Unterrichtung

Landesbeauftragter für den Datenschutz
Niedersachsen

Hannover, den 22. Dezember 2000

An den
Herrn Präsidenten des Niedersächsischen Landtages

Hannover

15. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Niedersachsen

Sehr geehrter Herr Präsident,

hiermit erstatte ich gemäß § 22 Abs. 3 Satz 1 und Abs. 6 Satz 3 des Niedersächsischen Datenschutzgesetzes den 15. Tätigkeitsbericht für die Kalenderjahre 1999 und 2000.

Mit dem Ausdruck meiner vorzüglichen Hochachtung

Burckhard Nedden

Inhaltsverzeichnis

Anlagen **Entschließungen der Datenschutzbeauftragten des Bundes und der Länder**

Abkürzungen

ABl.	Amtsblatt
Abs.	Absatz
ADV	Automatisierte Datenverarbeitung
AG	Aktiengesellschaft
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS Innere Sicherheit (PIOS = Personen, Institutionen, Objekte, Sachen)
Art.	Artikel
Aufl.	Auflage
AuslG	Ausländergesetz
AVNot	Ausführungsvorschriften für die Angelegenheiten der Notare
BAG	Bundesarbeitsgericht
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
BNotO	Bundesnotarordnung
BND	Bundesnachrichtendienst
BRRG	Beamtenrechtsrahmengesetz
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
Buchst.	Buchstabe
BVerfG(E)	Bundesverfassungsgericht (Entscheidungssammlung)
BVerwG	Bundesverwaltungsgericht
bzgl.	bezüglich
CD-ROM	Compact Disc Read Only Memory
CR	Computer und Recht
DDV	Deutscher Direktmarketing Verband e.V.
DONat	Dienstordnung für Notare
DNA	Desoxyribonukleinsäure
DNA-IFG	DNA-Identitätsfeststellungsgesetz
DÖV	Die Öffentliche Verwaltung
DSB	Datenschutzbeauftragter
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
EC	Eurocheque
ED	Erkennungsdienst
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaften
EGGVO	Einführungsgesetz zum Gerichtsverfassungsgesetz
einschl.	einschließlich
EU	Europäische Union
EUROPOL	Europäisches Polizeiamt
evtl.	eventuell
FeV	Fahrerlaubnis-Verordnung
f(f).	und folgende Seite(n)
ftp	File Transfer Protocol
GBA	Generalbundesanwalt beim Bundesgerichtshof
GBO	Grundbuchordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GewAnz-VwV	Gewerbeanzeigenverwaltungsvorschrift
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GMBl.	Gemeinsames Ministerialblatt
GVBl.	Gesetz- und Verordnungsblatt
GVG	Gerichtsverfassungsgesetz

G 10	Gesetz zu Art. 10 GG
HTML	Hypertext Markup Language
ICD	International Classification of Disease
IDEA	(Verschlüsselungsalgorithmus)
INPOL	(bundesweites) Informationssystem der Polizei
InSo	Insolvenzordnung
ISDN	Integrated Services Digital Network
IT	Informationstechnik
IuK-	Informations- und Kommunikations-
i. V. m.	in Verbindung mit
izn	Informatikzentrum Niedersachsen
JR	Juristische Rundschau
JVA	Justizvollzugsanstalt
JUH	Johanniter-Unfall-Hilfe
JZ	Juristenzeitung
KBA	Kraftfahrt-Bundesamt
LAN	Local Area Network
LfD	Landesbeauftragter für den Datenschutz
LKAN	Landeskriminalamt Niedersachsen
LRH	Landesrechnungshof
LT-Drs.	Landtagsdrucksache
MDK	Medizinischer Dienst der Krankenversicherung
MF	Finanzministerium
MFAS	Ministerium für Frauen, Arbeit und Soziales
MI	Innenministerium
MiStra	Mitteilungen in Strafsachen
MK	Kultusministerium
MRRG	Melderechtsrahmengesetz
MV	Mecklenburg-Vorpommern
MVS/VM	Multiple Virtual Storage/Virtual Machine (Großrechner-Betriebssystem)
MVS/RACF	Multiple Virtual Storage/Resource Access Control Facility
NAbfG	Niedersächsisches Abfallgesetz
NBG	Niedersächsisches Beamtengesetz
NDR	Norddeutscher Rundfunk
Nds.	Niedersächsische(r/s)
Nds. ÄGInSO	Nds. Gesetz zur Ausführung der Insolvenzordnung
NDSG	Niedersächsisches Datenschutzgesetz
Nds. GVBl	Niedersächsisches Gesetz- und Verordnungsblatt
Nds. MBl.	Niedersächsisches Ministerialblatt
Nds. Rpfl.	Niedersächsische Rechtspflege
NGDG	Niedersächsisches Gesundheitsdienstgesetz
NGefAG	Niedersächsisches Gefahrenabwehrgesetz
NGO	Niedersächsische Gemeindeordnung
Nieders.	Niedersächsische(r/s)
NJW	Neue Juristische Wochenschrift
NKWG	Niedersächsisches Kommunalwahlgesetz
NLfV	Niedersächsisches Landesamt für Verfassungsschutz
NLO	Niedersächsische Landkreisordnung
NMeldDÜV	Nds. Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
NMG	Niedersächsisches Meldegesetz
NSchG	Niedersächsisches Schulgesetz
NVerfSchG	Niedersächsisches Verfassungsschutzgesetz
NWG	Niedersächsisches Wassergesetz
OK	Organisierte Kriminalität
OLG	Oberlandesgericht
OWi	Ordnungswidrigkeiten
PersVG	Personalvertretungsgesetz
PC	Personal Computer
PGP	Pretty Good Privacy
PIN	Personal Identification Number

POLAS	Polizeiliches Auskunftssystem (in Niedersachsen)
PsychKG	Gesetz über Hilfen für psychisch Kranke und Schutzmaßnahmen
RACF	Ressource Access Control Facility (Zugriffsschutzmodul)
RDV	Recht der Datenverarbeitung
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren
RSA-	Rivest-Shamir-Adleman-
RdErl.	Runderlass
RVO	Reichsversicherungsordnung
S.	Seite
Sächs-VerfGH	Sächsischer Verfassungsgerichtshof
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SchuVVO	Schuldnerverzeichnisverordnung
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SIJUS-Straf	(ADV-System der Staatsanwaltschaften)
SPUDOK	(polizeiliches) elektronisches Spurendokumentationssystem
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
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstgesetz
TDSV	Telekommunikationsdiensteunternehmen-Datenschutzverordnung
TierSchG	Tierschutzgesetz
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TOA	Täter-Opfer-Ausgleich
TÜ	Telefonüberwachung
UDSV	Teledienstunternehmen-Datenschutzverordnung
UiG	Umweltinformationsgesetz
UNICEF	United Nations International Children's Emergency Fund
UNIX	(ADV-Betriebssystem für Mehrplatzsysteme)
USA	Vereinigte Staaten von Amerika
VGH	Verwaltungsgerichtshof
vgl.	vergleiche
VGO	Vollzugsgeschäftsordnung
VOB	Verdingungsordnung für Bauleistungen
VOF	Verdingungsordnung für freiberufliche Leistungen
VOL	Verdingungsordnung für Leistungen
VV	Verwaltungsvorschrift
VW	Volkswagen
VwVfG	Verwaltungsverfahrensgesetz
VZR	Verkehrszentralregister
Windows NT	(PC-Netzwerk-Betriebssystem)
WORM	Write Once Read Many
WWW	World-Wide-Web
z. B.	zum Beispiel
ZDF	Zweites Deutsches Fernsehen
ZFER	Zentrales Fahrerlaubnisregister
ZFR	Zentrales Fahrzeugregister
ZKA	Zentraler Kreditausschuss
ZPO	Zivilprozeßordnung
ZRP	Zeitschrift für Rechtspolitik
ZSchG	Zeugenschutzgesetz

ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

1 Vorbemerkung

Der vorliegende XV. Tätigkeitsbericht betrifft die beiden Kalenderjahre 1999 und 2000. Redaktionsschluss war der 20. November 2000. Im Interesse der Lesbarkeit des Tätigkeitsberichts habe ich für Substantive, die sich auf beide Geschlechter beziehen, nur die männliche Form verwendet.

Der Bericht behält bei der Behandlung der einzelnen Sachpunkte im Wesentlichen die seit vielen Jahren eingeführte Gliederung und die gewohnten Kapitelüberschriften bei, um die rasche Orientierung des Lesers zu unterstützen. Kapitel 28 bis 36 enthalten den Bericht über den Datenschutz im nicht-öffentlichen Bereich (§ 22 Abs. 6 Satz 3 NDSG).

Neu aufgenommen sind zwei Kapitel:

In Kapitel 2 sind unter der Überschrift „Datenschutzpolitischer Handlungsbedarf" die Punkte aus dem Tätigkeitsbericht in einer Übersicht zusammengestellt, bei denen Gesetzgebung oder Exekutive aus meiner Sicht konkret und aktuell tätig werden müssen, um zum Beispiel offenkundige datenschutzrechtliche Defizite zu beseitigen oder um bei neuen Fragestellungen verbindliche Vorgaben für den datenschutzgerechten Umgang mit personenbezogenen Daten zu schaffen; auf die entsprechende Einzeldarstellung im Tätigkeitsbericht wird jeweils verwiesen. Ich gehe davon aus, dass mit dieser zusammenfassenden Darstellung die Lesbarkeit des Tätigkeitsberichts noch einmal verbessert wird, und erhoffe mir damit vor allem auch eine Belebung und Konzentration der Diskussion zum Tätigkeitsbericht im Landtag bzw. im zuständigen Ausschuss für innere Verwaltung.

Kapitel 5 enthält unter der Überschrift „Schwerpunkte" die Einzeldarstellung zu vier Themenbereichen, die im Berichtszeitraum für meine Arbeit von besonderer Bedeutung waren oder die künftige Arbeit stark bestimmen werden und die deshalb außerhalb der regulären Gliederung an vorgezogener Stelle behandelt werden. Auch hierdurch soll der Bericht noch besser strukturiert und zugleich die Auseinandersetzung mit besonders bedeutsamen datenschutzrechtlichen Fragestellungen oder Entwicklungen gefördert werden.

Die vorstehend beschriebenen Neuerungen bezeichnen einen Teil der Veränderungen, die seit meinem Amtsantritt am 1. Juni 1999 in einem intensiven Diskussionsprozess mit den Mitarbeiterinnen und Mitarbeitern der Geschäftsstelle erarbeitet worden sind. Diese Veränderungen, die in den Kapiteln 3 (unter 3.1) und 4 (unter 4.1 und 4.2) eingehender beschrieben sind, haben ihren gemeinsamen Bezugspunkt in einem Aufgabenverständnis, das neben die Funktion des Landesbeauftragten als staatliche Kontrollinstanz noch stärker die Beratungsfunktion als Teil seiner Aufgaben in den Vordergrund stellt.

Im Jahr 2000 habe ich den Vorsitz in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder von meinem Kollegen aus Mecklenburg-Vorpommern, Herrn Dr. Werner Kessel, übernommen. Die 59. Konferenz hat am 14./15. März 2000 in Hannover und die 60. Konferenz am 12./13. Oktober 2000 in Braunschweig stattgefunden. Die während der Konferenzen sowie die darüber hinaus im Umlaufverfahren verabschiedeten Entschließungen sind in den Anlagen zum Tätigkeitsbericht dokumentiert. Im Jahre 2001 wird der Vorsitz in der Konferenz turnusgemäß auf die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Frau Bettina Sokol, übergehen.

2 Datenschutzpolitischer Handlungsbedarf

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

- Die Datenschutzaufsicht über den nichtöffentlichen 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 (3.3 unter 6).
- 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 (3.4).
- Im NDSG bzw. im NGefAG müssen gesetzliche Regelungen zur Videoüberwachung im öffentlichen Raum geschaffen werden (5.1).
- Für die Verarbeitung von Gesundheitsdaten im Krankenhausbereich ist eine landesgesetzliche Regelung seit Jahren überfällig; durch die Vorgaben in Artikel 8 der EG-Datenschutzrichtlinie wird der Handlungsbedarf noch einmal unterstrichen (5.2).
- Die Landesregierung sollte Bemühungen zum datenschutzgerechten E-Government nachhaltig unterstützen. Zur Sicherung der Authentizität bei einem elektronischen Dokumentenaustausch im Verwaltungsverfahrensrecht ist die digitale Signatur als Surrogat der eigenhändigen Unterschrift einzuführen (5.4 / 6.5).
- Beim Anschluss ans Internet müssen alle Dienststellen die Sicherheit der Daten von Bürgerinnen und Bürgern durch technische und organisatorische Maßnahmen gewährleisten (6.4).
- 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 der Datensparsamkeit orientiert (9.4.1).
- Für in polizeilichen Kriminal- bzw. Sachakten gespeicherte Daten Dritter müssen Prüf- und Löschungsfristen eingeführt werden (11.2).
- Es muss sorgfältig geprüft werden, ob der räumliche Anwendungsbereich der verdachtsunabhängigen Kontrollen gem. § 12 Abs. 6 NGefAG vor dem Hintergrund des Urteils des Landesverfassungsgerichts Mecklenburg-Vorpommern zur sog. Schleierfahndung zu beschränken ist (11.3).
- 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 (11.4).
- 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 (11.6).
- Für das Niedersächsische Verfassungsschutzgesetz ergeben sich entsprechende Regelungsnotwendigkeiten (13.1).

