherchen der Bediensteten erheblich ist, weise ich in diesem Zusammenhang hin.

Die bei mir eingehenden Anfragen zeigen auch, dass vielfach große Unsicherheit bestehen, welche Daten bei der Nutzung von Internet und E-Mail überhaupt protokolliert werden dürfen und unter welchen Voraussetzungen es zulässig ist, Protokolldaten zum Zwecke der Überwachung des Nutzerverhaltens auszuwerten. Viele meinen, es sei schon aufgrund der gesetzlichen Zweckbindung verboten, personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, für andere Zwecke, etwa zur Verhaltens- und Leistungskontrolle der Beschäftigten, zu verwenden (vgl. § 31 BDSG, § 10 Abs. 4 NDSG, § 101 Abs. 6 NBG). Es sei daher nicht zulässig, Abmahnungen, Kündigungen oder sonstige dienst- und arbeitsrechtliche Maßnahmen wegen unerlaubter Internetnutzungen auf die einem Verwertungsverbot unterliegenden Protokolldaten zu stützen. Außerdem stehe auch das Fernmeldegeheimnis aus Art. 10 GG einer Kontrolle der Internutzung entgegen. Die derzeitige Rechtslage ist sehr kompliziert, sodass schon von daher Anlass besteht, eindeutige gesetzliche Regelungen in einem von mir und anderen Datenschützern seit längerem eingeforderten Arbeitnehmerdatenschutzgesetz zu schaffen.

Vielfach ist den Beschäftigten und den Mitarbeitervertretungen nicht bekannt, welche Protokolldaten überhaupt durch die zuständige Systemadministration zum Zwecke der Datensicherung und des ordnungsgemäßen Betriebs der Datenverarbeitungsanlage erhoben und gespeichert werden und auf welche Weise Rückschlüsse auf das Nutzerverhalten gezogen werden können.

Viele Unternehmen oder Behörden betreiben Proxyserver oder Firewall-Systeme, um ihre internen Netzwerke gegen Angriffe von außen zu schützen. Die eingesetzten Firewall- und Proxyserver sind in der Lage, verschiedene Arten von Daten zu erfassen und zu speichern. Zu unterscheiden sind dabei Bestands-, Verbindungs-, Nutzungs- und Inhaltsdaten, die durch das Surfen entstehen. Eine Protokollierung ist grundsätzlich auf allen Firewall- und Proxyservern möglich. Die Protokolldateien enthalten alle Anfragen an den zentralen Proxyserver mit Datum, Uhrzeit, aufgerufener Internetadresse (URL), Größe des angefragten Objekts, Zeit für die Beantwortung der Anfrage, Informationen zu Übertragungsmethoden und Zugriffswege sowie die IP-

Adresse des Netzes oder des Rechner aus der die Anfrage kam. Da die IP-Adresse oftmals einem bestimmten Arbeitsplatz-PC zugeordnet werden kann und am Arbeitsplatz-PC ermittelt werden kann, wer zur fraglichen Zeit angemeldet war, kann ein Personenbezug hergestellt werden.

Bei der Beantwortung der Frage, ob und unter welchen Voraussetzungen der Arbeitgeber berechtigt ist, Kontrollen der Internetnutzung durchzuführen, ist von entscheidender Bedeutung, ob das Internet durch die Beschäftigten ausschließlich zu dienstlichen oder betrieblichen Zwecken oder darüber hinaus auch zum privaten Gebrauch genutzt werden darf. Abhängig von den jeweiligen Gegebenheiten und Nutzungsbedingungen vor Ort sind bei der Bewertung der Rechtslage die unterschiedlichsten Rechtsvorschriften aus dem Bereich des Tele- und Mediendiensterechts, des allgemeinen Datenschutzrechts oder des Dienst- und Arbeitsrechts zu berücksichtigen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung die an eine datenschutzgerechte Internet-Nutzung zu stellenden Anforderungen beschrieben. Darüber hinaus hat der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz“ zu diesem Thema detaillierte Hinweise veröffentlicht. Die Orientierungshilfe kann unter „Home/Service/Empfehlungen Recht/Internutzung“ aus meinen Internetangebot herunter geladen oder dort eingesehen werden (siehe auch Anlage 21). Ich empfehle, die folgenden Leitplanken einzuhalten:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internet am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.

2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.

3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.

4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.

5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.

6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.

7. Die gleichen Bedingungen wie bei der Nutzung des Internet müssen prinzipiell bei der Nutzung von Intranets gelten.

Arbeitgeber sind befugt, bei ausschließlich dienstlicher oder betrieblicher Nutzung die Protokolldaten stichprobenartig oder bei Verdacht auf Missbrauch auszuwerten. Die besondere Zweckbindung der Protokolldaten steht in diesen Fällen einer Nutzung zu Kontrollzwecken nicht entgegen. Ich empfehle, eine Dienst- oder Betriebsvereinbarung über die Nutzung von Internet und E-Mail abzuschließen, in der die Nutzungsbedingungen und insbesondere auch die Protokollierung und Auswertung zu Kontrollzwecken eindeutig und zweifelsfrei geregelt sind.

8.4 Briefwahlunterlagen über das Internet - sicher?

Zur Bundestagswahl 2002 konnten Wähler, die am Wahltag verhindert waren, die Briefwahlunterlagen bei vielen Kommunen erstmals neben dem bislang üblichen schriftlichen Antragsverfahren per Post oder Fax auch elektronisch per E-Mail anfordern.

Der für die Bundestagswahlen zuständige Bundeswahlleiter hat für dieses Verfahren gefordert, zur Authentifizierung der Wahlberechtigten neben Namen und Anschrift auch das Geburtsdatum und die auf der Wahlbenachrichtigungskarte enthaltene Nummer des Wählerverzeichnisses vom Antragsteller zu erfragen. Mit dem erweiterten Datenkatalog stellte sich die Frage der sicheren und vertraulichen Kommunikation. Dies gilt auch für die persönlichen Angaben zu den Gründen für die Inanspruchnahme der Briefwahl. Unverschlüsselte E-Mails bieten - wie offene Postkarten - vielfältige Angriffsmöglichkeiten für Verletzungen der Vertraulichkeit von Daten; sie können eingesehen, verändert und verfälscht werden.

Den niedersächsischen Kommunen habe ich in Übereinstimmung mit dem Landeswahlleiter empfohlen, den Wählern bei Anwendung dieses neuen Internet-Dienstes ein verschlüsseltes Antragsverfahren anzubieten. Einige niedersächsische Kommunen haben dies bereits mit Erfolg praktiziert. Bei den im kommenden Februar stattfindenden Wahlen zum Niedersächsischen Landtag sollte diese datenschutzfreundliche Lösung allen Wählern zur Verfügung stehen. Entsprechende Formulardienste stehen im Internet zur Verfügung.

8.5 Ratsprotokolle im Internet

In einer Vielzahl niedersächsischer Kommunen wird der kommunale Sitzungsdienst mittlerweile über Ratsinformationssysteme gesteuert, die es der Verwaltung und den Ratsmitgliedern ermöglichen, sich zeitnah über Beschlussvorlagen und sonstige

Vorgänge zu informieren. Im Rahmen von eGovernment-Anwendungen wird darüber hinaus den Bürgern die Möglichkeit eröffnet, sich per Internet über das kommunale Geschehen zu informieren. Derartige Systeme dienen einerseits der Steigerung der Effizienz der Aufgabenerledigung und erhöhen andererseits gleichzeitig auch die Transparenz der Entscheidungsfindung. Zu der von Kommunen und Ratsmitgliedern im Zusammenhang mit der Einführung von Ratsinformationssystemen an mich herangetragenen Fragestellung, ob es zulässig sei, Niederschriften der öffentlichen Rats- oder Ausschusssitzungen in das Internet einzustellen, habe ich mich wie folgt geäußert:

Datenschutzrechtlich ist die Einsichtnahme in personenbezogene Daten aus Niederschriften öffentlicher Sitzungen über das Internet als Abruf aus Datenbeständen, die jeder Person offen stehen oder deren Inhalt veröffentlicht werden darf, zu bewerten. Gemäß § 12 Abs. 5 des Niedersächsischen Datenschutzgesetzes (NDSG) finden bei einem Abruf aus solchen Datenbeständen die Regelungen des § 12 Abs. 1 bis 4 NDSG über die Zulässigkeit der Einrichtung und Ausgestaltung automatisierter Abrufverfahren keine Anwendung.

Die Veröffentlichung von Niederschriften der öffentlichen Sitzungen der Räte und Ausschüsse im Internet ist nach meiner Auffassung auch ohne vorherige Einwilligung der Betroffenen grundsätzlich zulässig. Dies gilt aber nur dann, wenn eine Einsichtnahme nach Maßgabe der kommunalverfassungsrechtlichen Vorschriften erfolgen kann und die Niederschriften auf der Grundlage einer entsprechenden Beschlussfassung des Rates auch in sonstiger Weise veröffentlicht werden dürften. Die Niederschriften dürfen nur solche Informationen enthalten, die jedermann zugänglich gemacht werden können. Letztlich bleibt es also dem Rat überlassen, darüber zu entscheiden, ob er es im Sinne der Bürgerfreundlichkeit, zur Verbesserung der Information und Erhöhung der Transparenz für angezeigt hält, die Niederschriften öffentlicher Sitzungen in das Internet einzustellen.

Da moderne Informations- und Kommunikationstechniken vielfältige Möglichkeiten bieten, personenbezogene Daten zielgerichtet auszuwerten und zu verarbeiten, kann sich eine Gefährdung des Rechts auf informationelle Selbstbestimmung aus einer möglichen Verknüpfung von Angaben einzelner Personen mit Informationen aus anderen Datenbeständen ergeben. Hierdurch könnten weitgehende Persönlichkeitsprofile entstehen. Aus datenschutzrechtlicher Sicht halte ich es daher für erforderlich, die zur Veröffentlichung über das Internet vorgesehenen Niederschriften datenschutzgerecht zu gestalten, d.h. personenbezogene Angaben nur dann in die Niederschriften aufzunehmen, wenn dies im Einzelfall zur Dokumentierung des Beschlusses erforderlich ist. So sollte in der Regel davon abgesehen werden, Wortprotokolle und Protokollierungen des Abstimmungsverhaltens einzelner Ratsfrauen oder Ratsherren in das Internet einzustellen.

8.6 Einzelfragen bei Tele- und Mediendiensten

8.6.1 Verarbeitung personenbezogener Daten durch Internet-Provider

Bei der Nutzung von Internetdiensten fallen bei Diensteanbietern eine Fülle personenbezogener Daten an. Dies ist zum einen technisch bedingt, da die bei einer Kommunikation über das Internet beteiligten Rechner durch Internetprotokoll-Adressen (IP-Adresse) identifiziert werden. Ein Teil der Daten ergibt sich aus der Vertragsvereinbarung zwischen Anbieter und Nutzer. Für die Leistungserbringung sind Bestandsdaten erforderlich, für die Abrechnung werden Verbindungs- und Nutzungsdaten benötigt. All diese Daten geben Auskunft über den Internet-Nutzer und sein individuelles Nutzungsverhalten.

Die Rechtsgrundlagen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Internetnutzern ergeben sich aus dem Teledienstedatenschutzgesetz (TDDSG) und aus dem Mediendienste-Staatsvertrag (MDStV). Die Vermittlung des Zugangs zum Internet (access providing) und E-Mail-Dienste sind Telekommunikatonsdienste, für die das Telekommunikationsgesetz (TKG) und die Telekommunikations-Datenschutzverordnung (TDSV) beachtet werden müssen. Diese Zuordnung soll künftig gesetzlich festgeschrieben werden.

Bei der Beurteilung der Zulässigkeit der Datenerhebung, Verarbeitung und Nutzung ist der Grundsatz der Datenvermeidung und Datensparsamkeit nach § 3a Bundesdatenschutzgesetz (BDSG) zu beachten. Über die in diesen Vorschriften enthaltenen gesetzlichen Befugnisse hinaus dürfen keine Daten erhoben und verarbeitet werden, es sei denn, eine andere gesetzliche Regelung lässt dies ausdrücklich zu. Soweit eine staatliche Stelle die Herausgabe von personenbezogener Daten bzw. die Überwachung eines E-Mail-Anschlusses verlangt, muss sie gegenüber dem Diensteanbieter die Rechtsgrundlage ihrer Forderung darlegen und gegebenenfalls notwendige richterliche Anordnungen beibringen. Der Diensteanbieter hat sich von der Einhaltung der formalen Anforderungen an eine entsprechende Maßnahme zu vergewissern, einer Verpflichtung zur inhaltlichen Prüfung der entsprechenden Anordnungen unterliegt er jedoch grundsätzlich nicht. Gegenüber Strafverfolgungsbehörden ist er verpflichtet, entsprechende Anordnungen zur Überwachung umzusetzen; dagegen ist er gegenüber Nachrichtendiensten unter den gesetzlichen Voraussetzungen zur Auskunft berechtigt, aber nicht verpflichtet.

Über den datenschutzgerechten Umgang mit personenbezogenen Daten durch Anbieter von Internetdiensten und über die Befugnisse zur staatlichen Überwachung klärt eine neu erstellte, sehr ausführliche Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder auf, die noch mit dem Düsseldorfer Kreis als Koordinierungsgremium für den nicht öffentlichen Bereich abgestimmt wird. Sie ist in meinem Internet-Angebot unter Service/Checklisten/Tele- und Mediendienste abrufbar.

8.6.2 Befugnisse von Strafverfolgungsbehörden zur Internet-Überwachung

Verbindungs- und Nutzungsdaten der Telekommunikation unterliegen dem Fernmeldegeheimnis. Polizei, Strafverfolgungsbehörden und Geheimdienste dürfen auf diese Daten nur auf Grund einer ausdrücklichen gesetzlichen Befugnis zugreifen. Eine generelle Verpflichtung der Tele- und Mediendiensteanbieter zur Speicherung dieser Daten für eine mögliche spätere Strafverfolgung besteht gegenwärtig nicht, sie würde zu einer unzulässigen Vorratsspeicherung führen. Das Bundesverfassungsgericht hat wiederholt festgestellt, dass die Speicherung personenbezogener Daten nicht zu einer Rundumbeobachtung der Bürger führen darf. Das wäre aber im Bereich der Internetnutzung der Fall. Dieses Verfahren würde den mit den Vorschriften über Tele- und Mediendienste normierten Datenschutz in unvertretbarer Weise abbauen.

Rechtsgrundlage für die Überwachung von Inhalten sind §§ 100a ff. StPO, § 39 Außenwirtschaftsgesetz (AWG) und das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10). Die Anordnung nach § 100a und § 100b StPO darf nur durch den Richter oder bei Gefahr im Verzuge - für die ersten drei Tage - auch durch die Staatsanwaltschaft, nicht aber durch deren Hilfsbeamte getroffen werden. Die angeordneten Maßnahmen berechtigen die Überwachung zukünftiger Telekommunikationsvorgänge und enthalten auch die Verpflichtung für den Diensteanbieter, die entsprechenden E-Mails einschließlich der Verbindungsdaten zu speichern bzw. an die zuständige Strafverfolgungsbehörde herauszugeben. Nach der Rechtsprechung des BGH stellt ein Zugriff von Strafverfolgungsbehörden auf Inhalte von E-Mail-Postfächern ebenfalls eine Telekommunikationsüberwachung dar. Das Eindringen in E-Mail-Systeme kann nicht auf die strafprozessualen Befugnisse zur Beschlagnahme von Gegenständen oder zur Durchsuchung von Räumen gestützt werden, insbesondere weil der Zugriff anders als bei den vorgenannten Maßnahmen im Regelfall geheim ist und auch die zukünftige Kommunikation umfasst. Die am 24. Oktober 2001 beschlossene Telekommunikations-Überwachungsverordnung (TKÜV) verpflichtet auch die Anbieter von E-Mail-Diensten (nicht jedoch sonstige Internet Service Provider und Access Provider) zur Bereitstellung technischer Möglichkeiten zur Überwachung der E-Mail-Kommunikation, die über die Kennungen abgewickelt wird, auf die sich die Überwachungsanordnung bezieht. Nutzungsdaten und die über das Internet kommunizierten Inhalte werden ebenfalls durch das Fernmeldegeheimnis (Art. 10 GG) geschützt, weil Tele- und Mediendienste auf Basis von Telekommunikationsdiensten abgewickelt werden und es sich deshalb um Inhalte der Telekommunikation handelt. Diese Daten dürfen grundsätzlich nur gemäß § 100a und § 100b StPO herausgegeben werden.

8.6.3 Recht auf unbeobachtete Kommunikation in Gefahr

Der Bundesrat hat am 31. Mai 2002 einen Gesetzentwurf auf den Weg gebracht, der die Telekommunikationsunternehmen und Internetprovider verpflichten soll, alle Daten über die Kunden und Nutzer zu speichern und für etwaige Anfragen der Polizei- und Geheimdienstbehörden bereitzuhalten. Es genügt den Initiatoren offenbar nicht mehr, unter bestimmten Bedingungen auf vorhandene Informationen zuzugreifen. Nun soll sogar dafür gesorgt werden, dass das Kommunikationsverhalten aller Bürger jederzeit nachvollziehbar aufgezeichnet wird. Die Verfechter des Gesetzesvorschlages bezeichnen ihr Vorhaben ganz offen und

ges bezeichnen ihr Vorhaben ganz offen und bedenkenlos als “Vorratsspeicherung”. Dabei steht “Vorratsspeicherung“ in der Rechtsprechung des Bundesverfassungsgerichts seit fast 20 Jahren als Synonym für eine verfassungswidrige staatliche Sammelwut.

Nachdem bereits mehrere Vorstöße im Bundesrat, Mindestspeicherfristen für die Internet- und Telekommunikationsnutzung einzuführen, gescheitert waren, ging man im Bundesrat aufs Ganze: Nicht nur zur Strafverfolgung, sondern für die Erfüllung sämtlicher Aufgaben von Polizei, Verfassungsschutz, Bundesnachrichtendienst, Militärischem Abschirmdienst und Zollkriminalamt sollen die ins Blaue hinein gesammelten Verbindungs-, Nutzungs-, Bestands- und Abrechnungsdaten von Millionen rechtstreuer Bürger genutzt werden können. Diese Forderung lässt sich vergleichen mit einer Verpflichtung der Post, sämtliche Absender- und Empfängerangaben im Briefverkehr für Zwecke einer möglichen späteren Strafverfolgung zu speichern und für den Zugriff der Sicherheitsbehörden bereitzuhalten. Der Versuch, das Internet für Zwecke der Strafverfolgung in ein Fahndungsnetz zu verwandeln, ist ungeeignet und unangemessen. Die bestehenden Befugnisse der Strafverfolgungsbehörden gewährleisten schon jetzt eine effektive Strafverfolgung im Internet. Es ist den Providern ohne weiteres technisch möglich, IP-Adressen ab dem Zeitpunkt eines entsprechenden richterlichen Beschlusses oder - bei Gefahr im Verzug - einer staatsanwaltlichen Anordnung vorzuhalten. Eine ständige Internet-Überwachung wäre zudem zur Verfolgung von schweren Straftaten untauglich, weil Straftäter ohne größere technische Schwierigkeiten auf Provider in anderen Ländern ausweichen könnten, für die derartige Verpflichtungen nicht bestehen. Der Antrag des Bundesrates ist durch den zwischenzeitlichen Ablauf der Legislaturperiode des Bundestages vorerst erledigt, es dürfte aber auch in der neuen Legislaturperiode wieder zu ähnlichen Vorstößen kommen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen Forderungen nach einer solchen generellen Protokollierungs- und Aufbewahrungspflicht bei der Internetnutzung ab (siehe auch Entschließung der 61. DSB-Konferenz „Datenschutz bei der Bekämpfung von Datennetzkriminalität“ - Anlage 4 -, Entschließung der 63. DSB-Konferenz „Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten“ - Anlage 22 -, Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24. Mai 2002 „Geplanter Identifikationszwang in der Telekommunikation“ - Anlage 23 -, Entschließung der 64. DSB-Konferenz „zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet“ - Anlage 25 -).

Wer plant, jeden Klick im Internet, jede E-Mail, jede Pager-Nachricht und jede SMS aufzuzeichnen und die Möglichkeit der Auswertung durch Polizei und Geheimdienste zu schaffen, der legt das Fundament für eine Gedankenpolizei.

8.6.4 Verschlüsselung von Informationen

Die derzeitige Rechtslage verpflichtet die Diensteanbieter dazu, durch technische und organisatorische Vorkehrungen sicherzustellen, dass die Nutzer Informations- und Kommunikationsdienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen

können (§ 4 Abs. 2 Nr. 3 Teledienstedatenschutzgesetz und § 13 Abs. 2 Nr. 3 Mediendienstestaatsvertrag). Ich beobachte aufmerksam die Marktsituation und gebe Empfehlungen über datenschutzfreundliche Lösungen.

8.6.5 Rechtsverbindlichkeit im Internet

Ein weiteres Problem im Internet stellt die noch immer mangelnde Rechtsverbindlichkeit dar. Es ist nicht sicher, dass Informationen, wie etwa Vertragsangebote von Privaten oder Anträge an Behörden auch von denjenigen stammen, die in ihr als Absender bezeichnet sind. Nachrichten können auf ihrem Weg durch das Internet viele Stationen passieren, an denen man sie abfangen und verändern kann. Eine Möglichkeit, die Unversehrtheit festzustellen, besteht darin, Nachrichten zu signieren und die verwendeten Signaturen durch Ausgestaltung einer Sicherungsinfrastruktur im Rechtsverkehr bestimmten Rechtssubjekten zuzuordnen.

Mit dem Signaturgesetz gibt es den notwendigen Rahmen zur Ausgestaltung einer solchen Sicherungsinfrastruktur. Normiert sind unter anderem die Voraussetzungen für die Genehmigung sowie die Anforderungen an die Tätigkeit und den Betrieb von Zertifizierungsdienstanbietern. Der Betrieb eines Zertifizierungsdienstes ist nicht genehmigungspflichtig. Die Aufnahme eine solchen Betriebes ist der Regulierungsbehörde für Telekommunikation und Post anzuzeigen, er unterliegt deren Aufsicht. Neben der Anzeige des Betriebs sieht das Signaturgesetz freiwillige Akkreditierungen von Zertifizierungsdienstanbietern vor. Damit soll es ermöglicht werden, durch eine Vorabkontrolle den Nachweis sicherer Verfahren zu führen.

Die nicht im Signaturgesetz behandelte Frage, in welcher Form künftig Willenserklärungen im Internet abgegeben werden dürfen, regelt das Gesetz zur Anpassung der Formvorschriften des Zivilrechts und anderer Vorschriften an den modernen Rechtsgeschäftverkehr. In Fällen, in denen gesetzlich die Schriftform für die Abgabe von Willenserklärungen vorgesehen und damit die eigenhändige Unterschrift erforderlich ist, können solche Erklärungen jetzt auch in elektronischer Form abgegeben werden. Das Gesetz sieht als wesentlichste Änderungen in den §§ 126a und 126b BGB eine elektronische Form und eine Textform vor. Die elektronische Form erfordert eine qualifizierte elektronische Signierung des Dokumentes nach dem Signaturgesetz.

Mit der Novellierung des Verwaltungsverfahrensgesetzes sind auch die rechtlichen Voraussetzungen für ein rechtswirksames elektronisches Handeln zwischen den Bürgern und der Verwaltung geschaffen worden. Bedauerlicherweise sind die von den Datenschutzbeauftragten des Bundes und der Länder vorgeschlagenen Ergänzungen und Änderungen unberücksichtigt geblieben. Dabei handelt es sich insbesondere um die Forderung nach ausdrücklicher Einwilligung des Empfängers zur Entgegennahme rechtsverbindlicher elektronischer Erklärungen der Verwaltung sowie nach Regelungen zur Sicherstellung einer langfristigen Verfügbarkeit elektronischer Dokumente. Damit entsprechen wesentliche Regelungen des novellierten Verwaltungsverfahrensrechts nicht den datenschutzrechtlichen Anforderungen. Die Umsetzung in Länderrecht steht aus.

Anonyme Internetnutzung ist nicht nur zulässig, sondern sogar rechtlich geboten. TDDSG und MDStV verpflichten den Dienstanbieter, dem Nutzer eine anonyme oder pseudonyme Inanspruchnahme zu ermöglichen. Mit dieser Verpflichtung hat der Gesetzgeber die im BDSG sowie verschiedenen Landesdatenschutzgesetzen normierten allgemeinen Grundsätze der Datenvermeidung und Datensparsamkeit für die Dienstanbieter konkret geregelt. Allerdings werden im eGovernment und eCommerce hohe rechtliche Anforderungen an eine sichere Identifizierung der Kommunikationspartner gestellt. Dies scheint durch die elektronische Signaturen nicht ohne weiteres möglich zu sein. Die elektronische Signatur ist als Unterschriftenersatz konzipiert und auch geregelt worden. Das Zertifikat bildet nur die Informationen ab, die auch mit einer eigenhändigen Unterschrift gegeben werden, nämlich Name und Vorname. Angaben über die Adresse des Signaturschlüsselinhabers fehlen grundsätzlich. Name und Vorname ermöglichen schon wegen der häufigen Namensgleichheiten keine eindeutige Identifizierung. Dies bringt erhebliche Probleme im gewohnten Identifizierungsverfahren, wo für manche Anwendungen der Personalausweis als zusätzliche Identifizierung erforderlich ist. Um Medienbrüche zu vermeiden, muss verstärkt über datenschutzgerechte Alternativen nachgedacht werden (die Handreichung zum datenschutzgerechten eGovernment, vgl. Kapitel 6.5, wird hierzu erste Hinweise geben).

8.6.6 Automatische Prüfung von Internetangeboten

Zur datenschutzrechtlichen Prüfung von Internetangeboten setze ich ein von der Gesellschaft „datenschutz nord GmbH“ angebotene Online-Prüftool ein. Mit OPTuM - Online-Prüfung von Tele- und Mediendiensten - lassen sich Internetangebote privater oder öffentlicher Stellen automatisiert überprüfen (vgl. dazu die Darstellung in Kapitel 5.2.2 und 5.3.11). Dazu werden sämtliche Seiten des zu prüfenden Angebots auf datenschutzrechtlich relevante Aspekte untersucht. Die Ergebnisse werden dem Prüfer übersichtlich präsentiert, der daraus ein Prüfbericht erstellt.

Mit OPTuM möchte ich meinen Prüf- und Beratungsauftrag gegenüber den vielen Tele- und Mediendienstanbietern angemessen und zeitgerecht erfüllen.

8.6.7 Das neue Verfahren der Rundfunkgebührenerhebung

Immer wieder wenden sich Studierende und Personen mit geringem Einkommen an mich und kritisieren die Datenerhebung bei der Beantragung der Rundfunkgebührenbefreiung. Sie haben wenig Verständnis, wenn ich sie auf den Datenschutzbeauftragten des Norddeutschen Rundfunks verweise, da mir in dieser Fragestellung keine Kontrollzuständigkeit übertragen ist. Zuständig bin ich dagegen in der Frage der datenschutzgerechten Antragsabwicklung der Rundfunkgebührenbefreiung durch die niedersächsischen Sozialämter. Neben der Reduzierung des Fragenkatalogs ist inzwischen auch eine Änderung im Verfahrensablauf eingetreten. Hierzu hat der NDR ein automatisiertes Verfahren entwickelt, das eine Online-Bearbeitung von Anträgen auf Befreiung von der Rundfunkgebührenpflicht in Sozialbehörden enthält. In gemeinsamen Gesprächen wurde eine Lösung erzielt, die auch von den beteiligten Datenschutzbeauftragten der norddeutschen Länder akzeptiert werden konnte. Das neue Online-Verfahren wird zunächst als Pilotverfahren eingeführt. Dabei werden die von

den Länder-Datenschutzbeauftragten problematisierten Daten im Sozialamt erfragt und geprüft, im Falle einer Befreiung aber nicht gespeichert. Eine Übermittlung dieser Daten an den NDR erfolgt nur in Zweifelsfällen, in denen der NDR die weitere Bearbeitung der Anträge übernimmt. Verbessert wurden zudem die Einwilligungserklärung und die Sicherheit bei der Datenübermittlung. In der Pilotphase wird statistisch erfasst, wie viele Anträge gestellt, positiv bzw. negativ beschieden und in welchen Fällen die Plausibilitätsdaten tatsächlich für eine Entscheidungsfindung beim NDR benötigt wurden. Verpflichtender Bestandteil des Verfahrens bildet ein Datenschutz- und Datensicherheitskonzept. Es wurde verabredet, nach Abschluss der Pilotphase das neue Verfahren zur Befreiung von der Rundfunkgebührenpflicht zu evaluieren.

9 Personaldatenschutz

9.1 Einführung der Neuen Steuerungsinstrumente

Es steht für mich schon aufgrund der haushaltswirtschaftlichen Notwendigkeiten außer Frage, dass es mehr denn je notwendig ist, die Arbeitsabläufe in den öffentlichen Verwaltungen durch die Einführung der Neuen Steuerungsinstrumente umfassend zu modernisieren und somit insgesamt effizienter und leistungsorientierter zu gestalten. Die mit der Einführung neuer und immer leistungsfähigerer automatisierter Verfahren der Haushaltsmittelbewirtschaftung einhergehenden Gefahren für die Persönlichkeitsrechte der betroffenen Beschäftigten liegen auf der Hand. Viele Beschäftigte und Personalvertretungen hegen Befürchtungen, dass durch die Verarbeitung der Personaldaten in den verschiedensten Verfahren, die zudem über Schnittstellen miteinander verknüpft sein werden, der „gläserne Bedienstete“ Realität wird. Meine Aufgabe wird es auch weiterhin sein, im Zusammenwirken mit den behördlichen Datenschutzbeauftragten, den Gewerkschaften und Personalvertretungen im Rahmen einer möglichst schon im Vorfeld greifenden Beteiligung auf datenschutzgerechte Lösungen hinzuwirken. In der Praxis hat sich gezeigt, dass der Datenschutz die Modernisierungsprozesse nicht behindert, sondern im Gegenteil in einem hohem Maße zur Steigerung der Akzeptanz bei den betroffenen Mitarbeitern beiträgt (siehe auch Nr. 14.3.1 des XV. TB LfD Nds. 1999/2000).

Beispielhaft möchte ich hierzu auf die im Bereich der Landesverwaltung laufenden Projekte eines leistungsorientierten Haushaltswirtschaftssystems (LoHN) und eines landeseinheitlichen Personalmanagementverfahrens (PMV) verweisen. In beiden Fällen war ich erfreulicherweise bereits in einer frühen Phase an der Herausarbeitung der Verfahrensanforderungen und an der Formulierung der mit den Spitzenorganisationen der Gewerkschaften zu treffenden Vereinbarungen beteiligt. Aus meiner Sicht ist es bei beiden Verfahren gelungen, die dem Persönlichkeitsschutz der betroffenen Mitarbeiter dienenden übergreifenden datenschutzrechtlichen Zielvorstellungen und Grundsätze weitestgehend umzusetzen:

- Personenbezogene Daten der Beschäftigten dürfen in den automatisierten Verfahren nur dann verarbeitet werden, soweit dies für die Aufgabenerfüllung erforderlich ist (Grundsatz der Erforderlichkeit).

- Gestaltung und Auswahl der Systeme haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten (Grundsatz der Datenvermeidung und Datensparsamkeit).
- Personaldaten dürfen zentral nur unter Einsatz datenschutzfreundlicher Technologien ausgewertet werden (Anonymisierung oder Pseudonymisierung).
- Die Datenübermittlung erfolgt verschlüsselt. Der Einsatz einer elektronischen Signatur ist zu prüfen.
- Eingangs- und Ausgangsschnittstellen zu anderen Verfahren sind inhaltlich und technisch zu dokumentieren.
- Die in den Systemen verarbeiteten Personaldaten werden nicht zur individuellen Verhaltens- und Leistungskontrolle verwendet.
- Für die Betriebssystemebene und für die Anwendungen sowie für die Auswertung und die Statistiken des Datenbestandes ist ein Berechtigungs- und Zugriffskonzept festzulegen. Protokollierungen und regelmäßige Kontrollen sind vorzusehen (Rechteverwaltung).
- Für die weitere Ausgestaltung der Datenschutz- und Datensicherungsmaßnahmen sind Sicherheitskonzepte und Dienstanweisungen zu erstellen.

9.2 Personalmanagementverfahren

Durch das landeseinheitliche Personalmanagementverfahren (PMV), mit dessen Einführung in ausgewählten Personalbereichen im Jahre 2004 begonnen werden soll, sollen folgende Ziele erreicht werden (vgl. Kapitel 7.6.4):

- Das Verfahren soll die vorhandenen Anwendungen im Bereich der Personal-/Stellen- und Dienstpostenverwaltung sowie der Personalkostenbudgetierung ablösen. Vorhandene Daten werden bei der Einführung automatisiert übernommen.
- Die Daten sollen künftig dort erfasst werden, wo sie zuerst anfallen. Dadurch entfallen in vielen Bereichen Doppeleingaben.
- Im Rahmen der Zugriffsregelung können alle nötigen Auswertungen getätigt werden.
- Für alle wiederkehrenden Aufgaben beim Schriftverkehr soll eine weitreichende Unterstützung erfolgen, z.B. durch automatisierte Dokumentenerstellung und elektronisches Mitzeichnungsverfahren.
- Die Personengrunddaten und die bezügerelevanten Daten, wie z.B. Zeitzuschläge, sollen über eine automatisierte Schnittstelle direkt in das Bezügeverfahren KIDICAP 2000 weitergeleitet werden. Bruttobezügedaten fließen zurück zum PMV, um die Personalkostenbudgetierung zu ermöglichen.

An der Auswahl des Verfahrens und der Gestaltung der mit den Gewerkschaften abgeschlossenen Vereinbarung nach § 81 NPersVG habe ich als Mitglied der ressortübergreifend unter Federführung des Finanzministeriums gebildeten Koordinierungsgruppe aktiv mitgewirkt (vgl. Nr. 14.3.2 des XV. TB LfD Nds. 1999/2000). Die im Ergebnis einer europaweiten Ausschreibung ausgewählte Software ePers-Inf der Firma Personal & Informatik AG (P&I) überzeugt durch ihre hohe Flexibilität, die es ermöglicht, Geschäftsabläufe, Mitzeichnungsverfahren, Datenfelder, Masken, Auswertungen und Zugriffsberechtigungen auch unter datenschutzrechtlichen Gesichtspunkten bedarfsgerecht zu definieren. Kernmodule des Verfahrens sind:

- Personalverwaltung und -entwicklung, Bewerberauswahl,
- Stellenbewirtschaftung,
- Dienstpostenverwaltung und
- Personalkostenbudgetierung.

Für Teilbereiche der Landesverwaltung, so etwa die Polizei, die Straßenbauverwaltung, den Justizvollzug und die Landeskrankenhäuser, soll darüber hinaus im Rahmen eines Teilprojektes ein zusätzliches Modul „Zeitwirtschaft“ ausgewählt werden. Zur Zeitwirtschaft gehört die bedarfsorientierte Schichtdienstplanung einschließlich der maschinellen Ermittlung von Zeitzuschlägen (für die Bezügeabrechnung) und die Zuordnung von Arbeitszeiten zu Produkten (Produkterfassung für das Projekt LoHN).

Die für das Personalmanagementverfahren ausgewählte Anwendung ePers-Inf kann alternativ zur Client/Server-Lösung auch über den Webbrowser bedient werden. Die Vertraulichkeit, Integrität und Authentizität der im Personalmanagementverfahren verarbeiteten Daten wird durch Verschlüsselungsverfahren und durch den Einsatz der elektronischen Signatur gewährleistet.

Dem Personalmanagementverfahren kommt eine zentrale Bedeutung innerhalb der IT-Landschaft des Landes zu, da in diesem System zentral die Personalstammdaten vorgehalten werden, die in anderen Anwendungen, etwa im Bezügeverfahren, im Haushaltswirtschaftssystem und sonstigen fachspezifischen Verfahren, benötigt werden. Diese Funktion kann das Personalmanagementverfahren nur dann erfüllen, wenn die Daten regelmäßig über Schnittstellen ausgetauscht und aktualisiert werden. Diese Schnittstellen sind aus datenschutzrechtlicher Sicht eindeutig zu definieren und durch geeignete technisch-organisatorische Maßnahmen abzusichern.

Meine Beteiligung in der Koordinierungsgruppe bleibt auch in der Einführungsphase erhalten. Ziel muss es sein, die weitere Implementierung des Verfahrens im Sinne eines ständigen Datenschutz- und Technikfolgencontrollings konstruktiv zu begleiten.

9.3 Leistungsorientierte Haushaltswirtschaft Niedersachsen

Auch die Einführung der betriebswirtschaftlichen Steuerungsinstrumente, so etwa der Kosten- und Leistungsrechnung, wird von vielen Bediensten mit großer Skepsis begleitet. Befürchtet wird, dass die aus der Kosten- und Leistungsrechnung gewonnenen Daten nicht nur für die eigentlichen Zielsetzungen, etwa zur Erhöhung der Transparenz der Mittelverwendung und Steigerung der Effizienz der Aufgabenerledigung, sondern gezielt auch zur Bewertung des persönlichen Leistungsvermögens herangezogen werden. Es ist daher sehr erfreulich, dass mich das federführende Finanzministerium an der Fortschreibung der Vereinbarung nach § 81 NPersVG zur Einführung von betriebswirtschaftlichen Steuerungsinstrumenten in der niedersächsischen Landesverwaltung im Rahmen des Projektes „Leistungsorientierte Haushaltswirtschaft Niedersachsen (LoHN)“ frühzeitig beteiligt hat.

Im Zusammenwirken mit den Gewerkschaften und Berufsverbänden ist es gelungen, nunmehr klarstellende und eindeutige Regelungen zur datenschutzgerechten Umset-

zung der im Rahmen des Projektes Lohn einsetzbaren Steuerungsinstrumente, so für die Bereiche Budgetierung, Zielvereinbarung, Kosten- und Leistungsrechnung sowie Controlling mit den Instrumenten Berichtswesen und Benchmarking, zu entwickeln. Im Einzelnen gilt hier Folgendes:

- Die im Rahmen des Projektes LoHN verarbeiteten personenbezogenen Daten der Beschäftigten sind zu einem frühestmöglichen Zeitpunkt, spätestens jedoch bei der Eingabe, zu pseudonymisieren (z.B. durch Vergabe einer Identifikationsnummer). Nur im Ausnahmefall und mit Zustimmung der Beschäftigten können sie nach Maßgabe von Dienstvereinbarungen offen weitergeleitet werden.

- Im Bereich des Controllings ist durch Anonymisierung sicherzustellen, dass Leistungsvergleiche zwischen Beschäftigten ausgeschlossen werden. Personenbezogene Berichte sind nicht zulässig.

- Die Personalkosten werden im Regelfall aus Gründen der Vergleichbarkeit und des Datenschutzes nach verwaltungsbereichsspezifischen Durchschnittssätzen berechnet. Hiervon abweichend können die Personalkosten in Landesbetrieben nach betriebsspezifischen Durchschnittssätzen berechnet werden.

- Falls die Personalkostenbudgets von Verwaltungsbereichen oder Landesbetrieben keine für eine Anonymisierung hinreichende Größe aufweisen, sind Durchschnittswerte aus den Budgets mehrerer vergleichbarer Verwaltungsbereiche bzw. Landesbetriebe zu bilden.

- Zur Gewährleistung der Vertraulichkeit sind Vertrauenspersonen von den Dienststellen im Einvernehmen mit den zuständigen Personalräten zu bestimmen. Sie sollen Unklarheiten, die sich im Rahmen der systemspezifischen Plausibilitätsprüfung oder der allgemeinen Schlüssigkeitsprüfung ergeben, mit den Beschäftigten klären. Die zu bestimmenden Vertrauenspersonen sollen nicht im Controlling beschäftigt sein.

- Die mit der Zeitaufschreibung erhobenen Daten werden weder zur unmittelbaren Leistungs- und Verhaltenskontrolle von Beschäftigten noch zur individuellen Stellenbewertung verwendet. Die Erfassungsbögen werden spätestens 3 Monate nach Eingabe vernichtet.

- Bei Beschäftigten, die allein ein Produkt erstellen, ist durch geeignete Maßnahmen (z.B. Zusammenfassung von ähnlichen Produkten oder Leistungen, Anonymisierung oder Aggregation im Berichtswesen oder bei Benchmark-Vergleichen) sicherzustellen, dass die aus der KLR gewonnenen Ergebnisse nicht zu Rückschlüssen auf Arbeitsverhalten und -leistung einzelner Beschäftigter verwendet werden können.

Es ist datenschutzrechtlich nicht unproblematisch, dass im Einzelfall aus den für das Controlling aus der Kosten- und Leistungsrechnung aufbereiteten Daten Rückschlüsse auf bestimmte Bedienstete gezogen werden können, wenn Leistungen oder Pro-

dukte in einem bestimmten Verwaltungsbereich nur von einer Person erbracht werden (sog. „1:1-Verhältnisse“ oder „Tabelleneinser“). Eine derart „personenbeziehbare“ Verarbeitung von Daten ist nach den Regelungen der Vereinbarung deshalb nur zulässig, sofern dies zu den in der Vereinbarung genannten Zwecken der Kosten-Leistungsrechnung, so etwa der Herstellung von Transparenz in den Kosten- und Leistungsstrukturen, zwingend notwendig ist. Derartige Fälle sind in den zur weiteren Umsetzung der Vereinbarung abzuschließenden Dienstvereinbarungen nach § 78 NPersVG gesondert zu regeln. Die Dienststellen werden daher gehalten sein, gegenüber den zuständigen behördlichen Datenschutzbeauftragten und den Personalvertretungen zu begründen, warum es im Einzelfall erforderlich ist, so genannte 1:1 Verhältnisse auf Kostenstellenebene auszuweisen.

10 Inneres

10.1 Innere Sicherheit

10.1.1 Die Terrorismusbekämpfungsgesetze des Bundes

Das erste Sicherheitspaket

Die schrecklichen Ereignisse des 11. September 2001 in den USA haben auch in Deutschland erhebliche Auswirkungen gehabt. Unmittelbar danach begannen nicht nur im Bund und in den Ländern Fahndungsmaßnahmen der Sicherheitsbehörden, auch die Politik wurde tätig. In einem ersten Sicherheitspaket wurden auf Bundesebene zwei Gesetzesänderungen auf den Weg gebracht. Zum einen wurde das sog. Religionsprivileg aus dem Vereinsgesetz gestrichen, wonach z.B. Vereinigungen, die sich die gemeinschaftliche Pflege einer Weltanschauung zur Aufgabe machen, nicht als Vereine galten, somit auch nicht verboten werden konnten. Dieses ist nunmehr bei Vorliegen der entsprechenden Voraussetzungen möglich. Die Gesetzesänderung trat bereits am 8. Dezember 2001 in Kraft. Zum anderen wurde ein neuer § 129b in das Strafgesetzbuch eingefügt, der die §§ 129 und 129a (Bildung krimineller bzw. terroristischer Vereinigungen) auch auf Vereinigungen im Ausland ausweitete. Diese Vorschrift trat allerdings aufgrund verfassungsrechtlicher Schwierigkeiten und wohl auch koalitionsinterner Probleme erst am 30. August 2002 in Kraft.

Das zweite Sicherheitspaket

Ohne dass eine kritische gesellschaftliche Debatte die politische Erörterung begleitet hat, trat bereits am 9. Januar 2002 das Gesetz zur Bekämpfung des internationalen Terrorismus rückwirkend zum 1. Januar 2002 in Kraft. Mit diesem sog. „Otto-Katalog“ wurden insgesamt 23 Gesetze geändert. Im Gegensatz zum ersten Sicherheitspaket, das datenschutzrechtlich keine besondere Bedeutung hat, sind in diesem Terrorismusbekämpfungsgesetz eine Vielzahl datenschutzrechtlich bedeutsamer Änderungen in den einzelnen Gesetzen vorgenommen worden. Der Grundrechtsschutz der Bürger, insbesondere ihr Recht auf informationelle Selbstbestimmung, ist in weiten Bereichen erheblich aufgeweicht worden. Hervorzuheben sind dabei insbesondere die Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes, des BKA-Gesetzes, des G 10-Gesetzes und des Sicherheitsüberprüfungsgesetzes.

Das Bundesamtes für Verfassungsschutz erhielt zur Erfüllung seiner Aufgaben im Bereich der Terrorismusbekämpfung wesentlich erweiterte Befugnisse. So kann es künftig bei Finanzdienstleistungsunternehmen Auskünfte zu Konten, Konteninhabern, Geldbewegungen und Geldanlagen einholen. Bei Postdienstleistungsunternehmen dürfen Auskünfte zu Namen, Anschriften, Postfächern und sonstigen Umständen des Postverkehrs eingeholt werden. Bei Luftverkehrsunternehmen dürfen Auskünfte zu Namen, Anschriften, zur Inanspruchnahme von Transportleistungen und sonstigen Umständen des Luftverkehrs erfragt werden. Es dürfen technische Mittel zur Ermittlung des Standortes eines aktiv geschalteten Handys und der Geräte- und Kartennummer eingesetzt werden (sog. IMSI-Catcher). Bei Anbietern von Telekommunikations- und Telediensten darf das Amt auch rückwirkend Daten über Berechtigungskennungen, Kartennummern und Nummern des anrufenden und angerufenen Anschlusses abfragen. Darüber hinaus darf sich das Amt nach Beginn und Ende der Verbindung nach den Endpunkten fest geschalteter Verbindungen sowie beim Handy nach der Standortkennung erkundigen. Außerdem erhält es unaufgefordert personenbezogene Informationen vom Bundesamt für die Anerkennung ausländischer Flüchtlinge, das künftig Bundesamt für Migration und Flüchtlinge heißen wird, und den Ausländerbehörden, wenn Anhaltspunkte bestehen, dass die Übermittlung zur Erfüllung der Aufgaben des Verfassungsschutzes erforderlich ist.

Die Zuständigkeit des Bundeskriminalamtes wurde auf Ermittlungen zu schweren Fällen der Datennetzkriminalität erweitert, sofern sich die Tat gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder gegen sicherheitsempfindliche Stellen lebenswichtiger Einrichtungen richtet. Nunmehr sollen auch verdeckte Ermittler, die nicht Mitarbeiter des Bundeskriminalamtes sind, technische Mittel, etwa zum Ausspähen von Wohnungen (Lauschangriff), einsetzen dürfen. Darüber hinaus kann das Bundeskriminalamt, soweit dies zur Erfüllung seiner Aufgabe als Zentralstelle erforderlich ist, auch ohne Vorliegen eines konkreten Anfangsverdachtes eigene Ermittlungen durchführen.

Der Bundesnachrichtendienst erhält ähnlich wie das Bundesamt für Verfassungsschutz das Recht, bei Postunternehmen, Banken, Luftverkehrsunternehmen usw. Auskünfte über Kunden- und Benutzungsdaten zu erheben.

Auch der militärische Abschirmdienst hat seit dem Beginn des Jahres 2002 das Recht, entsprechende Daten von Telekommunikations- und Teledienstleistern abzufragen.

Das Sicherheitsüberprüfungsgesetz wurde in seinem Anwendungsbereich erheblich erweitert. Für eine Sicherheitsüberprüfung, die einer kompletten „informationellen Durchleuchtung“ des Betroffenen gleich kommt, reicht nunmehr u.a. eine Tätigkeit in einer Einrichtung aus, die für das Funktionieren des Gemeinwesens unverzichtbar ist und deren Beeinträchtigung erhebliche Unruhen in großen Teilen der Bevölkerung und somit Gefahren für die öffentliche Sicherheit oder Ordnung entstehen lassen würde. Darunter fallen zum Beispiel auch Krankenhäuser oder Einrichtungen im Bereich der Energieversorgung.

Weitere Gesetze zur Terrorismusbekämpfung

Durch die Änderungen im Geldwäschebekämpfungsgesetz vom 8. August 2002 wird Kreditinstituten und sonstigen Finanzdienstleistungsinstituten auferlegt, eine Fülle personenbezogener Daten bei ihrer Kundschaft zu erheben und zu verarbeiten (Identifizierungspflicht). Hierdurch soll neben der Geldwäsche auch die Finanzierung des Terrorismus bekämpft werden. In Verdachtsfällen der Geldwäsche ist neben den zuständigen Strafverfolgungsbehörden auch eine im Bundeskriminalamt eingerichtete „Zentrale Analyse- und Informationsstelle“ zu unterrichten.

Im 4. Finanzmarktänderungsgesetz vom 21. Juni 2002 wurde im § 24c des Gesetzes über das Kreditwesen (KWG) eine Rechtsgrundlage für die Bundesanstalt für Finanzdienstleistungsaufsicht für den automatisierten Abruf von Kontoinformationen geschaffen. Im Einzelnen geht es um die Nummer eines Kontos oder Depots, den Tag der Errichtung und Auflösung und den Namen (bei natürlichen Personen auch das Geburtsdatum) des Inhabers und des Verfügungsberechtigten. Durch diesen automatisierten Abruf werden allerdings keine Angaben über den Kontostand oder über Kontenbewegungen übermittelt. Diese Informationen muss sich die Bundesanstalt dann durch eine gezielte Einzelanfrage bei dem betreffenden Institut holen. Dieses ist gemäß § 44 Abs. 1 KWG verpflichtet, der Bundesanstalt Auskünfte über alle Geschäftsangelegenheiten zu erteilen und bei Bedarf entsprechende Unterlagen vorzulegen.

Die Strafprozessordnung schließlich wurde zum 14. August 2002 durch die Einfügung des § 100i dahingehend geändert, dass die Strafverfolgungsbehörden die Befugnis erhielten, unter bestimmten Voraussetzungen durch technische Mittel den Standort eines aktiv geschalteten Mobilfunkendgerätes ermitteln zu dürfen.

Die nach dem 11. September 2001 im Ausländerrecht vorgenommenen erheblichen Änderungen sind in Kapitel 10.2.1 dargestellt.

Fazit

Die Gesetzesänderungen in den beiden Sicherheitspaketen und den anderen Gesetzen tangieren zentrale rechtsstaatliche Prinzipien (vgl. oben unter Kapitel 4.3) und haben bisher nichts Nachweisbares zur Aufklärung oder Verhütung terroristischer Straftaten beigetragen, sodass sich die Frage aufdrängt, inwieweit sie hierzu überhaupt geeignet sind, eine Frage, die die Datenschutzbeauftragten schon sehr frühzeitig an die Politik gerichtet hatten. Ich verweise insoweit auf die Entschließungen vom 1. Oktober 2001 (Anlage 11) und 24./26. Oktober 2001 (Anlage 12). Die bisherigen Erfolge der Ermittlungsbehörden beruhen nicht auf den neuen Kompetenzen, die in weiten Bereichen völlig Unverdächtige in die Ermittlungen hineinziehen, sondern auf herkömmlicher kriminalistischer Arbeit.

Immerhin ist es in der letzten Phase der Gesetzesberatungen zum Terrorismusbekämpfungsgesetz gelungen, für die Änderungen im Bundesverfassungsschutzgesetz, MAD-Gesetz, BND-Gesetz, Art. 10-Gesetz, Sicherheitsüberprüfungsgesetz und im § 7 Abs. 2 des BKA-Gesetzes eine Befristung auf fünf Jahre im Gesetz festzuschreiben. Nach Ablauf dieser Zeit gelten vorbehaltlich einer erneuten Gesetzesänderung wieder die ursprünglichen Regelungen. Darüber hinaus sind die Neuregelungen vor

Ablauf der Befristung zu evaluieren, d.h. ihre Wirksamkeit und Angemessenheit ist durch eine begleitende wissenschaftliche Forschung zu überprüfen. Im Koalitionsvertrag der neuen Bundesregierung ist diese Verpflichtung noch einmal bekräftigt worden; Maßnahmen zur Vorbereitung dieser Evaluierung sind bisher allerdings noch nicht erkennbar.

10.1.2 Terrorismusbekämpfung in Niedersachsen

Änderungen des Niedersächsischen Gefahrenabwehrgesetzes

Auch vor der Novellierung des Gefahrenabwehrgesetzes durfte die Polizei öffentlich zugängliche Orte mittels Bildübertragung offen beobachten, wenn dies u.a. zur Gefahrenabwehr erforderlich war. Aufgezeichnet werden durften jedoch nur die Bilddaten solcher Personen, bei denen Tatsachen die Annahme rechtfertigten, dass sie Straftaten oder nicht geringfügige Ordnungswidrigkeiten begehen werden. Durch die Gesetzesänderung vom 25. Oktober 2001 wurde diese Befugnis der Polizei dahingehend erweitert, dass sie nunmehr losgelöst von dieser Einschränkung bereits dann die erhobenen Bilddaten aufzeichnen darf, wenn Tatsachen die Annahme rechtfertigen, dass an dem videoüberwachten Ort künftig Straftaten von erheblicher Bedeutung begangen werden. In den Gesetzesberatungen habe ich u.a. darauf hingewiesen, dass durch diese Gesetzesänderung bewirkt wird, dass künftig auch das Verhalten unbeteiligter, gesetzestreuer Bürger aufgezeichnet wird, nur weil diese sich zufällig an einem Ort befinden, an dem künftig möglicherweise Straftaten von erheblicher Bedeutung begangen werden. Dieses stelle einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar, da ohne Differenzierung der Personen aufgezeichnet werden dürfe, wenn lediglich angenommen wird, dass künftig Straftaten von erheblicher Bedeutung an einem bestimmten Ort begangen werden, ohne dass man weiß, von welchen Personen. Es handele sich somit um den typischen Fall einer - nicht zulässigen - Datenhaltung auf Vorrat. Ich habe darüber hinaus darauf hingewiesen, dass die Einführung einer Aufzeichnung zur „vorbeugenden Strafverfolgung“ nicht zielführend sei, da erfahrungsgemäß hierdurch keine Straftaten verhindert werden könnten, allenfalls sei ein Verlagerungseffekt zu nicht videoüberwachten Stellen die Folge. Auch rechtfertige eine lediglich personelle Entlastung der Polizei bei der künftigen Strafverfolgung keinen Eingriff in die Grundrechte unbeteiligter Dritter. Angesichts des sicherheitspolitischen Klimas in der Zeit unmittelbar nach dem 11. September 2001 konnte ich mich mit dieser Argumentation jedoch leider nicht durchsetzen.

Eine weitere Änderung des Niedersächsischen Gefahrenabwehrgesetzes bestand in der Einfügung eines neuen § 45a, der der niedersächsischen Polizei den Datenabgleich mit anderen Dateien, die sog. Rasterfahndung, zu Gefahrenabwehrzwecken ermöglicht. Anlass für diese Gesetzesergänzung war die Tatsache, dass zwar auf Bund-Länder-Ebene die bundesweite Rasterfahndung nach sog. terroristischen Schläfern vereinbart worden, eine solche vorbeugende Rasterfahndung nach der niedersächsischen Gesetzeslage jedoch nicht zulässig war. Bei einer Rasterfahndung werden durch die Polizei bei anderen öffentlichen oder privaten Stellen Daten erhoben, die bestimmten, aus dem jeweiligen Fahndungsansatz abgeleiteten Kriterien entsprechen. In einem zweiten Schritt werden diese Daten zum einen mit anderen

polizeilichen Dateien, zum anderen aber insbesondere untereinander abgeglichen. Unabhängig von einer persönlichen „Nähe“ der Betroffenen zu der abzuwehrenden Gefahr werden ihre Daten also durch die Polizei erhoben und verarbeitet. Bei dieser besonderen Ermittlungsmethode der Polizei wird im Ergebnis gegen eine große Zahl von Menschen ermittelt, die sich völlig gesetzestreu verhalten. Da die Sinnhaftigkeit der Rasterfahndung in bestimmten Fällen jedoch nicht auszuschließen ist, habe ich mich nicht grundsätzlich gegen die Einfügung des § 45a in das NGefAG gewandt.

Wegen der großen Eingriffstiefe habe ich jedoch gefordert, dass diese Ermittlungsmethode mit gesetzlichen Leitplanken versehen wird, damit unbescholtene Bürger nicht zum bloßen Objekt staatlichen Handelns werden. Ich bin insbesondere dafür eingetreten, dass die Rasterfahndung nur bei besonderen Gefahren für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person zulässig sein dürfe, dass bei der Anordnung die Merkmale für den Abgleich zuvor schriftlich festzulegen sind, dass mitgelieferte „Verbunddaten“ nicht zu anderen Zwecken genutzt werden dürfen, dass die Daten unverzüglich gelöscht werden, sobald sie zur Zweckerreichung nicht mehr erforderlich sind, und dass die Betroffenen nach Durchführung über den Abgleich unterrichtet werden müssen. Außerdem habe ich mich dafür ausgesprochen, dieses neue Fahndungsmittel im Gesetz zeitlich zu befristen und die Rasterfahndung einer ergebnisoffenen Erfolgskontrolle zu unterziehen. Der niedersächsische Gesetzgeber hat demgegenüber jedoch entschieden, dass eine Rasterfahndung bereits dann durchgeführt werden darf, wenn lediglich Tatsachen die Annahme rechtfertigen, dass künftig Straftaten von erheblicher Bedeutung begangen werden. Allerdings muss die Rasterfahndung „ultima ratio“ sein. Ebenfalls wurde die Unterrichtungspflicht nicht in das Gesetz aufgenommen. Nicht eindeutig ist im Gesetz geklärt, ob die Polizei mitgelieferte Verbunddaten unter bestimmten Voraussetzungen für andere Zwecke nutzen darf. Allerdings ist im § 98a der Strafprozessordnung, der die Rasterfahndung zu Strafverfolgungszwecken regelt, ausdrücklich festgelegt, dass mitgelieferte Verbunddaten nicht genutzt werden dürfen. Es ist nicht ersichtlich, dass für entsprechende Daten bei einer Maßnahme nach § 45a NGefAG etwas anderes gelten kann. Auch ein generelles Löschungsgebot nach der Zweckerreichung findet sich im Gesetz leider nicht. Allerdings ist die Polizei nur unter den einschränkenden Voraussetzungen des § 39 Abs. 4 NGefAG zur zweckändernden Nutzung der Daten befugt.

Positiv an der gesetzlichen Regelung ist zu bewerten, dass die Polizei im Rahmen einer Rasterfahndung keine Übermittlung von Daten verlangen darf, die einem Amts- oder Berufsgeheimnis unterliegen. Diese besonders sensiblen Daten, z.B. Sozialdaten oder ärztliche Daten, sind also vor einem Zugriff durch eine Rasterfahndung geschützt. Als positiv ist weiterhin herauszustellen, dass die schriftlich begründete Anordnung zur Rasterfahndung durch die Behördenleitung der Zustimmung des Niedersächsischen Innenministeriums bedarf und dass ich von dieser Maßnahme unverzüglich zu unterrichten bin.

Nach In-Kraft-Treten der Gesetzesänderung am 30. Oktober 2001 stimmte das Niedersächsische Innenministerium noch am gleichen Tage der Anordnung einer Rasterfahndung nach terroristischen Schläfern durch das Landeskriminalamt Niedersachsen

zu und informierte mich darüber. Hierdurch wurde ich in die Lage versetzt, die Rasterfahndung in Niedersachsen von Anbeginn an aus datenschutzrechtlicher Sicht zu begleiten.

Die „vorgezogene“ Rasterfahndung

Bereits rund einen Monat vor In-Kraft-Treten der vorstehend beschriebenen Gesetzesänderung wandte sich das Niedersächsische Innenministerium an die Ausländerbehörden und wies diese an, alle ausländischen Studenten aus 23 im Einzelnen aufgeführten islamischen Herkunftsländern nach bestimmten Merkmalen zu erfassen, ggf. Einzelheiten bei den Hochschulen abzuklären und die so erlangten Daten an das Landeskriminalamt zur dortigen Auswertung weiter zu leiten. Die Hochschulen wurden gebeten, die Ausländerbehörden bei dieser Maßnahme so weit wie möglich zu unterstützen. Die Daten sollten von den Ausländerbehörden in einer Excel-Datei per E-mail an das Landeskriminalamt übermittelt werden. Ich habe gegenüber dem Innenministerium moniert, dass es sich bei dieser Maßnahme um den Fall einer Datenerhebung und Übermittlung nach dem Muster einer Rasterfahndung zur Gefahrenabwehr handele, für die eine Rechtsgrundlage noch nicht vorhanden war, sondern ja gerade erst geschaffen werden sollte. Es wurden Angaben über eine nur nach sehr allgemeinen Merkmalen beschriebene, vom zahlenmäßigen Umfang her völlig unbestimmte Personengruppe durch die Ausländerbehörden zusammen getragen. Die Ausländerbehörden haben darüber hinaus diese Daten mit Daten aus den Hochschulen angereichert und sodann dem Landeskriminalamt übermittelt. Zwar ist es richtig, dass die Polizei diesen Datenabgleich zwischen den Daten der Ausländerbehörden und denen der Hochschulen bzw. die Datenanreicherung nicht selbst durchgeführt hat, sie hat dieses jedoch durch die Ausländerbehörden vornehmen lassen. Es wurde also gewissermaßen durch die Ausländerbehörden eine Rasterfahndung „im Auftrage“ durchgeführt.

Angesichts der Tatsache, dass eine derartige Fahndungsmaßnahme nach der zwischenzeitlich erfolgten Novellierung des Gefahrenabwehrgesetzes nunmehr grundsätzlich zulässig ist, es sich also insoweit um einen einmaligen Rechtsverstoß gehandelt hat, habe ich von einer förmlichen Beanstandung gem. § 23 NDSG abgesehen. Das Innenministerium hat meine Sichtweise nicht akzeptiert und sich hinsichtlich der Rechtsgrundlage für diese Maßnahme auf die meiner Meinung nach nicht einschlägigen §§ 76 ff. AuslG und die allgemeine Datenerhebungsbefugnis der Polizei gem. § 31 NGefAG gestützt. Nicht bestritten wurde hingegen mein Vorhalt, dass durch diese Aktion auch gegen § 7 Abs. 2 Nr. 10 NDSG verstoßen worden ist, wonach sicherzustellen ist, dass bei der Übermittlung personenbezogener Daten diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle). Durch den unverschlüsselten Datentransfer per E-Mail zum Landeskriminalamt Niedersachsen wurde gegen diese Verpflichtung verstoßen.

Die „richtige“ Rasterfahndung

Noch am 30. Oktober 2001, dem Tag des In-Kraft-Tretens der oben beschriebenen Änderungen des NGefAG, stimmte das Niedersächsische Innenministerium der Anordnung des Landeskriminalamts zur Rasterfahndung zu. Im unmittelbaren Anschluss begann die Erhebung von Datenbeständen der Meldebehörden, Hochschulen sowie

weiterer Stellen durch das LKA. Diese Daten wurden im LKA „vorgerastert“. Als Ergebnis wurden dem BKA die Datensätze solcher ausländischen Studenten mit einem Wohnsitz in Niedersachsen zur Einstellung in die sog. Verbunddatei „Schläfer“ gemeldet, die den Rasterkriterien entsprachen. Besondere Datensätze, die eine zusätzliche Qualifikation einzelner Personen (z.B. Inhaber einer Fluglizenz) beinhalten, wurden durch das LKA in eine gemeinsame Abgleichdateiensammlung der Länder (und des Bundes) beim BKA eingestellt. In die Verbunddatei „Schläfer“ haben alle Bundesländer ihre Datensätze aus der jeweiligen Länderrasterfahndung übermittelt, um sie durch das BKA (zentral) untereinander und mit der genannten Dateiensammlung abgleichen zu lassen. Bei einer Übereinstimmung (sog. Namensidentität) erfolgt eine weitere Überprüfung durch das Landeskriminalamt, welches den Grunddatensatz in die Verbunddatei eingestellt hat.

Ich habe mich entsprechend meinem gesetzlichen Auftrag fortlaufend über die Durchführung der Rasterfahndung und die dabei vorgenommenen Arbeitsschritte im LKA informiert und aus Datenschutzsicht auf die Einhaltung der gesetzlichen und der weiteren Vorgaben aus der niedersächsischen Rasterfahndungsanordnung geachtet. Nach wie vor habe ich grundsätzliche Zweifel an der Eignung und Verhältnismäßigkeit dieser, vor allem unbescholtene Personen treffenden Maßnahme, bei der bei dem vereinbarten bundesweit einheitlichen Vorgehen personenbezogene Daten Hunderttausender in polizeiliche Fahndungsmaßnahmen einbezogen werden. Meine diesbezüglichen generellen Bedenken haben allerdings bislang kein entsprechendes Gehör gefunden. Nachdenklich müsste aber doch eigentlich jedermann stimmen, dass die Rasterfahndungsmaßnahme nach mehr als einem Jahr weder irgendeinen Ermittlungserfolg gebracht hat noch überhaupt absehbar ist, wann der vom BKA durchgeführte Datenabgleich abgeschlossen werden kann.

In Niedersachsen haben zwei ausländische Studenten vor dem Verwaltungsgericht Hannover Anträge auf Erlass einer einstweiligen Anordnung gestellt, um die Weitergabe ihrer personenbezogenen Daten an das Bundeskriminalamt zu verhindern. Über die Fälle wurde am 11. April 2002 mündlich verhandelt. Die Verfahren wurden für erledigt erklärt, nachdem sich die Parteien darauf geeinigt hatten, dass die entsprechenden Datensätze erst weitergereicht werden, wenn ich von einer endgültigen Liste sog. Abgleichdateien des BKA Kenntnis erhalten habe. Diese Liste sollte die Dateien (und deren Inhalt) bezeichnen, mit denen u.a. die niedersächsischen Rasterfahndungsdaten abgeglichen werden, um bestimmte besondere Personenmerkmale zu erkennen (z.B. Erwerb einer Fluglizenz, Tätigkeit in einem besonders gefährdeten Bereich). Eine vorläufige Liste dieser erwähnten Dateien wurde mir am 12. April 2002 durch das LKA überreicht. Bis zum heutigen Tag bin ich nicht im Besitz einer endgültigen und damit abschließenden Auflistung der Dateien, mit denen die von Niedersachsen zugelieferten Datenbestände nun tatsächlich beim BKA abgeglichen wurden und noch werden. Es ist allerdings mittlerweile sichergestellt, dass keine weiteren Abgleichdateien beim BKA oder in den Ländern erstellt werden, die mir vorliegende Liste stellt also den Rahmen des maximal Möglichen dar.

Insgesamt ergeben sich Zweifel, ob die zentrale Rolle des BKA bei diesem Vorgehen in vollem Umfang von den geltenden Regelungen gedeckt ist. Das BKA hat nämlich in

großem Umfang eigenständige Erhebungen durchgeführt; es ist z.B. an zahlreiche Wirtschaftsverbände mit der Bitte herangetreten, die verbandsangehörigen Unternehmen zu einer „freiwilligen Herausgabe“ bestimmter Datenbestände über deren Mitarbeiter zum Zweck des automatisierten Abgleichs zu veranlassen. Als Rechtsgrundlage wurde auf § 7 Abs. 2 BKA-Gesetz verwiesen, der aber nach meinem Verständnis nur eine auf den Einzelfall bezogene und ergänzende Datenerhebung durch das BKA zulässt, während es hier zu einer massenhaften Erhebung personenbezogener Daten durch das BKA nach dem für eine Rasterfahndung typischen Handlungsansatz gekommen ist. Diese Vorgehensweise war zwar, wie ich mich überzeugt habe, mit den Ländern abgesprochen worden, ihr liegen jedoch auf Länderseite als Befugnisregelungen die Bestimmungen zur Rasterfahndung zugrunde, während der Bund unstreitig über eine solche Befugnis nicht verfügt und deshalb ja auch um eine „freiwillige“ Hergabe der Daten gebeten hat. Daher bleibt mein Eindruck, dass die Erhebungsregelung des § 7 Abs. 2 BKA-Gesetz in diesem Fall mit der abgestimmten arbeitsteiligen Vorgehensweise im Rahmen einer bundesweiten Rasterfahndung deutlich „überstrapaziert“ worden ist. Hinsichtlich der Freiwilligkeit der Datenübermittlung durch die Unternehmen an das BKA ist im Übrigen darauf hinzuweisen, dass die davon eigentlich Betroffenen, nämlich die Mitarbeiter in den Unternehmen, dabei in keiner Weise beteiligt worden sind, sodass insoweit eine freiwillige Übermittlung eindeutig nicht gegeben ist.

Die durchgeführten Abgleichmaßnahmen des BKA stützen sich auf den § 28 BKA-Gesetz, nach welchem das BKA personenbezogene Daten mit dem Inhalt von Dateien abgleichen darf, für die es u.a. zur Erfüllung seiner Aufgaben die Berechtigung zum Abruf hat. Weiter muss dieser Abgleich zur Erfüllung einer dem BKA obliegenden Aufgabe (im vorliegenden Fall kann es sich nur um die Zentralstellenfunktion gem. § 2 Abs. 1 BKA-Gesetz handeln) erforderlich sein. Für die Verbunddatei „Schläfer“ hat das BKA unstreitig eine Berechtigung zum Abruf; der Abgleich mit der Abgleichdateiensammlung scheint auch erforderlich zu sein, um der Zentralstellenfunktion gerecht zu werden. Auch hier stellt sich allerdings die Frage, ob bei der in Rede stehenden Vorgehensweise, bei der das BKA mit der Durchführung der Abgleichmaßnahmen ja nicht nur technische Hilfestellung für die Länder gegeben, sondern dabei in erheblichem Umfang auch selbst erhobene Datensätze mit den von den Ländern zugelieferten Rasterdatensätzen abgeglichen hat, der Verweis auf die Zentralstellenfunktion des BKA gemäß § 2 Abs. 1 BKA-Gesetz nicht eine Überstrapazierung der gesetzlichen Regelung bedeutet und ob nicht stattdessen eine Qualifizierung als Datenverarbeitung im Auftrag der Länder sachgerechter und geboten wäre. Dadurch könnte auch der fortwirkenden Verantwortung der Länder für „ihre“ Daten besser Rechnung getragen werden. Unabhängig von der Beantwortung dieser Frage muss allerdings in jedem Fall sichergestellt sein, dass die Abgleichdateien nur solche personenbezogenen Daten enthalten, die durch das BKA und die Länderpolizeien rechtmäßig erhoben worden sind. Bedeutsam ist in diesem Zusammenhang, dass in mehreren Sitzungen des BKA und der Länderpolizeien eine Abstimmung über die jeweiligen Abgleichdateien erfolgte. In den Abgleich wurden nur die Datensätze einbezogen, die durch alle Ländervertreter einstimmig beschlossen wurden. Für den Fall, dass bei einigen Abgleichdateien Zweifel angemeldet wurden, wurden diese konkreten Dateien nicht für einen weiteren Abgleich genutzt.

Es besteht Übereinstimmung und ist in der Errichtungsanordnung zur Verbunddatei „Schläfer“ auch ausdrücklich festgelegt, dass die dem BKA gemeldeten Länderdatensätze in der Verfügungsgewalt und weiteren datenschutzrechtlichen Verantwortung der einzelnen Länder bleiben. Dem versucht das weitere Verfahren beim Abgleich in folgender Weise Rechnung zu tragen: Ergeben sich zu einem niedersächsischen Rasterfahndungsdatensatz durch eine Abgleichmaßnahme im BKA Erkenntnisse, werden diese Datensätze entsprechend mit einem sogenannten Merker gekennzeichnet und dem niedersächsischen LKA zur weiteren Überprüfung übermittelt. Dadurch wird erkennbar, durch welche Stelle diese zusätzlichen Informationen bzw. Daten bereitgestellt wurden. Nach Auskunft des BfD ist die Nachvollziehbarkeit jederzeit gesichert; eine Vermischung verschiedener Datensätze findet zu keinem Zeitpunkt statt. Durch diesen Umstand ist gewährleistet, dass ich meine datenschutzrechtliche Kontrolle über die niedersächsischen Rasterdatensätze im niedersächsischen LKA jederzeit wahrnehmen kann.

Die Rechtsgrundlage zur Rasterfahndung in Niedersachsen enthält - wie bereits erwähnt - insofern eine wesentliche Einschränkung der Übermittlungsverpflichtung für die öffentlichen und nicht öffentlichen Stellen, als die Übermittlung von personenbezogenen Daten, die einem Amts- oder Berufsgeheimnis unterliegen, nicht verlangt werden darf (vgl. § 45a Abs. 1 S. 3 NGefAG). Ich konnte mich in Zusammenarbeit mit dem BfD davon überzeugen, dass in den erwähnten Abgleichdateien des BKA keine Daten enthalten sind, die einem Amts- oder Berufsgeheimnis unterliegen. Die Abgleichdatensätze enthalten ausschließlich den Vor- und Zunamen, die Geburtsdaten, die Nationalität und ggf. besondere weitere Merkmale der erfassten Personen. Es kann somit definitiv ausgeschlossen werden, dass die niedersächsischen Datensätze beim Abgleich im BKA mit Daten in Berührung kommen, die einem Berufs- oder Amtsgeheimnis unterliegen.

Der konkrete Ablauf der Rasterfahndung in Bund und Ländern mit der abgestimmten, arbeitsteiligen Vorgehensweise macht deutlich, dass die vom BKA vertretene Auslegung der geltenden Regelungen das BKA in die Lage versetzt, auf diese Weise Maßnahmen durchzuführen, die sich zum einen im tatsächlichen Ablauf nicht wesentlich von den Rasterfahndungen in den Ländern unterscheiden und die zum anderen im Ergebnis eine bundesweite polizeiliche Rasterfahndung unter der Federführung des BKA ermöglichen. Es stellt sich die Frage, ob dies der Intention des Gesetzgebers und der Kompetenzordnung von Bund und Ländern im Bereich der Gefahrenabwehr entspricht oder ob hier nicht Änderungen oder Klarstellungen im BKA-Gesetz geboten sind. Ich habe den Bundesbeauftragten für den Datenschutz gebeten, sich dieser Fragen anzunehmen.

Ich werde die Abgleichmaßnahmen bei der Rasterfahndung nach den so genannten Schläfern bis zu ihrem endgültigen Abschluss weiter intensiv begleiten. Über den weiteren Verlauf werde ich berichten.

Zu der Einschränkung des § 45a Abs. 1 Satz 3 NGefAG hat mich die Anfrage des Leiters eines niedersächsischen Landeskrankenhauses erreicht, der wissen wollte, ob

und inwieweit das Landeskrankenhaus verpflichtet wäre, die Anwesenheit von Patienten in einem psychiatrischen Krankenhaus der Polizei auf deren Ersuchen im Rahmen einer Rasterfahndung mitzuteilen. Ich habe ihm geantwortet, dass auch der Aufenthalt in einem Landeskrankenhaus zu den Tatsachen gehört, die einem Amts- oder Berufsgeheimnis unterliegen, sodass die Polizei die Übermittlung solcher Daten nicht verlangen darf. Daneben handelt es sich bei diesen Daten um Angaben, die in dem Verzeichnis gem. § 20 Abs. 2 und 3 NMG (Krankenhäuser und Heime) gespeichert sind. Der Aufenthalt in einem niedersächsischen Landeskrankenhaus ist nur einem beschränkten Personenkreis bekannt und der Betroffene hat an der Geheimhaltung ein schutzwürdiges Interesse. Insbesondere ist § 20 Abs. 2 Satz 3 NMG nicht einschlägig, da diese Vorschrift lediglich eine Auskunft im Einzelfall beim Vorliegen des im Gesetz genannten Gefährdungsgrades (gegenwärtige und erhebliche Gefahr) erlaubt. Diese Gefährdungslage ist bei der Datenerhebung und -übermittlung für die Zwecke der aktuellen Rasterfahndung eindeutig noch nicht erreicht. Eine Übermittlungsbefugnis besteht daher auch nach melderechtlichen Vorschriften nicht.