- Einer Ausweitung der Überwachungsbefugnisse des Verfassungsschutzes nach dem G 10-Gesetz auch auf extremistische Einzeltäter darf von Seiten des Landes nicht zugestimmt werden (13.2).
- 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 (14.1).
- Für die Teilnahme der Schwerbehindertenvertretung an Auswahlgesprächen bei der Personaleinstellung ist eine gesetzliche Grundlage zu schaffen (14.2).
- 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 (15).
- Es ist dringend erforderlich, die seit mehr als zwei Jahren geforderte Anonymisierung des Abrechnungsverfahrens bei Schwangerschaftsabbrüchen umzusetzen (18.6).
- 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 Betroffenen umfassend und ordnungsgemäß belehrt werden (26.3.1).
- 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 (26.4).
- 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 (26.4).

3 Zur Situation des Datenschutzes

3.1 Datenschutz im Internet-Zeitalter

Der Übergang von der klassischen Industriegesellschaft in die Informations- und Wissensgesellschaft, in dem sich - in unterschiedlicher Geschwindigkeit - weltweit alle entwickelten Gesellschaften befinden, ist das prägende Merkmal unserer Zeit. Wie schon im letzten Tätigkeitsbericht hervorgehoben (vgl. XIV TB 2.1), sind neben Arbeit, Kapital und Rohstoffen Informationen zum vierten, zunehmend wichtiger werdenden Produktionsfaktor geworden, wobei die Verfügbarkeit von Informationen und damit die Möglichkeit, sie zum Inhalt von Wissen und Handlungsaktivitäten zu machen, durch die rasante Weiterentwicklung der IuK-Technik und die weltweite Vernetzung praktisch grenzenlos ist. Die Globalisierung der Wirtschaft fordert und fördert diesen weltweiten Informations- und Wissenstransfer. Gleichzeitig generieren neue technische Lösungen im Bereich der IuK-Technik ständig neue Inhalte und Formen wirt-

schaftlicher Betätigung, mitunter mit Wertschöpfungsketten, die - verglichen mit den Branchen der traditionellen Wirtschaft der Industriegesellschaft - sich geradezu atemberaubend entwickeln. So war etwa der Aktienwert der Internet-Plattform Yahoo im Sommer 2000 mit rund 170 Milliarden DM rund viermal so hoch wie der von VW, obwohl der Autokonzern bei Umsatz und Beschäftigten Yahoo noch um mehr als das Hundertfache übertrifft. Und auch die 100 Milliarden DM, die die Versteigerung der UMTS-Lizenzen erbracht hat, lassen erahnen, welches gewaltige wirtschaftliche Potenzial hinter den Möglichkeiten von Mehrwertdiensten steckt, die in Zukunft über das Handy standortbezogen angeboten und genutzt werden können.

Die Leistungsfähigkeit der Systeme wird sich weiter steigern; Prognosen gehen davon aus, dass die Rechenkapazität der Computer bis 2030 um den Faktor 1 Millionen größer als heute sein wird. Damit wird es möglich sein, ganz neue Wissensbereiche zu erschließen und für jedermann verfügbar zu machen. Der Einblick beispielweise in die genetischen Strukturen von Menschen, heute nur für wenige Wissenschaftler mit Hilfe hochspezialisierter Technik möglich, wird von der technischen Seite schon bald eine Allerweltsanwendung sein. In New York ist der Prototyp eines handtellergroßen Mini-Labors vorgestellt worden, das innerhalb von zwei Minuten aus einem Haar oder dem Speicheltropfen einer Person ein DNS-Profil erstellen kann. Die Entschlüsselung des menschlichen Erbgutes und die Entwicklung von Gentests werden gewaltige Fortschritte im Bereich der Diagnose, der Prävention und der Therapie genetisch bedingter Krankheiten ermöglichen, werfen aber auch schwierige ethische, soziale und datenschutzrechtliche Fragen auf (vgl. dazu 5.3). Wie gehen wir mit diesem zuwachsenden Wissen um, das Einblicke in einen Menschen ermöglicht, die ungleich viel tiefer gehen als alle bisher zu einem Individuum verfügbaren Informationen? Wer darf sich dieses Wissen für welche Zwecke verschaffen? Wann darf, wann muss dieses Wissen dem Betroffenen offenbart werden?

Die Chancen und Gefahren der absehbaren technologischen Entwicklung, auch und gerade für die Zukunft gesellschaftlicher Werte und individueller Rechte, sind vielfach beschrieben und analysiert worden. Besonders weit reichend sind die Überlegungen, die William Joy, Gründer und Chef-Wissenschaftler von Sun Microsystems, dazu angestellt hat. In seinem Essay „Warum die Zukunft uns nicht braucht“ (abgedruckt in der FAZ vom 6. Juni 2000) hat er dargestellt, dass die Weiterentwicklung der Informationstechnik und ihre Verknüpfung mit der Bionik, der Robotik und der Nanotechnologie „intelligente“ technische Systeme hervorbringen werde, die in immer stärkerem Maße Handlungsfelder übernehmen würden, die bislang dem Menschen vorbehalten sind, und die sich schließlich selbst reproduzieren könnten. Die Fähigkeit, aus der Verknüpfung von Informationen und Kreativität Neues entstehen zu lassen, werde nicht mehr ausschließlich menschlichen Gehirnen vorbehalten bleiben. Um das Jahr 2029, so lautet die Prognose von Ray Kurzweil, einem der einflussreichsten Wissenschaftstheoretiker Amerikas, in seinem Buch Homo sapiens (erschienen bei Kiepenheuer und Witsch) kann das menschliche Gehirn gescannt und in einem Computer dupliziert werden. Und er verbindet damit die Einschätzung: „Computer werden einen freien Willen haben. Sie werden spirituelle Erfahrungen für sich reklamieren. Und die Menschen, deren Denken noch immer von der Arbeit organischer Neuronen abhängt, werden ihnen glauben“. Mit dieser technologischen Weiterentwicklung schafft der Mensch die Voraussetzungen zu seiner Abschaffung, lautet zugespitzt die Kernthese von William Joy („Es drängte sich mir ein anderer Gedanke auf: dass ich mich möglicherweise an der Entwicklung von Instrumenten beteilige, aus denen die Technologie hervorgehen könnte, die unsere Spezies verdrängen wird.“). Er hat dafür Zustimmung, aber auch vielfache Ablehnung erfahren. Ich empfehle die Lektüre dieses Essays und der sich daran anschließenden Veröffentlichungen, die im Feuilletonteil der FAZ gut doku-

mentiert sind, damit jeder für sich selbst nachvollziehen kann, ob er den Thesen von William Joy folgen mag oder nicht.

Bestandteil unserer Alltagsrealität sind bereits die vielfachen neuen Nutzungsmöglichkeiten des Internets geworden, die nicht mehr nur für eine kleine Schar Technikbegeisterter, sondern praktisch für jedermann zur Verfügung stehen. Die Zuwachsraten in der Verbreitung des Internets sind beeindruckend in ihrer Geschwindigkeit: Im ersten Halbjahr 2000 hat die Zahl der deutschen Haushalte, die über einen Internetzugang verfügen, um 30% zugenommen; bis Ende 2000 gehen die Prognosen von 30 Millionen Nutzern in Deutschland aus. Gleichzeitig wird eine Zugangstechnologie marktfähig gemacht, die auch anspruchsvolle Nutzungen des Internets über das Handy und damit mobil ermöglicht. Bundesregierung und alle Landesregierungen forcieren diese Entwicklung mit gezielten und breit angelegten Förderprogrammen, die auch dem Ziel dienen, Informationsgerechtigkeit durch Internet-Zugangs- und Nutzungsmöglichkeiten für alle zu schaffen und die sonst drohende Spaltung der Gesellschaft zu verhindern. Nutzungsangebote für das Internet werden nicht mehr nur von der Wirtschaft, sondern immer stärker auch von der öffentlichen Verwaltung entwickelt. Aus Sicht der Bürgerinnen und Bürger stehen bei der Nutzung des Internets gerade die Verbesserung der Kommunikation und der Leistungsaustausch mit der Verwaltung an erster Stelle. Die Erschließung dieses Mediums für alle Sparten der öffentlichen Verwaltung ist zu einer der wichtigsten Aufgaben im Rahmen der Verwaltungsmodernisierung geworden und bildet auch einen Schwerpunkt für die Arbeit meiner Geschäftsstelle (vgl. dazu die Ausführungen unter 5.4 und 14.7).

Das Internet wird heute nicht nur zur Abfrage und Entgegennahme von Informationen genutzt, sondern zunehmend auch zur Abwicklung von Rechtsgeschäften aller Art, sodass die Gewährleistung von Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit immer wichtiger wird. Auf der anderen Seite sind die personenbezogenen digitalen Spuren, die bei jeder Internet-Nutzung entstehen, nicht nur als Kundendaten von hohem Interesse für Adressenhändler und Direktmarketingunternehmen, sondern werden auch zu ganz anderen, oftmals kriminellen Zwecken ausspioniert und missbraucht. Es ist derzeit noch offen, ob und in welcher Weise es gelingen wird, für das Internet, für das nationale Regelungen immer nur auch im eigentlichen Wortsinne begrenzte Ansätze liefern können, datenschutzgerechte Lösungen mit übergreifender Wirkung durchzusetzen. Aus der Sicht der Bürgerinnen und Bürger haben Sicherheit und verlässliche Kommunikation bei der Nutzung des Internets erfreulicherweise einen hohen Stellenwert und begründen zumindest in Deutschland eine derzeit noch deutlich spürbare Zurückhaltung etwa in der Nutzung des elektronischen Einkaufs. Da die Wirtschaft diese Zurückhaltung nicht auf Dauer hinnehmen wird, sehe ich gute Chancen, dass die Entwicklung datenschutzfreundlicher Produkte in der nächsten Zeit Fortschritte machen wird. Es ist eine Aufgabe gerade auch der Datenschutzbeauftragten, diese Entwicklungsprozesse zu fordern und zu fördern.

An diesem Beispiel lässt sich auch verdeutlichen, dass Datenschutz im Internet-Zeitalter nicht mehr und ausschließlich mit den Instrumenten und Strategien der Vergangenheit arbeiten kann. So ist beispielsweise mittlerweile unumstritten, dass der normative Datenschutz - nicht nur wegen des schon angesprochenen begrenzten Zugriffs des nationalen Gesetzgebers auf Erscheinungsformen wie das global ausgerichtete Internet - an seine Grenzen stößt. Mit schöner Deutlichkeit hat Spiros Simitis, der „Vater" des deutschen Datenschutzrechts, dies formuliert: „Wo Anonymität zur Fiktion gerät, Datensammlung zur Routine wird, Verarbeitungsvorgänge von beliebigen Stellen aus zu ebenso beliebigen Zeiten durchgeführt werden können und sich die Spuren der Betroffenen zwar immer weiter verdichten, die Spuren des Zugriffs auf ihre Daten sich aber immer mehr

verlieren, lassen sich mit rein normativen Vorgaben bestenfalls Intentionen umschreiben. Ihre Realisierung ist dagegen fraglicher denn je."

Praktizierter Datenschutz im Internet-Zeitalter muss daher anders aussehen als in den Zeiten, in denen es „nur" um die Massendatenverarbeitung in einer überschaubaren Zahl von zentral organisierten großen Rechenzentren ging und die Vernetzung eher ein randständiges Thema war. Datenschutz muss sich einlassen auf die schon eingetretenen und noch zu erwartenden technischen Weiterentwicklungen im IuK-Bereich und auf die vielen neuen Nutzungsmöglichkeiten dieser Technik, ohne in jedem Fall für alle Fragestellungen schon Antworten im geltenden Recht zu finden. Datenschutz muss heute sehr viel stärker als früher im Vorfeld Einfluss nehmen und bei der Ausformung sowohl der technischen Lösungen als auch der rechtlichen Begleitregelungen konstruktiv und aktiv mitzugestalten versuchen. Dabei müssen sehr viel stärker als bisher die Möglichkeiten datenschutzfreundlicher Technik- und Systemgestaltung genutzt werden, wozu Datenvermeidung und Datensparsamkeit, u. a. auch durch Anonymisierung und Pseudonymisierung, ebenso zu zählen sind wie Verschlüsselung und Hilfen für einen wirkungsvollen Datenselbstschutz. So notwendig es ist, diese Elemente und Prinzipen auch rechtlich zu verankern und dadurch festzuschreiben, ihre praktische Umsetzung ist allein dadurch nicht zu gewährleisten, sondern erfordert aktives Handeln gerade auch der Datenschutzbeauftragten. Nicht das „nachsorgende" Herausfinden von Datenschutzverstößen, sondern die vorsorgende aktive Beratung und Mitgestaltung bei der Entwicklung von datenschutzgerechten und datenschutzfreundlichen Produkten und Lösungen in Wirtschaft und Verwaltung sowie die intensive Aufklärung der Bürgerinnen und Bürger über Gefährdungen ihres Rechts auf informationelle Selbstbestimmung und über Möglichkeiten und Instrumente des Selbstschutzes müssen für die Datenschutzbeauftragten Priorität haben. Darüber besteht erfreulicherweise auch weitgehend Konsens. Bei der praktischen Umsetzung neuer Ansätze gibt es bei den Datenschutzbeauftragten in Bund und Ländern viel Kreativität und Ideenreichtum, die in der nächsten Zeit ihre Bewährung erfahren werden. Einige Elemente dieses neu verstandenen Datenschutzes sind im Kapitel 4 unter 4.2 näher beschrieben. Sie finden sich auch im Leitbild wieder, das sich die Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle erarbeitet und als Grundlage ihres Handelns festgeschrieben haben.