10.1.3 Änderung des Niedersächsischen Verfassungsschutzgesetzes

Das Innenministerium arbeitet zurzeit an einer Novellierung des Niedersächsischen Verfassungsschutzgesetzes, mit dem offensichtlich vor allem die im Terrorismusbekämpfungsgesetz neu geschaffenen Befugnisse der Verfassungsschutzbehörden in das Landesrecht übernommen werden sollen. Ein Entwurf liegt mir noch nicht vor. Ich werde dieses Gesetzesvorhaben aufmerksam begleiten und hoffe, dass in diesem Zusammenhang dem Landesamt für Verfassungsschutz keine weiteren, über den originären Auftrag des Verfassungsschutzes hinausgehenden Aufgaben (etwa im Bereich der Bekämpfung der organisierten Kriminalität) übertragen oder neue Befugnisse eingeräumt werden, die über den im Terrorismusbekämpfungsgesetz vorgezeichneten Rahmen hinausgehen.

10.1.4 Änderungen des Niedersächsischen Gesetzes zur Ausführung des Gesetzes zu Artikel 10 Grundgesetz

Das sog. BND-Urteil des Bundesverfassungsgerichts vom 14. Juli 1999 (BVerfGE 100, 313 ff.) und die daraufhin auf Bundesebene erfolgte Neufassung des Artikel 10-Gesetzes erforderten eine Anpassung des Niedersächsischen Ausführungsgesetzes zum G 10-Gesetz. Ich hatte hierauf bereits in Nr. 13.2 des XV. TB LfD Nds. 1999/2000 hingewiesen. Ende September 2002 übersandte mir das Innenministerium einen ersten Entwurf, um mir gemäß § 22 Abs. 1 NDSG Gelegenheit zur Stellungnahme zu geben.

In meiner Stellungnahme habe ich insbesondere gefordert, dass angesichts der besonderen Tiefe der Eingriffe durch G 10-Maßnahmen die Entscheidungen der G 10-Kommission einstimmig zu treffen sind. Der Entwurf sah hingegen entsprechend der bisherigen Geschäftsordnung der Kommission vor, eine Mehrheitsentscheidung ausreichen zu lassen. Gleiches gilt auch für die Entscheidung der Kommission, mit der endgültig festgestellt wird, dass die Betroffenen von der Maßnahme nicht unterrichtet werden müssen. Die Benachrichtigung von einer G 10-Maßnahme ist jedoch die letzte Möglichkeit für die Betroffenen, hiergegen Rechtsschutz einzufordern. Eine einstimmige Entscheidung der Kommission ist also auch in diesen

einstimmige Entscheidung der Kommission ist also auch in diesen Fällen erforderlich. Das Innenministerium scheint dieser Auffassung jedoch leider nicht folgen zu wollen.

Letztlich habe ich deutlich gemacht, dass unabhängig von den regelmäßigen Löschungsüberprüfungen im Gesetz festgelegt werden muss, dass die Daten spätestens mit der endgültigen Entscheidung der Kommission, die Betroffenen nicht zu unterrichten, zu löschen sind. Die Gesetzesberatungen sind bislang noch nicht abgeschlossen.

10.1.5 Änderungen des Niedersächsischen Sicherheitsüberprüfungsgesetzes

Ende September 2002 übersandte mir das Innenministerium einen ersten Entwurf zur Stellungnahme. Bereits in früheren Stellungnahmen zu den damaligen Entwürfen eines Niedersächsischen Sicherheitsüberprüfungsgesetzes habe ich insbesondere die vielen unbestimmten Rechtsbegriffe in zentralen Punkten, wie Lebenspartnerin oder Lebenspartner, Sicherheitsrisiko usw. abgelehnt. Diese Ablehnung halte ich nach wie vor aufrecht. In dem aktuellen Entwurf verstärkt sich diese Tendenz leider erheblich. Da nicht nur die in einem sicherheitsempfindlichen Bereich arbeitende Person, sondern auch ihr „Umfeld“ bei einer Sicherheitsüberprüfung durchleuchtet wird, sind Begriffe wie „eine auf Dauer angelegte Gemeinschaft“ mangels entsprechender Eindeutigkeit in keiner Weise geeignet, die tiefgreifenden Einschnitte in das Recht auf informationelle Selbstbestimmung der Betroffenen zu rechtfertigen. Gleiches gilt für die Einfügung der Begriffe „Lebensgefährtin oder Lebensgefährte“.

Grundsätzlich ist aus datenschutzrechtlicher Sicht zu beklagen, dass der Personenkreis, der sich einer Sicherheitsüberprüfung zu unterziehen hat, durch den Gesetzentwurf erheblich ausgeweitet wird. Für eine Sicherheitsüberprüfung reicht nunmehr u.a. eine Tätigkeit in einer Einrichtung aus, die für das Funktionieren des Gemeinwesens unverzichtbar ist und deren Beeinträchtigung erhebliche Unruhen in großen Teilen der Bevölkerung und somit Gefahren für die öffentliche Sicherheit oder Ordnung entstehen lassen würde. Die tiefgreifenden Einschnitte in das Recht auf informationelle Selbstbestimmung sind angesichts einer lediglich „erheblichen Unruhe“ und von nur allgemeinen „Gefahren für die öffentliche Ordnung“ nicht zu rechtfertigen.

10.1.6 Neue Datenverarbeitungssysteme bei der Polizei

Das zurzeit bei den Polizeien des Bundes und der Länder im Betrieb befindliche INPOL-System wurde bereits Anfang der siebziger Jahre konzipiert und in mehreren Stufen realisiert. Es erreichte Ende der achtziger Jahre sowohl fachlich als auch technisch seine Grenzen. Damit begann die Neukonzipierung eines gemeinsamen Informations- und Fahndungssystems der deutschen Polizei. Im Jahre 1990 wurde in den INPOL-Grundsätzen definiert, dass INPOL das gemeinsame, arbeitsteilige, elektronische Informationssystem der Polizeien der Länder und des Bundes zur Unterstützung vollzugspolizeilicher Aufgaben ist, in dem die dafür genutzten IT-Einrichtungen der Länder in einem Verbund zusammenwirken.

Im April 2001 sollte das Projekt INPOL-neu gestartet werden und in den sog. Echtbetrieb übergehen. Dies ist gescheitert, weil das ganze Projekt offensichtlich bislang

überdimensioniert war. Nach diesem Fehlstart wurde INPOL-neu einer umfangreichen Revision durch einen unabhängigen Gutachter unterworfen. Die Untersuchung ergab, dass die von der Polizei an INPOL-neu gestellten Anforderungen an die Grenze der Machbarkeit gehen und zu einer völlig unzureichenden Performance führen würden. Als Zeitpunkt für einen neuen Startversuch einer „abgespeckten“ Version wird Ende 2003 angegeben. Meine datenschutzrechtlichen Bedenken zu INPOL-neu habe ich bereits in den vergangenen Tätigkeitsberichten dargestellt. Seit 1996 berät eine „Arbeitsgruppe INPOL-neu“ der Datenschutzbeauftragten des Bundes und der Länder die Projektgruppe beim BKA. Die dort aufgeworfenen datenschutzrechtlichen Bedenken wurden durch die Polizei leider nur in geringem Umfang aufgegriffen. Es ist aus datenschutzrechtlicher Sicht insbesondere nicht zu verantworten, dass der Kriminalaktennachweis (KAN) um Fälle unterhalb der im Gesetz verankerten Relevanzschwelle erweitert werden soll. Weiterhin ist es nicht zu akzeptieren, dass die Bedeutung von Straftaten (und damit die Speicherung der entsprechenden Daten) in den teilnehmenden Ländern unterschiedlich beurteilt wird. Auch ist sicherzustellen, dass bei der Übernahme der Daten aus INPOL-aktuell in INPOL-neu die gesetzlichen Vorgaben für die Einspeicherung von Daten nach dem BKA-Gesetz eingehalten werden. Ein weiteres Hauptaugenmerk werde ich auf geplante Dateien legen, die Aufzeichnungen in Form von Lichtbildern und Videos von Personen beinhalten.

Die Niedersächsische Landesregierung hat im Jahr 2000 das Innenministerium mit dem Projekt beauftragt, die Datenverarbeitung bei der niedersächsischen Polizei durch die Entwicklung eines Vorgangsbearbeitungssystems (Arbeitsname: Mikado-neu) so auszugestalten, dass eine Teilnahme am bundesweiten Verbund INPOL-neu sichergestellt werden kann. Die oben geschilderte Neukonzeption des gemeinsamen Informationssystems der Polizeien des Bundes und der Länder erfordert nämlich auch die Anpassung der niedersächsischen polizeilichen Datenverarbeitungssysteme. Das Projekt soll ein umfassendes IT-System realisieren, das alle vollzugspolizeilichen Prozesse der Vorgangsbearbeitung, Auswertung und Statistik beinhaltet und eine Bedienung und Nutzung von INPOL-neu gewährleistet. Die Gesamtverantwortung für das Projekt besitzt der sog. Lenkungsausschuss, der die notwendigen Leitentscheidungen trifft. Der Ausschuss setzt sich aus Vertretern des Innenministeriums, der Direktoren der Polizei, des Finanzministeriums und des Justizministeriums zusammen. In dem Datenverarbeitungssystem werden in naher Zukunft eine Vielzahl von personenbezogenen Daten, auch sensibelster Art, verarbeitet. Aus diesem Grund habe ich mich seit Beginn des Projekts fortlaufend über den Sachstand informiert und nehme regelmäßig an den Lenkungsausschusssitzungen teil. Insgesamt kann ich bislang feststellen, dass die datenschutzrechtlichen Gesichtspunkte und Anforderungen bei der Entwicklung des Systems beachtet werden. Neue Aspekte werden frühzeitig an mich herangetragen und gemeinsam gelöst.

Am 26. April 2002 wurde zum Abschluss eines landesweiten Ideenwettbewerbs der neue Name für dieses System vorgestellt; er lautet „NIVADIS“ (**Ni**edersächsisches **V**organgsbearbeitungs-, **A**nalyse-, **D**okumentations- und **I**nformations**s**ystem). Um sicherzustellen, das „NIVADIS“ auf eine breite Akzeptanz bei den Anwendern trifft, wurden bereits mehrere Tests mit den späteren Anwendern durchgeführt. Über den weiteren Verlauf der Projekte werde ich berichten.

10.1.7 Videoeinsatz in Funkstreifenwagen der Polizei

Die zahlreichen gewalttätigen Übergriffe auf Polizeibeamte in der jüngeren Vergangenheit hatten den Wunsch der Polizei zur Folge, auch technische Hilfsmittel zur Steigerung der Eigensicherung im täglichen Funkstreifendienst einzusetzen. Der Arbeitskreis II der Ständigen Innenministerkonferenz hat daher beschlossen, eine breit angelegte Erprobung zur Ausstattung von Funkstreifenwagen mit Videosystemen für Eigensicherungszwecke in den Ländern durchzuführen. Das niedersächsische Innenministerium hat mit Erlass vom 13. Dezember 2001 die Polizeidirektion Hannover mit der technischen Erprobung und Bewertung von sog. Prototypen beauftragt.

In zwei Funkstreifenwagen der Polizeidirektion Hannover wurde eine Aufzeichnungsanlage eingebaut, die von außen kaum erkennbar ist. Die Kamera wird aktiviert, wenn die Leuchtschrift „Stop Polizei“ aufleuchtet, um einen vorausfahrenden Wagen anzuhalten. Gleichzeitig wird der Ton („das gesprochene Wort“) im Innenraum des Funkstreifenwagens aufgezeichnet. Es ist den eingesetzten Polizeibeamten auch möglich, die Aufzeichnung manuell (unabhängig von einer konkreten Kontrollsituation) zuzuschalten. Das aufnehmende Objektiv ist am Innenspiegel des Funkwagen befestigt und zeigt in Fahrtrichtung. Es wird ungefähr die Situation aufgezeichnet, die der Fahrer beim Heraussehen aus dem Fahrzeug wahrnimmt. Es wird (zunächst) durch keine Maßnahme auf die Videokontrolle hingewiesen. Der Erlass schreibt jedoch vor, die Betroffenen zu Beginn der Kontrolle hierauf mündlich hinzuweisen. Als Rechtsgrundlage in Niedersachsen ist § 32 Abs. 3 NGefAG einschlägig. Danach darf die Polizei öffentlich zugängliche Orte mittels Bildübertragung offen beobachten, wenn dies u.a. zur Gefahrenabwehr und -vorsorge erforderlich ist. Die Bilder dürfen darüber hinaus auch aufgezeichnet werden, wenn Tatsachen die Annahme rechtfertigen, dass an diesem Ort künftig Straftaten von erheblicher Bedeutung begangen werden.

Aus meiner Sicht liegen solche Tatsachen bei Anhalte- und Kontrollsituationen in aller Regel nicht vor, sodass nur eine offene Beobachtung, nicht aber die Aufzeichnung statthaft wäre. Auf diesen Umstand habe ich das Niedersächsische Innenministerium hingewiesen. Allerdings ist es unstreitig, dass nur eine entsprechende Aufzeichnung zur Verbesserung der Eigensicherung beitragen kann, eine reine Beobachtung kann den angestrebten Zweck nicht erreichen. Ich habe daher meine Bereitschaft zu einer einvernehmlichen Lösung erklärt, denn auch ich halte den angestrebten Technikeinsatz für eine gute Möglichkeit, die Sicherheit der Polizeibeamten in ihrem täglichen Einsatz zu erhöhen. Aus diesem Grund habe ich angeboten, vor einem Echteinsatz der Videotechnik an der entsprechenden Erlassregelung intensiv mitzuarbeiten, um eine insgesamt datenschutzgerechte Lösung zu erreichen. Insbesondere muss die zeitgerechte Löschung der Aufnahmen (direkt im Anschluss an eine Streifenfahrt ohne besondere Vorkommnisse) festgeschrieben werden. Auch ist sicherzustellen, dass nur explizit genannte Personen die gespeicherten Filme betrachten können. Natürlich dürfen die Aufzeichnungen auch nicht zu einer Verhaltens- oder Leistungskontrolle der eingesetzten Beamten genutzt werden. Bei entsprechenden Vorgaben würde ich das Verfahren aus meiner Sicht unterstützen.

10.2 Ausländerangelegenheiten

10.2.1 Der gläserne Ausländer

Der 11. September 2001 hat auch das deutsche Gemeinwesen aufgeschreckt. Wie jedes Mal, wenn die Menschen sich bedroht fühlen, steigt der Stellenwert der Sicherheit und bekommt Vorrang vor den individuellen Freiheitsrechten, besonders wenn es nicht um die eigenen Freiheitsrechte geht.

Eine Reaktion des Staates auf den 11. September war das Terrorismusbekämpfungsgesetz (vgl. Kapitel 10.1.1). Es enthält nicht nur für deutsche Bürger, sondern insbesondere für die in Deutschland lebenden bzw. nach Deutschland - sei es auch nur zu einem Besuch - strebenden Ausländer einschneidende Regelungen für ihr Recht auf informationelle Selbstbestimmung.

Mit diesem Artikelgesetz wurden insgesamt 23 Gesetze und Verordnungen geändert. Insbesondere für Ausländer bedeutsam sind die Änderungen im Bundesverfassungsschutzgesetz, Ausländergesetz, Asylverfahrensgesetz und Ausländerzentralregistergesetz. Hier sind Regelungen geschaffen worden, durch die Eingriffe in das Recht auf informationelle Selbstbestimmung von Ausländern in der Zukunft in wesentlich größerem Umfang möglich sind als bisher.

Zu den Verschärfungen im Einzelnen:

- Das Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) und die Ausländerbehörden erhalten gem. § 18 Abs. 1a des Bundesverfassungsschutzgesetzes (BVerfSchG) das Recht, von sich aus personenbezogene Informationen an das Bundesamt für Verfassungsschutz (BfV) zu übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Kenntnis dieser Daten für die Aufgabenerfüllung des BfV gemäß § 3 Abs. 1 BVerfSchG erforderlich ist. Für den Asylbereich ist zu besorgen, dass damit eine Vielzahl von Informationen aus dem jeweiligen Asylverfahren beim Verfassungsschutz landen werden. Da die Begründung der Asylanträge höchst sensible Angaben über politische Aktivitäten der Betroffenen enthält, muss im Auge behalten werden, dass die Verfassungsschutzbehörden auch auf internationaler Ebene zusammenarbeiten und Informationen austauschen. So kann nicht ausgeschlossen werden, dass diese sensiblen Daten im Zuge der internationalen Zusammenarbeit u.a. auch bei dem Staat landen, aus dem die Betroffenen geflohen sind. Die Verwendung der Daten durch das Herkunftsland ist natürlich von Deutschland aus kaum zu beeinflussen oder auch nur zu kontrollieren.
- Die Aufnahme weiterer biometrischer Merkmale (Angaben zu Fingern, Händen oder Gesicht) in Pässe und Personalausweise der deutschen Bevölkerung ist durch ein Gesetz zu regeln. Vergleichbare Ausländerausweise bzw. -dokumente werden diese Änderungen ebenfalls erhalten, jedoch bedarf es zur Einführung lediglich einer entsprechenden Rechtverordnung (vgl. § 5 Abs. 6 Ausländergesetz [AuslG]). Durch die Aufnahme einer maschinenlesbaren Zone in die Dokumente sind diese biometrischen Merkmale als Personenkennzeichen verwendbar und

können somit genutzt werden, um die unterschiedlichsten Datenbanken zu erschließen.

- Gemäß § 41 Abs. 2 AuslG, § 16 Abs. 2 Asylverfahrensgesetz (AsylVfG) darf nunmehr das „gesprochene Wort“ eines Ausländers zur Bestimmung des Herkunftsstaates aufgenommen und ausgewertet werden. Die Sprachproben werden 10 Jahre lang aufbewahrt, auch wenn durch ein Gutachten die Herkunft des Betroffenen bereits geklärt ist. Die Möglichkeit, die Sprachproben auch für Zwecke eines Strafverfahrens oder zur Gefahrenabwehr nutzen zu dürfen, stellt alle Betroffenen zunächst unter einen Generalverdacht und bedeutet insofern eine unzulässige Datenhaltung auf Vorrat.
- Bereits nach der bisherigen Gesetzeslage wurden von allen Bürgerkriegsflüchtlingen Fingerabdrücke zur Identitätssicherung erhoben. Dieses Verfahren wird nun auf weitere Ausländergruppen ausgeweitet (§ 41 Abs. 3 AuslG), auch wenn bei diesen kein Zweifel an ihrer Identität besteht, weil sie z.B. in einen Drittstaat zurückgeschoben werden. Außerdem sind von allen mindestens vierzehn Jahre alten Ausländern, die unerlaubt eingereist sind oder sich illegal und ohne Duldung in Deutschland aufhalten, die Abdrücke aller zehn Finger zu erfassen. All diese Daten werden zentral beim Bundeskriminalamt bis zu zehn Jahre gespeichert (§ 78 Abs. 4 AuslG). Dadurch, dass auch diese Daten nach § 78 Abs. 3 AuslG bzw. § 16 Abs. 5 AsylVfG für Zwecke eines Strafverfahrens oder zur Gefahrenabwehr genutzt werden dürfen, sind wiederum alle Betroffenen unter einen entsprechenden Generalverdacht gestellt und die Daten insoweit auf Vorrat gespeichert.
- Bei der Visaerteilung und vor der Erteilung oder Verlängerung einer sonstigen Aufenthaltsgenehmigung werden nunmehr zur Feststellung extremistischer Bestrebungen Regelanfragen beim Bundesamt für Verfassungsschutz, dem Bundesnachrichtendienst, dem Militärischen Abschirmdienst, dem Bundeskriminalamt und dem Zollkriminalamt gestellt, wenn die Betroffenen aus sog. Schurkenstaaten kommen. Die mit den Anfragen zwangsläufig übermittelten Daten dürfen diese Sicherheitsbehörden für ihre eigenen Zwecke nutzen.
- Nach § 3 Abs. 5 des Gesetzes über das Ausländerzentralregister (AZRG) darf nunmehr die „freiwillige Angabe zur Religionszugehörigkeit“ gespeichert werden. Nach § 29 dieses Gesetztes sollen derartige Angaben auch in der Visadatei gespeichert werden. Weiterhin erhielten die Landesluftfahrtbehörden gem. § 15 AZRG die Befugnis zum Datenabruf aus dem Ausländerzentralregister für Zwecke der Zuverlässigkeitsüberprüfungen. Die Geheimdienste, die bisher nur in eilbedürftigen Fällen und nur auf Personalien und Verwaltungsdaten zugreifen durften, haben nunmehr das Recht, auf den gesamten Bestand des Ausländerzentralregisters automatisiert, also online, zuzugreifen.
- Das Zuwanderungsgesetz vom 20. Juni 2002 soll zum 1. Januar 2003 in Kraft treten. Hierdurch soll das (noch stark polizeirechtlich ausgerichtete) Ausländergesetz durch ein reines Aufenthaltsgesetz ersetzt werden. Dennoch sind alle durch das Terrorismusbekämpfungsgesetz erfolgten (polizei- und sicherheitsrechtlichen) Änderungen in das neue Gesetz übernommen worden. Zudem werden in dem Bundesamt für Migration und Flüchtlinge (BAMF) alle bisherigen Ausländerbehörden des Bundes organisatorisch zusammengeführt. Es entsteht somit eine Behörde, die praktisch alle Daten gespeichert hat, die es über Ausländer in Deutschland und, soweit sie ein Visum benötigen, auch über solche im Ausland gibt.

10.2.2 Wertgutscheine für Asylbewerber

Bereits 1995 hatte ich mich gegen eine im Runderlass des Niedersächsischen Innenministeriums vom 14. August 1995 vorgesehene Regelung, nach der Gutscheine möglichst auf den Namen einer bestimmten Person ausgestellt werden sollten, erfolgreich gewandt. Die Regelung wurde daraufhin gestrichen. Aufgrund von Beschwerden Betroffener und Hinweisen von dritter Seite, dass mit der Ausgabe bzw. Einlösung von Wertgutscheinen an Asylbewerber eine Offenbarung personenbezogener Daten erfolge, habe ich mich der Problematik erneut zugewandt.

Im Zuge meiner weiteren Kontaktaufnahmen zum Innenministerium teilte dieses mit, bei der Ausgabe von Wertgutscheinen handele es sich um „nicht übertragbare“ personenbezogene Leistungen nach dem Asylbewerberleistungsgesetz (AsylbLG). In der Vergangenheit seien Wertgutscheine in Bargeld umgetauscht worden und Betrugsfälle bekannt geworden, wodurch sich die namentliche Kennzeichnung der Wertgutscheine mit der Möglichkeit einer Identitätskontrolle aufgedrängt habe. Wie sich in Besprechungen mit dem Innenministerium herausstellte, hatte dieses bis dahin selbst kein genaues Bild über die Verfahrensweise der einzelnen Kommunen/Leistungsträger. Eine detaillierte Umfrage des Ministeriums bei den Leistungsträgern konnte inzwischen abgeschlossen werden. Sie hatte zum Ergebnis, dass von den Leistungsträgern, die mit einer Firma, die für die Mehrzahl der Leistungsträger in Niedersachsen Wertgutscheine erstellt, zusammenarbeiten, für die Erstellung der Wertgutscheine keine personenbezogenen Daten übermittelt werden. Die Wertgutscheine selbst enthalten keine personenbezogenen Daten, sondern nur eine laufende Nummer, weil dies aus drucktechnischen Gründen erforderlich ist. Nach Angaben des Ministeriums haben von 50 Leistungsträgern in Niedersachsen 25 einen Vertrag mit der betreffenden Firma abgeschlossen. Die anderen Leistungsträger haben, wie weiter mitgeteilt wird, entweder eigene Verfahren oder bedienen sich anderer Dritter. Im Ergebnis bestehen datenschutzrechtliche Bedenken lediglich gegen die Verfahrensweise bei sieben der von 50 Leistungsträgern angewendeten Verfahren. Meine Kontakte zum Ministerium und die gemeinsamen Bemühungen zur Erreichung eines datenschutzgerechteren Verfahrens dauern an.

10.2.3 Einbürgerungen

§ 85 Abs. 1 Nr. 1 Ausländergesetz (AuslG) regelt, dass Ausländer unter bestimmten Voraussetzungen dann einen Anspruch auf Einbürgerung haben, wenn sie sich gegenüber der Einbürgerungsbehörde ausdrücklich zur freiheitlichen demokratischen Grundordnung der Bundesrepublik Deutschland bekennen und eine entsprechende Loyalitätserklärung abgeben (1. Alternative) oder glaubhaft machen, dass sie sich von der früheren Verfolgung oder Unterstützung verfassungswidriger Bestrebungen abgewandt haben (2. Alternative). § 86 AuslG besagt, dass dieser Einbürgerungsanspruch dann nicht besteht, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass der Einbürgerungsbewerber Bestrebungen gegen die Verfassung der Bundesrepublik Deutschland verfolgt oder verfolgt hat (Nr. 2) oder wenn in seiner Person ein staatsschutzrechtlich motivierter Ausweisungsgrund nach § 46 Nr. 1 AuslG vorliegt (Nr. 3).

Fraglich war, ob und in welcher Weise die Behörde abklären darf, ob die Loyalitätserklärung auch „materiell wahrheitsgemäß“ ist. Mit nicht veröffentlichtem RdErl. des Innenministeriums vom 1. Februar 2001 wurde Folgendes bestimmt: Das Bekenntnis zur freiheitlichen demokratischen Grundordnung und die Loyalitätserklärung sind grundsätzlich im Anschluss an die Belehrung über die Bedeutung des Bekenntnisses und der Erklärung schriftlich oder zur Niederschrift zu geben. Ergeben sich tatsächliche Anhaltspunkte für eine politisch-extremistische Betätigung des Einbürgerungsbewerbers, ist eine Anfrage an das Niedersächsisches Landesamt für Verfassungsschutz zu richten, ob Sicherheitsbedenken gegen die Einbürgerung bestehen (anlassbezogene Prüfung). Eine Regelanfrage an die Verfassungsschutzbehörde findet nicht statt. Datenschutzrechtlich bestehen hiergegen aus meiner Sicht keine Einwände.

10.2.4 Datenschutz im Asylverfahren - Abschiebung einer Familie

Ein Petent hat sich bei mir darüber beschwert, dass ein Amtsträger einer Kreisverwaltung in einem Zeitungsbericht personenbezogene Daten einer nach Albanien abgeschobenen Familie veröffentlicht und hierdurch in das Recht auf informationelle Selbstbestimmung der Betroffenen eingegriffen habe. Die von mir um Stellungnahme gebetene Behörde teilte mit, dass in der Presse unzutreffende Behauptungen aufgestellt worden seien und dass diese hätten richtig gestellt werden müssen. Durch die Richtigstellung in der Öffentlichkeit bis dahin unbekannter Sachverhalte kam es jedoch erst zu der gerügten Datenübermittlung. Für eine Richtigstellung unzutreffender Behauptungen und zum Schutz der Mitarbeiter des Ausländeramtes vor weiteren unbegründeten Vorwürfen hätte es genügt, zu erklären, dass die veröffentlichten Darstellungen unzutreffend sind; eine Bekanntgabe konkreter Einzelheiten hätte aber zur Wahrung des Rechts auf informationelle Selbstbestimmung der Betroffenen unterbleiben müssen. Ich habe dieses Verhalten kritisiert.

10.2.5 Aufenthaltsrechtliche Behandlung von Ausländern in gleichgeschlechtlichen Lebensgemeinschaften

In einer Eingabe beschwerte sich ein Petent darüber, dass dem ausländischen Lebenspartner eines Deutschen in seine Aufenthaltserlaubnis (§ 27a AuslG) der folgende Vermerk eingetragen wurde: „Erlischt mit Beendigung der gleichgeschlechtlichen Lebensgemeinschaft“. Der Eintrag sollte nach Ansicht der zuständigen Ausländerbehörde eine sog. Nebenbestimmung zur Aufenthaltsgenehmigung nach § 12 AuslG sein. Für den Petenten bedeutete der Eintrag in jeder Situation, in der er seinen Pass vorzeigen muss, ein „Zwangsouting“. Er fühlte sich hierdurch in seinem Recht verletzt, selbst darüber zu entscheiden, wem er die Information weitergeben will, dass er homosexuell ist.

Das von mir eingeschaltete Innenministerium verwies auf seinen Erlass vom 17. Mai 2000, in dem es folgenden Formulierungsvorschlag für den Text einer auflösenden Bedingung für die Aufenthaltserlaubnis eines ausländischen gleichgeschlechtlichen Lebenspartners gemacht hatte: „Die Aufenthaltserlaubnis erlischt mit der Beendigung des Aufenthaltszwecks“. In dem Erlass hat das Ministerium darauf hingewiesen, dass Ausländer bei einer Aufenthaltsbeendigung aufgrund der Auflösung einer gleichge-

schlechtlichen Lebensgemeinschaft u. U. im Heimatland einer strafrechtlichen Verfolgung ausgesetzt sein könnten, weil durch die in ihrem Pass eingetragene Bedingung ein Hinweis auf die gleichgeschlechtliche Lebensgemeinschaft gegeben wurde. Die empfohlene neutrale Formulierung trägt den datenschutzrechtlichen Anforderungen Rechnung.

10.3 Meldewesen

Das vom Bundestag mit Zustimmung des Bundesrates am 25. März 2002 beschlossene Gesetz zur Änderung des Melderechtsrahmengesetzes und anderer Gesetze ist am 4. April 2002 in Kraft getreten. Mit dem Gesetz wird u.a. das Ziel verfolgt, die erforderlichen Rahmenbedingungen für die Nutzung moderner Informations- und Kommunikationstechnologien zu schaffen und unnötige Meldepflichten abzuschaffen. Weitere Änderungen sollen der Verbesserung der Bürgerfreundlichkeit und des Datenschutzes sowie der Erhaltung der Rechtssicherheit im Meldewesen dienen. Von den Herausforderungen der neuen Informations- und Kommunikationstechnologien ist das Meldewesen in besonderem Maße betroffen, weil in diesem Verwaltungsbereich ein häufiger Kontakt mit Bürgern besteht. Die in vielen Bereichen der Gesellschaft bereits gegebenen Möglichkeiten der elektronischen Kommunikation konnten dort bislang noch nicht genutzt werden, weil die geltenden gesetzlichen Bestimmungen dies nicht zuließen.

Mit dem Änderungsgesetz werden die rechtlichen Voraussetzungen zur Nutzung der elektronischen Dienste geschaffen. Im Einzelnen wird die elektronische Anmeldung zugelassen, mit der das sowohl für die Bürger als auch für die Verwaltung kosten- und zeitaufwendige Anmeldeverfahren mittelfristig erheblich vereinfacht und beschleunigt werden kann. Voraussetzung hierfür ist eine zügige und flächendeckende Verbreitung der qualifizierten elektronischen Signatur nach den Vorschriften des Signaturgesetzes. Des Weiteren erhält der Betroffene künftig einen elektronischen Zugang zu den über ihn im Melderegister gespeicherten Daten. Auch für die elektronische Übermittlung von Meldedaten an Behörden des Inlands, Mitgliedsstaaten der EU und Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR-Vertragsstaaten), Stellen der europäischen Gemeinschaften sowie an Privatstellen werden Regelungen geschaffen. Dabei war durch technisch-organisatorische Vorgaben zu gewährleisten, dass in diesen Fällen durch den Technik-Einsatz die materiell-rechtlichen Voraussetzungen für einen Zugriff auf Meldedaten nicht unterlaufen werden.

Zu den datenschutzrechtlich relevanten Änderungen im Einzelnen:

Mit der Abschaffung der Abmeldepflicht bei Umzügen im Inland und dem Verzicht auf die Mitwirkungspflicht des Wohnungsgebers beim Meldevorgang bricht das Gesetz erfreulicherweise mit einer jahrzehntelangen Praxis, weil sich herausgestellt hat, dass diese Meldepflichten für die Richtigkeit des Melderegisters nur noch von untergeordneter Bedeutung sind, jedoch die Meldepflichtigen und die Meldebehörden in einem nicht mehr vertretbaren Umfang belasten.

Das Gesetz sieht vor, dass Einwohner künftig die Möglichkeit haben, nach näherer Maßgabe des Landesrechts auch im Wege des automatisierten Abrufs über das Internet Auskunft über ihre im Melderegister gespeicherten Daten zu erlangen. Dabei ist zu gewährleisten, dass dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden, die insbesondere die Vertraulichkeit und die Unversehrtheit der im Melderegister gespeicherten und an den Betroffenen übermittelten Daten gewährleisten. Der Nachweis der Urheberschaft des Antrags ist durch eine qualifizierte elektronische Signatur nach dem Signaturgesetz zu führen.

Ebenso kann durch Landesrecht bestimmt werden, dass auch die Anmeldung durch elektronische Datenübertragung erfolgen kann (§ 11 Abs. 2). Dabei ist wie bei der Auskunft an den Betroffenen zu gewährleisten, dass dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden. Auch hier ist der Nachweis der Urheberschaft der Anmeldung durch eine qualifizierte elektronische Signatur nach dem Signaturgesetz zu führen.

Bei Anmeldung eines Einwohners hat die Meldebehörde die bisher zuständige Meldebehörde und die für weitere Wohnungen zuständigen Meldebehörden davon unter Einhaltung der notwendigen Datensicherheitsmaßnahmen unverzüglich möglichst auf automatisiert verarbeitbaren Datenträgern oder durch Datenübertragung zu unterrichten.

Die Regelung zur Datenübermittlung an andere Behörden oder sonstige öffentliche Stellen erstreckt sich auch auf öffentliche Stellen in anderen EU-Staaten, in EWR-Vertragsstaaten oder Organe und Einrichtungen der Europäischen Gemeinschaften im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen. Auch in diesen Fällen dürfen die Daten nach Maßgabe des Landesrechts auf automatisiert verarbeitbaren Datenträgern oder durch Datenübertragung übermittelt werden, wenn über die Identität der anfragenden Stelle kein Zweifel besteht und Übermittlungssperren und Auskunftssperren nicht vorliegen. Auch hier müssen die notwendigen Datensicherungsmaßnahmen getroffen werden.

Aus datenschutzrechtlicher Sicht besonders bedeutsam ist die Regelung in § 21 Abs. 1a, wonach künftig auskunftssuchenden Personen von der Meldebehörde einfache Melderegisterauskünfte (Auskunft über Vor- und Familiennamen, Doktorgrad und Anschriften einzelner bestimmter Einwohner) auf automatisiert verarbeitbaren Datenträgern, durch Datenfernübertragung oder im Wege des automatisierten Abrufs über das Internet erteilt werden dürfen. Voraussetzung ist, dass

1. der Antrag in der amtlich vorgeschriebenen Form gestellt ist,
2. der Antragsteller den Betroffenen mit Vor- und Familiennamen sowie mindestens zwei weiteren gespeicherten Daten bezeichnet hat und

3. die Identität des Betroffenen durch einen automatisierten Abgleich der im Antrag angegebenen mit den im Melderegister gespeicherten Daten des Betroffenen eindeutig festgestellt worden ist.

Ein automatisierter Abruf über das Internet ist allerdings dann nicht zulässig, wenn die Betroffenen dieser Form der Auskunftserteilung widersprochen haben. Diese Einschränkung ist auf Anregung der Datenschutzbeauftragten in das Gesetz aufgenommen worden und soll der besonderen Gefährdungssituation Rechnung tragen, die bei einer Übertragung von Daten über das Internet nach wie vor gegeben ist. Die der Meldebehörde überlassenen Datenträger oder übermittelten Daten sind nach Erledigung des Antrags unverzüglich zurückzugeben, zu löschen oder zu vernichten.

Bei Bestehen einer Auskunftssperre, also wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange glaubhaft gemacht worden war, war nach den bisherigen Bestimmungen des MRRG jede Melderegisterauskunft unzulässig. Diese Regelung hat sich bewährt. Aus Datenschutzsicht ist daher zu bedauern, dass nunmehr trotz entsprechender Gefahrenlage eine Risikoabwägung im Einzelfall vorzunehmen ist, ob eine Melderegisterauskunft erteilt werden darf (§ 21 Abs. 5 Satz 2 MRRG).

Die Forderung der Datenschutzbeauftragten des Bundes und der Länder, gesetzlich zu regeln, dass eine Einwilligung der Betroffenen Voraussetzung für Datenweitergaben an Parteien, Wählergruppen pp. im Zusammenhang mit Wahlen zum Deutschen Bundestag oder zum Europäischen Parlament sein soll, findet sich im Gesetz nicht wieder. Bedauerlicherweise bestimmt das MRRG lediglich, dass die Wahlberechtigten auf ihr Widerspruchsrecht bei der Anmeldung und spätestens acht Monate vor Wahlen durch öffentliche Bekanntmachung hinzuweisen sind. Auch der Forderung der Datenschutzbeauftragten des Bundes und der Länder, die Hotelmeldepflicht abzuschaffen, da die hiermit verbundene millionenfache Datenerhebung auf Vorrat unverhältnismäßig ist, wurde im Gesetz leider nicht entsprochen.

Die sich aus der Neufassung des MRRG für das Landesrecht ergebenden Folgerungen hat Niedersachsen bislang noch nicht umgesetzt. Erfahrungen mit der Handhabung der neuen technischen Möglichkeiten im Meldeverfahren liegen deshalb noch nicht vor.

11 Justiz

11.1 Rechtspflege

11.1.1 eJustice

In Nr. 5.4 des XV. TB LfD Nds. 1999/2000 hatte ich bereits meine Überzeugung zum Ausdruck gebracht, dass die öffentliche Verwaltung die neuen Wege zum eGovernment gehen muss. Mein besonderes Anliegen war und ist es dabei, die öffentliche Verwaltung hierbei tatkräftig zu unterstützen. Dies galt z.B. auch für das Projekt „Datenschutzgerechtes eGovernment der Stadt Hannover“. Das Projekt will Wege zu mehr Bürgerfreundlichkeit aufzeigen und Perspektiven für effektive und effiziente

Arbeitsabläufe in der Verwaltung entwickeln. Gleiche Ziele verfolgen Planungen im Bereich der Justiz durch Einführung des elektronischen Rechtsverkehrs bei Gerichten und Staatsanwaltschaften. Der Begriff „Elektronischer Rechtsverkehr“ beinhaltet eine neue Qualität und Form der Wahrnehmung anfallender Aufgaben und wird immer dann gebraucht, wenn sowohl die Übermittlung der einzelnen Erklärungen von den Beteiligten zum Gericht und der Entscheidungen und Mitteilungen des Gerichts an die Beteiligten als auch die Speicherung bzw. gerichtsinterne Verarbeitung dieser Erklärungen in elektronischer Form erfolgen. Werden die Erklärungen lediglich elektronisch übermittelt, im Übrigen jedoch auf Papier ausgedruckt und in Akten verwaltet, wird der Begriff „Elektronische Kommunikation“ verwendet.

Aus meiner Sicht ist die Einbeziehung der neuen Informations- und Kommunikationstechniken in die Geschäftsabläufe der Justiz nachdrücklich zu begrüßen, auch wenn sich dabei viele Fragen stellen, die so bei den herkömmlichen Bearbeitungsverfahren nicht auftraten. Ich bin im Rahmen meiner personellen Ressourcen gerne bereit, bei dieser Zukunftsentwicklung in gleicher Weise wie gegenüber der Verwaltung beim eGovernment Beratungshilfe zu leisten und tatkräftig an der Entwicklung von Lösungen mitzuwirken, die den Anforderungen von Datenschutz und Datensicherheit Rechnung tragen und zugleich eine nutzerfreundliche Verfahrensausgestaltung beinhalten.

Die Datenschutzbeauftragten des Bundes und der Länder haben im Arbeitskreis Justiz eine Arbeitsgruppe gebildet, die am 23. Januar 2002 erstmals zusammentrat und einzelne Arbeitsaufträge an die Teilnehmer vergeben hat, etwa zu Fragen des Zugänglichmachens von gerichtlichen Entscheidungen, des Zugangs der Parteien zum Gericht oder der privaten Nutzung öffentlicher Register. Außerdem sind die von der Arbeitsgruppe „Elektronischer Rechtsverkehr“ der Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz (BLK) erarbeiteten organisatorisch-technischen Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften (OT-Leit-ERV) als Grundlage für den Erlass von Rechtsverordnungen zur Einführung sowie zur Anwendung des elektronischen Rechtsverkehrs datenschutzrechtlich bewertet worden. Aus personellen Gründen konnte ich meine ursprünglich vorgesehene Beteiligung in der Arbeitsgruppe des Arbeitskreises Justiz leider aktuell nicht wahrnehmen. Ich werde den Fortgang der Arbeiten der Arbeitsgruppe „Elektronischer Rechtsverkehr“ aus datenschutzrechtlicher Sicht jedoch weiterhin kritisch begleiten.

11.1.2 Öffnung von Registern und anderen Datenbanken für das Internet

Nach dem vorläufigen Schlussbericht der BLK stellt der elektronische Rechtsverkehr für den Bereich des Grundbuch- und Registerwesens die konsequente Fortsetzung der Führung der elektronischen Register dar. Bereits heute eröffnen das elektronisch geführte Grundbuch und viele Register die Möglichkeit, elektronisch Auskunft zu erteilen und bestimmte Mitteilungen elektronisch zu übermitteln.

Wenngleich durch das Registerverfahrenbeschleunigungsgesetz vom 20. Dezember 1993 die Automation des Grundbuchs und Handelsregisters und der weiteren öffentlichen Register ermöglicht wurde, ist auf der Grundlage der bestehenden Gesetze der nächste Schritt in Richtung des elektronischen Rechtsverkehrs im Grundbuchverfah-

ren und Registerverfahren allerdings noch nicht möglich, weil die dazu notwendige Änderung von Vorschriften über die Grund- und Registerakten noch nicht erfolgt ist. Durch das Registerverfahrenbeschleunigungsgesetz wurden die Landesregierungen ermächtigt, das Grundbuch sowie die in § 126 Abs. 2 Grundbuchordnung (GBO) bezeichneten Verzeichnisse in maschineller Form als automatisierte Datei zu führen. Einen wesentlichen Arbeitsbereich der maschinellen Grundbuchführung stellt hier die Einsicht in das Grundbuch im automatisierten Abrufverfahren mittels Datenübertragung dar. Das automatisierte Abrufverfahren soll jedoch nur die technische Durchführung der Grundbucheinsicht vereinfachen, nicht dagegen die Einsichtsbefugnisse ausdehnen. Ein Abruf ist somit nach wie vor nur insoweit möglich, als ein berechtigtes Interesse im Sinne der §§ 12, 12a GBO dargelegt wird. Gegen die künftige Digitalisierung von Grundakten bestehen nach der Schaffung der erforderlichen Rechtsgrundlagen keine datenschutzrechtlichen Bedenken. Allerdings wäre ihr Zugang für „jedermann“ problematisch.

Mit der Digitalisierung von Registern (Handels-, Vereins-, Partnerschafts- und Genossenschaftsregister und Verzeichnisse) ergeben sich bei der Übermittlung von Daten neue Fragestellungen. Grundsätzlich muss zwischen zwei Benutzerkreisen unterschieden werden, für die unterschiedliche Voraussetzungen gelten: Im Rahmen der internen Auskunft können Gerichte, Justiz- und sonstige Behörden Online-Zugriff auf Register nehmen; im Rahmen der externen Auskunft benennt der Schlussbericht der BLK als Ziel, jedermann den Online-Zugriff auf die öffentlichen Daten des Registers zu ermöglichen.

Mit dem inzwischen in Kraft getretenen Gesetz über elektronische Register und Justizkosten für Telekommunikation vom 10. Dezember 2001 werden neue Zugriffsmöglichkeiten auf Register eröffnet. Dies betrifft das Handelsregister, das Genossenschaftsregister, das Vereinsregister und das Partnerschaftsregister. Beim Online-Abruf aus Registern muss die Authentizität der Daten und die Identität der berechtigten veröffentlichenden Stellen gewährleistet werden. Hier kommt das Mittel der qualifizierten elektronischen Signatur in Betracht.

Register dienen dem Zweck, bestimmte Umstände dauerhaft zu dokumentieren, im Gegensatz zu den meist temporären Veröffentlichungen, z.B. im Insolvenzverfahren. Auf die Registerdaten kann dauerhaft zugegriffen werden. Das Problem, dass nach dem Ablauf einer Löschungsfrist die Daten noch zugänglich sind, stellt sich hier nicht. Allerdings können sich auch die Registerdaten ändern. Durch Dritte ins Internet eingestellte Daten wären damit nicht mehr aktuell. Deshalb sollte grundsätzlich auch in diesem Bereich angestrebt werden, das Kopieren der Daten zu verhindern. Für die Kontrolle der ordnungsgemäßen Nutzung der Registerdaten scheint ein höheres Schutzniveau geboten als in § 9a HGB vorgesehen. Die Kontrolle durch Stichproben bietet nur einen relativ schwachen Schutz, zumal die einzige Sanktion der Ausschluss des Nutzers von dem automatisierten Abrufverfahren ist. So könnte bei Online-Abfragen eine Registrierung vorgeschaltet werden. Zu erwägen wäre ebenfalls, auch hier eine Bußgeldpflicht einzuführen.

Zwangsvollstreckung

Der Versteigerungstermin für eine Zwangsversteigerung wird gem. § 39 Abs. 1 Zwangsversteigerungsgesetz (ZVG) durch das Gericht in dem für Bekanntmachungen des Gerichts bestimmten Blatt bekannt gemacht. Eine zusätzliche Veröffentlichung des Zwangsversteigerungstermins im Internet dürfte unter § 40 Abs. 2 ZVG fallen. Danach ist das Gericht befugt, zusätzlich andere Veröffentlichungen vorzunehmen. Dies ist auch sinnvoll, da Sinn und Zweck dieser Regelung die Unterrichtung einer möglichst breiten Öffentlichkeit ist, um einerseits eine bestmögliche Verwertung des Versteigerungsobjektes zu gewährleisten und andererseits allen, deren Rechte von der Versteigerung berührt werden, die Wahrung dieser Rechte zu ermöglichen.

Der Arbeitskreis „Zwangsvollstreckung“ der BLK schlägt eine Änderung des § 39 Abs. 1 ZVG dahingehend vor, dass die Veröffentlichung in dem für amtliche Bekanntmachungen des Gerichtes bestimmten Blatt oder in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystems erfolgen soll. Dies würde der mittlerweile erfolgten Änderung von § 9 Abs. 1 Satz 1 InsO entsprechen. Dadurch wird die Möglichkeit einer Internet-Veröffentlichung deutlich aufgewertet.

Zu hinterfragen ist insbesondere vor dem Hintergrund zunehmender Bekanntmachungen im Internet jedoch, ob die derzeitige Formulierung des § 38 ZVG - „Die Terminbestimmung soll die Bezeichnung des... eingetragenen Eigentümers ... enthalten“ - aus datenschutzrechtlicher Sicht heute noch vertretbar ist. Diese Bestimmung enthält die aus Datenschutzsicht unzulässige Aufforderung, grundsätzlich den Namen des eingetragenen Eigentümers zu veröffentlichen und davon nur abzusehen, wenn ein besonderer Anlass besteht. Hier bin ich mit den anderen Datenschutzbeauftragten des Bundes und der Länder der Auffassung, dass in diesem Punkt eine Änderung des § 38 ZVG notwendig ist.

Das maschinell geführte Grundbuch

Mit der Einfügung der §§ 126 - 134 in die Grundbuchordnung wurden die rechtlichen Grundlagen für ein maschinelles Grundbuch geschaffen. Die Verordnung über das maschinell geführte Grundbuch vom 17. Mai 2001 ordnet an, in Niedersachsen die Grundbücher in maschineller Form als automatisierte Dateien zu führen. Mit dem elektronischen Grundbuch sollen die Grundbucheintragungs-, Mitteilungs- und Auskunftsverfahren beschleunigt und rationalisiert werden. Wird der Grundbuchinhalt ausschließlich in elektronischer Form gespeichert, können (befugte) Stellen oder Personen außerhalb der Justiz, die das Grundbuch einsehen müssen (z.B. Notare, Kreditinstitute, Öffentlich bestellte Vermessungsingenieure usw.), über Datenleitungen im automatisierten Abrufverfahren unmittelbar und beliebig oft Einsicht nehmen, ohne sich zu den Bürozeiten in ein Grundbuchamt begeben oder auf die Erteilung von Abschriften warten zu müssen. Die Einschätzung des Justizministeriums, dass mit dem Einsatz moderner Technik in den Grundbuchämtern, zudem erste Maßnahmen in Richtung des elektronischen Rechtsverkehrs ergriffen werden können, teile ich.

Bei all diesen „Öffnungen“ ist zur Sicherung der Unversehrtheit und der Authentizität eine qualifizierte elektronische Signatur und ein zusätzlicher Schutz durch eine Verschlüsselung vorzusehen.

11.1.3 Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet

Mit der Änderung der Insolvenzordnung (InsO) wurde in § 9 geregelt, dass die öffentliche Bekanntmachung der Eröffnung des Insolvenzverfahrens auch in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem erfolgen kann. Nähere Regelungen finden sich in der „Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet“. Durch die Veröffentlichung im Internet sollen einerseits Veröffentlichungskosten eingespart, andererseits eine effektivere Publizität erreicht werden.

Die Datenschutzbeauftragten des Bundes und der Länder hatten bereits mit Blick auf die Änderung der InsO ihre Entschließung „Veröffentlichung von Insolvenzinformationen im Internet“ vom 24. April 2001 verfasst (vgl. Anlage 9) und u.a. die Besorgnis formuliert, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können, dass ihre Speicherung zeitlich nicht beherrschbar ist und dass die Daten vielfältig ausgewertet werden können. Sie sahen keine Gewähr für die ordnungsgemäße Pflege und dafür, dass die Löschung dieser personenbezogenen Daten sichergestellt ist.

Ich hatte gegenüber dem Justizministerium u.a. darauf hingewiesen, dass die beabsichtigte Regelung zum Kopierschutz eine Verpflichtung statuiert, die objektiv nach derzeitigen technischen Möglichkeiten nicht erfüllbar ist, da es noch keinen verlässlichen Kopierschutz gibt. Diese und andere in diesem Zusammenhang von mir geäußerte Bedenken sind vom Justizministerium gegenüber dem Bundesjustizministerium vorgebracht, in der Verordnung bedauerlicherweise aber nicht berücksichtigt worden. Das Bundesjustizministerium hat die Verordnung am 12. Februar 2002 erlassen und in § 2 Abs. 1 u.a. nur festgelegt, dass nach dem Stand der Technik dafür Sorge zu tragen ist, dass die genannten Daten durch Dritte elektronisch nicht kopiert werden können.

Die Frage, wie verhindert werden kann, dass Daten nach Ablauf der gesetzlichen Löschungsfrist durch Dritte über das Internet verbreitet werden, war auch Gegenstand einer Prüfbitte des Deutschen Bundestages. Dieses Problem durch eine neue rein insolvenzrechtliche Bußgeldvorschrift zu lösen, die die Ahndung eine solchen Verhaltens zulässt, wird als unzureichend angesehen. Die Bundesministerien der Justiz und Inneres haben die Anregung des Bundesbeauftragten für den Datenschutz positiv aufgenommen, durch Änderung der §§ 29 und 43 Bundesdatenschutzgesetz (BDSG) einen besseren Schutz der Betroffenen zu bewirken. Der Vorschlag sieht die Änderung des § 29 BDSG dahingehend vor, dass die Erhebung und Speicherung von Daten zum Zwecke der Übermittlung und die Übermittlung dieser Daten im Internet, wenn sie von öffentlichen Stellen nur vorübergehend im Rahmen gesetzlicher Fristen in das Internet eingestellt sind, nur innerhalb dieser Fristen zulässig sind. In § 43 Abs. 2 Nr. 1 und 2 BDSG soll jeweils das Merkmal „nicht allgemein zugänglich“ in

„nicht oder nicht mehr allgemein zugänglich“ geändert werden. Ein Verstoß gegen § 29 BDSG könnte dann als Ordnungswidrigkeit geahndet werden. Von dieser Lösung ist allerdings noch nicht die Alternative erfasst, bei der ein Wirtschaftsinformationsdienst oder eine Auskunftei die Daten den Bekanntmachungen in Papierform (Bundesanzeiger, regionale Blätter) entnimmt und in das Internet einstellt. Insoweit bedürfte es einer Regelung (oder zumindest Klarstellung), wonach auch bei allen amtlichen Bekanntmachungen in Papierform die darin enthaltenen Daten nicht über die gesetzlichen Fristen der Verordnung zu § 9 InsO oder gleichartige Fristen hinaus durch Dritte im Internet veröffentlicht werden dürfen. Ich werde die hierzu weiter anzustellenden Überlegungen kritisch verfolgen.

11.1.4 Allgemeine Verfügung „Ausführung der Bundesrechtsanwaltsordnung (BRAO)“

Durch Verordnung vom 10. Juni 1999 (Nds. GVBl. S. 128) sind die Aufgaben und Befugnisse der Justizverwaltung in Angelegenheiten der Rechtsanwälte auf die Rechtsanwaltskammern übertragen worden; außerdem gelten eine Reihe neuer gesetzlicher Regelungen im Anwaltsbereich. Das Justizministerium hat mir mitgeteilt, dass die Allgemeine Verfügung (AV) „Ausführung der Bundesrechtsanwaltsordnung (BRAO)“ vom 8. August 1972 (Nds. Rechtspflege S. 207), zuletzt geändert durch AV vom 26. April 1995 (Nds. Rechtspflege S. 121, 122), ebenso wie andere Verwaltungsvorschriften in Anwaltsangelegenheiten dadurch weitgehend überholt sind und durch neue Regelungen ersetzt werden müssen. Es hat mir meine Beteiligung zugesagt, sobald nach Anhörung des Geschäftsbereichs und der Rechtsanwaltskammern feststeht, welcher Bedarf insbesondere für Übermittlungsregelungen besteht. Informationen über neue Regelungen bzw. beabsichtigte neue Regelungen liegen mir bislang noch nicht vor.

11.1.5 Weitergabe von Daten an gemeinnützige Einrichtungen

Meine seit Jahren andauernden Bemühungen, die Überweisung von Geldauflagen an gemeinnützige Einrichtungen datenschutzgerecht zu gestalten, vgl. Nr. 26.8 des XV. TB LfD Nds. 1999/2000, hat das Justizministerium auch in diesem Berichtszeitraum nicht aufgegriffen. Das Ministerium hat mir seine Ansicht mitgeteilt, im Hinblick auf die neue Rechtslage (Art. 1 Nr. 15 Strafverfahrensänderungsgesetz 1999 [StVÄG 1999]) sei es nunmehr gemäß § 483 Abs. 1 StPO Gerichten und Strafvollzugsbehörden gestattet, personenbezogene Daten in Dateien zu speichern, zu verändern und zu nutzen, soweit dies für Zwecke des Strafverfahrens erforderlich sei. Nach § 487 Abs. 1 Satz 1 StPO dürften die nach § 483 Abs. 1 StPO gespeicherten Daten den „zuständigen Stellen“ übermittelt werden, soweit dies für die in dieser Vorschrift genannten Zwecke erforderlich sei. Es sei davon auszugehen, dass unter „zuständigen Stellen“ im Sinne dieser Vorschrift auch Empfänger von Geldauflagen zu verstehen seien, denn der Gesetzgeber habe auf die Benennung eines abgeschlossenen Empfängerkreises bewusst verzichtet, um Lücken zu vermeiden (BT-Drs. 14/1484, S. 33). Im Hinblick auf diese neue Rechtslage kann nach Auffassung des Justizministeriums an der bisherigen Verfahrensweise in Niedersachsen festgehalten werden.

Ich vertrete nach wie vor die Auffassung, dass bei der niedersächsischen Verfahrensweise den Empfängern der Geldauflagen personenbezogene Daten in einem Umfang bekannt werden, wie er für die bei ihnen zu erledigenden Arbeitsschritte nicht erforderlich ist, und bedauere sehr, dass weder meine Vorschläge zu einer anderen Gestaltung des Verfahrens aufgegriffen worden sind noch eine in Bayern verwirklichte datenschutzrechtlich angemessene Verfahrensweise in Niedersachsen übernommen werden soll.

11.1.6 DNA-Analyse auch bei nicht erheblichen Sexualstraftaten?

Dem Bundesrat wurde am 12. Juni 2002 ein Antrag des Landes Baden-Württemberg zum Entwurf eines Gesetzes zur Erweiterung des Einsatzes der DNA-Analyse bei Straftaten mit sexuellem Hintergrund zugeleitet (BR-Drs. 517/02). Der Entwurf sieht vor, dass der Katalog der sog. Anlasstaten für eine DNA-Analyse für Zwecke künftiger Strafverfahren auf alle (und somit auch nicht erhebliche) Straftaten mit sexuellem Hintergrund erweitert wird. In Zukunft soll es möglich sein, zum Zwecke der Identitätsfeststellung einem Beschuldigten, der einer sonstigen Straftat mit sexuellem Hintergrund verdächtig ist, Körperzellen zu entnehmen und zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch zu untersuchen, wenn wegen der Art der Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen einer solchen Straftat zu führen sind (Entwurf zur Änderung des § 81g Abs. 1 StPO). In der Begründung des Gesetzesantrages wird ausgeführt, dass bei einer entsprechenden Prognose eine Analyse auch bei einem Delikt mit sexuellem Hintergrund möglich sein soll, bei welchem eine Straftat von erheblicher Bedeutung (bisherige gesetzliche Schwelle für eine DNA-Identitätsfeststellung gemäß § 81g StPO) nicht vorliegt. Als Beispiele wurden exhibitionistische Handlungen und Beleidigung mit sexuellem Hintergrund angeführt. Es sollen wissenschaftliche Erkenntnisse vorliegen, wonach ein nicht unerheblicher Prozentsatz exhibitionistischer Täter später schwere Sexualdelikte begehen wird (sog. „Steigerungskarriere“). Eine genauere Betrachtung der zitierten wissenschaftlichen Untersuchung der Kriminologischen Zentralstelle über „Legalbewährung und kriminelle Karrieren von Sexualstraftätern“ (vgl. Kriminologie und Praxis, Band 33, Wiesbaden 2001) bestätigt diese These jedoch nicht. Dort heißt es: „Sich (vor Kindern) exhibierende Männer mögen besonders rückfallgefährdet sein; ein Steigerungsverhalten war bei „klassischen“ Exhibitionisten - die ihre Taten insbesondere nicht schon im Jugend- oder Heranwachsendenalter begangen hatten - jedoch durchweg nicht festzustellen.“ Auch der von der Landesregierung im Oktober 2002 vorgestellte Bericht zur Inneren Sicherheit in Niedersachsen für die Jahre 1992 bis 2001 spricht nur davon, dass lediglich 2 bis 7 % aller rückfälligen Exhibitionisten im Verlauf ihrer Karriere schwerere sexuelle Gewaltdelikte begehen.

Dies zeigt, dass eine derartige Prognose der Steigerung in den Bereich der schweren Sexualdelikte aufgrund der wissenschaftlichen Erhebungen nicht haltbar ist. Aus datenschutzrechtlicher Sicht stellt sich die Frage, ob eine molekulargenetische Untersuchung in diesen Fällen erforderlich ist, da der § 81g StPO der Identifizierung des Täters einer künftigen Straftat dienen soll. Eine derartige Maßnahme scheidet im Regelfall bei Delikten aus, bei denen Täter nach kriminalistischen Erfahrungen bei der Tatausführung keine Körperzellen ausscheiden oder absondern, die molekulargene-

tisch untersucht werden können. Dies dürfte u.a. bei einer Beleidigung mit sexuellem Hintergrund regelmäßig zutreffen. Ich bin der Ansicht, dass es sich bei der geplanten Änderung (insbesondere bei den geschilderten Fällen) um einen Ansatz zur Vorratsdatenspeicherung in der DNA-Datenbank handelt, dem ich entgegengetreten bin.

Auch andere Vorstöße, die DNA-Analyse als regelmäßiges Instrument einer erkennungsdienstlichen Behandlung bei allen Straftätern einzusetzen (vgl. etwa Entschließungsantrag der CDU vom 16. Oktober 2002, LT-Drs. 14/3775), sind aus datenschutzrechtlicher Sicht schon deshalb strikt abzulehnen, weil sie auf eine unverhältnismäßige und deshalb rechtswidrige Vorratsdatenhaltung hinauslaufen.

11.1.7 Datenschutzrechtliche Kontrolle der praktischen Umsetzung der Richtlinie für den Täter-Opfer-Ausgleich im allgemeinen Strafrecht

Durch Kontrollbesuche bei der Gerichtshilfestelle einer Staatsanwaltschaft und einer mit der Durchführung des Täter-Opfer-Ausgleichs beauftragten privaten Stelle habe ich die praktische Umsetzung der §§ 155a und 155b StPO sowie der am 1. Mai 2000 in Kraft getretenen Richtlinie für den Täter-Opfer-Ausgleich im allgemeinen Strafrecht (TOA-Richtlinie) überprüft und ermittelt, ob der Datenschutz gewährleistet ist oder sich Lücken ergeben, die ggf. durch eine Ergänzung der TOA-Richtlinie geschlossen werden müssen.

Ich habe die Erkenntnisse meiner Überprüfung eingehend mit den kontrollierten Stellen erörtert und die Ergebnisse in einem ausführlichen Abschlussbericht niedergelegt. Schwerwiegende datenschutzrechtliche Mängel bei der Handhabung des Täter-Opfer-Ausgleiches habe ich nicht festgestellt. Auch für die TOA-Richtlinie hat sich kein gravierender Änderungs- oder Ergänzungsbedarf ergeben. Die Anregungen meines Abschlussberichtes hat das Niedersächsische Justizministerium inzwischen überwiegend umgesetzt. Es hat durch Erlass die Generalstaatsanwälte und die Präsidentin bzw. die Präsidenten der Oberlandesgerichte des Landes um Beachtung der datenschutzrechtlichen Vorgaben ersucht, die sich aus meinem Abschlussbericht und der ergänzenden Stellungnahme des Justizministeriums ergeben. Damit dürfte eine landeseinheitliche Handhabung, die den Belangen des Datenschutzes Rechnung trägt, sichergestellt sein.

11.1.8 Verfahrensbeschreibungen gemäß § 8 Abs. 1 NDSG

Nach § 8 NDSG hat jede öffentliche Stelle, die Verfahren zur automatisierten Verarbeitung personenbezogener Daten einrichtet oder ändert, bestimmte Merkmale in einer Beschreibung festzulegen. Dies gilt nicht für die Verarbeitung solcher Daten, bei denen eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung nicht zu erwarten ist. In diesen Fällen kann auch die Pflicht zur Bestellung einer oder eines behördlichen Datenschutzbeauftragten eingeschränkt werden. Mit der Verordnung über Ausnahmen von der Pflicht zur Bestellung von Datenschutzbeauftragten vom 10. Juli 2002 hat die Landesregierung u.a. bestimmt, dass die ausschließlich zweckgebundenen, automatisierten Verarbeitungen personenbezogener Daten zur Abwicklung der Amtstätigkeit und der Dienstgeschäfte der Notare sowie der Beschäftigungsverhältnisse der bei ihnen beschäftigten Personen Verarbeitungen sind, von denen

eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung der Betroffenen nicht zu erwarten ist. Damit sind Notare auch von der Verpflichtung befreit, eine Verfahrensbeschreibung zu erstellen.

11.2 Strafvollzug

11.2.1 Datenschutz im Strafvollzug

Wie ich in Nr. 27 des XV. TB LfD Nds. 1999/2000 dargelegt habe, ließ sich in Gesprächen mit dem Justizministerium und verschiedenen Strafvollzugsanstalten nicht feststellen, dass die Vorgaben des 4. Strafvollzugsänderungsgesetzes vom 26. August 1998 zu spürbaren Initiativen zur Vermeidung datenschutzrechtlicher Defizite geführt haben.

Die von mir angekündigte Orientierungshilfe „Datenschutz im Strafvollzug“ mit rechtlichen Rahmenbedingungen und Checklisten wurde im Rahmen einer Projektarbeit zwischenzeitlich fertiggestellt. Die niedersächsischen Justizvollzugsanstalten haben zahlreiche Exemplare der Orientierungshilfe erhalten. Die Bitte verschiedener Anstalten um Auslieferung weiterer Exemplare dieser Broschüre und die positiven Rückmeldungen aus dem Strafvollzugsbereich zeigen, dass mit ihr ein Leitfaden vorliegt, der für die Lösung datenschutzrechtlicher Probleme bei der praktischen Arbeit der Bediensteten in den Justizvollzugsanstalten eine hilfreiche und geeignete Handreichung darstellt und dazu beiträgt, die Aufgaben in den Justizvollzugsanstalten datenschutzgerecht zu erledigen. Noch sind allerdings nicht alle Ausführungsvorschriften und Erlasse des Justizministeriums, das die Erarbeitung der Handreichung konstruktiv begleitet hat, dem Stand angepasst worden, der sich aus den Darlegungen und Empfehlungen in der Handreichung ergibt.

11.2.2 Unterrichtung der Opfer von Straftaten über Vollzugslockerungen und den Stand der Entlassungsvorbereitungen des Täters

Das Justizministerium hat die Frage aufgeworfen, ob dem Sicherheitsempfinden von Opfern von Straftaten dadurch Rechnung getragen werden kann, dass sie auf ihren Wunsch hin künftig über den Verbleib und die rechtliche Behandlung des Täters z.B. über beabsichtigte Vollzugslockerungen, Urlaubsgewährungen, Verlegungen in den offenen Vollzug und bevorstehende Entlassungen besser informiert werden. Als zentrale Informations- und Vernetzungsstelle sollten dazu die im Laufe des Jahres überall in Niedersachsen einzurichtenden Opferhilfebüros tätig werden, deren Mitarbeiter im Auftrag und in Vertretung der Opfer entsprechende Auskünfte einholen können.

Rechtsgrundlage für die Informationserteilung bei Gefangenen ist § 180 Abs. 5 Strafvollzugsgesetz (StVollzG). Nach dieser Vorschrift dürfen die Vollzugsanstalten auf schriftlichen Antrag nicht öffentlichen Stellen mitteilen, ob sich eine Person in Haft befindet sowie ob und wann ihre Entlassung innerhalb des kommenden Jahres bevorsteht, soweit ein berechtigtes Interesse an der Mitteilung glaubhaft dargelegt wird und der Gefangene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Den Verletzten können darüber hinaus auch auf schriftlichen Antrag Auskünfte über die Entlassungsadresse oder die Vermögensverhältnisse des Gefange-

nen erteilt werden, wenn die Erteilung zur Feststellung oder Durchsetzung von Rechtsansprüchen im Zusammenhang mit der Straftat erforderlich ist.

Für Opfer ist von mindestens ebenso großem Interesse, ob das Ende der Unterbringung in einer psychiatrischen Anstalt oder einer Entziehungsanstalt (§§ 63, 64 StGB) bevorsteht oder ob dem Täter Urlaub und Lockerungen gewährt werden. Zu prüfen war daher auch, ob aus datenschutzrechtlicher Sicht Bedenken gegen die Weitergabe von Informationen über Urlaub, Lockerungen, Verlegungen und Entlassungen an die Opfer eines im Maßregelvollzug untergebrachten Täter sprechen.

Datenschutzrechtlich relevant ist nicht nur die Auskunft über den Gesundheitszustand eines Patienten, sondern schon über die Tatsache des Krankenhausaufenthalts einer Person. Diese stellt eine Offenbarung besonders schutzwürdiger personenbezogener Daten dar und unterfällt der ärztlichen Schweigepflicht. Somit ist schon die bloße Auskunft über den Aufenthalt in einem Landeskrankenhaus nur zulässig, wenn hierfür ein Rechtfertigungsgrund vorliegt. Für Datenübermittlungen im Zusammenhang mit der Maßregel der Sicherheitsverwahrung sind gemäß § 130 Strafvollzugsgesetz die Vorschriften über den Vollzug der Freiheitsstrafe entsprechend zu beachten. Nach § 130 StVollzG gelten für die Sicherungsverwahrung die Vorschriften über den Vollzug der Freiheitsstrafe (§§ 3 bis 126, 179 bis 187) entsprechend. Die Bekanntgabe von Vollzugslockerungen, Urlaubsgewährungen oder Verlegungen in den offenen Vollzug ist in § 180 Abs. 5 StVollzG nicht geregelt. Eine Befugnis zur Weitergabe der fraglichen Daten an Opferhilfebüros vermag ich daher nicht zu sehen.

12 Finanzen

12.1 Steuergeheimnis - kein Stolperstein für Datenschutzkontrollen

Noch in jüngster Zeit haben sich Finanzämter unter Hinweis auf das Steuergeheimnis geweigert, mir Einsicht in Steuerakten zu geben, wenn ich einer Beschwerde über einen behaupteten Datenschutzverstoß der Steuerverwaltung nachgehen wollte. Bis vor kurzem bestanden auch Meinungsverschiedenheiten mit dem Finanzministerium über den Umfang meiner Prüfungsbefugnisse. Dabei sollten diese Probleme seit langem beseitigt sein.

Um in dieser zwischen der Finanzverwaltung und den Datenschutzbeauftragten (früher) streitigen Frage Klarheit zu schaffen, hat der Bundesgesetzgeber im Jahre 1990 in § 24 Abs. 2 BDSG klargestellt, dass das Steuergeheimnis sowie Berufs- und besondere Amtsgeheimnisse einer Datenschutzkontrolle nicht entgegengehalten werden können. Um dies auch gegenüber den Datenschutzbeauftragten der Länder auszuschließen, ordnet das BDSG die entsprechende Anwendung dieser Vorschrift auch für den Landesbereich an (§ 24 Abs. 6).

Dennoch hat sich das Niedersächsische Finanzministerium im Berichtszeitraum im Zusammenhang mit der beabsichtigten Kontrolle eines Finanzamtes zunächst weiter auf den Standpunkt gestellt, bei Vorgängen, die dem Steuergeheimnis unterliegen, habe der Landesbeauftragte eine uneingeschränkte Kontrollbefugnis nur dann, wenn

es sich um eine automatisierte Datenverarbeitung handele. Bei herkömmlicher Datenverarbeitung in Akten komme eine Datenschutzkontrolle von Steuersachverhalten dagegen nur in Betracht, wenn hinreichende Anhaltspunkte für eine Rechtsverletzung vorlägen oder der vom Steuergeheimnis geschützte Steuerpflichtige seine Einwilligung erteile. Diese Einschränkung leitete das Finanzministerium daraus ab, dass nach der (damaligen) Regelung des BDSG der Bundesbeauftragte für den Datenschutz im Gegensatz zu den Landesbeauftragten generell keine uneingeschränkte Kontrollbefugnis für die Datenverarbeitung in Akten besaß.

Die Rechtsauffassung des Finanzministeriums ist unzutreffend. Die entsprechende Anwendung der Bundesregelung, wonach das Steuergeheimnis einer Datenschutzkontrolle nicht entgegengehalten werden darf, bedeutet für den Landesbereich natürlich nicht, dass damit auch die Einschränkung der Kontrollbefugnisse des Bundesbeauftragten auf die Landesbeauftragten zu übertragen wäre. Eine derartige Regelung lag weder in der Absicht des Bundesgesetzgebers noch wäre sie unter Kompetenzgesichtspunkten möglich gewesen. Es bedarf keiner weiteren Begründung, dass der Bund keine Gesetzgebungskompetenz zur Festlegung der Prüfungsbefugnisse des Landesbeauftragten für den Datenschutz, dessen Aufgabe im Kern in der Niedersächsischen Verfassung (Art. 62) geregelt ist, besitzt.

Mit der Novellierung des BDSG vom 23. Mai 2001 sind überdies die bisherigen Beschränkungen der Kontrollbefugnisse des Bundesbeauftragten für den Datenschutz entfallen. Der Rechtsauffassung des Finanzministeriums ist damit auch der letzte Argumentationsansatz entzogen.

Nachdem Finanzämter auch nach der angesprochenen Rechtsänderung nicht bereit waren, ihr Verhalten zu ändern und mich in meiner Aufgabenwahrnehmung weiter behindert haben, habe ich den Problembereich nochmals mit dem Finanzministerium erörtert. Das Fachressort stimmt meiner rechtlichen Beurteilung nunmehr zu. Ich hoffe, das diese Behinderung meiner Arbeit in der Finanzverwaltung damit der Vergangenheit angehört.

12.2 Datenschutzgerechte Novellierung der Abgabenordnung

In meinem vorletzten Tätigkeitsbericht habe ich unter der Überschrift "Kein Happy End in Sicht" über den zähflüssigen Prozess einer datenschutzgerechteren Ausgestaltung der Abgabenordnung berichtet. Nun scheint der Versuch, grundlegende Datenschutzregelungen in der AO zu verankern, ein Stück weit voranzukommen.

Aus Sicht des Datenschutzes wäre es geboten, datenschutzrechtliche Regelungen in der AO so übersichtlich und transparent zu gestalten, dass sich ihr Verständnis dem Rechtsanwender ohne weiteres erschließt. Dies würde Vorschriften erfordern, die sich am Aufbau des Bundesdatenschutzgesetzes bzw. der Landesdatenschutzgesetze orientieren, indem sie die einzelnen Phasen der Datenverarbeitung in gegliederter Ordnung regeln. Eine solche Struktur lässt die AO bisher vermissen. Die Finanzverwaltungen in Bund und Ländern stehen diesem Ansatz leider weiterhin ablehnend gegenüber. Die Finanzressorts haben sich aber bereit erklärt, über konkrete datenschutzrechtliche Ergänzungen der AO eine eingehende Diskussion zu führen.

Dazu hat der Bundesbeauftragte für den Datenschutz dem Bundesminister für Finanzen einen mit den Landesbeauftragten für den Datenschutz abgestimmten Gesamtvorschlag zur Änderung der AO übermittelt. Diese Arbeitsgrundlage für die künftige Diskussion enthält konkrete Formulierungsvorschläge für die geforderten Regelungen und begründet diese im Einzelnen. Mit einer Umsetzung der Vorschläge würden zentrale datenschutzrechtliche Forderungen in der AO verankert.

Die Datenschutzbeauftragten schlagen insbesondere Regelungen vor

- zur Weitergabe von Kontrollmitteilungen
  Bislang übermitteln die Finanzbehörden untereinander ohne normenklare Rechtsgrundlage Steuerdaten, wenn sie annehmen, diese könnten für ein anderes Besteuerungsverfahren von Bedeutung sein.