Auch wenn manche das „Ende der Privatheit" heraufbeschwören und einige Erscheinungsformen insbesondere der Fernseh-Unterhaltung ein Maß der Selbst-Entblößung zeigen, das in eine andere Richtung zu weisen scheint, belegen doch Umfragen gerade aus jüngster Zeit, dass der gesellschaftliche und individuelle Stellenwert von informationeller Selbstbestimmung wie insgesamt der Wert von „privacy" in Zukunft eher eine steigende Bedeutung haben werden. Es gilt allerdings in diesem Zusammenhang eine Entwicklung sehr sorgfältig zu beobachten, auf die der schon zitierte William Joy in einem Vortrag auf dem Weltwirtschaftsforum in Davos im Januar 2000 hingewiesen hat. Er hat davor gewarnt, dass „privacy" etwas werden könnte, was man sich entweder leisten will und kann oder aber nicht mehr bekommt. „Privacy" stehe in der Gefahr zur Ware zu werden, die ihren Preis kosten wird.

An diese Einschätzung fühlt man sich unwillkürlich erinnert, wenn heute Mineralölfirmen oder Einkaufszentren die Gewährung von Rabatten beim Kauf ihrer Produkte an die Benutzung einer „Payback-Card knüpfen, mit deren Hilfe alle Käufe einer Person elektronisch erfasst, gespeichert und ausgewertet werden können. In der Tat kostet die Abschirmung des individuellen Kaufverhaltens vor der Neugier des Verkäufers ihren Preis, nämlich den Verzicht auf die Gewährung von Rabatten. Anders als früher bei den ohne Personenbezug zugeteilten Rabattmarken, die man in ebenso neutrale Rabatthefte einkleben konnte, soll hier der Käufer nicht nur für Kauftreue belohnt werden. Es wird ihm zugleich

eine personenbezogene Gegenleistung abverlangt, nämlich die Einwilligung in eine Speicherung, Verarbeitung und Auswertung von Informationen über sein individuelles Kaufverhalten. Ich bezweifle, dass die personenbezogene Auswertung des Käuferverhaltens den betreffenden Firmen wirklich nennenswerte Erkenntnisse erbringt, die über das hinausgehen, was auch durch ein anonymes Auswerteverfahren zu erfahren wäre. Ich verweise in diesem Zusammenhang auf die nachfolgenden Ausführungen zu Data-Warehouse und Data-Mining (vgl. 6.7).

Ich fürchte, dass sich die neuen Rabattsysteme gleichwohl durchsetzen werden, weil die Aussicht, etwas billiger zu bekommen, in der individuellen Einschätzung häufig gewichtiger sein wird als das Bewusstsein um den Wert von informationeller Selbstbestimmung und den Schutz persönlicher Daten. Mein Ansatz wird es sein, die Bürgerinnen und Bürger intensiv darüber aufzuklären, welche Einblicke in ihr persönliches Verhalten durch die Nutzung von pay-back-Karten ermöglicht werden, und auf eine datenschutzgerechte Ausgestaltung der Einwilligungserklärung zu dringen, die vor Aushändigung der Karte dem Nutzer zur Unterschrift vorgelegt wird. Angesichts des Erfindungsreichtums der Marketingstrategen in der Wirtschaft wird es aber sicher auch in Zukunft schwer bleiben, Datenschutzbewusstsein bei den Bürgerinnen und Bürgern nicht nur zu wecken, sondern auch so zu stabilisieren, dass sie der Versuchung widerstehen, sich ihre informationelle Selbstbestimmung für einen kleinen Preisnachlass abkaufen zu lassen.

3.2 Die Situation des Datenschutzes beim Bund

Bereits in meinem letzten Tätigkeitsbericht (XIV. TB 2.2) habe ich die fehlende Umsetzung der EU-Datenschutzrichtlinie vom 24. Oktober 1995 beklagt. Am 14. Juni 2000 hat das Bundeskabinett nun endlich einen Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes beschlossen. Die parlamentarischen Beratungen sind im Herbst aufgenommen worden. Mit dem In-Kraft-Treten des Gesetzes wird für Anfang des Jahres 2001 gerechnet.

Die von der Richtlinie festgelegte Umsetzungsfrist ist bereits am 24. Oktober 1998 abgelaufen. Die EU-Kommission hat wegen der erheblichen Fristüberschreitung ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland sowie gegen Frankreich, Luxemburg, die Niederlande und Irland eingeleitet, die ebenfalls mit der Umsetzung säumig sind. Die Kommission hat inzwischen formell beschlossen, die Bundesrepublik Deutschland vor dem Europäischen Gerichtshof zu verklagen.

Der Gesetzentwurf der Bundesregierung beschränkt sich im Wesentlichen auf eine Anpassung des BDSG an die EU-Richtlinie, nimmt jedoch in einigen Punkten - beispielhaft seien genannt der Grundsatz der Datenvermeidung bzw. Datensparsamkeit, Regelungen über die Videoüberwachung und zum Datenschutzaudit - auch Forderungen zur zeitgemäßen Anpassung des Datenschutzrechts an die zwischenzeitlich eingetretenen Veränderungen insbesondere in der Datenverarbeitungstechnik auf. Leider werden nicht alle diese Regelungen vom Bundesrat unterstützt. Dieser hat sich insbesondere gegen eine Vorschrift über die Einführung eines Datenschutzaudits ausgesprochen, die es Unternehmen u. a. ermöglichen würde, Datenverarbeitungssysteme und -programme unter Datenschutzgesichtspunkten überprüfen zu lassen, um so Vorteile im Wettbewerb um den Einsatz datenschutzfreundlicher Produkte zu erreichen. Die Konferenz der Datenschutzbeauftragten des Bundes und Länder hat den Bundesrat in ihrer Entschließung vom 12./13. Oktober 2000 aufgefordert, seine Blockadehaltung in diesem Punkt aufzugeben (vgl. Anlage 23).

Die von den Datenschutzbeauftragten seit längerem geforderte grundlegende Fortentwicklung des Datenschutzrechts soll in einer zweiten Stufe der BDSG-Novellierung erfolgen. In diesem Zusammenhang soll das Datenschutzrecht auch verständlicher und anwenderfreundlicher gestaltet werden. Die Vorarbeiten für diese zweite Stufe haben bereits begonnen. Im Rahmen des Reformprozesses, an dem sich die Datenschutzbeauftragten des Bundes und der Länder intensiv beteiligen werden, wird zunächst eine umfassende Bestandsaufnahme erarbeitet und sind Gutachtenaufträge vergeben worden. Der Diskussionsprozess soll durch eine Kommission und Expertengruppen für bestimmte Themenbereiche begleitet werden. Insgesamt soll technischer und rechtlicher Sachverstand auf breiter Basis in das Projekt einfließen.

3.3 Anpassung des NDSG an die EU-Datenschutzrichtlinie

Den mühsamen Prozess der Umsetzung der EU-Datenschutzrichtlinie habe ich in meinem letzten Tätigkeitsbericht (vgl. XIV. TB 6.2) näher dargestellt. Auch der wesentliche Inhalt des Gesetzentwurfs, den die Landesregierung im August 1999 dem Landtag zugeleitet hat, ist dort beschrieben. Die Beratung des Entwurfs in den Landtagsausschüssen ist nach der Anhörung der kommunalen Spitzenverbände und von mir für längere Zeit ausgesetzt worden, um die Beschlussfassung der Bundesregierung über den Entwurf des BDSG zur Anpassung an die Richtlinie abzuwarten. Diese Verfahrensweise war sinnvoll, um die absehbaren Änderungen des Bundesrechts bei der Novellierung des NDSG berücksichtigen zu können und eine weitgehende Rechtseinheitlichkeit zu erhalten, sie hat die Beratungen insgesamt jedoch beträchtlich verzögert.

Inhaltlich beschränkt sich der Gesetzentwurf der Landesregierung leider fast ausschließlich darauf, die EU-Datenschutzrichtlinie von 1995 umzusetzen. Die schon seit Jahren geführten Diskussionen über die Fortentwicklung des Datenschutzrechts insbesondere angesichts der fortschreitenden technischen Entwicklung nimmt er nicht zur Kenntnis. Forderungen nach dem Einsatz datenschutzfreundlicher Technologien, nach Datenvermeidung und Datensparsamkeit greift er nicht auf. Auch die Vorgaben der Richtlinie werden nicht konsequent umgesetzt. So enthält der Entwurf keinerlei Regelungen zum Schutz besonders sensibler Daten, die in der Richtlinie besonders angesprochen werden. Überdies ist der Gesetzentwurf wenig anwenderfreundlich. Dies hängt u. a. damit zusammen, dass die Entwurfsverfasser von einem strikten Ansatz der Deregulierung ausgehen, der rechtliche Problemlösungen vielfach als bekannt voraussetzt. Als Beispiel für eine solche Regelung, mit der die Praxis unnötige Schwierigkeiten haben dürfte, nenne ich die Bestimmungen über die automatisierte Datei. Wie wenig der Gesetzentwurf Gesichtspunkte der praktischen Handhabbarkeit berücksichtigt, wird auch darin deutlich, dass meine Forderung, eine Bekanntmachung des Gesetzes in einer Neufassung vorzusehen, die es den Rechtsanwendern ersparen würde, sich zuerst durch eine Vielzahl von Änderungsgesetzen hindurcharbeiten zu müssen, um den geltenden Gesetzestext festzustellen, zunächst abgelehnt wurde. Erfreulicherweise hat das Innenministerium jedoch in diesem Punkt inzwischen seine Auffassung geändert und unterstützt nunmehr meinen Vorschlag.

Im Gesetzgebungsverfahren habe ich vor allem folgende Änderungen vorgeschlagen:

1. Technische und organisatorische Maßnahmen

   Die Regelungen über technische/organisatorische Maßnahmen, die eine rechtmäßige Datenverarbeitung sicherstellen, sollten grundlegend überarbeitet werden. Die derzeitigen „10 Gebote der Datensicherung“ sind nicht

mehr zeitgemäß; sie knüpfen an einen seit langem überholten Stand der Technik an. Ihnen liegt die Vorstellung einer zentralistisch organisierten Datenverarbeitung in Rechenzentren zu Grunde. Hierauf sind z. B. Datensicherungsmaßnahmen wie die Zugangskontrolle, die den physischen Zugang zu Räumen verwehren will, in denen sich Datenverarbeitungsanlagen befinden, oder die Datenträgerkontrolle, bei der die Vorstellung bestand, Datenträger in einem entsprechenden Archiv zusammenzuführen, zugeschnitten. Die heutige automatisierte Datenverarbeitung ist dagegen - wie der PC-Einsatz zeigt - durch eine dezentrale, in der Regel vernetzte Verarbeitung geprägt. Mit der Datenverarbeitung hat auch die Datensicherung am Arbeitsplatz stattzufinden. Anzuknüpfen ist nicht mehr an den Schutz der Geräte, sondern vielmehr an den Schutz der Daten selbst.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb eine Empfehlung erarbeitet, die für die veränderte IuK-Technik verbindliche, vom Einsatz der jeweiligen Technik unabhängige Sicherungsziele vorschreibt. Dies sind

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

Diese Sicherungsziele, die einen allgemein gültigen umfassenden Sicherheitsrahmen bilden, sollten in das NDSG übernommen werden; dies beseitigt die bisher aufgetretenen Unzulänglichkeiten und dient der Vereinheitlichung der Technikregelungen.

2. Grundsatz der Datenvermeidung/Datensparsamkeit/Anonymisierung/Pseudonymisierung

Entsprechend den Regelungen im Tele- und Mediendiensterecht sollte der Grundsatz der Datenvermeidung bzw. Datensparsamkeit auch im NDSG verankert werden. Dieser Grundsatz erlegt den Daten verarbeitenden Stellen auf, Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Mit dem Erforderlichkeitsprinzip darf dieser Grundsatz nicht verwechselt werden. Er betrifft nicht die Frage der materiell-rechtlichen Zulässigkeit der Datenverarbeitung, sondern zielt auf eine entsprechende Technik- und Systemgestaltung. Diesem Ansatz kommt angesichts der rasant fortschreitenden Technikentwicklung immer stärkere Bedeutung zu. Gesichtspunkte der Datensparsamkeit und der Datenvermeidung müssen deshalb bereits bei der Auswahl einschlägiger Produkte und beim Technikeinsatz (z. B. beim Einsatz von Videokameras oder im Rahmen von Abrechnungsverfahren bei Mautgebühren für eine Straßennutzung) berücksichtigt werden. Die neueren Datenschutzgesetze der Länder sowie der Entwurf des Bundesdaten-

schutzgesetzes enthalten übereinstimmend diesen Grundsatz.