- zu Auskunft und Akteneinsicht
  In einer bürgerfreundlichen und serviceorientierten modernen Verwaltung, wie sie im Rahmen des Projekts "Finanzamt 2003" vom Niedersächsischen Finanzminister angestrebt wird, sollte es selbstverständlich sein, Bürgern die Möglichkeit zu geben, Kenntnis von den Daten zu erlangen, die die Steuerverwaltung über sie gespeichert hat.

- zum Outsourcing
  Die Finanzverwaltung hat bereits ohne eindeutige Rechtsgrundlage begonnen, Teile ihrer Aufgaben von anderen Stellen wahrnehmen zu lassen. Dazu gehört z.B. die automatisierte Verarbeitung von Steuerdaten durch das Informatikzentrum Niedersachsen, das Drucken von Lohnsteuerkarten durch private Unternehmen oder die Vernichtung von Steuerakten durch darauf spezialisierte Firmen. Gegen ein solches Vorgehen sind zwar keine grundsätzlichen datenschutzrechtlichen Einwände zu erheben. Es bedarf jedoch einer gesetzlichen Regelung, da hierbei regelmäßig sensible Steuerdaten nach außen gelangen.

- zu grenzüberschreitenden Datenübermittlungen.

- zur Datenlöschung.

Ich hoffe, dass auch in der Finanzverwaltung die Einsicht wächst, dass Datenschutz keineswegs die sachgerechte Aufgabenerfüllung behindern will, sondern gerade den Modernisierungsprozess zu einer stärkeren Bürgerorientierung wirkungsvoll fördern kann.

Die weitere Diskussion über die von den Datenschützern vorgeschlagenen gesetzlichen Regelungen wird zunächst in einer Koordinierungsgruppe geführt werden, der neben Vertretern der Finanzverwaltung der Bundesbeauftragte sowie drei Landesbeauftragte für den Datenschutz (darunter Niedersachsen) angehören. Erste Vorgespräche mit dem Niedersächsischen Finanzministerium lassen eine aufgeschlossene

Haltung gegenüber den Vorschlägen erkennen. Ich sehe dem Fortgang des Vorhabens daher mit verhaltenem Optimismus entgegen.

12.3 Datenschutzrechtliche Aspekte des besonderen Kirchgeldes

Neben der Kirchensteuer erheben inzwischen mehrere Religionsgemeinschaften das so genannte besondere Kirchgeld. Es wird von steuerpflichtigen Kirchenmitgliedern eingezogen, deren Ehegatte keiner Kirchensteuer erhebenden Religionsgemeinschaft angehört und die zusammen zur Einkommensteuer veranlagt werden. Betroffen von dieser Regelung sind vor allem Ehen, in denen der nicht- oder geringverdienende Ehepartner der Kirche angehört, der Ehepartner mit dem höheren Einkommen jedoch nicht. In derartigen Fällen fällt keine oder eine nur geringe Kirchensteuer an. Das besondere Kirchgeld wird jedoch regelmäßig nach dem gemeinsamen zu versteuernden Einkommen bemessen; auf die Kirchenzugehörigkeit und die Einkünfte des einzelnen Ehepartners kommt es daher nicht an.

Das besondere Kirchgeld wird durch die Finanzverwaltung im Rahmen der Einkommensteuerveranlagung mit berechnet und verbunden mit dem Einkommensteuerbescheid festgesetzt. Die entrichteten Kirchgeldbeträge werden gesammelt und an die Religionsgemeinschaften weitergeleitet.

Dieses Verfahren gibt insoweit keinen Anlass zu datenschutzrechtlicher Kritik, denn es ist zum einen in der beschriebenen Weise gesetzlich geregelt (insbesondere durch das Kirchensteuerrahmengesetz) und zum anderen erfolgt die Weiterleitung der eingezogenen Beträge, ohne dass ein Rückschluss auf den einzelnen Zahlungspflichtigen möglich ist.

Datenschutzrechtliche Probleme ergeben sich aber bei Widerspruchs-, Stundungs- und Erlassverfahren in Kirchgeldsachen. Denn für derartige Verfahren sind die kirchlichen Stellen selbst zuständig. Im Rahmen solcher Verfahren kommt es deshalb häufig zu Datenübermittlungen von der Finanzverwaltung an die kirchlichen Stellen. Viele Steuerpflichtige leiten ihre Rechtsbehelfe oder sonstigen Anträge zum Kirchgeld den Finanzämtern zu. Dies ist verständlich, weil der Steuerbescheid von dort kommt. Die Widersprüche oder Anträge werden von der Finanzverwaltung anschließend unter Erteilung einer Abgabenachricht an die kirchlichen Stellen weitergeleitet. Im Rahmen der Bearbeitung fordern diese ggf. Unterlagen oder Auskünfte aus den Steuerakten bei den Finanzämtern an, falls nicht alle erforderlichen Daten von den Betroffenen zur Verfügung gestellt werden. Zumeist werden die Finanzämter um Übersendung einer Kopie des betreffenden Steuerbescheides oder um Übermittlung von Angaben aus diesem Bescheid ersucht.

Die Übermittlung von Daten, die für die Bearbeitung des Rechtsbehelfs oder Antrages erforderlich sind, ist nicht zu beanstanden. Diese Angaben sind den kirchlichen Stellen nach § 10 Kirchensteuerrahmengesetz auf Anforderung von den Finanzämtern zur Verfügung zu stellen. Entsprechend gestattet § 31 Abgabenordnung den Finanzämtern die Übermittlung von solchen Steuerdaten, die Besteuerungsgrundlage für das besondere Kirchgeld sind. Allerdings werden hiervon nur wenige in einem Einkommensteuerbescheid enthaltene Daten erfasst. Folgerichtig hat die Finanzverwal-

tung in einer Verwaltungsanweisung geregelt, dass bei Übersendung von Bescheidkopien die nicht erforderlichen Angaben unkenntlich zu machen sind. Auch in dem Musterschreiben einer Landeskirche für die Anforderung eines Steuerbescheides beim Finanzamt wird zutreffend darauf hingewiesen, dass nicht erforderliche Daten unkenntlich gemacht werden können.

In der Praxis wird hiernach jedoch offenbar nicht immer verfahren. In einem mir vorgetragenen Fall hatte sich der Petent telefonisch gegenüber dem Finanzamt einverstanden erklärt, dass sein Widerspruch gegen die Kirchgeldfestsetzung an die zuständige kirchliche Stelle weitergeleitet wurde. Das Finanzamt übersandte jedoch nicht - wie vom Petenten erwartet - lediglich sein Widerspruchsschreiben, sondern fügte den vollständigen Steuerbescheid und weitere Unterlagen aus der Steuerakte bei.

Hierüber war der Steuerbürger zu Recht erbost. Die Vermutung, es handele sich lediglich um ein Versehen in einem Einzelfall, erwies sich leider als unrichtig. Es stellte sich heraus, dass das Finanzamt einen amtsinternen Vordruck für die Übersendung von Steuervorgängen an kirchliche Stellen verwendet hatte, in dem die Beifügung einer Bescheidkopie und weiterer Unterlagen generell vorgesehen ist. Das Finanzministerium hat umgehend die Änderung der Verwaltungspraxis bei dem betroffenen Finanzamt veranlasst und die übrigen Finanzämter um Beachtung der bestehenden Verwaltungsanweisung gebeten. Ich gehe deshalb davon aus, dass sich der dargestellte Rechtsfehler nicht wiederholen wird.

Neben den angesprochenen Kritikpunkten bei der Behandlung seines Widerspruchs sieht der Petent in der Erhebung von Kirchgeld bei glaubensverschiedenen Ehen ein grundsätzliches verfassungsrechtliches Problem. Er leitet aus dem Prinzip der Trennung von Staat und Kirche und aus einer Entscheidung des Bundesverfassungsgerichts von 1965, die dem Staat verbiete, einer Religionsgemeinschaft hoheitliche Befugnisse gegenüber Personen zu verleihen, die keiner Religionsgemeinschaft angehören, ab, dass die Erhebung eines besonderen Kirchgeldes und damit auch Datenübermittlungen für diesen Zweck verfassungswidrig seien.

Die datenschutzrechtliche Beurteilung hängt in der Tat von der Ausgangsfrage ab, ob die Heranziehung von Einkünften eines nicht der Kirche angehörenden Ehrgatten für die steuerliche Heranziehung des kirchlich gebundenen Ehepartners rechtlich zulässig ist. Dies haben insbesondere das Bundesverfassungsgericht (z.B. BVerfGE 19, 268 und BVerfGE 73, 388) und das Bundesverwaltungsgericht (BVerwGE 52, 104) mehrfach bejaht. Aus Sicht des Datenschutzes sehe ich deshalb keinen Anlass, die im Wesentlichen in §§ 4 und 10 Kirchensteuerrahmengesetz geregelten Datenverarbeitungsvorgänge in Frage zu stellen.

Der Petent hat angekündigt, zu dieser Frage eine verwaltungsgerichtliche Entscheidung herbeiführen zu wollen. Sie bleibt abzuwarten.

12.4 Steuernummern nicht mehr geheim

Steuernummern gehören zu den Daten, die bislang dem strengen Steuergeheimnis des § 30 Abgabenordnung unterlagen. Jetzt hat der Gesetzgeber allerdings durch Änderungen des Einkommens- und Umsatzsteuergesetzes diesen Schutz aufgehoben. Steuernummern sind danach nicht mehr geheim. Sowohl die Freistellungsbescheinigungen für den Steuerabzug bei Bauleistungen als auch Rechnungen, die ein Unternehmer für ein anderes Unternehmen ausstellt, sind nach der Rechtsänderung mit der Steuernummer zu versehen. Die genannten Unterlagen sind entsprechend ihrer Funktion zur Weitergabe an Dritte bestimmt.

Eine Vielzahl von Bürgern hat sich an mich gewandt und sich besorgt über die Auswirkungen dieser Regelungen geäußert. Befürchtet wird insbesondere, dass hierdurch Missbrauchsmöglichkeiten geschaffen werden könnten. Dabei wurde an erster Stelle die Befürchtung genannt, mit Kenntnis der Steuernummer könnten unbefugte Dritte steuerliche Daten der Betroffenen durch telefonische Anfragen bei Finanzämtern in Erfahrung bringen.

Auf meine Anfrage hat das Finanzministerium mitgeteilt, aus Sicht der Finanzverwaltung werde einer solchen Missbrauchsmöglichkeit hinreichend entgegengewirkt. Den Bediensteten sei die neue Rechtslage bekannt. Die Kenntnis der Steuernummer werde deshalb nicht mehr als Identifikationsmerkmal eines Anrufers akzeptiert. Im Übrigen sollten die Bediensteten durch gezielte sachdienliche Rückfragen feststellen, ob Anrufer auskunftsberechtigt sind. Bei dann noch verbleibenden Zweifeln könne in geeigneten Fällen ein Rückruf erfolgen; ggf. sei die Auskunft abzulehnen bzw. auf ein schriftliches Verfahren zu verweisen.

Die Praxis wird zeigen müssen, ob die Umsetzung dieser Handlungsanweisungen zu dem gewünschten, datenschutzrechtlich gebotenen Verwaltungshandeln führt. Aus dem Kreis der Bediensteten waren hieran Zweifel zu vernehmen. Solche Unsicherheiten sind verständlich. Denn ein Bediensteter, der durch unrichtige Angaben veranlasst worden ist, Steuerdaten einem Unbefugten fernmündlich zu offenbaren, muss mit dem Risiko leben, dass zur Prüfung seines Verhaltens ein Disziplinarverfahren gegen ihn eingeleitet wird.

12.5 Zweitwohnungssteuer - ein datenschutzrechtliches Spannungsfeld

Durch Eingaben sind wiederholt datenschutzrechtliche Defizite bei der Durchführung von Zweitwohnungssteuerverfahren bemängelt worden. Ich habe mich deshalb entschlossen, über die an mich herangetragenen Einzelfälle hinaus dieses Problemfeld näher zu beleuchten. Zu diesem Zweck habe ich mir von 12 Kommunen, die diese Steuer erheben, Satzungen und Verwaltungsvordrucke übersenden lassen. Zudem habe ich mich bei zwei Kommunen vor Ort über die dortigen Verfahren informiert.

Traditionell erheben insbesondere Kommunen in Ferien- und Kurgebieten Zweitwohnungssteuer, aber auch Städte, in denen z.B. Studenten oder Wochenendpendler mögliche Steuerpflichtige sind. Anknüpfungspunkt für die Steuer ist regelmäßig das "Innehaben" einer Zweitwohnung. Steuerpflichtige können daher zum Beispiel Eigen-

tümer oder Dauermieter von Ferienwohnungen sein, Arbeitnehmer, die an ihrem Dienstort eine zusätzliche Wohnung anmieten oder - bei entsprechender Ausgestaltung der Satzung - auch Mieter von Dauerstellplätzen auf Campingplätzen.

Erste datenschutzrechtliche Kritikpunkte haben sich bei Durchsicht der kommunalen Satzungen ergeben. In einer wiederholt vorgefundenen Satzungsformulierung „ermächtigen“ sich Kommunen in einer Art Rundumschlag, Daten bei einer Vielzahl anderer Stellen wie Finanzämtern, Grundbuchämtern, Katasterämtern, Strom- und Wasserversorgungsunternehmen und sonstigen Stellen zu erheben. Nach ihrem Wortlaut lassen diese Satzungsregelungen eine vorbehaltslose Datenerhebung bei Dritten zu. Rechtlich sind die Kommunen bei der Erhebung kommunaler Steuern jedoch nach § 11 Niedersächsisches Kommunalabgabengesetz an die Vorschriften der Abgabenordnung gebunden. Die AO sieht Datenerhebungen bei Dritten nur unter den Voraussetzungen des § 93 AO vor, nämlich dann, wenn eine Datenerhebung bei den Betroffenen nicht zum Ziel führt oder keinen Erfolg verspricht. Weil die genannten Satzungsregelungen dem NKAG widersprechen, sind sie in diesem Punkt zu ändern.

In der Praxis konnte ich zwar nicht feststellen, dass von der Vorschrift exzessiv Gebrauch gemacht wird. In den mir bei der Prüfung bekannt gewordenen Fällen sind die benötigten Daten vielmehr zumeist bei den Betroffenen erhoben worden bzw. wurde zumindest ein entsprechender Versuch unternommen. Petenten sind dagegen in anderen Fällen auf die Frage nach der rechtlichen Grundlage für ein Herantreten an Dritte die in Rede stehenden Satzungsbestimmungen genannt worden.

Es hat sich herausgestellt, dass die kritisierten Regelungen auf eine Mustersatzung des Niedersächsischen Städtetages zurückgehen. Ich habe deshalb mein Augenmerk zunächst nicht darauf gerichtet, einzelne Kommunen von der Notwendigkeit einer Rechtsänderung zu überzeugen, sondern darauf hinzuwirken, eine Änderung der Mustersatzung herbeizuführen, um die Quelle für diesen Rechtsfehler zu beseitigen. Meine Bemühungen, hierüber mit den kommunalen Spitzenverbänden ins Gespräch zu kommen, waren bislang allerdings noch nicht erfolgreich. Meinem Wunsch, an einer Erörterung der Problematik zwischen dem Innenministerium und den kommunalen Spitzenverbänden teilzunehmen, wurde leider nicht entsprochen. In der Sache haben sich die kommunalen Spitzenverbände gegenüber dem Fachressort inzwischen bereit erklärt, bei nächster Gelegenheit das Satzungsmuster zu ändern und des Satzungstext zu erläutern. Da ich - anders als das Innenministerium - bei den kritisierten Regelungen nicht nur die Gefahr von Missverständnissen, sondern einen rechtlichen Mangel sehe, werde ich auf zügige Änderungen drängen.

Die für die Steuerfestsetzung erforderlichen Daten werden regelmäßig mit Hilfe von Erklärungsvordrucken erhoben. Die Durchsicht dieser Vordrucke, die den Betroffenen leider nur teilweise zusammen mit Erläuterungen und Ausfüllhinweisen übermittelt werden, hat ein unterschiedliches Bild ergeben. Überwiegend erheben die Kommunen Daten, die tatsächlich erforderlich sind. Zum Teil werden aber auch Angaben verlangt, deren Kenntnis für das Zweitwohnungssteuerverfahren nicht erforderlich ist. Beispiele hierfür sind Fragen nach dem Beruf des Steuerpflichtigen, nach dem „Familienstand lt. Lohnsteuerkarte", nach dem Finanzamt des Wohnungsinhabers, nach

der genauen Anzahl Erwachsener und Kinder bei der Vermietung an Feriengäste oder nach Ausstattungsdetails der Wohnung. Die Erhebung solcher nicht zur Aufgabenerfüllung erforderlicher Daten ist unzulässig.

Mit der Zweitwohnungssteuer machen die Kommunen den Aufwand für den persönlichen Lebensbedarf, der im Innehaben einer Zweitwohnung zum Ausdruck kommt, zur Grundlage der Steuererzielung. Von diesem Ansatz aus darf allerdings nach höchstrichterlicher Rechtsprechung keine Zweitwohnungssteuer erhoben werden, wenn die Zweitwohnung nicht für den persönlichen Lebensbedarf, sondern als reine Kapitalanlage angeschafft wurde. Denn in diesen Fällen liegt keine Einkommensverwendung im Sinne eines Konsums vor, die von der Zweitwohnungssteuer getroffen werden soll, sondern die Absicht, Einkünfte zu erzielen. Aus dieser rechtlichen Differenzierung ergeben sich datenschutzrechtliche Folgeprobleme. Die Einordnung der jeweiligen Zweitwohnung als "reine Kapitalanlage" hat eine Steuerbefreiung zur Folge. Eine so genannte Mischnutzung (teils Vermietung, teils Selbstnutzung) kann zu einer in vielen Satzungen vorgesehenen Steuerermäßigung führen. Steuerbefreiung bzw. Steuerermäßigung werden von Zweitwohnungsinhabern gern beantragt. Ein Ermäßigungstatbestand kann jedoch häufig nur unter Schwierigkeiten belegt werden. Die Kommunen verweisen aber zu Recht auf die Besteuerungsgrundsätze der AO und ihre sich daraus ergebende Verpflichtung, Steuerverkürzungen zu unterbinden. Kommunen fordern deshalb beispielsweise folgende Unterlagen an:

- Mietverträge,
- Vermittlungs-/Agenturverträge,
- Belegungslisten bei Vermietung an Feriengäste,
- Einkommensteuerbescheide nebst die Wohnung betreffende Anlagen.

Die zum Teil heftige Kritik, die von Zweitwohnungsinhabern oft an einer solchen Vorgehensweise geübt wird, ist nach meinen Feststellungen in dieser generellen Weise nicht berechtigt. Die Kommunen sehen sich vielfach aufgrund ihrer Erfahrungen veranlasst, hohe Anforderungen an einen Nachweis von beantragten Steuerbefreiungen und -ermäßigungen zu stellen. Nach der Rechtsprechung des Bundesverfassungsgerichts sind die Steuer erhebenden Behörden verpflichtet, das Steuerverfahren so zu organisieren, dass die Steuerzahlung nicht im Wesentlichen von der Bereitschaft des Pflichtigen zur Erklärung über die für die Steuerfestsetzung maßgeblichen Verhältnisse abhängt. Daraus ergibt sich für die Steuerbehörden die Verpflichtung zur Überprüfung.

Vor diesem Hintergrund verlangt die Rechtsprechung bei nicht ganzjährig vermieteten Zweitwohnungen Angaben über die einzelnen Mietverhältnisse. Die Forderung einer Belegungsliste ist deshalb nicht zu beanstanden. Bei Dauervermietung ist die Vorlage des Mietvertrages erforderlich, um das Vorliegen einer steuerfreien Kapitalanlage bzw. die Höhe der festzusetzenden Steuer ermitteln zu können. Ebenso wird von der Rechtsprechung bei gewerblicher Zwischenvermietung die Vorlage des Vermittlungsvertrages gefordert.

Abschließend noch eine Stellungnahme zu zwei häufiger aufgetretenen Einzelproblemen:

1. Auf die Anforderung von Einkommensteuerbescheiden sollte verzichtet werden. Die Aussagekraft hinsichtlich der Einordnung einer Zweitwohnung als Kapitalanlage ist äußerst gering. Insbesondere bei Vorhandensein mehrerer Vermietungsobjekte lassen sich dem Bescheid keine weiterführenden Erkenntnisse entnehmen. Angesichts der sonstigen sensiblen Daten in Einkommensteuerbescheiden (z.B. Freibeträge wegen Behinderungen, Parteispenden) ist die Anforderung in der Regel nicht verhältnismäßig. Soweit sie im Einzelfall unverzichtbar sein sollte, muss dem Betroffenen freigestellt werden, nicht erforderliche personenbezogene Angaben unkenntlich zu machen.

2. Soweit die zwei Kommunen neben der Zweitwohnungssteuer auch Kurbeiträge erheben, mag gelegentlich ein Abgleich der Daten beider Abgaben nahe liegen.

   Zu unterscheiden ist zunächst zwischen einem Jahreskurbeitrag, den in der Regel der Zweitwohnungsinhaber neben der Zweitwohnungssteuer zu entrichten hat, und den Kurbeiträgen, die für Ferien- bzw. Kurgäste von Vermietern (dies sind regelmäßig auch die Zweitwohnungssteuerpflichtigen) abzuführen sind.

   Ein Abgleich für Zwecke des Jahreskurbeitrages ist gemäß § 11 Abs. 1 Nr. 1 Bustabe c Buchstaben aa NKAG zulässig, weil es sich um ein anderes Abgabenverfahren desselben Abgabenpflichtigen handelt.

   Ein Abgleich mit Daten aus den Kurbeitragsanmeldungen, die der Zweitwohnungssteuerpflichtige für seine Feriengäste vorzunehmen hat, stellt datenschutzrechtlich eine Datenerhebung bei Dritten (hier bei der für die Verwaltung der Kurbeiträge zuständigen Stelle) dar. Dafür gelten - wie oben dargestellt - die einschlägigen AO-Vorschriften, insbesondere § 93 AO. Ein derartiger Abgleich ist somit nur unter den dort genannten Voraussetzungen zulässig. Eine Kommune, die den Abgleich grundsätzlich in allen Fällen durchführt, habe ich aufgefordert, diese Praxis entsprechend zu ändern.

13 Umwelt, Landwirtschaft, Verkehr

13.1 Videoüberwachung von Abfall-Depotbehälterstandplätzen

Die Frage, ob für die Überwachung von Abfall-Depotbehälterstandplätzen mittels Videotechnik ausreichende Rechtsgrundlagen vorhanden sind, konnte im Berichtszeitraum in Abstimmung mit dem Umweltministerium geklärt werden.

Durch das Gesetz zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes (NGefAG) vom 25. Oktober 2001 ist § 32 Abs. 5 (neu: § 32 Abs. 3) geändert worden. Danach dürfen auch Verwaltungsbehörden öffentlich zugängliche Orte mittels Bildübertragung offen beobachten, wenn dies zur Erfüllung von Aufgaben nach § 1 Abs. 1 NGefAG erforderlich ist. Da § 45 Abs. 2 des Niedersächsischen Abfallgesetzes auf

die ergänzende Anwendung des Niedersächsischen Gefahrenabwehrgesetzes verweist - und damit auch auf § 32 Abs. 3 NGefAG -, ist eine Rechtsgrundlage für die Bildüberwachung (Übertragung) von Abfalldepotbehälterstandplätzen gegeben. Die Befugnis, die nach § 32 Abs. 3 Satz 1 NGefAG übertragenen Videobilder aufzuzeichnen und auszuwerten, hat gem. § 32 Abs. 3 Satz 2 jedoch nur die Polizei. Eine Aufzeichnung (und damit Datenspeicherung) der übertragenen Bilder durch Verwaltungsbehörden ist, wie das Umweltministerium mir mitgeteilt hat, jedoch nicht beabsichtigt. Damit ist geklärt, dass eine Bildübertragung und Simultanbeobachtung (Datenerhebung) rechtlich abgesichert, eine Bildaufzeichnung (Datenspeicherung) hingegen aus rechtlichen Gründen derzeit unzulässig ist. Sofern beabsichtigt ist, eine Bildaufzeichnung vorzunehmen und auszuwerten, bedarf es nach wie vor einer erst noch zu schaffenden bereichsspezifischen Rechtsgrundlage.

13.2 Kataster zu Standorten von Mobilfunksendeanlagen

Erhebliche Aktualität hat die Frage erlangt, ob und inwieweit Kommunen befugt sind, Standorte von Mobilfunksendeanlagen für ihren Bereich in einem Kataster zu erfassen und dies im Internet zu veröffentlichen oder auf Anfrage bekannt zu geben. Die Kommunen erhalten Angaben über die Mobilfunksendeanlagen wie Standortadresse, Art des Funksystems, Montagehöhe, Hauptstrahlrichtung und Sicherheitsabstände aus einer bei der Regulierungsbehörde Telekommunikation und Post (Reg TP) geführten Datenbank. Diese Übermittlung dient ausschließlich dem Zweck einer umfassenden und rechtzeitigen Information der Kommunen über die bestehenden und zukünftigen Antennenstandorte für Mobilfunknetze, einer abgestimmten Vorgehensweise beim Bau neuer Sendeanlagen und allgemeinen Maßnahmen, die vor allem die zukünftige Entwicklung betreffen. Für Zwecke der Veröffentlichung im Internet in Form eines Katasters sind diese Angaben nicht vorgesehen. Die Datenbank bzw. der Datenaustausch beruhen auf einer „Vereinbarung über den Informationsaustausch und die Beteiligung der Kommunen beim Ausbau der Mobilfunknetze“ vom 5. Juli 2001 zwischen sechs Mobilfunknetzbetreibern mit den auf Bundesebene tätigen kommunalen Spitzenverbänden. Eine Rechtsgrundlage für die Führung eines entsprechenden Katasters ergibt sich weder aus dem Immissionsschutzrecht noch aus dem Bauordnungsrecht. Dass die Führung eines Katasters einer Rechtsgrundlage bedarf, zeigen Beispiele wie § 6 Niedersächsisches Bodenschutzgesetz (Altlastenkataster), § 11 ff. Niedersächsisches Vermessungs- und Katastergesetz, § 300 Abs. 3 Baugesetzbuch (Baulandkataster) und § 46 Bundesimmissionsschutzgesetz (Emissionskataster). Hierauf hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung auf ihrer 64. Konferenz hingewiesen (vgl. Anlage 26) und den Gesetzgeber zur Schaffung einer entsprechenden Rechtsgrundlage aufgefordert, in der auch zu regeln ist, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist.

Die Übermittlung von Daten aus dem Kataster über Mobilfunksendeanlagen ist datenschutzrechtlich insoweit relevant, als dieses personenbezogene bzw. personenbeziehbare Daten, nämlich die genaue Anschrift, enthält, wenn die betroffenen Liegenschaften, auf denen sich die Anlagen befinden, im Eigentum bzw. in der Nutzung von natürlichen Personen oder Personengesellschaften stehen. Für datenschutzrechtlich

unproblematisch halte ich hingegen die Übermittlung von Daten über sichtbar angebrachte, von außen für jedermann erkennbare Sendeanlagen. Straßenbezeichnung und Hausnummer der Mobilfunkstation sind in diesem Falle offenkundige Daten; einer Weitergabe dieser Daten entgegenstehende schutzwürdige Interessen betroffener Dritter sind nicht ersichtlich.

Bei den Angaben zu Mobilfunksendeanlagen handelt es sich um umweltrelevante Daten. Jeder Bürger hat nach § 4 Abs. 1 UIG einen Anspruch auf freien Zugang zu Umweltinformationen, die bei einer Behörde vorliegen, ohne dass er ein besonderes Interesse oder ein Recht an der Bekanntgabe dieser Informationen haben oder nachweisen muss. Ausgenommen sind lediglich die Informationen, deren Weitergabe aufgrund der §§ 7 und 8 UIG ausgeschlossen oder beschränkt ist. Dabei werden von der Regelung des § 8 UIG nur solche Standorte betroffen, bei denen es sich um nicht offenkundige Anlagen auf Gebäuden oder Grundstücken handelt, die im Eigentum einer Privatperson oder einer Personengesellschaft stehen. Informationen, die offenkundig sind, fallen nicht unter den Schutzbereich des § 8 UIG, d.h. in diesen Fällen dürfen auch die personenbeziehbaren Daten an den Anfragenden übermittelt werden.

Sofern durch das Bekanntwerden der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden, besteht nach § 8 Abs. 1 Nr. 1 UIG kein Anspruch auf Herausgabe der Daten, soweit nicht im Einzelfall bei einer Abwägung das Interesse an der Herausgabe der Informationen überwiegt. In diesen Fällen ist der Eigentümer des Grundstückes vor einer Herausgabe seiner personenbezogenen Daten gemäß § 8 Abs. 2 UIG anzuhören. Um eine Vielzahl und ggf. auch Wiederholung von Einzelanfragen in konkreten Einzelfällen zu vermeiden, würde es sich aus meiner Sicht anbieten, alle betroffenen Grundstückseigentümer (das sind gemäß der oben genannten Einschränkung nur die Privatpersonen oder Personengesellschaften) vorab mit der Fragestellung anzuschreiben, ob die auf ihrem Grundstück vorhandene Mobilfunkanlage vom öffentlich zugänglichen Raum sichtbar ist. Nur wenn dies nicht der Fall ist, sollten sie weiter um Angabe von Gründen gebeten werden, die einer eventuellen Mitteilung ihrer personenbeziehbaren Daten (genaue Adresse) an Anfragende entgegenstehen könnten. Diese Gründe würden dann anlässlich einer entsprechenden Anfrage bei der erforderlichen Abwägung nach § 8 Abs. 1 Nr. 1 UIG (werden schutzwürdige Interessen des betroffenen Grundstückseigentümers durch das Bekanntwerden der Information beeinträchtigt?) zugrunde gelegt werden.

Die Einstellung von Einzeldaten über Standorte von Mobilfunksendeanlagen in das Internet, der eine andere Rechtsqualität zukommt als einem einzelnen Auskunftsersuchen, ist nicht nach dem Umweltinformationsgesetz (UIG), sondern ausschließlich nach dem Datenschutzrecht zu beurteilen. (Zwar gibt es in der neuen Informationszugangsrichtlinie auch die Verpflichtung zur aktiven Verbreitung bestimmter umweltbezogener Informationen, dies ist jedoch noch mit Bezug auf die deutschen Verhältnisse bei der Neufassung des UIG zur Umsetzung der neuen RL zu konkretisieren; dennoch halte ich eine verstärkte Nutzung des Internets zu einer initiativen, ohne Personenbezug erfolgenden Information der Bevölkerung auch heute schon für sinnvoll, da hierdurch evtl. vermehrte Einzelanfragen vermieden werden können.) Auch im Fall

einer Veröffentlichung im Internet sind nur die nicht offenkundigen Anlagen auf Gebäuden/Grundstücken von Privatpersonen oder Personengesellschaften problematisch, weil nur hier das im Datenschutzrecht geschützte Recht auf informationelle Selbstbestimmung des Grundstückseigentümers berührt sein kann. Solche Anlagen dürfen im Internet nur in anonymisierter Form dargestellt werden, d.h. ein Bezug auf den Grundstückseigentümer darf nicht herstellbar sein. Ggf. würde sich anbieten, die Gesamtbelastung von Gebieten - ähnlich wie bei einem Lärmschutzkataster - darzustellen. Jedoch müsste darauf geachtet werden, dass hierbei die relevanten Emissionspunkte nicht so konkret dargestellt werden, dass daraus ein grundstücksbezogener Standort abgeleitet werden kann und somit doch wieder ein Personenbezug herstellbar ist.

13.3 Gewährung von Rinderprämien bei der Ausfuhr in Drittländer

Damit ein Landwirt für den Verkauf von Rindern eine Prämie nach den o.a. Verordnungen erhalten kann, muss er die Ausfuhr seiner Tiere den Behörden nachweisen. Dieser Nachweis erfolgte mittels einer Kopie der Ausfuhranmeldung, auf der bislang der Name und die Adresse des Empfängers der Tiere geschwärzt waren. Dadurch erfuhren die Landwirte nicht, an wen die Tiere von ihren Händlern veräußert wurden. Eine Viehhandlung kritisierte diese aus Datenschutzgründen vorgenommene Schwärzung, weil sie zu einer Verfälschung prämienrelevanter Unterlagen führe.

Das in die Klärung der Frage eingeschaltete Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft hat erläutert, dass gegen die Schwärzung der Adressen der Viehempfänger keine Einwendungen bestehen, sofern alle erforderlichen Angaben (wie insbesondere Exporteur, Zahl der Tiere, deren Ohrmarkennummern, Bestimmungsland, Abfertigungsgrund des Zolls) aus den Dokumenten zu entnehmen sind. Begründet wird dies damit, dass nach den Vorschriften von Artikel 35 Abs. 1 Unterabsatz 5 Buchstabe b) der VO (EG) Nr. 2342/99 die Angabe des Empfängers der Tiere im Drittland nicht prämienrelevant ist. Zwecks Kontrolle der dem Prämienantrag in Kopie beigefügten Ausfuhrdokumente kann sich die Prämienbehörde die Originaldokumente vom Ausführer vorlegen lassen oder auch bei stichprobenweisen Kontrollen beim Ausführer einsehen. Außerdem erhält die Prämienbehörde im Rahmen des Abgleichs mit dem Hauptzollamt Hamburg-Jonas eine beglaubigte Kopie der Ausfuhrdokumente mit der von der Ausgangszollstelle bestätigten Ausfuhr der Tiere, in denen auch der Empfänger angegeben ist. Meine Auffassung, dass die - datenschutzrechtlich erforderliche - Schwärzung auch fachlich vertretbar ist, sehe ich damit bestätigt.

13.4 Mautgebühr - „Der gläserne Verkehrsteilnehmer“?

Am 12. April 2002 trat das Gesetz zur Einführung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen mit schweren Nutzfahrzeugen in Kraft. Ab 2003 ist neben der manuellen Erhebung von Gebühren ein automatisches System geplant, mit dem eine streckenbezogene Maut für Lastkraftwagen erhoben werden soll. Für das automatische System sollen das Satellitennavigationssystem „Global Positioning System“ (GPS) und die Mobilfunktechnologie genutzt werden. Durch diese Nutzung soll weitestgehend auf stationäre Erfassungseinrichtungen verzichtet

werden. Das System lässt sich problemlos auf den Bereich von Bundesstraßen und auf das Ausland erweitern. Entsprechendes Interesse aus dem benachbarten Ausland wurde bereits bekundet. Dieses Verfahren birgt die datenschutzrechtliche Gefahr einer Totalüberwachung des Straßenverkehrs in sich, da jederzeit feststellbar ist, wer wann wo und wie unterwegs ist (bis hin zur Anfertigung exakter Bewegungsprofile). Deshalb ist die Beachtung des Prinzips der Datensparsamkeit, der frühestmöglichen Löschung und der strikten Zweckbindung im Falle des Entstehens elektronischer Bewegungsprofile unverzichtbar.

In einer Entschließung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder Anforderungen an Systeme zur automatischen Erhebung von Benutzungsgebühren formuliert (vgl. Anlage 13). Hiernach darf insbesondere die Identität eines Zahlungspflichtigen nur aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht entrichtet worden sind. Das gesamte Verfahren der Gebührenerhebung und -kontrolle muss für die Mautpflichtigen transparent gestaltet sein. Vorzuziehen sind Systeme, bei denen die Gebühren vorab gezahlt werden können und Bewegungsdaten allenfalls beim Zahlungspflichtigen anfallen.

Des Weiteren trat am 6. September 2002 ein Gesetz in Kraft, das die Erhebung von Mautgebühren an privat finanzierten Bundesfernstraßen (wie z.B. Tunneln und Brücken) vorsieht. Auch hier muss darauf geachtet werden, dass keine Bewegungsprofile der Verkehrsteilnehmer entstehen. Es ist zu begrüßen, dass dieses Gesetz bereits die Möglichkeit der anonymen direkten Barbezahlung vorsieht.

14 Bildung

14.1 Internet-Anschluss für alle niedersächsischen Schulen

Das in meinem letzten Tätigkeitsbericht dargestellte Aktionsprogramm der Landesinitiative „N-21: Schulen in Niedersachsen Online“ ist so weit fortgeschritten, dass in Niedersachsen nahezu alle Schulen mittlerweile Internetzugang haben.

In Abstimmung mit dem Kultusministerium habe ich eine Orientierungshilfe und einen Fragenkatalog der am häufigsten gestellten Fragen zum Umgang mit dem Internet im Schulbereich erarbeitet, die bei Bedarf von meiner oder der Homepage der Landesinitiative abrufbar sind.

Trotzdem werden mir immer wieder Fragen gestellt, die ich in den von mir zur Verfügung gestellten Unterlagen bereits beantwortet habe. „Dürfen wir auf unserer Homepage Bilder und personenbezogene Daten wie Adressen oder Telefonnummern von Lehrern oder von Schülern veröffentlichen?“ ist die häufigste Frage. Viele Schulleitungen wissen offenbar noch nicht, dass sie für die (weltweite) Veröffentlichung solcher Daten die Einwilligung der Eltern bzw. der volljährigen Schüler benötigen.

Ich kann ich mich des Eindrucks nicht erwehren, dass sich nicht wenige Schulen mit den datenschutzrechtlichen Aspekten ihrer schulischen Aufgaben noch nicht genügend auseinandergesetzt haben. Zur Vermittlung von Medienkompetenz gehört nicht

nur das Wissen um das Funktionieren der Technik, sondern auch der Hinweis auf die Risiken und die Schutzmechanismen, mit denen diesen entgegengewirkt werden kann.

Die auch für die Schulen zu bestellenden behördlichen Datenschutzbeauftragten werden sich mit diesem Problembereich stärker befassen müssen.

Ich werde meine Zusammenarbeit mit den schulischen Datenschutzbeauftragten verstärken und auch durch Beratung vor Ort, z.B. in Schulleiterkonferenzen, zur Lösung praktischer Datenschutzprobleme im Schulalltag beitragen.

14.2 Bekämpfung des Schulschwänzens

Im Jahr 2000 wurden bundesweit 10 460 Schüler sowie ihre Lehrkräfte zum Schulschwänzen befragt, nachdem sich in vorangegangenen Pilotstudien gezeigt hatte, dass dieses Thema aus pädagogischer, psychologischer und kriminologischer Perspektive relevant ist, in Deutschland bislang jedoch nur unzureichend erforscht war. Die Befragung fand unter der wissenschaftlichen Begleitung des Kriminologischen Forschungsinstituts Niedersachsen (KFN) statt und zeigte, dass Schulschwänzen ein weit verbreitetes Phänomen darstellt. Insgesamt 52,9 % aller Schüler erklärten, dass sie im letzten Schulhalbjahr schon einmal die Schule geschwänzt hätten. Massives Schwänzen, d.h. fünf Tage oder mehr im Schulhalbjahr, wurde von 14,8 % der Befragten angegeben. Es war auffallend, dass ein großer Teil der Jugendlichen berichtete, dass auf ihr Schulschwänzen keine Reaktionen durch Lehrkräfte erfolgt seien.

In Niedersachsen wurde eine interministerielle Arbeitsgruppe unter Beteiligung des Ministeriums für Frauen, Arbeit und Soziales, des Innenministeriums, des Justizministeriums, des Kultusministeriums und dem Landespräventionsrat mit dem Ziel eingerichtet, ein Programm zur Bekämpfung des Schulschwänzens zu erarbeiten. Die Landesregierung billigte im Mai 2002 das Eckpunkteprogramm der Arbeitsgruppe, welches u.a. vertragliche Vereinbarungen zwischen Schule und Erziehungsberechtigten (z.B. telefonische Erreichbarkeit während des Tages), ein Ansprechpartnersystem (zwischen Schule und Jugendhilfe), ein sog. Unterstützungsteam aus Lehrkräften und Vertrauensschülern innerhalb der Schule, begleitende kriminalpräventive Maßnahmen der Polizei (zielgerichtete Kontrollen während der Schulzeit an bekannten Jugendtreffpunkten) und die Bildung eines „runden Tisches“ zwischen den beteiligten Kooperationspartnern vorsieht.

Meine datenschutzrechtlichen Bedenken, insbesondere zu dem Informationsaustausch im Ansprechpartner-System und im Rahmen des „runden Tisches“, wurden ausgeräumt; die genannten Unterstützerteams kommen nur zum Einsatz, wenn die Freiwilligkeit bei allen Beteiligten eindeutig feststeht. Der „runde Tisch“ wirft aus Datenschutzsicht deshalb Probleme auf, weil viele unterschiedliche öffentliche und private Stellen in enger Kooperation dem Schulschwänzen entgegenwirken sollen. Hierbei müssen allerdings die datenschutzrechtlichen Grenzen der Übermittlung personenbezogener Informationen berücksichtigt werden, die sich aus den jeweiligen Fachgesetzen (z.B. Sozialgesetzbuch, Schulgesetz, Gefahrenabwehrgesetz) ergeben. Die aus meiner Sicht beste Lösung wäre es, Problemfälle in anonymisierter bzw. pseudony-

misierter Form zu erörtern. Unter Namensnennung der Betroffenen dürfen Einzelheiten über Schulschwänzer nur so weit am „runden Tisch“ thematisiert werden, wie die Daten allen Teilnehmern nach den einschlägigen Vorschriften übermittelt werden dürfen. Durch ein Gespräch mit den projektleitenden Polizeibeamten konnte ich mich davon überzeugen, dass insbesondere die begleitenden kriminalpräventiven Maßnahmen datenschutzgerecht durchgeführt werden. Ich habe mir vorbehalten, das Projekt nach seiner Einführung zum 1. August 2002 weiter zu begleiten und die datenschutzkonforme Umsetzung an praktischen Einzelfällen zu überprüfen.

14.3 Datenübermittlungen von Schulen an Private

Zur Orientierung der Verwaltung an den Interessen der Bürger gehört insbesondere, dass die Verwaltungsstellen sich als Dienstleister verstehen und die Servicefunktion ihres Handelns betonen. Diese Entwicklung ist uneingeschränkt zu begrüßen, ein solches Aufgabenverständnis darf aber gesetzliche Grenzen des Verwaltungshandelns nicht beiseite schieben.

Darauf habe ich mehrfach Landesbehörden wie Kommunen hinweisen müssen, die unter Berufung auf ihre Bürgerorientierung Datenübermittlungen vorgenommen haben, für die eine Rechtsgrundlage nicht vorhanden war.

So teilten mehrere kommunale Schulämter Namen und Anschriften der Elternratsvorsitzenden ihrer Schulen Kommunal- und Landespolitikern mit, die diese Personen zu politischen Diskussionsveranstaltungen einladen wollten, um mit ihnen strukturelle Veränderungen im Schulbereich zu erörtern.

Dieses Vorgehen wurde zum Teil mit der Einschätzung gerechtfertigt, mit schulpolitischen Diskussionen werde ein Beitrag zur politischen Willensbildung geleistet, den man von kommunaler Seite unterstützen müsse. In einem Fall meinte ein Landkreis gar, ein Parlamentarier bzw. eine politische Partei habe aufgrund des Parteiengesetzes ein rechtliches, d.h. auf die Durchsetzung von Rechtsansprüchen abzielendes Interesse an der Kenntnis solcher Daten. Die Bürger, die sich am mich wandten, sahen dies anders. Sie haben Recht.

Eine Datenübermittlung an Private (dazu zählen auch die Parteien) kommt auch bei dem hier anzunehmenden öffentlichen, mindestens aber zu bejahenden berechtigten privaten Interesse nur in Betracht, wenn die von der Datenübermittlung Betroffenen dem nicht widersprochen haben. Die Elternratsvorsitzenden hätten somit zunächst auf die beabsichtigte Datenweitergabe und ihre Möglichkeit, dieser Verfahrensweise zu widersprechen, hingewiesen werden müssen. Erst beim Ausbleiben eines Widerspruchs durften die Daten übermittelt werden (§ 13 Abs. 1 Nr. 3 NDSG).

In der Regel haben sich die betroffenen Kommunen nach entsprechender Aufklärung dieser rechtlichen Beurteilung angeschlossen. In einem Fall musste ich allerdings das Verhalten einer Stadt beanstanden, weil sie sich trotz eines vorausgegangenen Hinweises der Bezirksregierung mit dieser Rechtslage nicht anfreunden wollte und sich auch mir gegenüber sträubte, den Rechtsverstoß einzusehen. Der Bürgermeister hat

daraufhin zwar bedauert, dass hierdurch der Handlungsrahmen der Stadt als Dienstleister eingeschränkt werde, sich aber schließlich der Rechtslage gefügt.

Die gleiche Rechtslage gilt auch für die immer wieder vorkommenden Fälle der Übermittlung personenbezogener Daten ehemaliger Schüler durch die Schulverwaltung. Ob es sich um „Gutscheinaktionen“ oder um andere Werbemaßnahmen der privaten Stellen handelt, die Übermittlung von Namen, Adressen oder Telefonnummern ehemaliger Schüler oder Schülerinnen ist nur mit deren Einwilligung oder unter den oben geschilderten gesetzlichen Voraussetzungen des § 13 Abs. 1 Nr. 3 NDSG zulässig.

14.4 Informations- und Auskunftsrecht von Eltern volljähriger Schüler

Der Amoklauf eines volljährigen Schülers in Erfurt, dem mehrere Lehrkräfte und Schüler zum Opfer gefallen sind, hat in den Ländern eine lebhafte Diskussion darüber ausgelöst, ob Eltern von der Schule über Auffälligkeiten im Verhalten volljähriger Schüler unterrichtet werden sollten. Gefordert wird diese Unterrichtung im Wesentlichen bei gravierenden Schulverstößen, verhängten Ordnungsmaßnahmen, Alkoholproblemen oder einem deutlichen Leistungsabfall der Heranwachsenden. Bayern hat dieses Problem inzwischen gesetzlich geregelt. Danach sollen die dortigen Schulen frühere Erziehungsberechtigte volljähriger Schüler, die das 21. Lebensjahr noch nicht vollendet haben, über Ordnungsmaßnahmen unterrichten. Auch eine Information über den Leistungsstand dieser Schüler ist zulässig. Andere Länder erwägen zum Teil, den Schulen durch entsprechende Erlassregelung eine solche Verpflichtung aufzuerlegen. Auch in Niedersachsen wird darüber diskutiert, mit welchen Mitteln diesem Problem begegnet werden kann. Ich habe das Fachressort darauf hingewiesen, welche datenschutzrechtlichen Gesichtspunkte hierbei zu beachten sind.

Die Unterrichtung der Eltern über das schulische Verhalten volljähriger Söhne und Töchter greift in deren Recht auf informationelle Selbstbestimmung ein. Nach der Rechtsprechung des Bundesverfassungsgerichts und dem Niedersächsischen Datenschutzgesetz besteht dieses Recht in der Befugnis, grundsätzlich selbst zu bestimmen, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Eine Information der Eltern kommt deshalb nur in Betracht, wenn entweder eine gesetzliche Regelung oder aber eine Einwilligung der betroffenen Schüler vorliegt.

Der Umstand, dass Schüler dieses Alters in der Regel noch zum Familienverband gehören und von ihren Eltern wirtschaftlich abhängig sind, spielt in diesem Zusammenhang keine ausschlaggebende Rolle. Rechtlich ist unbestritten, dass das Recht der Eltern auf Pflege und Erziehung mit fortschreitendem Alter des Kindes abnimmt und mit dessen Volljährigkeit erlischt. Die Personensorge beschränkt sich nach ihrer rechtlichen Ausgestaltung auf minderjährige Kinder. Deshalb kann mit diesem Gesichtspunkt kein Vorrang eines Informationsanspruchs der Eltern gegenüber dem informationellen Selbstbestimmungsrechts der volljährigen Schülerin oder des volljährigen Schülers begründet werden.

Ob es praktikabel ist, die in Rede stehende Datenübermittlung auf eine Einwilligung zu stützen, mag man bezweifeln. Schüler, die in gespannten Familienverhältnissen leben, werden eine solche Einwilligung oftmals von vornherein nicht geben. Im Übrigen kann eine erteilte Einwilligung jederzeit für die Zukunft widerrufen werden. Schon deshalb dürfte sie kaum eine verlässliche Grundlage für entsprechende schulische Mitteilungen darstellen. Eine Lösung kann auch nicht darin gesehen werden, dass die Einwilligung unterstellt wird.

Aus anderen Ländern sind mir Überlegungen bekannt geworden, wonach eine Einwilligung angenommen werden soll, solange die Schüler der Unterrichtung ihrer Eltern nicht widersprechen. Auch wenn die Heranwachsenden zuvor auf diese Widerspruchsmöglichkeit hingewiesen worden sind, ist eine solche Verfahrensweise mit dem Datenschutzrecht nicht zu vereinbaren. Die Einwilligung bedarf grundsätzlich der Schriftform (§ 4 Abs. 2 NDSG). Besondere Umstände, die ausnahmsweise eine andere Form zulassen könnten, liegen hier nicht vor. Ein bloßes Schweigen kann deshalb nicht als Zustimmung gewertet werden.

§ 13 Abs.1 Nr. 3 NDSG lässt eine Widerspruchslösung für eine Datenübermittlung an Private allerdings dann zu, wenn diese entweder im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird. Ob ein öffentliches Interesse bejaht werden kann, mag zweifelhaft sein. Ein berechtigtes Interesse der Eltern ist fraglos gegeben. Es kann jedoch von der Schule nicht unterstellt, sondern muss nach der gesetzlichen Regelung bekundet werden. Dieses Verfahren setzt deshalb zunächst voraus, dass die Eltern von der Schule auf die Unterrichtung angesprochen werden und ihr Interesse daran geltend machen. Danach würde die Schule die Schüler über die beabsichtigte Datenübermittlung unterrichten und auf die Möglichkeit des Widerspruchs hinweisen. Unterbleibt dieser, kann die Unterrichtung der Eltern erfolgen.

Will man die praktischen Probleme einer Einwilligungs- oder Widerspruchslösung vermeiden, kommt nur eine gesetzliche Regelung in Betracht. Durch Verwaltungsvorschrift, auch wenn sie nur vorläufigen Charakter bis zum In-Kraft-Treten einer Gesetzesvorschrift haben sollte, ist es nicht möglich, in grundrechtlich geschützte Rechtspositionen, wie das informationelle Selbstbestimmungsrecht, einzugreifen. Ein solcher Eingriff, der in der Übermittlung der Schülerdaten an die Eltern liegt, ist nach der Rechtsprechung des Bundesverfassungsgerichts nur durch eine normenklare gesetzliche Regelung möglich, die durch ein überwiegendes öffentliches Interesse gerechtfertigt ist. Dieses Interesse dürfte mit dem Personensorgerecht der Eltern nicht zu begründen sein, da sich dieses Recht nicht mehr auf volljährige Kinder erstreckt. Ob außerhalb des Personensorgerechts ein überwiegendes Interesse der Öffentlichkeit an der Unterrichtung der Eltern besteht, das den Eingriff in das Grundrecht der Betroffenen auf Datenschutz rechtfertigen kann, müsste im Falle einer beabsichtigten gesetzlichen Regelung eingehend geprüft und überzeugungskräftig darlegt werden. Sofern eine solche gesetzliche Regelung für bestimmte Fallgestaltungen die Entscheidung in das Ermessen der Schule stellen sollte, muss sichergestellt sein, dass die aus Sicht der volljährigen Schülerin oder des volljährigen Schülers zu berücksich-

tigenden Gesichtspunkte von der Schule in die Abwägung mit einbezogen werden können.

Das Kultusministerium hat sich für die Einwilligungslösung entschieden. Es hat in die Grundsatzerlasse für die einzelnen Schulformen eine Regelung aufgenommen, wonach eine Information der Eltern erfolgen soll, wenn eine schriftliche Einwilligung der volljährigen Kinder vorliegt.

Um Missverständnisse zu vermeiden, möchte ich betonen, dass eine Unterrichtung der Erziehungsberechtigten minderjähriger Schüler auf der Grundlage des Niedersächsischen Schulgesetzes (§ 31) problemlos möglich ist.

14.5 Das neue Hochschulgesetz

14.5.1 Einzelregelungen zum Datenschutz treffen die Hochschulen selbst

Mit dem am 24. Juni 2002 vom Niedersächsischen Landtag beschlossenen Gesetz zur Hochschulreform ist eine Neufassung des Niedersächsischen Hochschulgesetzes (NHG) verabschiedet worden. Dieses Gesetz stärkt die Selbstständigkeit der Hochschulen und gibt ihnen neue Gestaltungsmöglichkeiten in wichtigen Datenschutzfragen. Allerdings werden die Hochschulen angehalten, normenklare Regelungen in eigenständigen Ordnungen zu treffen, zum Beispiel für die Nutzung personenbezogener Daten. In diesem Zusammenhang sind insbesondere die §§ 5 und 17 von Bedeutung. Während § 17 allgemeine Grundlagen zur Verarbeitung personenbezogener Daten durch die Hochschulen legt, befasst sich § 5 ausführlich mit Fragen der Evaluation. Insbesondere dieser Bereich hatte in der Vergangenheit Anlass zur kritischen Auseinandersetzung mit der Praxis einiger Hochschulen gegeben.

14.5.2 Verarbeitung personenbezogener Daten an Hochschulen

§ 17 Abs. 1 NHG bildet die generelle Grundlage für die Verarbeitung personenbezogener Daten an Hochschulen, soweit es sich um Daten von Hochschulangehörigen, Mitgliedern oder Studienbewerbern handelt, die für die Einschreibung, die Teilnahme an Lehrveranstaltungen und Prüfungen, die Nutzung von Hochschuleinrichtungen sowie die Kontaktpflege mit ehemaligen Hochschulmitgliedern erforderlich sind. Diese Verarbeitung muss in hochschuleigenen Ordnungen festgelegt sein. Die Daten dürfen auch für die Erfüllung der übrigen Aufgaben der Hochschulen sowie für Zwecke der Evaluation nach § 5 verwendet werden. Weiter gibt das Gesetz den Hochschulen Möglichkeiten an die Hand, mit Hilfe von Ordnungen die Verwendung von mobilen Speichermedien (Chipkarten o.Ä.) verpflichtend zu regeln.

In § 17 Abs. 2 NHG sind Regelungen des alten Hochschulgesetzes übernommen worden, die es erlauben, von Hochschulmitgliedern und -angehörigen Daten zur Beurteilung von Bewerbungssituation, der Lehr- und Forschungstätigkeit, des Studienangebots sowie des Ablaufs von Studium und Prüfung zu verarbeiten. Sollen Auskunftspflichten begründet oder Erhebungen ohne Einwilligung der Betroffenen zugelassen werden, kann dies nur über eine hochschulinterne Ordnung geschehen, die eine Reihe von Vorgaben zu erfüllen hat. Daten, die in diesem Rahmen erhoben werden, sind zum frühestmöglichen Zeitpunkt zu anonymisieren.

14.5.3 Evaluation

§ 5 NHG gibt den Hochschulen auf, die Erfüllung ihrer Aufgaben in regelmäßigen Abständen zu begutachten und zu bewerten.

Das Verfahren der internen Evaluation hat die Hochschule in einer Ordnung zu regeln. Auf der Grundlage der internen Evaluation erfolgt in regelmäßigen Abständen eine externe Evaluation; die Ergebnisse der Evaluationen sollen veröffentlicht werden. Für den begrenzten Bereich der Evaluation im Bereich der Lehre sieht die Vorschrift vor, dass den Studierenden Gelegenheit zu geben ist, die Qualität der Lehrveranstaltungen zu bewerten. Die Ergebnisse sind dem Präsidium der Hochschule vorzulegen und zusammen mit den erforderlichen Maßnahmen Gegenstand der Rechenschaftspflicht des Präsidiums. Das Bewertungsverfahren und das Verarbeiten der personenbezogenen Daten des wissenschaftlichen oder künstlerischen Personals hat die Hochschule in einer Ordnung zu regeln; dabei ist auf die frühestmögliche Anonymisierung der Daten hinzuwirken.

Da es im Ministerium für Wissenschaft und Kultur keine Planungen für die Entwicklung von Musterordnungen für die entsprechenden Bereiche gibt, werden die Hochschulen mit der Notwendigkeit, Regelungen in Form von Ordnungen zu treffen, leider allein gelassen. Daher versuche ich in einem Arbeitskreis mit Vertretern der Hochschulverwaltungen und deren behördlichen Datenschutzbeauftragten einen Rahmen für die benötigten Ordnungen zu entwickeln, der die wesentlichen datenschutzrechtlichen Aspekte vorgibt und von den Hochschulen als Ausgangspunkt für eigene Ordnungen genutzt werden kann. Durch eine datenschutzgerechte Gestaltung der jeweiligen Hochschulordnungen könnte künftig eine erhebliche Anzahl von Eingaben aus diesem Bereich vermieden werden. In der Vergangenheit wurde insbesondere die Lehr-Evaluation kritisiert.

15 Soziales

Angesichts knapper Kassen in allen öffentlichen Bereichen ist es unabwendbar geworden, ungerechtfertigte Sozialleistungen zu vermeiden. Die Finanznot der öffentlichen Hände hat im Sozialbereich eine Entwicklung angestoßen, die zu zunehmenden Datenabgleichen zwischen unterschiedlichen Leistungsträgern und sonstigen Stellen führt, um einem Leistungsmissbrauch entgegenzuwirken. Einzelheiten zu diesen Verfahren habe ich in meinem XIV. Tätigkeitsbericht unter Nr. 18.1 dargestellt.

Aus den Eingaben Betroffener im Berichtszeitraum habe ich den Eindruck gewonnen, dass über diese Datenabgleiche hinaus in der Praxis der Sozialämter die Voraussetzungen von Leistungsansprüchen weitaus gründlicher geprüft werden als noch vor Jahren. Die mit einer solchen Verfahrensweise notwendigerweise verbundenen Datenerhebungen berühren natürlich auch die persönlichkeitsrechtlichen Belange der betroffenen Personen. Datenschutzrechtlich ist gegen ein solches „schärferes“ Vorgehen der Sozialbehörden solange nichts einzuwenden wie es die gesetzlichen Grenzen nicht überschreitet. Dies musste ich Petenten immer wieder mitteilen, die in einer geänderten Verwaltungspraxis datenschutzrechtliche Probleme sahen. Das behördliche Verhalten darf allerdings die Hilfesuchenden nicht einer Totalkontrolle

unterwerfen. Das Verhältnismäßigkeitsprinzip ist selbstverständlich auch hier zu beachten. Auch pauschale Einwilligungserklärungen, die den Sozialbehörden eine Datenerhebung bei Dritten ermöglichen sollen, dürfen den Hilfesuchenden nicht „abgenötigt“ werden. Trotz zahlreicher Hinweise zu dieser Problematik werden mir immer wieder Fälle vorgetragen, in denen Sozialämter sich inhaltlich unbestimmte, für die Hilfesuchenden nicht durchschaubare „Einwilligungen“ für eine nicht erforderliche Datenverarbeitung erteilen lassen.

In meiner Beratungs- und Kontrolltätigkeit habe ich besonderes Augenmerk darauf gelegt, dass die verstärkte Kontrolldichte nicht dazu führt, die grundgesetzlich geschützten Belange Hilfesuchender beiseite zu drängen.

Über solche Änderungen in der Verwaltungspraxis hinaus werden die verstärkten Bemühungen zur Bekämpfung der Arbeitslosigkeit zu einem grundlegenden Umbau der Sozialverwaltung und der bisherigen Vermittlungspraxis führen.

Mit dem Gesetz zur Verbesserung der Zusammenarbeit zwischen Arbeitsämtern und Trägern der Sozialhilfe vom 2. November 2000 hat der Gesetzgeber bereits neue Wege der Zusammenarbeit zwischen Arbeits- und Sozialämtern zugelassen. Weitreichende strukturelle Änderungen werden sich künftig durch die grundlegende Neuausrichtung der Arbeitsmarktpolitik aufgrund der Vorschläge der Hartz-Kommission ergeben. Die Kommission will eine Halbierung der Arbeitslosenzahlen bis Ende 2005 erreichen, für Beitrags- und Steuerzahler werden Einsparungen von 20 Milliarden Euro angestrebt. Unmittelbar nach dem Bekanntwerden dieser Vorschläge hat die Bundesregierung erklärt, sie werde dieses Konzept umsetzen. Dazu soll die Arbeitsverwaltung neu strukturiert und die Arbeitsverteilung zwischen Arbeits- und Sozialverwaltung neu festgelegt werden.

15.1 Verstärkte Prüfung von Leistungsansprüchen

Um ein Urteil darüber zu ermöglichen, ob die verschärfte Kontrollpraxis zu datenschutzrechtlichen Nachteilen für die Hilfesuchenden geführt hat, habe ich zunächst bei einzelnen Sozialämtern mit einer Querschnittsprüfung begonnen, die im Ergebnis zu einer Bestandsaufnahme der Datenschutzpraxis bei der herkömmlichen Datenverarbeitung führen soll.

Angesichts des Eindrucks, den an mich herangetragene Beschwerden nahe legen, war bei den bisher von mir geprüften Stellen die im Kern positive Einstellung zum Datenschutz bemerkenswert. Trotz der bestehenden starken Arbeitsbelastung begegnete ich durchgängig offenen und engagierten Mitarbeitern. In der Regel war man bemüht, die von mir festgestellten Mängel und Verstöße umgehend abzustellen. Insbesondere Mängel in der Datensicherheit, z.B. nicht abschließbare Aktenschränke, überfüllte Archive oder veraltete Schließanlagen, waren nicht auf die Sorglosigkeit der Mitarbeiter und Mitarbeiterinnen, sondern auf fehlende Mittel im Haushalt der Kommunen zurückzuführen.

Problematischer war die Situation hinsichtlich der bereits angesprochenen pauschalen Einwilligungen. Die Anträge auf Sozialhilfe waren jeweils mit einer Einwilligungs-

erklärung zur Befreiung vom Bankgeheimnis versehen, welche von jedem Hilfesuchenden abzugeben war.

Ich habe darauf hingewirkt, dass diese Einwilligungen nur noch in besonderen, begründeten Einzelfällen unter Beachtung der Grundsätze der Erforderlichkeit und Verhältnismäßigkeit angefordert werden.

Ein geeignetes Mittel zur stärkeren Kontrolle wird von Sozialämtern vor allem in Hausbesuchen bei den Hilfesuchenden gesehen. Wiederholt erreichten mich Eingaben, in denen aufgebrachte Petenten die Frage stellten: „Dürfen Hausbesuche überhaupt durchgeführt werden?“ Die Antwort ist: “Ja, aber nur wenn diese Form der Datenerhebung wegen der Besonderheiten des Falles gerechtfertigt ist.“ Zu bedenken ist vor allem, dass Hausbesuche das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 GG) tangieren. Nur unter besonderen Voraussetzungen sind sie deshalb ein geeignetes und angemessenes und damit auch datenschutzrechtlich zulässiges Mittel der Bedarfsfeststellung. Gegen den Willen des Wohnungsinhabers dürfen sie aber nicht durchgeführt werden.

Was bei Hausbesuchen zu beachten ist, sollte vorab in einer Dienstanweisung wie folgt festgelegt werden:

- Vor Durchführung eines Hausbesuches ist stets zu prüfen, ob nicht andere Möglichkeiten der Sachverhaltsklärung bestehen, die weniger tief in die Rechte der Betroffenen eingreifen.
- Es müssen konkrete Anhaltspunkte bestehen, die einen Hausbesuch rechtfertigen.
- Die Gründe für den Hausbesuch müssen den Betroffenen offen gelegt werden.
- Die Wohnungsinhaber müssen auf ihr Recht hingewiesen werden, dem Hausbesuch zu widersprechen. Über die zu erwartenden Folgen ihrer Weigerung sind sie aufzuklären.
- Eine Hausdurchsuchung ist unzulässig.
- Befragungen Dritter sind nur zulässig, wenn die Voraussetzungen des § 67a Abs. 2 SGB X vorliegen.
- Der Hausbesuch muss von legitimierten Mitarbeitern der Sozialämter durchgeführt werden.

Als sinnvoll kann sich die Einrichtung eines zentralen Außendienstes erweisen. Dadurch kann ein einheitliches Vorgehen unter Beachtung der genannten Grundsätze sichergestellt werden.

Weitere Hinweise zu diesem Thema finden Sie auf meiner Homepage unter dem Stichwort „Sozialhilfeermittlungen“ (Themen-Sozialdaten-Sozialhilfeermittlungen).

15.2 Umbau der Sozialverwaltung zur Bekämpfung der Arbeitslosigkeit

Mit dem Gesetz zur Verbesserung der Zusammenarbeit von Arbeitsämtern und Trägern der Sozialhilfe vom 20. November 2000 hat der Gesetzgeber mit den §§ 421d SGB III und 18a BSHG Experimentierklauseln geschaffen, die es ermöglichen sollen,

in Modellprojekten neue Formen der Zusammenarbeit zwischen Arbeits- und Sozialämtern zu erproben. Bundesweit haben sich ca. 30 Arbeits- und Sozialämter zu entsprechenden Modellvorhaben zusammengefunden, drei davon in Niedersachsen.

Unter der Bezeichnung MoZART (Modellvorhaben zur Verbesserung der Zusammenarbeit zwischen Arbeitsämtern und Trägern der Sozialhilfe) werden Arbeitssuchende beraten und vermittelt. Im Rahmen der Modellvorhaben müssen Probleme, die sich aus der unterschiedlichen Zielsetzung und organisatorischen Zuordnung der beteiligten Behörden ergeben, gelöst werden. Aufgabe der Sozialämter ist bisher in erster Linie die Sicherung des notwendigen Lebensunterhalts, die Arbeitsämter hingegen sind für die Arbeitsvermittlung zuständig. Das örtliche Arbeitsamt unterliegt als Teil der Bundesanstalt für Arbeit der Kontrolle des Bundesarbeitsministers, die Sozialhilfegewährung ist dagegen eine kommunale Selbstverwaltungsaufgabe der Kreise und der kreisfreien Städte, die der Aufsicht des Landes unterliegen. Aus Datenschutzsicht ergeben sich u.a. folgende Fragen:

- Welche personenbezogenen Daten dürfen an einen potenziellen Arbeitgeber übermittelt werden?
- Dürfen Bedienstete des Sozialamtes die Datenbestände des Arbeitsamtes einsehen und umgekehrt oder ist die Zugriffsmöglichkeit auf die jeweils am konkreten Projekt beteiligten Bediensteten dieser Ämter beschränkt?
- Wem gegenüber sind die Betreiber des Modellprojektes verantwortlich und wer übt die Aufsicht und die Kontrolle aus?

Auf diese und andere datenschutzrechtliche Fragen gibt das Gesetz keine konkrete Antwort. Die Regierungsfraktionen SPD und BÜNDNIS 90/DIE GRÜNEN haben seinerzeit durch Einbringung eines Fraktionsentwurfs im Bundestag das interministerielle Abstimmungsverfahren „umgangen“. Datenschutzgesichtspunkte sind deshalb allenfalls am Rande zur Sprache gekommen. Für die Verwaltungspraxis haben sich dadurch vielfältige datenschutzrechtliche Probleme ergeben.

Im Rahmen einer Begleitforschung zu MoZART ist das „infas-Institut für angewandte Sozialwissenschaft“ vom Bundesministerium für Arbeit und Sozialordnung beauftragt worden, eine wissenschaftliche Evaluation zu diesen Modellvorhaben durchzuführen. Diese Evaluation soll die Modellvorhaben mit empirischen Ergebnissen unterstützen, die Wirkung der unterschiedlichen Erprobungsmodelle bewerten und tragfähige Empfehlungen für die Gesetzgebung aussprechen.

Um die für die Durchführung dieser Evaluation erforderliche Genehmigung der obersten Landesbehörde für die Übermittlung von Sozialdaten (§75 SGB X) zu erhalten, wurde das Evaluationsvorhaben vom „infas-Institut“ den Datenschutzbeauftragten der Länder und des Bundes vorgestellt. Nach der Erörterung der datenschutzrechtlichen Belange und mehreren „Nachbesserungen“ des Instituts wurde die Genehmigung vom Ministerium für Frauen, Arbeit und Soziales erteilt.

Um die an den Modellvorhaben beteiligten niedersächsischen Sozialämter zu unterstützen, werde ich die datenschutzrechtlichen Probleme mit ihnen erörtern.

Der Umbau der Arbeitsverwaltung nach den Vorstellungen der Hartz-Kommission geht weit über den Ansatz von MoZART hinaus, trifft sich mit diesem Vorhaben aber in der Zielsetzung, Arbeits- und Sozialämter als Jobcenter organisatorisch zusammenzulegen. Bei den Jobcentern oder bei Privatvermittlern sollen Personalservice-Agenturen angesiedelt werden, die Arbeitslosen eine Beschäftigung als Leiharbeiter anbieten. Das Hartz-Konzept setzt voraus, das personenbezogene Daten zwischen Arbeits- und Sozialverwaltung ausgetauscht werden. Die Einbindung privater Stellen macht es außerdem notwendig, an diese sowohl Daten zu übermitteln wie von ihnen Daten zu erhalten. Sichergestellt werden muss dabei insbesondere, dass keine Sozialdaten an eine Stelle gelangen, die diese Daten für ihre gesetzlich auszugestaltende Aufgabenwahrnehmung nicht benötigt. Unter datenschutzrechtlichen Gesichtspunkten werde ich zusammen mit den Datenschutzbeauftragten aus Bund und Ländern den künftigen Gesetzgebungsprozess kritisch begleiten und darauf achten, dass die datenschutzrechtlichen Belange der Betroffenen gewahrt bleiben.

16 Gesundheit

16.1 Gesundheitsdatenschutz in Niedersachsen

Nachdem es bereits zur Routine geworden war, in meinen Tätigkeitsberichten auf die Notwendigkeit der Schaffung bereichsspezifischer Regelungen zur Verarbeitung von Gesundheitsdaten hinzuweisen (so zuletzt in Nr. 5.3 des XV. TB LfD Nds. 1999/2000), kann ich nunmehr berichten, dass die Arbeiten zur Schließung dieser datenschutzrechtlichen Lücke im Ministerium für Frauen, Arbeit und Soziales aufgenommen wurden.

Im Februar 2002 habe ich in einer Besprechung mit Vertretern des Ministeriums vereinbart, für die Regelung der datenschutzgerechten Verarbeitung von Gesundheitsdaten eine gemeinsame Arbeitgruppe einzurichten, die zunächst die regelungsbedürftigen Bereiche ermitteln und anschließend Vorschläge für die konkrete Umsetzung vorlegen soll. Die Arbeitsergebnisse sollen innerhalb eines Jahres vorliegen, um zu Beginn der XV. Legislaturperiode des Landtages in das Gesetzgebungsverfahren eintreten zu können.

Die Arbeitsgruppe hat die umfangreichen Materialien zur weiteren Bearbeitung in vier Themenblöcke und einen allgemeinen Teil gegliedert. Es sind dies: Öffentlicher Gesundheitsdienst (Gesundheitsämter, Gesundheitsberichterstattung, Sozialpsychiatrische Dienste, Heilpraktikerwesen), Stationärer Gesundheitssektor (Krankenhäuser, Landeskrankenhäuser, Maßregelvollzug, Reha-/ Versorgungseinrichtungen), Ambulanter Gesundheitssektor (Suchtberatungsstellen, Ausübung der Heilkunde nach dem Heilpraktikergesetz, Kammergesetz für Heilberufe), Allgemeine und Grundsatzfragen (Verarbeiten von Daten, Subsidiarität, Einwilligung, Datenverarbeitung im Auftrag, Rechte von Patienten, Auskunft und Akteneinsicht, Outsourcing, Löschen von Daten).

Für die einzelnen Themenblöcke hat die Arbeitsgruppe zwischenzeitlich erste Regelungsvorschläge erarbeitet. Bei den bisherigen Überlegungen wurde die Frage aus-

geklammert, ob die erforderlichen bereichsspezifischen Regelungen in einem eigenen Gesundheitsdatenschutzgesetz wie in Nordrhein-Westfalen umgesetzt werden sollten.

Ich werde die Arbeiten an diesem von mir seit langem geforderten Regelungswerk zum Datenschutz im Gesundheitswesen aufmerksam und konstruktiv begleiten und verbinde damit die Hoffnung, dass ein Aufgreifen dieser Problematik in zukünftigen Tätigkeitsberichten von mir nicht mehr angemahnt werden muss.

16.2 Regelungen zum datenschutzgerechten Umgang mit Gentests sind dringend notwendig

Nachdem mit der Erstellung einer detaillierten Karte des menschlichen Erbgutes die erste Phase des Humangenomprojektes (vgl. XV. TB LfD Nds. 1999/2000) abgeschlossen worden ist, werden Gentests als Mittel der medizinischen Diagnostik in rasanten Schritten weiterentwickelt. Ende 2000 wurden in Deutschland Gentests für über 300 verschiedene Krankheiten angeboten. Die Entwicklung der sog. Genchip-Technologie führt dazu, dass mit einer einzigen Probe eine Vielzahl von Tests durchgeführt und deren Ergebnisse elektronisch weiterverarbeitet werden können. Da die Tests immer leistungsfähiger, leichter zu handhaben und billiger werden, gehören sie in den verschiedensten Bereichen der Medizin, zunehmend aber auch außerhalb der eigentlichen medizinischen Diagnostik, fast schon zum „Alltagsgeschäft“. So gibt es

- Gentests zur Diagnosesicherung bereits aufgetretener Erkrankungen,
- Tests zur Diagnostik von Krankheitsdispositionen, ohne dass die Krankheit bereits ausgebrochen ist (sog. „prädiktive“ Gentests , die der Vorhersage dienen, ob die getestete Person z.B. das Brustkrebs- oder Alzheimer-Gen besitzt),
- Anwendungen im Rahmen der vorgeburtlichen Diagnostik,
- Genetische Reihenuntersuchungen (Screenings) z.B. als Angebot von Krankenversicherungen oder in der Arbeitsmedizin,
- Pharmakogenetische Tests zur Ermittlung genetisch bedingter Unterschiede in der Reaktion auf bestimmte pharmazeutische Wirkstoffe,
- Abstammungstests (sog. Vaterschaftstests),
- Gentests zur Identifizierung im Rahmen der Strafverfolgung (sog. genetischer Fingerabdruck).

Unter den ohnehin sensiblen Gesundheitsdaten nehmen genetische Daten eine Sonderstellung ein, denn genetische Informationen haben gegenüber anderen medizinischen Informationen ein deutlich höheres prädiktives Potential und sind damit in der Regel nicht nur für den Getesteten selbst, sondern auch für Familienangehörige von elementarer Bedeutung. Bei missbräuchlicher Verbreitung und Verwendung des Wissens können soziale Stigmatisierung und Diskriminierung die Folge sein (z.B. negative Auswirkungen auf Arbeits- und Versicherungsverhältnisse). Genetische Proben bieten über den eigentlichen Anlass der Probenentnahme und Untersuchung hinaus ein hohes Nutzungspotential für weitere (Forschungs-)Zwecke (Genchiptechnologie, Aufbau von Gendatenbanken), die die betroffene Testperson nicht ohne weiteres überblicken und beeinflussen kann. An den Umgang mit erhobenen genetischen Daten sind daher besondere Anforderungen zu stellen.