In diesen Zusammenhang gehört auch die Forderung, von Verfahren der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der dadurch entstehende Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck dieser Maßnahmen steht.

3. Behördlicher Datenschutzbeauftragter

Der Gesetzentwurf stärkt die Stellung des behördlichen Datenschutzbeauftragten und konkretisiert seine Aufgaben. Dies wird von der EU-Richtlinie gefordert. Nach ihren Regelungen genügt es nicht, einen Datenschutzbeauftragten lediglich formal zu bestellen, er muss vielmehr seine Aufgabe auch effektiv wahrnehmen. Unterlässt er dies, greift nach der Richtlinie die Meldepflicht für automatisierte Dateien, die durch die Bestellung von Datenschutzbeauftragten gerade vermieden werden soll (vgl. hierzu XIV. TB 6.2.4), wieder ein. Zur sachgerechten Aufgabenwahrnehmung ist es deshalb aus meiner Sicht erforderlich, dass ein behördlicher Datenschutzbeauftragter im erforderlichen Umfang von anderen Aufgaben freigestellt wird. Auch Klagen aus der Praxis, insbesondere aus dem Hochschulbereich, dass die zur Aufgabenerfüllung nötige Zeit nicht zur Verfügung stehe, bestärkt mich in der Forderung, eine ausreichende Freistellung gesetzlich festzulegen.

Einwände, die auf die hierdurch entstehenden Kosten oder auf angebliche Fehlentwicklungen bei der Freistellung für Personalratsarbeit hinweisen, überzeugen mich in diesem Zusammenhang nicht. Der Datenschutzbeauftragte handelt für seine Behörde. Datenschutzprobleme, die er aufarbeitet, würden selbstverständlich auch dann auftreten, wenn sich kein Datenschutzbeauftragter ihrer annähme, sie müssten dann in anderen Organisationseinheiten geklärt werden. Mit einem Mitglied der Personalvertretung ist der Datenschutzbeauftragte nicht vergleichbar. Anders als die Personalvertretung hat er die gesetzliche Aufgabe, seine Dienststelle zu unterstützen. Er arbeitet mit ihr zusammen an der Erledigung einer gemeinsamen Aufgabe. Aus diesem Aufgabenverständnis ergibt sich, dass auch die Behörde, die den Datenschutzbeauftragten bestellt hat, ihn wiederum bei seiner Aufgabenwahrnehmung unterstützen muss. Sie muss ihn insbesondere über ihre Vorhaben der automatisierten Datenverarbeitung unterrichten, damit er seinem Beratungsauftrag nachkommen kann. Die Unterstützungs- sowie die Unterrichtungspflicht sollten gesetzlich geregelt werden.

4. Datenschutzkontrolle der Personalvertretung

Schließlich ist eine Regelung zur Kontrollbefugnis gegenüber der Personalvertretung notwendig. Das Bundesarbeitsgericht hat mit Beschluss vom 11. November 1997 - 1 ABR 21/97 - NJW 1998, 2466 - entschieden, dass der Betriebsrat nicht der Kontrolle durch betriebliche Datenschutzbeauftragte unterliegt. Ein solches Kontrollrecht müsse gesetzlich ausdrücklich geregelt werden. Für den Bereich der Personalvertretung ist die Frage bislang nicht höchstrichterlich geklärt. Ich habe dazu in meinem XII. Tätigkeitsbericht (15.3) die Auffassung vertreten, dass eine Kontrolle durch behördliche Datenschutzbeauftragte (nur) in Betracht kommt, soweit sie die eigenständige Aufgabenstellung der Personalvertretung unberührt lässt. Überträgt man die Grundsätze der BAG-Entscheidung auf den Personalrat, so kann an dieser Einschätzung nicht länger festgehalten werden. Eine gesetzliche Regelung ist deshalb geboten.

5. Verarbeitung besonders sensibler Daten

Art. 8 der EU-Datenschutzrichtlinie untersagt die Verarbeitung von Daten über rassische und ethnische Herkunft, politische Meinungen, religiöse oder

philosophische Überzeugungen, Gewerkschaftszugehörigkeit oder Sexualleben. Von dem grundsätzlichen Verbot werden jedoch zahlreiche Ausnahmen zugelassen.

Das Innenministerium geht in Übereinstimmung mit der Richtlinie zutreffend davon aus, dass schon nach der geltenden Rechtslage die Verarbeitung dieser Daten nicht auf die allgemeinen Vorschriften des NDSG gestützt werden kann, sondern bereichsspezifische Befugnisnormen erfordert. Solche fehlen in Niedersachsen im Gesundheitsbereich. Für die Rechtsanwender ist aus dem Wortlaut des NDSG nicht erkennbar, dass es für die Verarbeitung dieser Daten einer besonderen Rechtsgrundlage bedarf. Ich habe deshalb eine klarstellende Regelung gefordert. Hierfür sieht das Innenministerium jedoch keine rechtliche Notwendigkeit.

Für den Fall einer Einwilligung in die Verarbeitung der genannten Daten verlangt Art. 8 der Richtlinie eine „ausdrückliche" Einwilligung. Während im Übrigen eine Einwilligung je nach den Umständen auch konkludent erfolgen kann, reicht dies bezüglich der hier in Rede stehenden Daten nicht aus. Eine entsprechende Regelung im NDSG ist deshalb unerlässlich.

6. Landesbeauftragter für den Datenschutz

Mit Wirkung vom 1. Februar 1992 hat die Landesregierung den LfD zur Aufsichtsbehörde im nichtöffentlichen Bereich bestimmt. Anders als bei der Aufgabenwahrnehmung im öffentlichen Bereich unterliegt der LfD nach § 22 Abs. 6 Satz 2 NDSG als Aufsichtsbehörde der Fachaufsicht der Landesregierung. Diese Regelung ist mit der EU-Datenschutzrichtlinie nicht vereinbar. Art. 28 der Richtlinie verlangt, dass die Kontrollstellen, die die Regelungen zur Umsetzung der Richtlinie zu überwachen haben, ihre Aufgaben „in völliger Unabhängigkeit" wahrnehmen. In den Erwägungsgründen zur Richtlinie wird diese Unabhängigkeit als wesentliches Element der Datenschutzaufsicht bezeichnet. Eine Bindung der Aufsichtsbehörde an Weisungen vorgesetzter Stellen sowie eine Einflussnahme auf ihre Meinungsbildung und ihr Handeln nach außen sind damit unzulässig. Ich habe deshalb verlangt, anstelle der bisherigen Fachaufsicht eine Rechtsaufsicht vorzusehen. Das Innenministerium, das zurzeit oberste Aufsichtsbehörde für den nichtöffentlichen Bereich ist, lehnt eine solche Rechtsänderung ab. Es versteht die von der Richtlinie geforderte Unabhängigkeit der Aufsichtsbehörde in der Weise, dass damit nur eine Unabhängigkeit von den zu kontrollierenden nichtöffentlichen Stellen gemeint sei. Zum Teil wird diese Auffassung auch von anderen Bundesländern vertreten. Ebenso wie Niedersachsen verweisen sie darauf, dass diese Auffassung von Länderseite bereits im Verfahren zur Erarbeitung der Richtlinie vorgetragen worden sei. Demgegenüber ist hervorzuheben, dass Kommission und Rat diese Position gerade nicht übernommen, vielmehr durch die Verstärkung der Formulierung („in völliger Unabhängigkeit") deutlich gemacht haben, dass eine bloße Unabhängigkeit von der zu kontrollierenden Stelle nicnt ausreichen soll.

Bislang haben - außer Niedersachsen - fünf Bundesländer die Datenschutzaufsicht im nichtöffentlichen Bereich den Landesbeauftragten für den Datenschutz übertragen. Soweit dies geschehen ist, findet jedoch eine Fachaufsicht nicht statt.

Störend auf die Aufgabenwahrnehmung wirkt sich im Übrigen die derzeitige Teilung der Zuständigkeiten im nichtöffentlichen Bereich zwischen dem Innenministerium und mir aus. Wie schon dargestellt ist nach der derzeitigen Konstruktion der LfD Aufsichtsbehörde und das Innenministerium oberste Aufsichtsbehörde. Von der rechtlich problematischen Frage der Fachaufsicht abgesehen, führt diese Aufteilung in der praktischen Arbeit zu Erschwernis-

sen und Doppelarbeit und zieht einen erheblichen Abstimmungsaufwand nach sich (z. B. bei Anfragen anderer Aufsichtsbehörden). Viele Fragen der praktischen Aufsichtstätigkeit und aktuelle datenschutzrechtliche Probleme aus dem nichtöffentlichen Bereich werden zwischen den Ländern im so genannten Düsseldorfer Kreis erörtert und abgestimmt, in dem das Innenministerium Sitz und Stimme hat, nicht aber der LfD. Zur Vorbereitung der Sitzungen wie in deren Nachbereitung sind daher umfangreiche gegenseitige Unterrichtungen und Zuarbeiten zwischen Innenministerium und meiner Geschäftsstelle erforderlich. Umzusetzen hat die Ergebnisse dann ohnehin der LfD. Eine sachgerechte Differenzierung der Aufgaben zwischen einer obersten und einer dieser nachgeordneten Aufsichtsbehörde bei der Datenschutzaufsicht im nichtöffentlichen Bereich ist praktisch kaum möglich und auch nicht vernünftig; sie folgt allein der Scheinlogik eines abstrakten Aufbauprinzips. Dass dieses Prinzip hier nicht passt, ergibt sich schon daraus, dass beide Aufsichtsinstanzen derselben Ebene angehören, nämlich der Ministerialebene. Sinnvoller wäre es, in Niedersachsen dieselbe Lösung zu wählen wie in allen anderen Ländern, in denen der LfD auch für den nichtöffentlichen Bereich zuständig ist: Dort ist nur eine Aufsichtsebene durch Übertragung der Aufgaben auf den jeweiligen LfD geschaffen worden. Die Funktion des Innenministeriums beschränkt sich dort auf die Wahrnehmung der Aufgaben einer obersten Landesbehörde, d.h. es nimmt die ministeriellen Aufgaben der Vorbereitung und Begleitung von einschlägigen Rechtsetzungsvorhaben im Lande wie - über den Bundesrat - auf Bundesebene wahr. Ich plädiere dringend dafür, diese Aufteilung der Zuständigkeiten auch für Niedersachsen zu übernehmen. Die anstehende Novellierung des NDSG gibt dafür eine gute Gelegenheit, zumal dann auch das Problem der nach der EU-Datenschutz-Richtlinie unzulässigen Fachaufsicht praktisch gelöst wäre.

Mein verändertes Aufgabenverständnis macht es notwendig, die Öffentlichkeitsarbeit erheblich zu verstärken (vgl. 4.3). Ich halte es für unerlässlich, dass sich der LfD in öffentliche Diskussionen zu Datenschutzfragen einschaltet, auf problematische Entwicklungen hinweist, Hinweise und Ratschläge zum Umgang von Behörden und privaten Stellen mit personenbezogenen Daten gibt. Das NDSG spricht die Aufklärungsfunktion bisher für den öffentlichen Bereich nur am Rande, für den nichtöffentlichen Bereich überhaupt nicht an. Ich habe deshalb eine Ergänzung des Gesetzes dahingehend gefordert, dass der LfD den Landtag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes im öffentlichen und nichtöffentlichen Bereich unterrichtet. Dies ist auch unter dem Gesichtspunkt angebracht, dass mit einer solchen Regelung rechtliche Probleme bei Warnungen vor konkreten Datenverarbeitungsvorhaben vermieden werden können. So hat z. B. im Verwaltungsrechtsstreit der Firma Tele-Info gegen den Bundesbeauftragten für den Datenschutz, der sich kritisch zum Vertrieb der Elektronischen Häuser- und Gebäudedatei dieser Firma (vgl. 36.1) geäußert hatte, auch die Frage zur Befugnis des BfD zu seiner Kritik eine Rolle gespielt.

3.4 Informationsfreiheit und Datenschutz zusammenführen

Bei dem Zugriff auf behördliche Informationen ging das deutsche Recht bisher von dem Prinzip der beschränkten Aktenöffentlichkeit aus, das Akteneinsichtsrechte immer nur an ein bestimmtes Verwaltungsverfahren anknüpfte. So gesteht § 29 VwVfG nur den Verfahrensbeteiligten ein Akteneinsichtsrecht zu und verlangt den Nachweis eines rechtlichen Interesses. Im Planfeststellungsverfahren wird zwar einerseits der Kreis der Einsichtsberechtigten auf alle erweitert, die ein berechtigtes Interesse darlegen können, andererseits wird aber der Einsichtsanspruch auf einen Anspruch auf ermessensfehlerfreie Entscheidung reduziert.