Zu bedenken ist darüber hinaus, dass mit Hilfe der Gentests auch Krankheiten diagnostiziert werden können, für die es bisher keine oder nur sehr eingeschränkte Therapiemöglichkeiten gibt. In vielen Fällen bedeutet der positive Befund aber lediglich, dass die Testperson die Anlage für eine bestimmte Krankheit hat. Ob und unter welchen Umständen die Krankheit jemals wirklich zum Ausbruch kommen wird, darüber sind im Regelfall keine verlässlichen Voraussagen möglich. Die betroffene Person wird damit zum „gesunden Kranken". Ein solches Wissen über eine mögliche Erkrankung im späteren Leben kann für die weitere Lebensgestaltung bis hin zur Familienplanung zu einer erheblichen psychischen Belastung werden.

Es ist daher unerlässlich, vor der Durchführung von Gentests strenge Maßstäbe an die Erforderlichkeit zu stellen und eine umfassende und qualifizierte Beratung der Betroffenen sicherzustellen.

Die rechtliche - insbesondere die datenschutzrechtliche - Absicherung konnte mit der sich ausweitenden Testpraxis bisher nicht Schritt halten, obwohl von vielen Seiten seit langem eine rechtliche Ausgestaltung des Umgangs mit genetischen Daten gefordert wird (vgl. Nr. 5.3 des XV. TB LfD Nds. 1999/2000). Abgesehen von der in der Strafprozessordnung und dem DNA-Identitätsfeststellungsgesetz von 1998 normierten Nutzung genetischer Fingerabdrücke im Rahmen der Strafverfolgung stehen gesetzliche Regelungen bislang noch aus.

Im Dezember 2000 hat die Enquête-Kommission „Recht und Ethik der modernen Medizin" des Bundestages an die Datenschutzbeauftragten des Bundes und der Länder einen umfangreichen Fragenkatalog gerichtet und um eine Bewertung der Problematik aus datenschutzrechtlicher Sicht gebeten. Unter der Federführung Hamburgs ist eine ausführliche Antwort erarbeitet und der Kommission im Februar 2001 zugeleitet worden (s. http://www.bundestag.de/gremien/medi/dbs_fragen.pdf).

Ebenfalls im Februar 2001 nahm die von der 60. Datenschutzkonferenz eingesetzte Arbeitsgruppe „Genomanalyse", an der ich mich beteiligt habe, die Arbeit auf. In vier ganztägigen Treffen wurde erstmals ein kompletter Regelungsentwurf für ein Gesetz zur Sicherung der Selbstbestimmung bei genetischen Untersuchungen (http://www.lfd.niedersachsen.de - Service / Empfehlungen Recht / Gentechnik) erarbeitet. Als Orientierungshilfen dienten dabei die entsprechenden Entwürfe aus der Schweiz sowie das österreichische Gentechnikgesetz.

Der Entwurf der Arbeitsgruppe befasst sich mit den allgemeinen Zulässigkeitsbedingungen für Gentests und macht Regelungsvorschläge für die wichtigsten Anwendungsfelder genetischer Untersuchungen in der Medizin, der Forschung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zur Abklärung der Abstammung und zur Identifizierung außerhalb der Strafverfolgung.

Folgende Kernanliegen des Entwurfs bilden auch die Grundlage für eine erneute zu dieser Thematik gefasste Entschließung der 62. Datenschutzkonferenz vom 25./26. Oktober 2001 (s. Anlage 16):

- Stärkung des Selbstbestimmungsrechts und des Rechts auf Nichtwissen 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 im Labor,
- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegenzunehmen,
- 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,
- gefordert wird auch eine grundlegende Norm im Strafgesetzbuch, um Gentests ohne gesetzliche Ermächtigung oder Einwilligung der betroffenen Person zu unterbinden.

Die Entschließung versteht sich als Anregung zu anstehenden Gesetzesinitiativen und zur gesellschaftspolitischen Diskussion.

Auch die Enquête-Kommision des Bundestages hat in ihrem am 14. Mai 2002 veröffentlichten Abschlussbericht (http://www.bundestag.de/btd/14/090/1409020.pdf) nachdrücklich die Schaffung einer gesetzlichen Grundlage für den Umgang mit genetischen Daten gefordert.

Zwar haben sich die Mitgliedsunternehmen des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) im Dezember 2001 freiwillig verpflichtet, prädiktive Gentests nicht zur Voraussetzung eines Vertragsabschlusses zu machen und bis zu einer bestimmten Prämienhöhe auch auf die Vorlage bereits durchgeführter Tests zu verzichten, sie haben dieses Moratorium jedoch bis zum 31. Dezember 2006 befristet.

Für die XV. Legislaturperiode des Bundestages besteht also dringender Handlungsbedarf. Die neue Bundesregierung hat sich im Koalitionsvertrag verpflichtet, den Entwurf eines Gentest-Gesetzes vorzulegen, der auf folgenden Prinzipien aufbaut:

- Freiwilligkeit,
- Diskriminierungsverbot,
- Datenhoheit der Patienten,
- umfassende Aufklärung und Beratung,
- strikter Arztvorbehalt,
- Nutzung des Ergebnisses nur für individuelle Therapien.

16.3 Datenaustausch mit dem Medizinischen Dienst der Krankenversicherung

Immer wieder erreichen mich Eingaben betroffener Bürger, die die Übermittlungspraxis von Sozialdaten der Krankenkassen zum Medizinischen Dienst der Krankenversicherung (MDK) beanstanden. Aber auch die Mitteilungspraxis des MDK war in der Vergangenheit wiederholt Gegenstand von Anfragen und Beschwerden. Dies war für mich Anlass, eine Datenschutzkontrolle bei einer Krankenkasse durchzuführen.

Die Aufgaben des MDK und der rechtliche Rahmen

Die Beziehungen der Krankenkassen zum MDK werden nach den §§ 276 und 277 Sozialgesetzbuch Teil V (SGB V) geregelt. Der MDK hat die Aufgabe, für die Krankenkassen Gutachten über das Vorliegen der Voraussetzungen sowie Art und Umfang von Leistungen zu erstellen. Seine Beteiligung kommt ferner in Betracht bei der Beurteilung von Arbeitsunfähigkeit, bei der Prüfung, ob Pflegebedürftigkeit vorliegt, oder bei der Prüfung der Voraussetzungen von Kurmaßnahmen. Darüber hinaus sollen die Krankenkassen den MDK zu Rate ziehen, wenn es um allgemeine medizinische Fragen der gesundheitlichen Versorgung und Beratung der Versicherten geht.
Nach § 276 Abs. 2 Satz 1 zweiter Halbsatz SGB V sind die Leistungserbringer in Fällen, in denen die Krankenkassen nach § 275 Abs. 1 bis 3 SGB V eine gutachterliche Stellungnahme oder Prüfung durch den MDK veranlasst haben, verpflichtet, Sozialdaten auf Anforderung des MDK unmittelbar an diesen zu übermitteln, soweit dies für die gutachterliche Stellungnahme und Prüfung erforderlich ist.

Die Praxis

Bei meiner Kontrolle fiel auf, dass die Krankenkasse für den MDK die erforderlichen Fremdbefunde/Krankenhausberichte usw. anforderte. Dies führte dazu, dass diese Unterlagen nicht direkt an den MDK, sondern der anfordernden Krankenkasse übersandt wurden, und zwar teilweise nicht in einem nur für den MDK bestimmten verschlossenen Umschlag, sondern im offenen Versand. Ich habe die Krankenkasse darauf hingewiesen, dass die Absender der ärztlichen Unterlagen schriftlich angehalten werden müssen, Unterlagen an die Krankenkasse nur in einem an den MDK adressierten verschlossenen Umschlag bzw. direkt an den MDK zu versenden. Nur so ist eine Wahrung der ärztlichen Schweigepflicht sichergestellt.

Zur Frage der Übersendung von ärztlichen Unterlagen hat das Bundessozialgericht (Az: B 3 KR 64/01 R) entschieden, dass die Krankenkassen grundsätzlich keinen Anspruch auf Einsichtnahme in Behandlungsunterlagen (Arztberichte, Krankenhausentlassungsberichte, Gutachten usw.) ihrer Versicherten haben. Sofern die Krankenkasse aus diesen Unterlagen anspruchsbegründende Folgerungen ableiten will, ist sie auf ein Tätigwerden des MDK angewiesen. Aus Datenschutzgründen ist eine eigene Auswertung nicht zulässig.

Bei Durchsicht der Leistungsfälle fiel auf, dass der Versicherte mitunter aufgefordert wurde, eine Einwilligungserklärung zur Entbindung von der ärztlichen Schweigepflicht zu erteilen. Einer Einwilligungserklärung des Versicherten zum Zwecke der Begutachtung bzw. Beratung durch den MDK bedarf es aber nicht, da die Erhebung der Daten aufgrund einer Ermächtigung im Gesetz (§ 276 Abs. 2 SGB V) erfolgt. Die Krankenkasse hat die bisherige Praxis durch Veränderung der entsprechenden Vordrucke angepasst.

Als datenschutzrechtlich problematisch hat sich auch die Gutachtenweitergabe durch den MDK an die Krankenkasse gezeigt. Der Gesetzgeber hat dies in § 277 Abs. 1 SGB V geregelt. Danach darf der MDK der Krankenkasse lediglich das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund mitteilen. In der Praxis erhalten die Krankenkassen vom MDK regelmäßig die kompletten von ihm erstellten Gutachten über die betroffenen Versicherten übersandt. Diese Gutachten enthalten jeweils die Vorgeschichte/Anamnese, sämtliche vom MDK erhobenen Angaben über den Befund, die Hauptdiagnose und ggf. weitere Diagnosen sowie Beurteilungen, Empfehlungen, Hinweise und evtl. weitere Bemerkungen des Gutachters.

Die Problematik des Gutachtenumfangs ist auch auf Bundesebene des MDK und der Krankenkassen erkannt worden. Es wird eine reduzierte Gutachtenversion angestrebt, die aber noch den Krankenkassen ermöglicht, die gutachterlichen Feststellungen nachzuvollziehen und somit über den Leistungsantrag zu entscheiden.

In einem anderen geprüften Fall habe ich festgestellt, dass bei Anträgen auf Heil- und Hilfsmitteln ein „technischer Berater“ eingeschaltet wurde. Dieser erstellte für die Krankenkasse ein Gutachten über die Notwendigkeit der Verordnung und der bestmöglichen Versorgung. Ich habe darauf hingewiesen, dass eine Hinzuziehung einer nicht im Sozialgesetzbuch genannten Stelle unzulässig ist. Lediglich der MDK hat das alleinige Recht die Krankenkassen hierbei zu beraten. Zurzeit wird auf Seiten der Krankenkasse geprüft, ob und inwieweit zukünftig der MDK die Beratung übernehmen kann.

Alles in allem hat die Prüfung der Krankenkasse keine gravierenden datenschutzrechtlichen Verletzungen ergeben. Zu hoffen ist, dass auch andere Krankenkassen sich an das geltende Datenschutzrecht halten und sich nur auf die erforderlichen und zugelassenen Datenerhebungen beschränken.

16.4 SAM und die AOK

Der Gesetzgeber hat 1996 den Wettbewerb unter den Krankenkassen eingeführt. Bis dahin wurden die jeweiligen Mitglieder einer Krankenkasse mehr oder weniger vom Gesetzgeber zugewiesen. Einen Wettbewerb unter Krankenkassen - wie er heute besteht - gab es nicht.

Schon früh haben die Allgemeinen Ortskrankenkassen (AOK) erkannt, dass mit der bisher eingesetzten AOK-Software IDVS II keine Ausrichtung auf den Versicherten bzw. potentiellen Kunden nach marktorientierten Grundsätzen möglich ist. Das vor

mehr als 25 Jahren entwickelte EDV-System war nur auf die seinerzeit gesetzlich zugewiesenen Aufgaben zur Sicherstellung der Gesundheitsversorgung zugeschnitten. Elemente wie Serviceorientierung, Customer Relationship Management, Qualitäts-, Leistungs- und Kostenmanagement, vertriebliche Ausrichtung, Controlling, Internetbasierte Kommunikationsmöglichkeiten, eCommerce oder individuelle Managementziele waren nicht integriert. Deshalb wurde der Entschluss gefasst, eine neue Krankenkassensoftware SAM (**S**AP-**A**OK-**M**aster) für alle Landesverbände der Ortskrankenkassen zu entwickeln. Daneben wurden Anpassungsprogramme für die alte Software IDVS II in eigenen Rechenzentren programmiert, um die Herausforderungen des Wettbewerbs in der Zwischenzeit so gut es geht zu meistern. Die Zeit bis zum Start der neuen Software soll so überbrückt werden.

Die Programmierung der neuen Software erfolgt unter Federführung von SAP Deutschland. Das hier entstehende Produkt wird als so genannte Branchenlösung entwickelt, die dann auch durch andere Krankenkassen nutzbar sein wird. Um die Software an die Bedürfnisse der AOK anzupassen, hat der Bundesverband der Ortskrankenkassen beschlossen, ein eigenes Softwarehaus, die „AOK Systems“ zu gründen. Diese 100%ige Tochterfirma der AOK als Endentwickler und Schnittstelle zu den Landesverbänden der AOK soll die Software für die spezifischen Bedürfnisse weiterentwickeln.

Voraussichtlich im März 2003 wird das erste Modul HR Organisationsmanagement installiert, sodass die fachliche Anwendung grundsätzlich danach starten kann. Ab dem 2. Quartal 2003 werden weitere Module in der Echtverarbeitung eingesetzt, beginnend mit einem Pilotprojekt „Internetanwendung für Arbeitgeber“. Die vollständige Ablösung von IDVS II wird sich über einen Zeitraum von sechs bis sieben Jahren erstrecken.

Aus datenschutzrechtlicher Sicht wird den Programmteilen Löschung von Daten, Datensperrung und dem Zugriffs- und Berechtigungsverfahren besondere Bedeutung beigemessen. Die im alten Programmverfahren IDVS II nur unzureichend berücksichtigten datenschutzrechtlichen Grundforderungen haben oberste Priorität.

In gemeinsamen Arbeitskreisen der Datenschutzbeauftragten des Bundes und der Länder sowie der AOK-Vertreter werden die Problemfelder erarbeitet und somit die Voraussetzung dafür geschaffen, dass datenschutzrechtliche Gesichtspunkte in die Entwicklung und Einführung der Software einfließen können. Der AOK Bundesverband wurde aufgefordert, datenschutzrechtliche Grundforderungen (z.B. Löschung von Daten, Datensperrung, Zugriffs- und Berechtigungsverfahren) bereits in die Branchenlösung zu implementieren, sodass später hiervon nicht nach Belieben von jeder Krankenkassengeschäftsstelle abgewichen werden kann.

Es bleibt abzuwarten, ob und wie die von der AOK zugesagte datenschutzgerechte Erstellung der neuen Software tatsächlich umgesetzt wird. Nur wenn der Schutz der Versichertendaten gewährleistet ist, werden die Kunden der AOK von heute und morgen dieser Krankenkasse ihr Vertrauen schenken.

Nicht öffentlicher Teil

17 Datenschutz in der Wirtschaft

17.1 Neue Aufgaben für die Datenschutzaufsicht

Mit dem am 23. Mai 2001 in Kraft getretenen novellierten BDSG sind nun endlich die Bestimmungen der europäischen Datenschutzrichtlinie 95/46/EG vom Oktober 1995 in nationales Recht umgesetzt und erste wichtige Eckpunkte für ein modernes Datenschutzrecht realisiert worden. Der Gesetzgeber hat für die Unternehmen gewissermaßen auf der ersten Ebene eine weitgehende Selbstkontrolle festgelegt, zu deren Sicherstellung jedes Unternehmen nach Maßgabe des § 4f BDSG einen Datenschutzbeauftragten zu bestellen hat. Gleichzeitig sind durch das novellierte BDSG auch den Aufsichtsbehörden, und das heißt für Niedersachsen meiner Geschäftsstelle, eine Reihe neuer Aufgaben übertragen oder bestehende Aufgaben erweitert worden. Von ihnen sind die folgenden von besonderer Bedeutung:

- Die Aufsichtsbehörden kontrollieren im nicht öffentlichen Bereich nicht mehr nur dann, wenn ihnen Anhaltspunkte für eine Datenschutzverletzung vorliegen, sondern können jederzeit auch ohne einen speziellen Anlass ihre Kontrolltätigkeit ausüben (Wegfall der Anlassaufsicht). Dies allein hat eine erhebliche quantitative und auch qualitative Ausdehnung meiner Aufsichtstätigkeit zur Folge.
- Der Transfer personenbezogener Daten in Drittländer ohne angemessenes Datenschutzniveau unterliegt in bestimmten Fällen der Genehmigungspflicht durch die Aufsichtsbehörde. Dabei ergeben sich neue Beratungs- und Prüfaufgaben im Zusammenhang mit der Bewertung von Vertragsklauseln oder verbindlichen Unternehmensregelungen.
- Die betrieblichen Datenschutzbeauftragten können bei der Vorabkontrolle in Zweifelsfällen die Hilfe der Aufsichtsbehörde in Anspruch nehmen.
- Die Aufsichtsbehörde überprüft die Vereinbarkeit von Verhaltensregeln, die sich Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, zur Förderung der Durchführung datenschutzrechtlicher Regelungen geben.
- Die Aufsichtsbehörden haben auch den Aufsichtsbehörden anderer Mitgliedsstaaten der Europäischen Union auf deren Ersuchen Amtshilfe zu leisten.

Der sich daraus ergebende erhebliche Aufgabenzuwachs musste im Wesentlichen ohne Zuweisung weiterer Stellen durch interne Umschichtungen innerhalb der Geschäftsstelle sowie durch Änderungen in der Vorgehensweise bewältigt werden.

17.2 Selbstverständnis und Prüfstrategien

Die bereits im letzten Tätigkeitsbericht angesprochenen, für den Datenschutz im nicht öffentlichen Bereich bedeutsamen Entwicklungen mit den Stichworten Internet-Wirtschaft, neue Dienstleistungen bei Tele- und Mediendiensten, eCommerce, Kommerzialisierung des Handels mit personenbezogenen Daten haben auch im Berichtszeitraum ihre besondere Bedeutung für die Datenschutzaufsicht in der Wirtschaft behalten. Zusammen mit den geschilderten Aufgabenerweiterungen aufgrund der

BDSG-Novellierung und weiteren Aufgabenveränderungen bei der Datenschutzaufsicht im behördlichen Bereich sind sie Anlass für eine Neuausrichtung der Handlungsansätze und der Prüfstrategien gewesen, die oben im Kapitel 5.2 im einzelnen beschrieben ist.

Die Neuausrichtung baut für den Bereich der Datenschutzaufsicht in der Wirtschaft auf folgenden Überlegungen auf:

Bei der Entwicklung neuer Kontrollstrategien und Handlungsansätze ist vor allem zu bedenken, dass der Datenschutz nicht isoliert betrachtet werden darf, da er im modernen Wirtschaftsleben in größere Zusammenhänge eingebettet ist, bei denen ganz andere Ziele im Vordergrund stehen. Allein der Hinweis auf rechtliche Handlungsnotwendigkeiten dürfte bei den Unternehmen regelmäßig noch nicht die nachhaltige Überzeugung hervorrufen, dass sie sich bei ihrer Tätigkeit dauerhaft für Gesichtspunkte des Datenschutzes und der Datensicherheit einsetzen sollten. Solange es nicht gelingt, wirklich nachvollziehbar zu vermitteln, dass

- es im wohlverstandenen eigenen Interesse der Unternehmen liegt, bei ihrem Handeln auf Datenschutz und Datensicherheit zu achten, weil dies auch eine Erwartung ist, die ihre Kunden heute ganz selbstverständlich haben,
- die vorbildhafte Einhaltung der Anforderungen von Datenschutz und Datensicherheit und das Angebot datenschutzfreundlicher Lösungen einen Wettbewerbsvorteil gegenüber konkurrierenden Unternehmen bedeuten kann,
- dies deshalb auch zunehmend eine Voraussetzung für geschäftlichen Erfolg ist,

werden die Aufsichtsbehörden im nicht öffentlichen Bereich nur begrenzten Erfolg haben können. Daher ist es wichtig, einen konstruktiven und kontinuierlichen Dialog mit den Akteuren zu führen und zu pflegen, sie zu beraten, gemeinsam aktuelle Entwicklungen aufzunehmen und gemeinsam möglichst frühzeitig praktikable datenschutzgerechte Lösungen zu entwickeln, bei denen auch die Ziele eines erfolgreichen, und das heißt im Ergebnis auch gewinnbringenden Wirtschaftens so weit wie möglich Berücksichtigung finden. Die Lösungen sollen zeigen, dass der Datenschutz nicht den Zugriff auf personenbezogene Daten und deren weitere Verarbeitung für geschäftliche Zwecke grundsätzlich verhindern will, sondern dass er dafür sorgt, dass der Zugriff dort endet, wo der Persönlichkeitsschutz der Betroffenen beginnt. Die Möglichkeiten, datenvermeidende oder datensparsame Lösungen zu entwickeln und einzusetzen, gewinnen dabei zunehmend an Bedeutung.

Sind solche datenschutzgerechten Lösungen im Konsens gefunden worden, müssen sie rasch, gegebenenfalls unter Einbeziehung der Verbandsebene kommuniziert werden, damit möglichst viele Unternehmen von dem Erfolg der gemeinsamen Bemühungen profitieren können. In diesem Zusammenhang sind auch Ansätze und Vorhaben der Selbstregulierung, die insbesondere durch die in § 38a BDSG verankerten „Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen“ der Verbände oder durch verbindliche Unternehmensregelungen verwirklicht werden können, von der Aufsichtsbehörde zu initiieren und nachhaltig zu unterstützen.

In der Konsequenz dieser Überlegungen liegt es auch, den Kontakt und die Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten zu verstärken und den Versuch zu unternehmen, sie sowohl untereinander als auch mit meiner Geschäftsstelle enger zu vernetzen. Die bereits bestehenden Erfa-Kreise in Hannover und Braunschweig sind wichtige Knotenpunkte in diesem Netzwerk.

Dies alles bedeutet natürlich nicht, dass auf die klassische Kontrolltätigkeit der Datenschutzaufsicht künftig verzichtet wird und dass Sanktionsinstrumente gegenüber der Wirtschaft nicht mehr zum Einsatz kommen. Aber diese Kontrollen werden verstärkt so ablaufen, wie es oben im Kapitel 5.2 unter dem Stichwort „Neue Prüfstrategien und Handlungsansätze“ geschildert ist, d.h. die Aufsicht wird nicht in erster Linie auf die nachsorgende Aufdeckung von Datenschutzverstößen ausgerichtet sein, sondern die Erarbeitung von Problemlösungen zum Ziel haben, die dann gegebenenfalls auch über den Kreis des geprüften Unternehmens hinaus als Muster- und Referenzlösung nutzbar gemacht werden können. Sanktionsinstrumente werden als ultima ratio selbstverständlich weiterhin genutzt werden, wenn nur so datenschutzgerechtes Verhalten durchgesetzt werden kann.

Ich bin sicher, dass diese Überlegungen auf breite Zustimmung stoßen und die Handlungsmöglichkeiten der Datenschutzaufsicht in der Wirtschaft weiter verbessern werden. Der Datenschutz wird dabei mehr gewinnen können als bei einer Beschränkung auf die Instrumente einer bürokratischen Nachsorgekontrolle.

In der letzten Zeit habe ich meine Aufsichtstätigkeit im Bereich der Wirtschaft schon verstärkt an den dargestellten Überlegungen ausgerichtet und damit gute Erfolge erzielt. Weil diese Erfolge vielfach im Vorfeld des Einsatzes neuer Verfahren oder technischer Anwendungen durch Beratung oder gemeinsame Problemlösung erreicht worden sind, mögen sie nicht so spektakulär sein wie die Aufdeckung eines datenschutzwidrigen Verhaltens im Einzelfall, sie sind aber mit Sicherheit für die Durchsetzung von Datenschutz wirksamer und vor allem auch nachhaltiger.

Zu diesen Aktivitäten zählen neben dem von mir initiierten und geleiteten Projekt „Datenschutzgerechtes Internet-Angebot der Wirtschaft“ (vgl. dazu Kapitel 19) unter anderem:

- der datenschutzgerechte Einsatz von Videoüberwachung in Straßenbahnen und Bussen des öffentlichen Personennahverkehrs sowie in Parkhäusern,
- die Gestaltung der Einwilligungserklärungen bei Kundenkarten oder anderen Kundenbindungssystemen,
- die datenschutzgerechte Abwicklung der Geschäftsvorgänge bei der Entwicklung von Photos in zentralen Labors,
- Hinweise zur Beachtung der Sperr- bzw. Löschfristen bei Versicherungsunternehmen,
- Maßnahmen zur Erhöhung der Datensicherheit bei einem Krankenversicherungsunternehmen,
- die datenschutzgerechte Abwicklung von Grabpflegeaufträgen,

- die datenschutzfreundliche Ausgestaltung des Aufnahmebereichs eines Krankenhauses,
- die Aufarbeitung eines Störfalls in einem bundesweit agierenden Rechenzentrum.

Abgerundet wird der von mir praktizierte Beratungs- und Kontrollansatz durch die regelmäßige Teilnahme an den Sitzungen der Erfa-Kreise. Durch den Gedankenaustausch mit den dort vertretenen betrieblichen Datenschutzbeauftragten vieler niedersächsischer Unternehmen erkenne ich frühzeitig datenschutzrechtliche Probleme der Wirtschaft und bin als Ansprechpartner für die Wirtschaft präsent.

18 Neue Aufgaben für betriebliche Datenschutzbeauftragte

Die Vorschriften über die Bestellung eines betrieblichen Datenschutzbeauftragten und seine Aufgaben wurden im neuen BDSG in den allgemeinen Teil übernommen. Die Verpflichtung für seine Bestellung ist nunmehr in § 4f, seine Aufgaben sind in § 4g geregelt. Lediglich Kleinbetriebe sind von der Bestellung eines Datenschutzbeauftragten befreit, soweit nicht mehr als vier Personen mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftig sind. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel weniger als 20 Personen beschäftigt sind. Derartige Kleinbetriebe haben gemäß § 4f Abs. 1 Satz 6 BDSG aber dann einen Datenschutzbeauftragten zu bestellen, wenn der Betrieb automatisierte Datenverarbeitungen vornimmt, die gemäß § 4d Abs. 5 BDSG einer Vorabkontrolle unterliegt, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung erhebt, verarbeitet oder nutzt. Durch die Novellierung wurde die Bedeutung des betrieblichen Datenschutzbeauftragten gestärkt, er hat im Wesentlichen zwei neue Aufgaben bekommen.

Die neuen Aufgaben

Die erste neue Aufgabe betrifft die Vornahme der Vorabkontrolle. Da automatisierte Datenverarbeitungen für das Persönlichkeitsrecht der Betroffenen besonders riskant sein können, sind Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen mit sich bringen, noch vor ihrer Inbetriebnahme einer Prüfung durch den betrieblichen Datenschutzbeauftragten zu unterziehen. Zwei Fallgruppen, in denen solche Risiken bestehen, nennt das Gesetz ausdrücklich. Erstens, wenn Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben verarbeitet werden. Zweitens, wenn das Verfahren dazu bestimmt ist, Persönlichkeitsprofile zu erstellen.

Die Vorabkontrolle ist ein Verfahren zur strukturierten Prüfung der materiellen Zulässigkeit der beabsichtigten Datenverarbeitung. Die verantwortliche Stelle hat den betrieblichen Datenschutzbeauftragten die für die Durchführung der Vorabkontrolle erforderlichen Angaben zur Verfügung zu stellen. Zu den erforderlichen Angaben zählen zum Beispiel die Beschreibung der Kategorien der betroffenen Personen und der zu erhebenden Daten und die Empfänger, denen die Daten mitgeteilt werden können. Auch ist der Datenschutzbeauftragte über die geplanten technisch-

organisatorischen Maßnahmen zu informieren, damit er beurteilen kann, ob sie zur Gewährleistung der Sicherheit der geplanten Verarbeitung angemessen sind

Die zweite neue Aufgabe der betrieblichen Datenschutzbeauftragten hat das Ziel, die Transparenz der Datenverarbeitung sicherzustellen. Das von mir bisher zu führende Register - die Zahl der meldepflichtigen Unternehmen hat sich aufgrund der Novellierung des BDSG von 455 im Jahr 2000 auf 90 reduziert - ist nach der Rechtsänderung bei der jeweils verantwortlichen Stelle vom betrieblichen Datenschutzbeauftragten zu führen. Auf Antrag hat er jedermann die im Register enthaltenen Angaben mit Ausnahme der Angaben zur Datensicherung verfügbar zu machen.

Wege zur Umsetzung der neuen Aufgaben

Die betrieblichen Datenschutzbeauftragten müssen sich zukünftig bereits im Planungsstadium bei Datenverarbeitungsvorhaben einbringen. Im Hinblick auf das Prinzip der Datensparsamkeit hat der betriebliche Datenschutzbeauftragte zukünftig verstärkt darauf hinzuwirken, dass die geplanten Datenverarbeitungssysteme so konzipiert werden, dass keine oder so wenig wie möglich personenbezogene Daten verarbeitet werden. Es ist von ihm daher zu prüfen, ob auf die Erhebung personenbezogener Daten verzichtet oder ihr Umfang minimiert werden kann. Auch hat er mit den Projektverantwortlichen zu erörtern, ob für die konkrete Aufgabenstellung auf den Einsatz von anonymen oder pseudonymen Verfahren zurück gegriffen werden kann. Ein geeignetes Instrument für die erfolgreiche Umsetzung dieser Gestaltungsansätze ist die Vorabkontrolle. Zukünftig werden die betrieblichen Datenschutzbeauftragten also verstärkt Vorabkontrollen durchzuführen haben, wenn sie ihrer durch das BDSG gestärkten Rolle und dem Gedanken der Selbstverantwortung sowie dem Prinzip der Eigenkontrolle gerecht zu werden wollen.

Um die betrieblichen Datenschutzbeauftragten bei ihren erweiterten Aufgaben zukünftig noch besser unterstützen zu können, werde ich mein Beratungsangebot für sie kontinuierlich erweitern.

19 Datenschutzgerechte Internetangebote

Internetauftritten kommt, auch nach dem Einbruch der New Economy, weiterhin eine hohe Bedeutung zu. Kaum ein Betrieb, der nicht mindestens eine Seite zur Selbstdarstellung im Netz hat. Darüber hinaus betreiben zahlreiche Unternehmen über dieses Medium Kundenbindungsmaßnahmen (vgl. Kapitel 20) oder Ein- und Verkäufe.

Vielen dieser Unternehmen, sowohl mittelständischen, aber auch Großunternehmen, ist noch immer nicht bewusst, dass bei den Internetangeboten zahlreiche datenschutzrelevante Vorgaben zu beachten sind. In einer Projektgruppe mit Vertretern der privaten Wirtschaft erarbeite ich zurzeit eine Handlungsanleitung, in der die bei den verschiedenen Internetangeboten zu ergreifenden Maßnahmen kompakt und praxisorientiert dargestellt werden. Diese Handlungsanleitung soll nach ihrer Fertigstellung in breiter Form veröffentlicht werden, damit sie möglichst viele Unternehmen als Leitfaden und praktische Umsetzungshilfe für eine datenschutzgerechte Gestaltung ihrer Internet-Auftritte nutzen können.

Bereits jetzt stehen unabhängig von der Art des Angebotes folgende gemeinsame Leitplanken fest:

- Transparenz des Angebotes
  Der Nutzer des Internetangebotes muss klar erkennen oder ohne weiteres in Erfahrung bringen können, wer für das besuchte Angebot verantwortlich ist, welche datenschutzrechtlichen Vorkehrungen der Betreiber getroffen hat und welche Gestaltungselemente, gerade auch sensibler Art, ihn erwarten.

  - Anbieterkennzeichnung
    Spätestens mit der Änderung des § 6 TDG sind Anbieter von Webseiten zu einer umfangreicheren Anbieterkennzeichnung verpflichtet. Diese muss leicht auffindbar sein.

  - Datenschutzerklärung oder Privacy Policy
    Der Anbieter soll erläutern, welche Daten innerhalb seines Angebotes gesammelt und gespeichert werden und zu welchem Zweck dies geschieht. Besonders sollte auch auf riskante Gestaltungselemente, wie z.B. Cookies oder ActiveX hingewiesen werden. Auch die Datenschutzerklärung muss an gut erreichbarer Stelle ausgebracht werden. Eine textliche Verbindung mit den Allgemeinen Geschäftsverbindungen lehne ich ab, da beide Regelungsbereiche nichts miteinander zu tun haben und die Erklärung dort leicht übersehen wird.

- Einhaltung gesetzlicher Vorschriften
  Aus den zahlreichen gesetzlichen Vorschriften kristallisieren sich einige besonders wichtige Regelungen heraus.

  - Grundlage der Datenverarbeitung
    Für die gewünschte Erhebung, Verarbeitung und Nutzung von Daten muss eine gesetzliche Erlaubnis vorliegen oder eine Einwilligung eingeholt werden.

  - Erforderlichkeit der Datenverarbeitung
    Die gewünschte Erhebung, Verarbeitung und Nutzung der Daten muss zur Wahrnehmung der Geschäftszwecke grundsätzlich unverzichtbar sein.

  - Zweckbindung der Verarbeitung
    Der Zweck der Erhebung, Verarbeitung und Nutzung von Daten ist auch dem Nutzer gegenüber eindeutig festzulegen und darf nicht durchbrochen werden.

  - Einwilligung des Nutzers
    Soweit notwendig wird für die Erhebung, Verarbeitung und Nutzung von Daten die freiwillige Einwilligung des Nutzers eingeholt. Die Erbringung einer Leistung darf jedoch nicht von der Einwilligung abhängig gemacht werden, wenn der Nutzer keine andere Möglichkeit hat, die Leistung zu erhalten.

    Des Weiteren muss der Inhalt der Einwilligung für den Nutzer gut erreichbar

und verständlich sein, ihm muss die Möglichkeit gegeben werden, die Einwilligung durch bewusstes Handeln zu erteilen oder abzulehnen.

- Datensparsamkeit
  Das Verfahren muss so ausgestaltet werden, dass die Daten so weit und so früh wie möglich anonymisiert oder pseudonymisiert werden.

- Technische und organisatorische Schutzmechanismen
  Der Betreiber hat durch den Einsatz von Technik und durch eine qualifizierte interne Organisation u.a. sicherzustellen, dass

  - Daten der Nutzer gegen Kenntnisnahme Dritter geschützt sind,
  - personenbezogene Daten aus unterschiedlichen Quellen nicht zusammengeführt werden,
  - Unbefugte keinen Zugriff auf den Datenbestand erlangen,
  - Zugriffe auf personenbezogene Daten nachvollzogen werden können,
  - Daten gegen zufällige Zerstörungen geschützt sind.

- Berücksichtigung der Verbraucherrechte
  Anbieter müssen gewährleisten, dass Nutzer auf ihre Rechte hingewiesen werden und sie geltend machen können und dass die Rechte auch Berücksichtigung finden.

Die meisten der genannten Punkte erschließen sich einem verbraucherfreundlich arbeitenden Unternehmen von selbst. Leider trägt die unübersichtliche Rechtslage jedoch nicht dazu bei, im Internet qualitativ hochwertigen Datenschutz sicherzustellen. Viele Betriebe sind ganz einfach überfordert, die notwendigen Informationen aus den verschiedenen Gesetzen zu gewinnen.

Ich betrachte es daher als meine Aufgabe, auf eine stärkere Transparenz der derzeitigen Regelungen hinzuarbeiten und bis dahin den Unternehmen die notwendigen Hilfestellungen und Anregungen zu geben, um die datenschutzgerechte Ausgestaltung der Internetangebote weiter voranzutreiben.

20 Kundendaten

20.1 Vom Konsumenten zum treuen Kunden?

In Zeiten gesättigter Märkte und weitgehend austauschbarer Produkte wird es für die Unternehmen immer schwieriger, neue Kunden zu gewinnen. Deshalb wächst die Bedeutung der langfristigen Kundenbindung.

Customer Relationship Management (CRM) ist die konsequente Ausrichtung aller bestehenden Unternehmensprozesse am Kunden. Es hat zum Ziel, die Bedürfnisse und Erwartungen des Kunden zu erkennen und individuell darauf reagieren zu können und dient somit vor allem der Schaffung von loyalen und damit auch profitablen Kunden.

Dementsprechend verbergen sich hinter dem Begriff CRM zahlreiche Aspekte und Maßnahmen, die das Sammeln von und den Umgang mit personenbezogenen Daten mit sich bringen.

20.2 Individualität - gespeichert und ausgewertet

Die Unternehmen glauben als eine wichtige Entwicklung ausgemacht zu haben, dass der Verbraucher ein steigendes Bedürfnis nach individuellen Angeboten hat. Diesem Bedürfnis muss der Anbieter Rechnung tragen, will er die Loyalität des Kunden gewinnen. Um die individuellen Ansprüche zu erkennen, werden in Data Warehouses alle verfügbare Daten über den Kunden gesammelt, sodass sämtliche Informationen, losgelöst von der operativen Verarbeitung, für beliebige Zwecke zur Verfügung stehen.

Über Data Mining werden zudem durch Verknüpfung vorhandener Daten aus einem oder verschiedenen Warehouses neue personenbezogene Informationen gewonnen, die für weitere Maßnahmen zur Kundenbindung eingesetzt werden.