Weitergehende Regelungen finden sich insofern im atom- und immissionsschutzrechtlichen Genehmigungsverfahren, als dort kein besonderes persönliches Interesse nachgewiesen werden muss; aber auch hier besteht nur ein Anspruch auf ermessenfehlerfreie Entscheidung, der zudem auch nur auf die Dauer des Genehmigungsverfahrens beschränkt ist. Im Kern dieser Regelungen geht es daher nicht um die Herstellung von Aktenöffentlichkeit, sondern um die Möglichkeit, die Durchsetzung von Individualinteressen zu sichern und damit unmittelbar auf eine bestimmte Verwaltungsentscheidung hinzuwirken.

Einen anderen Ansatz verfolgt das Umweltinformationsgesetz vom 8. Juli 1994, das die E(W)G-Richtlinie über den freien Zugang zu Informationen über die Umwelt vom 7. Juni 1990 umsetzt: Hier ist ein Jedermann-Recht auf Informationszugang geschaffen worden, das weder den Nachweis eines besonderen persönlichen Interesses noch die Anbindung an ein konkretes Verwaltungsverfahren voraussetzt. Der grundsätzlich freie Zugang aller Bürgerinnen und Bürger zu den behördlichen Umweltinformationen verfolgt im Prinzip drei Ziele:

- verstärkte Kontrolle der Verwaltungstätigkeit
- bessere Informationsgrundlagen für behördliche Entscheidungen als Ergebnis eines verbesserten Dialogs mit interessierten Bürgerinnen und Bürgern sowie Verbänden
- höhere Akzeptanz der Verwaltungsentscheidung.

Anders als bei der Gewährung von Akteneinsicht im herkömmlichen Sinne geht es hier also vorrangig nicht um die Wahrung eines individuellen Rechtsschutzinteresses, sondern um die Förderung öffentlicher Interessen. Das Umweltinformationsgesetz macht sich „das Informationsbedürfnis der Bürger, sei dieses nun altruistischer oder auch egoistischer Natur, zunutze, um letztlich die Richtigkeit, Effizienz und Legitimität des Verwaltungshandelns sicherzustellen“ (König, DÖV 2000, S. 45, 50).

Diese Zielsetzung ist aber über den Umweltbereich hinaus für die Verwaltung insgesamt nutzbar zu machen. Sie entspricht im Übrigen dem gemeinschaftsrechtlichen Ansatz, die Bürgerinnen und Bürger zur Unterstützung des demokratischen Prozesses in die dezentrale Vollzugskontrolle der Verwaltung einzubeziehen.

Die beschriebene Zielsetzung trifft sich auch mit einem Ansatz, der seit der Diskussion im Jahre 1997 im Sonderausschuss „Verfassungsreform“ des Schleswig-Holsteinischen Landtages und auf der Staatsrechtslehrertagung desselben Jahres zum Thema „Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung“ unter dem Stichwort „Teilhabe an der Informationsgesellschaft“ zunehmend Gefolgschaft gefunden hat. Immer mehr setzt sich die Einsicht durch, dass die klassische abwehrrechtliche Funktion der Informationsfreiheit (Art. 5 Abs. 1 Satz 1 Halbsatz 2 GG) durch eine objektiv-rechtliche Dimension ergänzt werden muss, die den Gesetzgeber von Verfassung wegen zur Herstellung von mehr Verwaltungsöffentlichkeit verpflichtet. Eine im Ergebnis vergleichbare perspektivische Erweiterung ist auch für das aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG abgeleitete Recht auf informationelle Selbstbestimmung geboten: Auch hier reicht unter den Bedingungen der modernen Informations- und Wissensgesellschaft eine Ausprägung als Schutz- und Abwehrrecht nicht mehr aus, sondern erfordert als Korrelat und gleichberechtigte Ergänzung ein allgemeines Informationszugangsrecht als Teilhaberecht. Die soziale Stellung und der Erfolg der Bürgerinnen und Bürger in ihrem ökonomischen Handeln wird zunehmend davon abhängen, dass sie einerseits Kompetenz gewinnen in der Beherrschung der modernen Informations- und Kommunikationstechniken und dass sie andererseits aber auch Zugang haben zu den für sie bedeutsamen Informationen. Dabei gewinnen die Informationen, die bei öffentlichen Stellen vorhanden sind, immer mehr an

Bedeutung, weil viele Informationen nur dort vorgehalten werden, der Staat oder seine Untergliederungen also gewissermaßen ein Informationsmonopol haben. Die Forderung nach einem erweiterten Zugangsrecht ergibt sich darüber hinaus auch aus Ansätzen der aktuellen Diskussion zur Staatsmodernisierung, die auf eine Ausweitung der bürgerschaftlichen Teilhabe an Planungs- und Entscheidungsprozessen, auf den Einsatz von marktwirtschaftlichen Elementen im Verhältnis Bürger / Verwaltung und auf eine neue Verantwortungsteilung zwischen Staat und Gesellschaft ausgerichtet sind.

Nachdem Brandenburg als erstes Bundesland im März 1998 in Umsetzung des dort in der Verfassung verankerten Grundrechts auf Informationszugang sein Akteneinsichts- und Informationszugangsgesetz verabschiedet hat (GVBl. Brandenburg 1998 I, S. 46), mit dem jeder Bürgerin/jedem Bürger ein gerichtlich durchsetzbarer Anspruch auf Informationszugang gewährt wird, haben mittlerweile auch Schleswig-Holstein (GVBl. Schleswig-Holstein 2000, S. 166) und Berlin (GVBl. Berlin 1999, S. 561) entsprechende Landesgesetze erlassen. In Hessen und in Bremen sind Gesetzentwürfe in der parlamentarischen Beratung bzw. im Ressortabstimmungsverfahren. Der Bund will seinerseits das in der Koalitionsvereinbarung vom 20. Oktober 1998 vorgesehene Informationsfreiheitsgesetz nunmehr für den Bereich der Bundesverwaltung umsetzen und allen Bürgerinnen und Bürgern prinzipiell das Recht auf freien Zugang zu Akten und Daten der Behörden einräumen, auch wenn sie nicht direkt betroffen sind. Leider haben sich die Länder im März 2000 im Rahmen einer Beschlussfassung der Innenministerkonferenz dem Weg eines auch die Länderverwaltungen bindenden Gesetzes versagt, sodass nunmehr eine auch für die Bürgerinnen und Bürger höchst unerfreuliche und für sie überhaupt nicht nachvollziehbare Uneinheitlichkeit beim Zugang zu behördlichen Informationen absehbar ist.

Die Abwehrhaltung der Länder ist umso bedauerlicher, als in fast allen anderen Mitgliedstaaten der EU den Bürgerinnen und Bürgern Informationszugangsrechte eingeräumt sind. Neben den skandinavischen Ländern, die in Europa Vorreiter waren, haben auch Frankreich, Spanien, Portugal, die Niederlande, Griechenland, Italien, Belgien, Österreich und Irland entsprechende Regelungen geschaffen; in Großbritannien liegt ein Gesetzentwurf der Regierung vor, der bald verabschiedet werden soll. Die EU hat für sich selbst den Zugang zu ihren Dokumenten in Art. 255 EGV erneut verankert. Auch der Entwurf der Charta der Grundrechte der EU enthält in Artikel 42 ein Recht der Unionsbürgerinnen und Unionsbürger sowie jeder natürlichen oder juristischen Person mit Wohn- oder Geschäftssitz in einem Mitgliedsstaat auf Zugang zu den Dokumenten des Europäischen Parlaments, des Rates und der Kommission. Man kann bei dieser Sachlage ohne Übertreibung feststellen, dass sich in der EU ein allgemeines Prinzip der Aktenöffentlichkeit und des freien Zugangs zu behördlichen Informationen als Standard herausgebildet hat. Mit ihrem Grünbuch über die Informationen des öffentlichen Sektors in der Informationsgesellschaft („Greenbook on Public Sector Information", KOM (98) 585 endg.; Ratsdok. 5580/99) hat die Europäische Kommission eine umfassende Diskussion über eine Erweiterung der Zugangsrechte zu öffentlichen Informationen eingeleitet und ihren Willen deutlich gemacht, zur Unterstützung des demokratischen Prozesses den fast überall erreichten Standard noch zu erweitern (die durch das Grünbuch angestoßene Diskussion mit den einzelnen Stellungnahmen kann im Internet unter http://www.echo.lu/legal/en/acesss.html verfolgt werden). Insgesamt ergibt sich hieraus für die Situation im deutschen Rechtsraum ein Harmonisierungs- und Anpassungsdruck, dem sich die Länder nicht länger widersetzen sollten.

Die angeführten Gegenargumente sind bekannt: Im Hinblick auf schützenswerte Rechte und Daten Dritter müssten zu viele Ausnahmen vom freien Informationszugang gemacht werden, das Herausfiltern dieser schützenwerten Daten verursache einen unvertretbaren Aufwand, die Verwaltungen würden durch eine

Häufung von Auskunftsersuchen lahmgelegt und an ihrer eigentlichen Arbeit gehindert.

Keines dieser Gegenargumente ist aber wirklich stichhaltig und geeignet, einen deutschen Sonderweg beim Zugang der Bürgerinnen und Bürger zu behördlichen Informationen dauerhaft zu rechtfertigen. Die langjährigen Erfahrungen in allen europäischen Ländern mit Informationszugangsrechten der Bürgerinnen und Bürger, die Erkenntnisse aus der Anwendung des seit 1994 in Deutschland geltenden Umweltinformationsgesetzes, nicht zuletzt aber auch die praktischen Erfahrungen in Brandenburg, wo immerhin seit über zwei Jahren das Akteneinsichts- und Informationszugangsgesetz in Kraft ist, belegen, dass Überforderungen oder gar Lähmungen der Verwaltungen nicht eingetreten sind. Dass der ohne Zweifel bestehende Zielkonflikt zwischen den Prinzipien des freien Informationszugangs und des Schutzes von Geheimnissen und personenbezogenen Daten regelungstechnisch beherrschbar ist und hier sachgerechte Grenzziehungen gefunden werden können, zeigen die einschlägigen Vorschriften in den europäischen Nachbarländern, aber auch die ganz aktuellen und dem deutschen Rechtskreis verpflichteten Lösungen in den Informationszugangsgesetzen von Brandenburg, Schleswig-Holstein und zuletzt Berlin. Die in diesen Ländern geführte Diskussion belegt auch, dass der Datenschutz nicht mehr als pauschales Abwehrargument gegen die Schaffung von Informationszugangsrechten benutzt werden kann. Für die Auflösung von im Einzelfall bei der praktischen Anwendung noch verbleibenden Konfliktsituationen zwischen Daten- und Geheimnisschutz einerseits und freiem Informationszugang andererseits drängt sich eine Übernahme des Lösungsansatzes auf, der nach dem Vorbild der Regelung in einigen kanadischen Provinzen in den genannten drei Bundesländern gewählt worden ist: die Einsetzung des Landesbeauftragten für Datenschutz als Schlichtungsinstanz. Da diese Einrichtung kraft Amtsauftrages dem Schutz personenbezogener Daten und von Geheimhaltungsinteressen in besonderer Weise verpflichtet ist, ist sie auch wie keine andere dazu geeignet, einen Zielkonflikt mit dem Prinzip des freien Informationszugangs, der auch nach Anwendung der vom Gesetzgeber vorgegebenen Abwägungsregeln sich für die praktische Handhabung im Einzelfall noch ergeben kann, mit einer Empfehlung aufzulösen.

Ich appelliere daher sehr nachdrücklich an die politischen Entscheidungsträger in Niedersachsen, die Diskussion über die Schaffung eines Akteneinsichts- und Informationszugangsgesetzes mit Geltung für den Bereich der unmittelbaren und mittelbaren Landesverwaltung rasch aufzunehmen und unvoreingenommen zu führen. Es wäre fatal und aus meiner Sicht mit dem immer wieder bekräftigten politischen Willen zu mehr Partizipation und Bürgerbeteiligung, zu mehr Transparenz und Information im öffentlichen Sektor sowie zu einer neuen Verantwortungsteilung zwischen Staat und Gesellschaft unvereinbar, wenn dieses Handlungsfeld nicht auch in Niedersachsen umgehend besetzt wird. Der Anpassungsdruck, der von dem fast überall sonst in Europa erreichen Standard ausgeht und der durch die für den Herbst 2000 angekündigte Vorlage eines Informationsfreiheitsgesetzes der Regierungskoalition in Berlin noch einmal erhöht werden wird, wird ein Ausweichen ohnehin nicht mehr lange zulassen.

4 Der Landesbeauftragte

4.1 Geschäftsstelle

Eine sehr erfreuliche Verstärkung der Geschäftsstelle ist dadurch erreicht worden, dass zum 3. April 2000 eine Steueroberinspektorin und zum 19. Juni 2000 eine Polizeioberkommissarin jeweils für die Dauer eines Jahres an die Geschäftsstelle abgeordnet worden sind. Beide Abordnungen haben das Ziel, einer-

seits der Geschäftsstelle für die Bearbeitung von datenschutzrechtlichen Fragestellungen im Bereich Polizei bzw. Steuerverwaltung spezifisches Fach- und Praxiswissen zur Verfügung zu stellen, andererseits die betreffenden Mitarbeiterinnen durch die Tätigkeit in der Geschäftsstelle mit den Inhalten und Zielen des Datenschutzes so vertraut zu machen, dass sie nach Ende ihrer Abordnungszeit in ihren Fachbereichen als Multiplikatoren mit dazu beitragen, dass den Gesichtspunkten des Datenschutzes bei der Facharbeit mehr Gewicht gegeben wird. Ich bin sehr dankbar, dass Innenministerium und Finanzministerium bereit waren, diesen neuen Weg mitzugehen. Es ist verabredet, dass bei einer Bewährung dieses Modells, bei dem sich bereits jetzt sehr deutliche positive Auswirkungen zeigen, die Abordnungen mit anderen Personen fortgesetzt werden. Eine Ausweitung dieses Modells auf andere Bereiche (z. B. Soziales, Gesundheit) wäre aus meiner Sicht sehr zu begrüßen.

Eine weitere wichtige Verstärkung ist durch die Besetzung einer Sachbearbeiterstelle zum 1. September 2000 erreicht worden.

Die genannten Kapazitätserweiterungen haben es ermöglicht, die interne Geschäftsverteilung neu zu ordnen und dabei das Arbeitsgebiet, in dem die Datenschutzaufsicht über den nichtöffentlichen Bereich geführt wird, um zwei Sachbearbeiter zu verstärken. Hierdurch kann nun endlich die seit langem angestrebte intensivere datenschutzrechtliche Betreuung und Beratung der Wirtschaft eingeleitet werden. Der dafür bestehende dringende Handlungsbedarf ist immer wieder dargelegt worden.

In Umsetzung des Leitbildes (vgl. 4.2) sind die Schwerpunkte der Arbeit der Geschäftsstelle in einem Jahresarbeitsprogramm abgebildet, das in vierteljährlichem Abstand fortgeschrieben wird. Bestandteil dieses Jahresarbeitsprogramms sind insbesondere solche Vorhaben, die neben dem Tagesgeschäft als Projekte geführt werden. Für diese Projekte werden in Form von Zielvereinbarungen die Ziele, der Ressourcenverbrauch (Zeitbedarf in Arbeitstagen, Haushaltsmittel, externe Unterstützung) und die Verantwortlichkeiten festgelegt.

Im nächsten Jahr sollen die eingeleiteten Veränderungen in der inneren Organisation der Geschäftsstelle (Einrichtung von vier Arbeitsgebieten und eines Verwaltungssekretariats) und in den Arbeitsabläufen verstärkt durch Maßnahmen der Personalentwicklung ergänzt werden. Dies ist auch deshalb geboten, weil auf vielen Dienstposten der Geschäftsstelle ein Personalwechsel stattgefunden hat, der sehr zu einer „Auffrischung" beigetragen hat. Die erforderliche kontinuierliche Begleitung durch in der Landesverwaltung vorhandene Personalentwicklungsberaterinnen bzw. -berater ist gesichert.

Die technische Ausstattung der Geschäftsstelle ist weiter ergänzt, der Aufbau des IT-Labors fortgeführt worden. Besondere Bedeutung hatte in den letzten Monaten die Installierung einer Firewall mit der das interne Netz der Geschäftsstelle zusätzlich zu den im iznNet geschaffenen Sicherungen gegen Angriffe von außen abgeschirmt wird.

Die informationstechnische Kompetenz der Mitarbeiterinnen und Mitarbeiter konnte durch gezielte zum Teil interne, zum Teil externe Fortbildungs- und Schulungsmaßnahmen verbessert werden. Um die aufgezeigten Entwicklungen im Bereich der Wirtschaft wie im Bereich der öffentlichen Verwaltung sachgerecht aus Datenschutzsicht begleiten und beurteilen zu können, ist es unerlässlich, dass alle Angehörigen der Geschäftsstelle ihr Wissen laufend auf dem Stand der Technik halten.

4.2 Leitbild und Aufgabenverständnis

Unter 3.1 ist bereits ausführlich dargelegt worden, dass Datenschutzaufsicht im Internet-Zeitalter sich nicht mehr nur auf die Wahrnehmung klassischer Kontrollaufgaben und die „nachsorgende" Aufdeckung von Datenschutzverstößen beschränken kann, sondern sich sehr viel stärker als früher im Vorfeld durch Beratung und Mitgestaltung um eine datenschutzgerechte Technikgestaltung und um datenschutzfreundliche Verfahren bemühen muss. Dies gilt in gleicher Weise gegenüber der öffentlichen Verwaltung wie gegenüber der Wirtschaft, wobei mittlerweile die größeren Gefahren für die informationelle Selbstbestimmung der Bürgerinnen und Bürger von dem „Datenhunger" der gewerblichen Wirtschaft und von der häufig unzureichend geschützten Kommunikation über das Internet ausgehen. Deshalb hat auch die Aufklärung der Betroffenen über solche Gefahren einen sehr viel höheren Stellenwert als früher.

Nach meiner Amtsübernahme am 1. Juni 1999 habe ich einen intensiven Diskussionsprozess mit allen Mitarbeiterinnen und Mitarbeitern der Geschäftsstelle initiiert, bei dem überprüft werden sollte, inwieweit Aufgabenverständnis, strategische Ausrichtung, Vorgehensweise und Instrumentarium den genannten Anforderungen entsprechen und welche Veränderungen notwendig sind. Als Ergebnis dieses Diskussionsprozesses ist das folgende Leitbild entwickelt worden:

Datenschutz ist Grundrechtsschutz:	
Standortbestimmung	Das Grundrecht auf informationelle Selbstbestimmung - der Datenschutz - ist Teil der Würde und Persönlichkeit des Menschen und zugleich elementare Funktionsbedingung eines freiheitlich-demokratischen Gemeinwesens. Es sichert das Recht des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen er seine persönlichen Lebensumstände offenbart. Ergänzt wird dieses Grundrecht durch das Recht auf Informationsfreiheit, das die politische Teilhabe des Einzelnen an der Gemeinschaft sichert und damit ebenso wie das Recht auf informationelle Selbstbestimmung Bestandteil einer aufgrundrechtsverwirklichung abzielenden politischen Ordnung ist.
Kernaufgabe	Unser Auftrag ist es, die informationelle Selbstbestimmung und ihre Beachtung im Gemeinwesen einzufordern.
Dafür treten wir ein:	
Anwalt des Bürgers	Wir vertreten als unabhängige Stelle die Interessen der Bürgerinnen und Bürger bei der Verarbeitung ihrer Daten durch Staat und Wirtschaft.
Datenschutz mit Augenmaß	Wir betrachten den Datenschutz nicht isoliert, sondern in Abwägung mit den sonstigen Interessen der Bürgerinnen und Bürger und den anerkannten Zielen der Gemeinschaft. Wir räumen dem Recht auf informationelle Selbstbestimmung im Zweifel den höheren Rang ein.
keine Bevormundung	Wir informieren intensiv über die Möglichkeiten, sich durch eigenes Zutun gegen einen Missbrauch seiner Daten zu schützen. Wir respektieren aber die Entscheidungssouveränität jedes Einzelnen und drängen keine überzogene staatliche „Fürsorge" auf.

Aufgeschlossen für neue Technologien	Wir treten dafür ein, dass der Einsatz der Technik nach dem geltenden Recht erfolgt und dass rechtliche Bestimmungen auch zeitnah technische Entwicklungen berücksichtigen. Wir sind neuen Entwicklungen gegenüber offen und setzen uns mit dem technischen und gesellschaftlichen Wandel auseinander. Wir unterstützen die Entwicklung datenschutzfreundlicher Technologien; Datensparsamkeit und Datenvermeidung sind der beste Datenschutz.
Kompetenter Ansprechpartner:	
Überzeugung, Konfliktfähigkeit	Wir versuchen zu überzeugen und einvernehmliche Lösungen zu finden, sind im Konfliktfall aber auch bereit, datenschutzgerechtes Handeln gegen Widerstände durchzusetzen.
Gestaltung, Beratung, Kontrolle	Wir gestalten den Umgang mit personenbezogenen Daten in der Gesellschaft intensiv mit. Wir beraten Betroffene über Gefährdungen und Rechte sowie Privatwirtschaft und öffentliche Verwaltung über erforderliche Regelungen und Maßnahmen, auch im Hinblick auf Datensparsamkeit und Datenvermeidung. Wir kontrollieren wirkungsvoll die Einhaltung von Datenschutzvorschriften.
Öffentlichkeit, aktivierender Datenschutz	Wir informieren Bürgerinnen und Bürger, Verwaltung und Wirtschaft sowie die Medien aktuell über unsere Erfahrungen, Forderungen und Empfehlungen. Wir unterstützen Bürgerinnen und Bürger sowie Institutionen dabei, sich selbst für den Datenschutz zu engagieren.
Moderne Geschäftsstelle	Wir verstehen uns als kompetente Ansprechpartner für Datenschutz und Datensicherheit, dessen Dienstleistung gern in Anspruch genommen werden soll. Unsere Aufgaben erfüllen wir fachkundig, seriös, schnell, freundlich und wirtschaftlich. Vertrauen und partnerschaftliche Zusammenarbeit bestimmen unser Handeln; Kritikfähigkeit gehört dazu. Wir gestalten die Arbeit in der Geschäftsstelle nach modernen Gesichtspunkten.

Seit Januar 2000 bildet dieses Leitbild für die Mitarbeiterinnen und Mitarbeiter und für mich die gemeinsame Grundlage für die Arbeit der Geschäftsstelle. Es dient als Orientierung bei der täglichen Aufgabenerledigung ebenso wie bei der Festlegung der Arbeitsschwerpunkte und Arbeitsziele im Jahresarbeitsprogramm. Die Inhalte des Leitbildes werden im Rahmen der Öffentlichkeitsarbeit intensiv nach außen kommuniziert, um auch gegenüber den unserer Aufsicht unterliegenden Stellen der öffentlichen Verwaltung, gegenüber der gewerblichen Wirtschaft und gegenüber den Bürgerinnen und Bürgern das neue Aufgabenverständnis deutlich zu machen.

Das veränderte Aufgabenverständnis hat sich in besonders deutlicher Weise in folgenden Aktivitäten niedergeschlagen:

- Im Herbst 1999 habe ich in einem Schreiben an alle Ministerinnen und Minister eine intensive und konstruktive Zusammenarbeit bei der Erarbeitung von Vorschriften mit datenschutzrechtlichen Bezügen angeboten und um eine möglichst frühzeitige Beteiligung, auch schon im Vorfeld entsprechender Vorhaben, gebeten. Bis Dezember 1999 habe ich daraufhin mit allen Ministerien auf Minister- bzw. Staatssekretärsebene Gespräche geführt, bei denen ich mein Anliegen näher erläutern konnte und weitere aktuelle Datenschutzfragen aus dem jeweiligen Ressortbereich angesprochen habe.

- Gegenüber den Unternehmen der gewerblichen Wirtschaft und ihren Verbänden sind in mehreren Veranstaltungen der neue Ansatz und das Angebot zu gemeinsamer Problemlösung erläutert worden. Die Resonanz ist außerordentlich erfreulich und ermutigend. Erste gemeinsame Projekte zu datenschutzrechtlichen Fragestellungen, etwa zum Problem der Videoüberwachung von Wohngebäuden, sind eingeleitet.

- Für den Bereich der Internet-Provider in Niedersachsen sind in Zusammenarbeit mit der IHK Hannover-Hildesheim mehrere Veranstaltungen durchgeführt worden, bei denen über die bestehenden Vorgaben des Multimediarechts sowie über die datenschutzfreundliche Ausgestaltung von Internet-Angeboten informiert worden ist (vgl. 9.1.3).

- Mit der Landeshauptstadt Hannover ist ein gemeinsames Projekt zum E-Government gestartet worden, das in Kapitel 5 unter 5.4.4 näher erläutert ist.

- In Zusammenarbeit mit dem Lehrgebiet Rechnernetze und Verteilte Systeme der Universität Hannover ist ein Selbstschutzprogramm entwickelt worden, mit dessen Hilfe jeder PC-Benutzer Sicherheitseinstellungen an seinem Gerät überprüfen kann. Die Nachfrage ist außerordentlich hoch, in den ersten vier Wochen haben 30 000 Internet-Nutzer den kostenlosen Selbsttest durchgeführt (vgl. 6.2.1).

4.3 Öffentlichkeitsarbeit

Ein wesentliches Gestaltungsfeld der Serviceorientierung meiner Geschäftsstelle ist die Presse- und Öffentlichkeitsarbeit. Sie muss zeitnah und umfassend über Erfahrungen, Empfehlungen und Forderungen des Datenschutzes berichten. Um mein Leitbild schnell und erfolgreich umzusetzen, habe ich eine interne Arbeitsgruppe „Öffentlichkeitsarbeit" mit der Neugestaltung der Presse- und Öffentlichkeitsarbeit beauftragt. Weiter wurden Experten aus den Pressereferaten der Ministerien, der Landespressekonferenz und eines Grafik- und Design-Unternehmens um Rat gefragt.