Die daraus resultierenden Probleme für die informationelle Selbstbestimmung, die ich bereits in Nr. 6.7 des XV. TB LfD Nds. 1999/2000 aufgezeigt habe, bestehen weiterhin. Die dort gestellten Fragen an die Betreiber von Data Warehouse und Data Mining-Lösungen sind bisher nicht oder unzureichend beantwortet worden.

Nach einer Erhebung der Katholischen Universität Eichstätt untersuchen erst 30% aller Großunternehmen in Deutschland regelmäßig ihre Kundendaten nach wiederkehrenden Mustern, um Kundengruppen zu identifizieren und gezielter ansprechen zu können. Gleichzeitig berichten 87% der Unternehmen, die Data Mining Projekte auflegen, von Erfolgen. Es ist also schon abzusehen, dass weitere Unternehmen sich der Methode des Data Mining bedienen werden.

Zudem ermöglichen immer leistungsfähigere EDV-Anlagen die Verknüpfung immer größerer Datenbestände. Der Segmentierung von Kunden, der Bildung von Zielgruppen und Potentialen und letztlich der Versorgung mit (angeblich) bedarfsgerechter Werbung sind damit kaum noch Grenzen gesetzt.

Es ist eine Herausforderung für den Datenschutz, die Entwicklung dieser Techniken kritisch zu begleiten, ohne sie zu verdammen. Stattdessen muss Entwicklern und Anbietern deutlich gemacht werden, dass Data Warhouses und Data Mining nur unter angemessener Berücksichtigung der informationellen Selbstbestimmung der Kunden zu betreiben sind. Dass dies u.a. durch frühzeitige Anonymisierung möglich wäre, habe ich bereits im letzten TB ausgeführt.

20.3 Meine Daten - verkauft

20.3.1 Kundenkarten - Konsumverhalten auf Plastik?

Kundenkarten erfüllen zwei Zwecke bei der Kundenbindung. Die Karten, die dem Benutzer meist nur einen geringen Rabatt auf den Kaufpreis gewähren, sind zum

einen ein anerkanntes Mittel für die Gewinnung der Loyalität des Kunden, zum anderen dienen sie zur lückenlosen Herstellung einer Konsumhistorie und damit zur Füllung des Data Warehouses (s.o.).

Dem regelmäßigen Benutzer der Kundenkarte geht jegliche Privatsphäre beim Konsum verloren. Das Unternehmen weiß, wann er wo, was und wie einkauft. Zusammengeführt mit den Auskünften, die der Kartenbesitzer bei der Antragstellung angegeben hat, lassen sich neue Informationen generieren, deren Ausmaß kaum abzusehen ist und die der Kunde auch nicht mehr beeinflussen kann.

Hinzu kommt das Problem der zunehmenden Konzernverflechtungen. Die Vielfalt in der privaten Unternehmenslandschaft nimmt, insbesondere in den letzten Jahren, stetig ab. Es wird schwieriger, die Verflechtungen zwischen den einzelnen konzernabhängigen Unternehmen zu erkennen. Für den Verbraucher bedeutet dies, dass sein Konsumverhalten immer flächendeckender erfasst wird und dass die Einkaufsgewohnheiten in den verschiedensten Lebensbereichen kombiniert und untersucht werden können. Dieser Trend wird außerdem verstärkt durch eine konzernübergreifende Zusammenarbeit.

Die Teilnahme an einem Kundenkartensystem, z.B. Payback, ist zwar grundsätzlich freiwillig, ohne Karte bekommt der Verbraucher jedoch keinen Rabatt. Die Wahrung der eigenen Privatsphäre ist demzufolge eine Ware, die mit wirtschaftlichen Nachteilen erkauft werden muss.

Daraus resultiert die Tendenz zur verstärkten Kommerzialisierung personenbezogener Informationen. Mehr und mehr Verbraucher sind bereit, ihre personenbezogenen Daten gegen materielle Vergünstigungen zur Verfügung zu stellen und insoweit auf die naheliegendste Form des Selbstdatenschutzes, nämlich die Nicht-Preisgabe persönlicher Informationen, zu verzichten. Insofern ist es wichtig, die eigenen Daten auch als Ware zu erkennen und diese nur gegen einen angemessenen Preis herauszugeben. Für die Ermittlung des angemessen Preises gibt es jedoch keine übergreifenden und objektivierbaren Maßstäbe; letztlich muss jeder selbst entscheiden, wie viel ihm der Verzicht auf die informationelle Selbstbestimmung im Einzelfall „wert“ ist.

Zur Stärkung des Problembewusstseins werde ich weiterhin in folgenden Feldern aktiv sein:

- Aufklärung über die Potentiale und Gefahren von Kundenkarten,
- Informationen zur Einschätzung des Wertes personenbezogener Daten,
- Anmahnen der Aufklärungspflichten der Unternehmen, insbesondere beim Einholen der Einwilligungserklärungen, und aktivierende Mitarbeit bei der Erfüllung dieser Pflichten,
- Betonung von Datensparsamkeit und Transparenz als unentbehrliche, aber auch werbewirksame Säulen bei der Weiterentwicklung von Kundenkartensystemen.

20.3.2 Call Center - „da werden Sie geholfen?“

Wie mit Kundenkarten soll auch mit den Dienstleistungen eines Call Centers der Kunde emotional an ein Unternehmen gebunden werden. In der Arbeit des Call Centers kann dies entweder als nach außen gerichtete Aktivität, d.h. den potentiellen Kunden ansprechend, oder nach innen gerichtet, als Kontaktmöglichkeit für den bereits gewonnenen Verbraucher, realisiert sein.

Ähnlich wie bei den Kundenkarten kann auch dieses Medium genutzt werden, um persönliche Daten für ein Data Warehouse zu gewinnen. Besonders Daten, wie sie nur bei einem telefonischen, d.h. mündlichen Kundenkontakt anfallen und die nicht unmittelbar den Geschäftszweck betreffen, sondern „nebenbei“ mitgeteilt werden, weil der Agent diese aufgrund ausgefeilter Fragetechniken in geschickter Weise ermittelt, sind für umfangreiche Auswertungen von großem Interesse. Es ist unstrittig, dass die Speicherung dieser Daten ohne Einwilligung der Betroffenen, zumindest wenn sie nicht vollständig und dauerhaft anonymisiert werden, unzulässig ist.

Häufig spricht ein Kunde nicht mehr direkt mit dem Unternehmen, um dessen Produkt es sich tatsächlich handelt, sondern mit einem externen Call Center, das als selbstständiger Auftragsdienst die telefonische Kundenbetreuung von einem oder mehreren Betrieben übernimmt.

In diesem Fall besteht ein Vertragsverhältnis zwischen Call Center und Auftraggeber. Dort müssen im Einzelnen der Umfang der übertragenen Aufgaben, die Verpflichtung zur Wahrung von Betriebsgeheimnissen und des Datengeheimnisses und die Speicherung, Übermittlung und Nutzung von Daten festlegt sein.

Zur Wahrung des Datenschutzes ist daher verstärkt darauf zu achten, dass im Call Center

- nur Daten gesammelt und gespeichert werden, die unbedingt benötigt werden,
- der Kunde darüber informiert wird, welche Daten verarbeitet werden und wie und wo er seine datenschutzrechtlichen Betroffenenrechte geltend machen kann,
- ein besonderer Hinweis erfolgt, wenn Daten nur mit Einwilligung des Betroffenen erhoben werden dürfen,
- dem Verbraucher deutlich gemacht wird, mit wem er telefoniert und wem er seine Daten überlässt,
- ausreichende technische und organisatorische Maßnahmen zur Sicherung der Kundendaten vorhanden sind,
- vor einem Gespräch darauf hingewiesen wird, dass z.B. im Falle des Agent Coaching (Ausbildung von Call Center-Mitarbeitern) Dritte mithören,
- die Befugnisse des Call Centers in einer Vereinbarung nach § 11 BDSG festgelegt sind.

21 Geo-Informationssysteme

Die traditionelle Kartographie wurde in den letzten Jahren zunehmend durch sog. Geo-Informationssysteme abgelöst bzw. weitergeführt. Geo-Informationssysteme sind

Werkzeuge zur Erfassung, Verwaltung, Bearbeitung, Analyse, Modellierung und Visualisierung raumbezogener Daten und ihrer Beziehungen. Aufgrund des zwischenzeitlich erlangten Reifegrades findet diese Technologie Anwendung in allen Bereichen, die in Abhängigkeit oder Beziehung zu raumbezogenen Daten stehen.

Grundsätzlich bestehen gegen die Erhebung und Verarbeitung rein raumbezogener Daten keine nachhaltigen datenschutzrechtlichen Bedenken. Die raumbezogenen Daten allein lassen einen Personenbezug in aller Regel nicht erkennen, so dass das Recht auf informationelle Selbstbestimmung nicht tangiert ist und eine Anwendung des Datenschutzgesetzes ausscheidet. Häufig gewinnen Geo-Informationssysteme erst durch die Einbeziehung weiterer Datensätze ihre Praxisrelevanz und damit auch ihren wirtschaftlichen Wert. Als datenschutzrechtlich problematisch stellt sich dabei gerade die Verknüpfung mit solchen Daten dar, die einzeln betrachtet unbedenklich sind, durch die Verknüpfung selbst jedoch Rückschlüsse auf bestimmbare Personen zulassen und damit personenbezogene Daten sind. Dies ist beispielsweise denkbar bei der Verknüpfung von Sozialdaten mit Geo-Informationen. Ein Vertriebsunternehmen könnte unter Rückgriff auf ein derart verknüpftes Geo-Informationssystem schon im Vorfeld beurteilen, ob der potentielle Kunde einem sozialstarken oder -schwachen Bezirk entstammt und somit als Kunde „attraktiv“ ist oder nicht. Ebenso ließe sich ein eventuelles Vertriebsengagement in bestimmten geographischen Bereichen schon im Vorfeld auf seine Erfolgsaussichten überprüfen.

Das Wissen um die Präsenz datenschutzrechtlich relevanter personenbezogener Daten und die Möglichkeit ihrer Verknüpfung mit raumbezogenen Daten veranlasst mich, die diesbezüglichen Entwicklungen aufmerksam zu verfolgen.

22 Kreditinformationssystem SCHUFA

Im Berichtszeitraum wurde die vollständige Zusammenführung der Regionalgesellschaften der SCHUFA unter das Dach der SCHUFA HOLDING AG vollzogen. Hierbei handelt es sich um eine strategische Maßnahme, mit der die SCHUFA auf die wachsenden Anforderungen der Märkte und des Wettbewerbs reagiert und sich als Service-Dienstleister für ihre Vertragspartner positioniert. Mit neuen Geschäftsfeldern, z.B. im Rahmen der bankaufsichtsrechtlichen Steuerung, unterstreicht die SCHUFA ihre Zukunftsausrichtung. In den Dateien der 20 Geschäftsstellen der SCHUFA waren im Jahr 2001 57 Millionen Bundesbürger erfasst, für sie speicherte die SCHUFA 299 Millionen Informationen und verarbeitete 66,4 Millionen Auskünfte und Nachmeldungen. Diese Zahlen belegen eindruckvoll, dass auch nicht öffentliche Stellen über eine große Zahl personenbezogener Daten verfügen und dass die in diesem Umfeld stattfindenden Erhebungen, Verarbeitungen und Nutzungen datenschutzrechtlich begleitet werden müssen, um so frühzeitig eventuelle Gefährdungen des Rechts auf informationelle Selbstbestimmung erkennen und ihnen begegnen zu können.

Die neue Gesellschaftsstruktur bei der SCHUFA

Zum 1. Januar 2002 wurden die bis dahin jeweils als GmbH organisierten selbstständigen SCHUFA-Regionalgesellschaften, die als verantwortliche Stellen im Sinne des Datenschutzrechts zu behandeln waren, zur SCHUFA Holding AG mit Sitz in Wiesbaden verschmolzen. Diese AG ist seither die einzige rechtlich selbstständige

SCHUFA-Gesellschaft und damit datenschutzrechtlich verantwortlich (§ 3 Abs. 7 BDSG). Schon vorher wurde die Bundes-SCHUFA-Vereinigung der Deutschen Schutzgemeinschaften für allgemeine Kreditsicherung e.V., die Beratungs- und Betreuungsaufgaben für die einzelnen SCHUFA-Gesellschaften wahrgenommen und das zentrale DV-System betreut hatte, mit der im Jahre 2000 neu geschaffenen SCHUFA Holding AG verschmolzen. Eigentümer der SCHUFA Holding AG sind im Wesentlichen die Banken und Sparkassen sowie Einzelhandels- und Versandhausunternehmen, die sich in Eignerpools mit unterschiedlichen Anteilsverhältnissen gliedern.

Konsequenzen für die Datenschutzaufsicht

Durch die vollzogene Umstrukturierung ist für die SCHUFA Holding AG nur noch eine Aufsichtsbehörde zuständig, dies ist das Regierungspräsidium in Darmstadt. Der betriebliche Datenschutzbeauftragte für die SCHUFA Holding AG nimmt seine Aufgaben in Wiesbaden wahr und hat die Meldung nach § 4d BDSG zum Register nunmehr gegenüber der allein zuständigen Aufsichtsbehörde in Darmstadt abzugeben.

Auch die gesamten Aufsichtsbefugnisse über die SCHUFA sind auf das Regierungspräsidium Darmstadt übergegangen. Allerdings sollen nach einer Verabredung zwischen der SCHUFA Holding AG und der Arbeitsgruppe Auskunfteien der obersten Aufsichtsbehörden ungeachtet der Frage der Zuständigkeit im Interesse der Bürgerfreundlichkeit Beratungen von anfragenden Bürgern sowie Standardfälle von den jeweiligen örtlichen Aufsichtsbehörden - aber unter Hinweis auf die an sich fehlende Zuständigkeit - bearbeitet werden. Wenn grundsätzliche Fragestellungen auftreten oder sich im Einzelfall Auffassungsunterschiede zu örtlichen SCHUFA-Stellen abzeichnen, ist der jeweilige Fall zuständigkeitshalber an das Regierungspräsidium Darmstadt abzugeben. Gleiches gilt auch auf Seiten der SCHUFA; kontroverse oder grundsätzliche Fälle werden von den Regionalleitern an die Zentrale in Wiesbaden abgegeben.

Bußgeldbescheide und sonstige Verwaltungsakte werden nur noch durch das Regierungspräsidium Darmstadt bzw. die zuständigen hessischen Behörden erlassen. Diese sind auch für die Erstattung von Strafanzeigen zuständig.

Über die neue Praxis soll zu gegebener Zeit ein Erfahrungsaustausch in der Arbeitsgruppe Auskunfteien erfolgen.

Konsequenzen für die Betroffenen

Die Bearbeitung von schriftlichen Anfragen und Eingaben von Betroffenen bei der SCHUFA soll schrittweise von den Regionalleitungsstandorten weg auf die Standorte Bochum und Hannover konzentriert werden. Langfristig kann auch hier eine Zentralisierung an einem Standort oder der Zentrale in Wiesbaden nicht ausgeschlossen werden.

Die Möglichkeit, als Betroffener Auskunft über die gespeicherten Daten durch persönliche Kenntnisnahme zu erlangen (§ 34 Abs. 6 BDSG), soll von dieser Zentralisierung der Anfragebearbeitung nicht betroffen sein, d.h. man kann als Betroffener weiterhin

an den Regionalleitungsstandorten oder den weiteren Standorten persönlich Kenntnis von den eigenen Daten nehmen.

Betroffene, die allgemeine Fragen zu den über sie bei der SCHUFA gespeicherten Daten haben, können sich auch weiterhin an mich wenden. Handelt es sich aber um eine Beschwerde, die die Organisation der SCHUFA oder die Struktur ihrer Datenverarbeitung betrifft, muss ich die Eingabe an die Aufsichtsbehörde in Darmstadt weitergeleiten. Sollte ein Unternehmen mit Sitz in Niedersachsen die Daten an die SCHUFA übermittelt haben und geht es um datenschutzrechtliche Fragen im Zusammenhang mit dieser Übermittlung, bleibt dagegen meine bisherige Zuständigkeit erhalten.

Ich werde die bei mir eingehenden Anfragen und Beschwerden in Sachen SCHUFA auch weiterhin auswerten, um so frühzeitig eventuellen Handlungsbedarf erkennen zu können. Insbesondere werde ich die Auswirkungen der Auflösung der bisher selbstständigen Regionalgesellschaften auf die Wahrnehmung der Betroffenenrechte beobachten.

23 Vorbereitung einer einheitlichen Wirtschaftsnummer

Am 22. Mai 2002 wurde das Gesetz zur Vorbereitung einer bundeseinheitlichen Wirtschaftsnummer beschlossen. Es dient der Erprobung einer derartigen Nummer - die im Jahr 2005 eingeführt werden soll - sowie der Erleichterung der elektronischen Datenübermittlung. Aufgrund der Erprobungsergebnisse soll bestimmt werden, welche wirtschaftlichen Einheiten eine Wirtschaftsnummer erhalten sollen und welche Vergabe- und Kontinuitätsregeln festzulegen sind.

In die Erprobung - die in Regensburg und den Gemeinden des Landkreises Neumarkt in der Oberpfalz erfolgt - werden Unternehmen, Betriebe und sonstige wirtschaftlich Tätige einbezogen. Die Wirtschaftsnummer soll im Verkehr mit Behörden, der amtlichen Statistik und anderen öffentlichen Stellen zur Bezeichnung und eindeutigen Identifizierung des wirtschaftlich Tätigen verwendet werden und die bestehende Nummernvielfalt ersetzen.

Mit der einheitlichen Wirtschaftsnummer, die zentral bei der Bundesanstalt für Arbeit gespeichert und gepflegt wird, soll ein Datensatz verknüpft werden, der die "Stammdaten" eines wirtschaftlich Tätigen enthält. Die Bundesanstalt darf die mit der Wirtschaftsnummer verknüpften Stammdaten an Finanzämter, Gewerbeaufsichtsbehörden und das Bayerische Landesamt für Statistik und Datenverarbeitung übermitteln. Ferner ist eine Übermittlung an die Industrie- und Handelskammern, die Handwerkskammern, die Kammern der freien Berufe, die Landwirtschaftskammern, die Berufsgenossenschaften, die Sozialversicherungsträger und die Monopolkommission zulässig. Voraussetzung für die Übermittlung ist, dass die Daten für die Aufgabenerledigung der jeweiligen Stelle erforderlich sind.

Die betroffenen wirtschaftlich Tätigen und die genannten Stellen sind verpflichtet, die Wirtschaftsnummer bei der schriftlichen oder elektronischen Datenübermittlung zu

nutzen. Damit erhalten sie die Möglichkeit, die aktuellen Stammdaten mit den in ihrem Zuständigkeitsbereich bereits erhobenen Daten zu verknüpfen. Dies kann sowohl für die wirtschaftlich Tätigen als auch für die Verwaltung erhebliche Vorteile haben.

Neben den Vorteilen ist aber auch das datenschutzrechtliche Gefahrenpotential für die wirtschaftlich Tätigen zu bedenken. Aus meiner Sicht ist an dem vorliegenden Gesetz kritikwürdig, dass keine expliziten Zweckbindungen vorgesehen sind. Auch muss vor der Verabschiedung einer bundesweiten Wirtschaftsnummer geklärt werden, ob der vorgesehene Stammdatensatz für die konkrete Aufgabenstellung der jeweiligen Stelle tatsächlich immer im vollen Umfang erforderlich ist. Ferner ist die fehlende Nutzungsbeschränkung zu kritisieren, da die Wirtschaftsnummer einem Personenkennzeichen gleichkommen kann. Unter diesen Voraussetzungen halte ich es für dringend nötig, die Auswertung der Erprobungsergebnisse aus datenschutzrechtlicher Sicht kritisch zu begleiten.

24 Arbeitnehmerdatenschutz

Seit mehr als einem Jahrzehnt appellieren die Datenschützer in Bund und Ländern im Einklang mit den Gewerkschaften an die Bundesregierung, den seit langem überfälligen und bereits für die vergangene Legislaturperiode angekündigten Entwurf eines Arbeitnehmerdatenschutzgesetzes nun endlich vorzulegen. Geschehen ist bisher, trotz gegenteiliger Ankündigungen, nichts.

Die in meiner Geschäftsstelle eingehenden Anfragen aus der Arbeitnehmerschaft und von Betriebsräten sind ein Beleg dafür, dass der oft beschworene „gläserne“ Arbeitnehmer in einigen Unternehmen bereits Realität ist. So sehen sich Arbeitgeber immer häufiger veranlasst, die Surfgewohnheiten und die E-Mail-Nutzung ihrer Arbeitnehmer umfassend zu kontrollieren. Daten der Bewerber und Bewerberinnen werden vereinzelt schon in Online-Bewerbungsverfahren über das Internet erfasst, ausgewertet und anschließend in immer leistungsfähigeren Personalinformationssystemen gespeichert. Videokameras und Webcams werden vielfach nicht nur zu Sicherungszwecken, sondern auch zur Überwachung der Beschäftigten eingesetzt, bisweilen auch ohne Kenntnis der Beschäftigten und der Betriebsräte. In den Einstellungsverfahren werden den Bewerbern vielfach Auskünfte zum Gesundheitszustand abverlangt und betriebsärztliche Untersuchungen etwa im Rahmen von "Drogen-Screenings" durchgeführt, ohne dass die hieraus gewonnenen Erkenntnisse für den Einsatz am Arbeitsplatz überhaupt von Bedeutung wären. Psychologische Einstellungstests sind längst gängige Praxis in den Betrieben.

Ich vertraue fest darauf, dass die neu gewählte Bundesregierung ihre in der Koalitionsvereinbarung getroffene Zusage einlöst, den Schutz der Daten der Arbeitnehmer erstmals in einem eigenen Gesetz zu verankern (siehe Seite 67 des Koalitionsvertrages), und einen entsprechenden Entwurf so rechtzeitig in das parlamentarische Verfahren einbringt, dass er bis zur Mitte der laufenden Legislaturperiode beraten und verabschiedet werden kann. Die notwendigen Inhalte eines solchen Entwurfs sind vielfach beschrieben worden. Ich beziehe mich insoweit auf die Erklärung von Datenschutzbeauftragten des Bundes und der Länder vom 27. Februar 2002 für einen

gesetzlichen Arbeitnehmerdatenschutz. Die Erklärung kann in meinen Internetangebot abgerufen werden.

25 Datenschutz im Verein

In immer weiteren Lebensbereichen werden personenbezogene Daten maschinell und elektronisch verarbeitet, so auch in Vereinen und Verbänden. Mit den Landesbeauftragten für den Datenschutz der Länder Bremen, Hamburg, Nordrhein-Westfalen und Schleswig-Holstein habe ich im Berichtszeitraum zu diesem Komplex gemeinsam Hinweise unter der Berücksichtigung des neuen Bundesdatenschutzgesetzes erarbeitet.

Diese als Orientierungshilfe konzipierten Hinweise richten sich sowohl an Vereinsfunktionäre als auch an Vereinsmitglieder, um sie über die datenschutzrechtlichen Rahmenbedingungen für den Umgang mit personenbezogenen Daten bei der Vereinsarbeit zu informieren. Um eine weite Verbreitung dieser Orientierungshilfe zu erreichen und um einen jederzeitigen Zugriff auf sie zu ermöglichen, habe ich sie als PDF-Dokument unter http://www.lfd.niedersachsen.de/ - Service / Empfehlungen Recht / Datenschutz im Verein - in das Internet gestellt. Die dort abgelegten Unterlagen stehen den Verbänden und Vereinen somit als „Druckvorlage“ zur Verfügung und können von ihnen für eigene Publikationen eingesetzt werden. Die bereits nach kurzer Zeit erfolgte Resonanz von Vertretern aus Verbänden und Vereinen zeigt mir, dass der gewählte Informationsweg auch kleine Vereine erreicht.

Der Inhalt der Orientierungshilfe gliedert sich in fünf Abschnitte:

- Zulässigkeit der Datenerhebung:
  Hier wird auf die anzuwendenden Regelungen des BDSG verwiesen und die Begriffsbestimmungen werden erläutert. Auch werden die Unterschiede für die Fälle dargestellt, in denen die Daten für eigene Zwecke des Vereins oder für fremde Zwecke erhoben, verarbeitet oder genutzt werden.

- Voraussetzung für die Erhebung, Speicherung und Nutzung von Daten:
  Dieser Abschnitt zeigt beispielhaft, welche datenschutzrechtlichen Fragen zu beachten sind bei der Mitglieder- und Spendenwerbung und unter welchen Voraussetzungen Mitgliederdaten hierzu verarbeitet und genutzt werden dürfen.

- Übermittlung von Mitgliederdaten:
  In diesem Themenfeld wird den Vereinen eine Anleitung und Hilfe zu Fragen der Datenübermittlung gegeben.

- Veröffentlichung im Internet:
  Immer mehr Vereine bedienen sich des Internets und unterrichten über dieses Medium über Vereinszweck, Aktivitäten und Mitglieder. Es werden die dabei zu beachtenden Regelungen dargestellt. Auch findet sich hier ein Muster einer Einwilligungserklärung zur Veröffentlichung personenbezogener Daten im Internet.

- Verwaltung von Mitgliederdaten:
  Auch und gerade bei der Verwaltung von Mitgliederdaten hat der Datenschutz einen sehr hohen Stellenwert. Die vom Verein zu treffenden Regelungen werden erläutert und das Muster einer Datenschutzerklärung für eine Vereinssatzung vorgestellt.

Für einen ersten Überblick habe ich zusätzlich auch ein kurzgefasstes Merkblatt zu diesem Thema in das Internet eingestellt. Damit ist es weiten Bevölkerungskreisen möglich, sich über die grundsätzlichen Regelungen und generellen Vorschriften zum Datenschutz im Verein in übersichtlicher Form zu informieren.

Anlagen Entschließungen der Datenschutzbeauftragten des Bundes und der Länder

Anlage 1 Novellierung des G 10-Gesetzes

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001

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 nichtleitungsgebundenen, 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 "strategischen Überwachung" nach § 5 G 10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

Anlage 2 Äußerungsrecht der Datenschutzbeauftragten

Entschließung der 61.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001

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, Behördenverhalten

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.

Anlage 3 Informationszugangsgesetze

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001

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 Artikel 255 EU-Vertrag und Artikel 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 entgegensteht, wenn die Privatssphäre 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.

Anlage 4 Datenschutz bei der Bekämpfung von Datennetzkriminalität

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001

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

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 Informationsgesell-

schaft 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.

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.

Anlage 5 Novellierung des Melderechtsrahmengesetzes

Entschließung der 61.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001

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 Melderegis-

terauskünfte 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 Wahlvorschlägen 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 Ziffer 6.

Anlage 6 Überlegungen des BMG für ein Gesetz zur Verbesserung der Datentransparenz

Beschluss der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001

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 -weiterleitungsstellen 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, inwieweit 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 Entwurfs 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.

Anlage 7 Datenschutz beim elektronischen Geschäftsverkehr

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001

Die Konferenz wendet sich mit Entschiedenheit gegen Anträge, die gegenwärtig dem Bundesrat zum Entwurf eines Gesetzes zum elektronischen Geschäftsverkehr (BR-Drs. 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.

Anlage 8 Anlasslose DNA-Analyse aller Männer verfassungswidrig

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 12. März 2001

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 verfassungsrechlich unzulässig. Darüber hinaus erscheint der erwartete Abschreckungseffekt äußerst fragwürdig.

Anlage 9 Veröffentlichung von Insolvenzinformationen im Internet

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24. April 2001

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (BT-Drs. 14/5680) vor. Danach sollen gerichtliche Entscheidungen - vor allem in Verbraucherinsolvenzverfahren - künftig auch über das Internet veröffentlicht werden können, um Kosten für Bekanntmachungen in Printmedien zu sparen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können. Darüber hinaus ist deren Speicherung zeitlich nicht beherrschbar, und die Daten können vielfältig ausgewertet werden. Dies kann dazu führen, dass Dritte, etwa Auskunfteien oder Wirtschaftsinformationsdienste, die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und diese über längere Zeit im Internet verfügbar sind. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit abrufbar am Schulden-Pranger stehen.

Der Gesetzgeber muss das Risiko für die betroffenen Verbraucherinnen und Verbraucher, aufgrund einer möglichen Auswertung justizieller Veröffentlichungen im Internet dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der beabsichtigten Senkung von Bekanntmachungskosten abwägen. Hierbei ist auch die gesetzgeberische Wertung zu berücksichtigen, 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 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. Dabei sollten die Erwägungen des Bundesverfassungsgerichtes im Beschluss vom 9. März 1988 (1 BvL 49/86) zu einem vergleichbaren Sachverhalt einbezogen werden.

Es erscheint zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung. Gerade das Internet bietet neue Chancen und Möglichkeiten, 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 Recht auf informationelle Selbstbestimmung der Betroffenen besser geschützt werden kann.

Auch in anderen Bereichen wird das Internet bereits genutzt, erprobt oder die Nutzung erwogen, um justizielle Informationen bereitzustellen, z.B. die Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckungsverfahren. Inwieweit das Internet als Medium der im Ergebnis unbegrenzbaren Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil in das 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 regeln, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern sowie eine automatische Übernahme der Daten zu verhindern (Kopierschutz).

Sollte sich der Gesetzgeber nach sorgfältiger Abwägung für eine Veröffentlichung über das Internet entscheiden, so muss er die Auswirkungen der Regelung auf Grund aussagefähiger Berichte der Landesjustizverwaltungen überprüfen. Gegenstand dieser Überprüfung muss auch sein, ob die eingetretene Kostensenkung tatsächlich - wie von der Bundesregierung erwartet - einer größeren Anzahl von Schuldnerinnen und Schuldnern den Weg zur Restschuldbefreiung eröffnet hat.

Anlage 10 Entwurf der Telekommunikations-Überwachungsverordnung

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 11. Mai 2001

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.

Anlage 11 Sondertreffen der Datenschutzbeauftragten des Bundes und der Länder zur Terrorismusbekämpfung

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 1. Oktober 2001

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, 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.

Anlage 12 Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./26. Oktober 2001

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 (BR-Drs. 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 Persön-

lichkeitsrechte 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.

Anlage 13 LKW-Maut auf Autobahnen und allgemeine Maut auf privat errichteten Bundesfernstraßen

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./26. Oktober 2001

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 Abrechungszwecke 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 Mauterstat-

tungsverfahrens 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 personenbezogenen 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.

Anlage 14 Datenschutzrechtliche Anforderungen an den "Arzneimittelpass" (Medikamentenchipkarte)

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./26. Oktober 2001

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 Patientinnen 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.

Anlage 15 Neue Medienordnung

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./26. Oktober 2001

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.

Anlage 16 Umgang mit genetischen Untersuchungen

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./26. Oktober 2001

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 Straf-

verfolgung - 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 17 Biometrische Merkmale in Personalausweisen und Pässen

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./26. Oktober 2001

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.

Anlage 18 EUROJUST - Vorläufer einer künftigen europäischen Staatsanwaltschaft?

Entschließung der 62 Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./26. Oktober 2001

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 Grundla-

ge 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 bindender 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.

Anlage 19 Biometrische Merkmale in Personalausweisen und Pässen

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. März 2002

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solcher Maßnahme nennt, zustimmend zur Kenntnis genommen.

Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.

2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z.B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.

3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.

4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.

5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

Anlage 20 Neues Abrufverfahren bei den Kreditinstituten

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. März 2002

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen können. Dies ist ein neuer Eingriff in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung die-

ses Abrufverfahrens eine Verpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine effektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten der Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mit Hilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (sog. “know your customer principle”). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

Anlage 21 Datenschutzgerechte Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. März 2002

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat detaillierte Hinweise hierzu erarbeitet .

Insbesondere gilt Folgendes:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internet am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.

2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.

3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.

4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwen-

dig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.

5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.

6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.

7. Die gleichen Bedingungen wie bei der Nutzung des Internet müssen prinzipiell bei der Nutzung von Intranets gelten.

Die Datenschutzbeauftragten fordern den Bundesgesetzgeber auf, auch wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben.

Anlage 22 Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. März 2002

Mit der rasch wachsenden Nutzung des Internet kommt dem datenschutzgerechten Umgang mit den dabei anfallenden Daten der Nutzerinnen und Nutzer immer größere Bedeutung zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit (Entschließung der 59. Konferenz "Für eine freie Telekommunikation in einer freien Gesellschaft") darauf hingewiesen, dass das Telekommunikationsgeheimnis eine unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft ist. Seine Geltung erstreckt sich auch auf Multimedia- und E-Mail-Dienste.

Die Datenschutzbeauftragten betonen, dass das von ihnen geforderte in sich schlüssige System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, nach wie vor fehlt. Die Strafprozessordnung (und seit dem 1.1.2002 das Recht der Nachrichtendienste) enthält ausreichende Befugnisse, um den Strafverfolgungsbehörden (und den Nachrichtendiensten) im Einzelfall den Zugriff auf bei den Anbietern vorhandene personenbezogene Daten zu ermöglichen. Für eine zusätzliche Erweiterung dieser Regelungen z.B. hin zu einer Pflicht zur Vorratsdatenspeicherung besteht nicht nur kein Bedarf, sondern eine solche Pflicht würde dem Grundrecht auf unbeo-

bachtete Kommunikation nicht gerecht, weil damit jede Handlung (jeder Mausklick) im Netz staatlicher Beobachtung unterworfen würde.

In keinem Fall sind Anbieter von Tele-, Medien- und Telekommunikationsdiensten berechtigt oder verpflichtet, generell Daten über ihre Nutzerinnen und Nutzer auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen Nachrichteninhalte, Verbindungsdaten und bestimmte Daten (Nutzungsdaten), die sie ursprünglich für eigene Zwecke benötigt haben und nach den Bestimmungen des Multimedia-Datenschutzrechts löschen müssten, den Strafverfolgungsbehörden (oder Nachrichtendiensten) zu übermitteln.

Anlage 23 Geplanter Identifikationszwang in der Telekommunikation

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24. Mai 2002

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der geschäftsmäßig Telekommunikationsdienste erbringt, dazu zu verpflichten, Namen, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für Telekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift "Schließen von Regelungslücken" stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig - teilweise nach jedem Telefonat - wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.

- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.

- Die Anbieter würden eine Reihe von Daten auf Vorrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.

- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.

- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z.B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereit gestellt werden und sie damit diese Daten auch für die Verknüpfung mit anderen Datenbeständen verwenden können.

- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das private Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.

- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weitreichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender Verordnungsentwurf bei der Beratung des Gesetzes vorliegt.

Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der Telekommunikationsunternehmen weitgehend vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikations-

gesetzes zu verzichten und vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.

Anlage 24 Datenschutzgerechte Vergütung für digitale Privatkopien im neuen Urheberrecht

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002

Zur Umsetzung der EU-Urheberrechtsrichtlinie wird gegenwärtig über den Entwurf der Bundesregierung für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft beraten. Hierzu hat der Bundesrat die Forderung erhoben, das bisherige System der Pauschalabgaben auf Geräte und Kopiermedien, die von den Verwertungsgesellschaften auf die Urheberinnen und Urheber zur Abgeltung ihrer Vergütungsansprüche verteilt werden, durch eine vorrangige individuelle Lizenzierung zu ersetzen. Zugleich hat der Bundesrat die Gewährleistung eines ausreichenden Schutzes der Nutzerinnen und Nutzer vor Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzungsprofilen gefordert.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in diesem Zusammenhang auf Folgendes hin: Das gegenwärtig praktizierte Verfahren der Pauschalvergütung beruht darauf, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internets ihre Berechtigung. Die Datenschutzkonferenz bestärkt den Gesetzgeber, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Sollte der Gesetzgeber - wie es der Bundesrat fordert - jetzt für digitale Privatkopien vom Grundsatz der Pauschalvergütung (Geräteabgabe) tatsächlich abgehen wollen, so kann er den verfassungsrechtlichen Vorgaben nur entsprechen, wenn er sicherstellt, dass die urheberrechtliche Vergütung aufgrund von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte (Digital Rights Management) müssen datenschutzfreundlich gestaltet werden.

Anlage 25 Systematische verdachtslose Datenspeicherung in der Telekommunikation und im Internet

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnnisses grundlegend in Frage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedsstaaten in den Bereichen “Justiz und Inneres” entsprechende Maßnahmen - allerdings unter weitgehendem Ausschluss der Öffentlichkeit - diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des WorldWideWeb), wie sie jetzt erwogen wird, ist ebensowenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weitergehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

Anlage 26 Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zurzeit in verstärktem Maße in der öffentlichen Diskussion. Mehrere kommunale Spitzenverbände haben sich diesbezüglich bereits an die jeweiligen Landesdatenschutzbeauftragten gewandt. Unbeschadet bereits bestehender Landesregelungen und der Möglichkeit, Daten ohne Grundstücksbezug zu veröffentlichen, fordert die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgrund der bundesweiten Bedeutung der Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden.

Dabei ist zu bestimmen, wie derartige Kataster erstellt werden sollen. Die gegenwärtige Regelung des Bundesimmissionsschutzgesetzes sieht keine ausdrückliche Ermächtigung zur Schaffung von Mobilfunkkatastern vor, sodass deren Erstellung und Veröffentlichung ohne Einwilligung der Grundstückseigentümer und -eigentümerinnen und der Antennenbetreiber keine ausdrückliche gesetzliche Grundlage hat. Bei der Novellierung ist insbesondere zu regeln, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist. Individuelle Auskunftsansprüche nach dem Umweltinformationsgesetz oder den Informationsfreiheitsgesetzen bleiben davon unberührt.

Stichwortverzeichnis