Die Arbeitsgruppe hat ein umfassendes Konzept für eine leistungsfähige und effiziente Öffentlichkeitsarbeit erstellt. Es soll das Auftreten und das Erscheinungsbild des Landesbeauftragten für den Datenschutz nach außen und nach innen in allen Facetten prägen und verbessern. Die Gesamtdokumentation steht Interessierten gern zur Verfügung. Öffentlichkeitsarbeit wird danach als Chance verstanden, Datenschutzbewusstsein in einem öffentlichen Diskurs zu wecken und gezielt zu fördern. Es erscheint möglich, auf diese Weise an der Gestaltung datenschutzfreundlicher Technologien mitzuwirken und Datenselbstschutz im privaten Bereich für Bürgerinnen und Bürger zu erreichen. Nutzer von Medienunternehmen und Medienvertreter, die bestimmte thematische Recherchen betreiben, Bürgerinnen und Bürger mit allgemeinen Informationswünschen oder mit individuellen Problemen, Interessengruppen, die als engagierte „Freaks" um Unterstützung ihrer Anliegen durch die Datenschutzaufsicht nachsuchen, sowie öffentliche Stellen und Unternehmen der Wirtschaft mit Beratungs- und Infor-

mationswünschen werden nunmehr schnell, in moderner Form und umfassend informiert und beraten.

Die Erfolge der neuen Presse- und Öffentlichkeitsarbeit bestätigen das Konzept. Mein Erfahrungsbericht „Ein Jahr im Amt" in der Landespressekonferenz am 23. August 2000 fand ein lebhaftes Echo in den Print-Medien sowie in Rundfunk und Fernsehen. Nach Verteilung meines Flyers „Ich habe doch nichts zu verbergen, aber..." sind zahlreiche Anforderungen von Datenschutz-Informationen eingegangen, die meine Geschäftsstelle wegen des gewünschten Umfangs leider nur nach und nach erfüllen kann. Die Anfragen nach Hilfen zur Selbstkontrolle, insbesondere der Abruf meiner Orientierungshilfen und Checklisten über das Internet, sind erfreulich hoch. Die Auflagenhöhe gedruckter Exemplare halte ich bewusst niedrig, um stets aktuelle Informationen „frisch aus dem Drucker" verschicken zu können. Der elektronische Abruf über meine Internet-Homepage übersteigt die Nachfrage nach Druckerzeugnissen inzwischen um ein Vielfaches.

Die Compact Disc (CD-ROM) ergänzt mein Serviceangebot und bietet den öffentlichen Stellen, Unternehmen sowie Bürgerinnen und Bürgern einen Offline-Zugang zum Datenschutzrecht und zu Datenschutzfragen in Niedersachsen. Die CD enthält eine Zusammenfassung aller datenschutzrelevanten Informationen - die Tätigkeitsberichte eingeschlossen - in digitaler Form. Mit HTML- und Hyperlink-Technik ist es einfach und komfortabel möglich, zwischen verschiedenen Informationen bzw. Informationsteilbereichen hin und her zu springen. Auch das Herunterladen von benötigten Informationen ist unproblematisch und schnell möglich. Im Berichtszeitraum sind 1000 CDs auf Anforderung verteilt worden.

Die Tradition, auf der CeBIT in Hannover - dem weltweit größten Schauplatz der Informations- und Kommunikationstechnologie - ein Datenschutz-Forum zu veranstalten, wurde 1999 und 2000 fortgesetzt. Die Themen „Datenschutz: Hemmnis oder Türöffner im Electronic Commerce?" und „Gefährdet der Datenschutz den E-Commerce zwischen Europa und USA?" fanden erneut großes Interesse. „Datenschutz darf nicht Störfaktor sein, sondern muss zur Förderung der Wirtschaft betrieben werden", war das Fazit. Die Auswahl der teilnehmenden Referenten erfolgte aus unterschiedlichen Interessengruppen, um eine kontroverse Diskussion zu erreichen. Auch zukünftig werden in dieser Themenreihe praktische, rechtliche sowie technische Aspekte berücksichtigt, um so möglichst Datenschutzexperten vieler Länder und unterschiedlicher Interessengruppen anzusprechen.

Mit der Informationsveranstaltung vom 18. Oktober 2000 „Know-how ist Know-where", in der Experten über ihre Erfahrungen beim Aufbau eines Wissensmanagements berichtet haben, habe ich eine neue Veranstaltungsreihe gestartet, die ebenfalls fortgesetzt werden soll. Hierzu lade ich Mitarbeiterinnen und Mitarbeiter der öffentlichen Verwaltung zu einem Diskurs über allgemeine Themen der Gegenwart ein, die nicht unbedingt im Focus des Datenschutzes stehen müssen.

4.4 Das virtuelle Datenschutzbüro wird real

Das „Virtuelle Datenschutzbüro" ist ein Zusammenschluss von Datenschutzaufsichtsbehörden der Bundesrepublik Deutschland, der Niederlande, der Schweiz und Kanadas. Es will die sich derzeit entwickelnden Kommunikationstechniken und -kulturen aufnehmen und für den „neuen Datenschutz" nutzbar machen. Eine Arbeitsteilung zwischen den Kooperationspartnern soll die Belastung der einzelnen Dienststellen verringern und eine Spezialisierung in den Bereichen er-

möglichen, die tiefergehend bearbeitet werden müssen. Ein verbesserter Workflow zwischen den und innerhalb der Dienststellen soll ermöglichen, dass sich Fachleute schnell und problemlos austauschen können.

Technologisch ist das virtuelle Datenschutzbüro ein Privacy-Backbone-Netz, das alle Kooperationspartner über gesicherte Netze (Virtuell Private Networks, VPN) verbindet. Alle Sicherungsmaßnahmen orientieren sich am Stand der Technik. Neue Sicherungsverfahren werden in IT-Labors der Kooperationspartner getestet. Damit soll sowohl bestehendes Recht in Technik umgesetzt als auch eine Rückkopplung der gesammelten Erfahrungen zum Gesetzgeber möglich werden. Dies trägt zur Evaluierung von Rechtsnormen bei. Sämtliche Internet-Dienste werden getestet und genutzt. Die Präsentation der Arbeitsergebnisse im World Wide Web ist selbstverständlich. Auf E-Mails von Bürgern soll schnell und kompetent reagiert werden. Sofern mangels Zuständigkeit Anfragen nicht beantwortet werden können, soll eine schnelle Weiterleitung an die zuständige Stelle erfolgen. Häufig gestellte Fragen (Frequently Asked Questions - FAQ's) werden zusammengefasst und öffentlich beantwortet. Eine Wissensdatenbank enthält das Material aus der Arbeit der Datenschutzbeauftragten mit Nachweis der jeweiligen Autoren und wird von den einstellenden Dienststellen gepflegt. Ich arbeite am Projekt des virtuellen Datenschutzbüros mit und werde meinen Beitrag zur Erprobung einer leistungsfähigen und sicheren Kommunikations-Infrastruktur zwischen Datenschutzexperten und -interessierten leisten.

5 Schwerpunkte

5.1 Videoüberwachung

Während die Videoüberwachung an Kriminalitätsschwerpunkten durch die Polizei breiten Raum in der öffentlichen und parlamentarischen Diskussion einnimmt, hat sich die Videoüberwachung durch Unternehmen und andere private Stellen (nachfolgend: nichtöffentliche Stellen) von der Öffentlichkeit häufig unbemerkt weiter ausgebreitet, geradezu wildwuchsartig, wie einige Kritiker meinen.

Gegenstand meiner Betrachtung ist hier die Beobachtung öffentlich zugänglicher Räume. Hierzu gehören nicht nur öffentliche Straßen, Wege und Plätze, sondern alle Örtlichkeiten, die von jedermann genutzt bzw. betreten werden können, also z. B. Kaufhäuser, Ladenpassagen, Verkaufsräume, Tankstellen, Schalterhallen oder auch Bahnhöfe. Soweit es um private Räumlichkeiten im engeren Sinne geht, z. B. Personalbereiche innerhalb eines Kaufhauses, berührt dies im Regelfall Fragen des Arbeitnehmerdatenschutzes, auf die ich unter 34.2 näher eingehe.

Die Einsatzfelder der Videoüberwachung durch nichtöffentliche Stellen sind nahezu unbegrenzt. Gleiches gilt für die Anzahl solcher Anlagen, die mangels entsprechender Erhebungen niemandem so recht bekannt ist. Man schätzt aber, dass in Deutschland mehr als eine halbe Million Videoüberwachungsanlagen im Einsatz sind.

Man sollte sich davor hüten, Videoüberwachung grundsätzlich zu verdammen oder als Allheilmittel zu preisen. Es kommt vielmehr immer auf den Zweck und die Umstände an. Aus zahlreichen Gesprächen, die ich zu diesem Thema insbesondere mit Anwendern geführt habe, hat sich immer wieder die bemerkenswerte Erkenntnis ergeben, dass die selbst eingesetzte Überwachung als unproblematisch und sinnvoll angesehen wird, während der Einsatz in anderen Bereichen sehr kritisch hinterfragt wird. Ein Grund hierfür ist sicher auch die mangelnde Transparenz, d. h. das Nichtwissen darum, ob jemand beispielsweise als Passant gerade von einer Videokamera erfasst wird und wer und zu welchen

Zwecken diese Bilder beobachtet, speichert und auswertet - kurz: was mit diesen Bildern passiert und in welchem (möglicherweise ganz anderem) Zusammenhang sie wieder auftauchen können.

Dieser mangelnden tatsächlichen Transparenz steht derzeit leider eine ebenso unklare Rechtslage gegenüber. Das für nichtöffentliche Stellen maßgebliche Bundesdatenschutzgesetz (BDSG) enthält noch keine Regelung zur Videoüberwachung, sodass erhebliche Rechtsunsicherheiten sowohl bei Anwendern als auch bei Betroffenen bestehen. Der dringende gesetzgeberische Handlungsbedarf ist auch von der Bundesregierung erkannt worden, die am 14. Juni 2000 einen Gesetzentwurf zur Novellierung des BDSG beschlossen und in die parlamentarische Beratung eingebracht hat (vgl. 3.2).

Der Entwurf der BDSG-Novellierung sieht folgende Regelung zur Videoüberwachung vor:

„§ 6 b

Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit dies zur Aufgabenerfüllung, zur Wahrnehmung des Hausrechts oder zur Erfüllung eigener Geschäftszwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Speicherung von nach Absatz 1 erhobenen Daten ist zulässig, wenn dies zum Erreichen des verfolgten Zwecks erforderlich ist.

(4) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen."

Bevor ich im Folgenden auf einige Beispiele eingehe, stellt sich an dieser Stelle natürlich die Frage, was an der Videoüberwachung denn - etwas überspitzt formuliert - so schlimm sein soll.

Zunächst einmal stellt jede Form der Beobachtung persönlichen Verhaltens durch Kameras einen Eingriff in das verfassungsmäßig geschützte allgemeine Persönlichkeitsrecht dar. Das Recht auf informationelle Selbstbestimmung als Teil dieses Persönlichkeitsrechts gewährt jedem Menschen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen; hierzu gehört auch die Abbildung seines Äußeren und seines Verhaltens.

Dieser Grundsatz wird durch die Videoüberwachung (und durch den Einsatz sonstiger optisch-elektronischer Aufnahmetechnik, auf die ich an späterer Stelle noch eingehen werde) im Wesentlichen in zweierlei Hinsicht eingeschränkt:

Erstens konnte bisher jedermann, soweit er sich in der Öffentlichkeit zugänglichen Räumen bewegt hat, abschätzen, welcher Kreis von Personen diesen Umstand wahrnehmen kann. Es macht nun aber einen erheblichen Unterschied, ob 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, nur von denjenigen wahrgenommen werden kann, die sich in der unmittelbaren Umgebung aufhalten, oder ob diese Situation von (tatsächlich vorhandenen oder nur vermeintlichen) Kameras erfasst wird. In

diesem Fall ist überhaupt nicht mehr erkennbar oder auch nur abschätzbar, wer alles Kenntnis nimmt oder nehmen kann, wer die Bilder zu welchem Zweck betrachtet und ggf. weiterverarbeitet. Insoweit ist das an dieser Stelle gern benutzte Argument nicht überzeugend, dass, wer sich in die Öffentlichkeit begebe, auch in Kauf nehmen müsse, von ihr wahrgenommen zu werden. Öffentlichkeit hat in den beiden Fallgestaltungen eine ganz unterschiedliche Qualität.

Zweitens kann die bloße Vermutung, man könnte gerade in diesem Augenblick von einer Kamera beobachtet werden, zu einem permanenten Anpassungsdruck führen: Wer nicht weiß, ob und ggf. von wem und zu welchem Zweck er beobachtet wird, verliert seine Unbefangenheit und wird sich im Zweifel vorsorglich auf diese Überwachungssituation einstellen, und zwar unabhängig davon, ob diese tatsächlich besteht oder nur vermutet wird. Diese Situation ist ein wenig vergleichbar mit der der vorsorglichen Selbstzensur (die berühmte „Schere im Kopf"), die eine tatsächliche Zensur überflüssig macht.

Dies soll nicht belegen, dass Videoüberwachung grundsätzlich von Übel sei. Diese Auffassung vertrete ich auch nicht. Es soll aber deutlich werden, dass diese Form des Beobachtetwerdens einen - im Einzelfall zulässigen oder unzulässigen - Grundrechtseingriff darstellt.

5.1.1 Videoüberwachung an Häusern und Wohnanlagen

Speziell bei größeren Wohnanlagen werden zur Beobachtung der Haustür und des umliegenden Eingangsbereichs zunehmend Videokameras eingesetzt, deren Bilder - je nach Ausgestaltung - vom Eigentümer bzw. seinem Verantwortlichen, vom jeweiligen Hausbewohner oder sogar von allen Hausbewohnern abgerufen werden können. Dieser Trend dürfte sich schon allein deswegen fortsetzen, weil die hierfür erforderliche Technik bei steigender Leistungsfähigkeit immer preisgünstiger wird und diese Verfahren neben den Sicherheitsinteressen auch den Komfortansprüchen von Bewohnern offensichtlich sehr entgegenkommen. Aufmerksam geworden bin ich auf diesen Komplex insbesondere durch ein auch in Niedersachsen eingesetztes System, das die am Eingangsbereich aufgenommenen Kamerabilder der Überwachungsanlage in das hauseigene Fernsehkabelnetz einspeist, die so von jedem Bewohner über sein Fernsehgerät abgerufen werden können. Ich bewerte dieses Verfahren als äußerst fragwürdig, da jeder Hausbewohner auf diese Weise bequem vom Fernsehsessel aus beobachten kann, wann, in welchem Zustand und in Begleitung welcher Personen die Nachbarn im Haus ein- und ausgehen bzw. von wem sie wie lange Besuch erhalten. Dass diese Bilder problemlos dann auch noch mit dem Videorecorder aufgezeichnet und damit dauerhaft „gesichert" werden können, kommt noch hinzu.

Trotz der eingangs dargestellten Rechtsunsicherheiten, jedenfalls bis zum In-Kraft-Treten des novellierten BDSG, erschien es mir sinnvoll und richtig, das Thema schon im Vorfeld mit den Interessenvertretern von Wohnungswirtschaft und Mietern zu erörtern und im Sinne einer Beratung gemeinsame Grundregeln für die Videoüberwachung festzulegen. Die Vertreter von Wohnungswirtschaft und Mieterbund haben dieses Kooperationsangebot positiv aufgenommen.

Als vorläufiges Ergebnis der gemeinsamen Erörterungen habe ich einen Entwurf allgemeiner Hinweise zur Videoüberwachung an Häusern und Wohnanlagen vorgelegt, der derzeit Grundlage für die Diskussion in den Interessenverbänden ist. Unter dem Vorbehalt, dass sich dadurch natürlich noch Änderungen ergeben können, möchte ich meine Überlegungen an dieser Stelle kurz darstellen:

– Ob Videoüberwachung eingesetzt werden darf oder nicht, setzt im Einzelfall eine Abwägung zwischen dem Schutz des allgemeinen Persönlichkeitsrechts der Bewohner, Besucher oder anderer Betroffener und dem durch die

Videoüberwachung verfolgten Zweck (z. B. Schutz der Gesundheit der Bewohner oder des Eigentums) voraus.

– Das Motiv einer allgemeinen abstrakten Gefahrenvorsorge reicht nicht aus. Soll Videoüberwachung dagegen der konkreten Gefahrenabwehr dienen, insbesondere der Verhinderung von Straftaten oder der Vorsorge für die spätere Strafverfolgung, haben die von der Beobachtung Betroffenen dies im Regelfall hinzunehmen, wenn belegbare Tatsachen die Annahme rechtfertigen, dass derartige schwerwiegende Beeinträchtigungen drohen.

– Die Möglichkeit, die Zulässigkeit einer Videoüberwachung durch die vorherige Einwilligung aller Hausbewohner zu begründen, ist auf den ersten Blick zwar wünschenswert, hier jedoch ungeeignet, weil es schon aus tatsächlichen Gründen unmöglich sein dürfte, alle hiervon potenziell Betroffenen (also auch Besucher und Passanten) zu ihrer Einwilligung zu befragen, bevor sie in den Aufnahmebereich der Kamera geraten. Diese Einwilligungslösung, die ich in anderen Bereichen grundsätzlich favorisiere, wäre hier im Übrigen auch deshalb wenig praktikabel, da eine einmal erteilte Einwilligung jederzeit wirksam zurückgenommen werden kann. Es bleibt aber natürlich sinnvoll und auch wünschenswert, die Hausbewohner umfassend über die geplante Videoüberwachung zu informieren.

– Eine verdeckte Videoüberwachung ist in jedem Fall unzulässig.

– Grundsätzlich gilt, dass nur diejenigen Personen Zugriff auf die Kamerabilder haben sollen, die hiervon unmittelbar betroffen sind. So kann der Monitor durchaus als eine Art „elektronischer Türspion“ benutzt werden, damit sich ein Bewohner seinen Besuch vorher ansehen kann, aber eben nicht den des Nachbarn.

– Wenn die Bilder auch gespeichert werden sollen, was unter bestimmten Voraussetzungen zulässig sein kann, muss dieser Umstand für die Betroffenen klar erkennbar sein. Dies gilt auch für die Frage, zu welchen Zwecken und durch wen die Aufzeichnungen erfolgen und wie lange diese aufbewahrt werden.

5.1.2 Videoüberwachung durch die Move-GmbH und auf der EXPO 2000

Die Move-GmbH nimmt hoheitliche Aufgaben des Verkehrswarndienstes, der Verkehrsbeobachtung und der Verkehrslenkung im Land Niedersachsen wahr. Grundlage hierfür ist das Verkehrs-Informations- und Lenkungsgesetz (VILG) in Verbindung mit einem öffentlich-rechtlichen Vertrag. Im Großraum Hannover ist ein Verkehrsleitsystem installiert worden, das für einen reibungslosen Verkehr von den Autobahnen zum Messegelände sorgen soll. Videokameras unterstützen die Verkehrsbeobachtung bzw. -lenkung. Rechtzeitig zur CeBIT 2000 konnte das System in Betrieb genommen werden.

Der Einsatz von Videokameras hat hier grundsätzlich datenschutzrechtliche Relevanz. Der Schutzbereich des Grundrechts auf informationelle Selbstbestimmung erstreckt sich auf die Verarbeitung personenbezogener Daten, wozu z. B. Videopersonenbilder, aber auch personenbeziehbare Daten wie z. B. Kfz-Kennzeichen gehören. Der Hauptanwendungsfall ist jedoch der Einsatz der Videokameras zur Übertragung von Übersichtsaufnahmen. Soweit sich die Videobeobachtung auf diese reinen Übersichtsbilder über Sachen als Bestandteil von Verkehrsströmen ohne Personenbeziehbarkeit beschränkt, ist dies einer datenschutzrechtlichen Bewertung entzogen.

Etwas anderes gilt in den Fällen der Bildvergrößerung bzw. des Heranzoomens, soweit dann einzelne Personen oder Kfz-Kennzeichen erkennbar werden. Eine

solche Erfassung und ggf. Aufzeichnung und Weitergabe stellt eine Verarbeitung personenbezogener Daten dar, also einen Eingriff in das Recht auf informationelle Selbstbestimmung. Mangels Zustimmung der Betroffenen zur Abgabe ihrer Daten fordert die Rechtslage - als Folge des Gesetzesvorbehalts in Art. 2 GG - eine erlaubende Rechtsgrundlage. Eine solche Befugnis vermag ich für die Verkehrsbeobachtung bzw. -lenkung in der StVO nicht zu erkennen.

Das NDSG enthält leider bislang keine spezielle Regelung zur Videobeobachtung bzw. -überwachung (ich habe einen entsprechenden Ergänzungsvorschlag in die parlamentarische Beratung eingebracht, vgl. 3.3 und 5.1.5). Für die Zeit der Erprobung halte ich es für vertretbar, die im NDSG verankerten Leit- und Wertentscheidungen als ausreichende Legitimation hinzunehmen. Dabei ist die Move-GmbH als öffentliche Stelle anzusehen, da ihr Aufgaben der öffentlichen Verwaltung übertragen worden sind, vgl. § 2 Abs. 1 Satz 2 NDSG.

Zum Einsatz der zoomfähigen Videokameras habe ich mich daher im Vorfeld der CeBIT 2000 mit der Move-GmbH auf folgenden Rahmen geeinigt:

- Grundsätzlich erfolgt nur eine Übertragung laufender Bilder, aufgezeichnet wird nur im Ausnahmefall.
- Manuell ausgelöste Aufzeichnungen werden nur zu folgenden Zwecken vorgenommen:
  - zur eigenen haftungsrechtlichen Absicherung bei Anordnung verkehrslenkender Maßnahmen,
  - zur Prüfung der Wirksamkeit verkehrslenkender Maßnahmen (Effizienzkontrolle) und
  - zur Prüfung der Verbesserung von Verkehrsabläufen.
- Eine Übermittlung der Bildübertragung („Weiterschaltung") an andere Nutzer im gemeinsamen Netz (Polizei, Üstra AG) erfolgt nur dann, wenn es zur eigenen Aufgabenerledigung oder zur Aufgabenerledigung der empfangenden Stelle erforderlich ist.
- Programme zur automatisierten Erkennung von Personen oder Sachen werden nicht eingesetzt.

Ich habe mich zudem mit dem Niedersächsischen Ministerium für Wirtschaft, Technologie und Verkehr in Verbindung gesetzt und auf die Notwendigkeit hingewiesen, bereichsspezifische Regelungen für die Verkehrsbeobachtung bzw. -lenkung im Straßenverkehrsrecht zu schaffen. Im Mai 2000 befassten sich daraufhin der Bund-Länder-Fachausschuss für den Straßenverkehr und die Verkehrspolizei mit diesem Thema. Der Ausschuss gelangte zu der Auffassung, dass datenschutzrechtliche Belange im Verkehrsrecht nicht geregelt werden könnten. Dieses vermag ich nicht nachzuvollziehen. Ich werde mich weiterhin für eine bereichsspezifische Regelung für die Verkehrsbeobachtung bzw. -lenkung einsetzen.

Ein zweites Großereignis im Jahre 2000 war in Hannover neben der CeBIT die Weltausstellung EXPO 2000. Auch wenn es auf den ersten Blick erstaunlich erscheinen mag, so handelte es sich hierbei doch um eine Veranstaltung, die von einer privaten Firma, der „EXPO 2000 Hannover GmbH" auf einem Privatgelände durchgeführt wurde. Obwohl die Anwendbarkeit des NDSG daher für die Videoüberwachung des EXPO-Geländes nicht gegeben war, habe ich mich mit der EXPO-GmbH auf eine Regelung verständigt, die der mit der Move-GmbH getroffenen entspricht. Zusätzlich wurde an allen Eingängen zur EXPO 2000 und an vielen Gebäuden auf dem Gelände auf die Videoüberwachung hingewiesen.

5.1.3 Videoüberwachung in öffentlichen Verkehrsmitteln

Der Verband Deutscher Verkehrsunternehmen, der die Unternehmen des öffentlichen Personennahverkehrs vertritt, hatte sich an die Datenschutzbeauftragten von Bund und Ländern mit dem Vorschlag gewandt, gemeinsam Handlungsempfehlungen und Verhaltenskodizes für die Videoüberwachung in Bussen und Bahnen zu entwickeln. Zu diesem Zweck haben sich Vertreter beider Seiten an einem Tisch zusammengesetzt, um möglichst bundesweit einen Konsens über Zulässigkeit und Umfang von Videoüberwachung in Bussen und Bahnen herzustellen.

Über wesentliche Punkte konnte inzwischen Einigkeit erzielt werden:

Danach ist die Videoüberwachung in öffentlichen Verkehrsmitteln datenschutzrechtlich unbedenklich, wenn sie der sicheren Beförderung der Fahrgäste oder der Verhinderung von Eigentumsstörungen dient, zu diesem Zweck erforderlich ist und die Rechte der Fahrgäste auf informationelle Selbstbestimmung nicht unverhältnismäßig beeinträchtigt werden. Soweit die übertragenen Kamerabilder tatsächlich simultan beobachtet werden (was überraschenderweise eher selten der Fall ist), muss bei einer konkreten Gefahrenlage auch die Möglichkeit des Eingreifens zum Schutz der Fahrgäste sichergestellt werden. Soweit die Bilder aufgezeichnet werden, darf eine Auswertung nur zweckentsprechend und nur durch die dafür befugten Personen erfolgen; nicht benötigte Aufzeichnungen sind unverzüglich zu löschen. Schließlich muss auf die Beobachtung und Aufzeichnung sowie die verantwortliche Stelle deutlich sichtbar hingewiesen werden. Die notwendigen Maßnahmen und Verantwortlichkeiten sind in einer Betriebsanweisung festzulegen.

Soweit die im Wesentlichen einvernehmlichen Grundlagen. Weiterer Erörterungsbedarf (sowohl mit dem Verband der Verkehrsunternehmen als auch zwischen den Datenschutzbeauftragten untereinander) besteht dagegen noch zu der Frage, ob ggf. für welchen Zeitraum die Aufzeichnung zulässig sein soll, also die Speicherung der Bilder. Hierzu muss man wissen, dass sich die Videoüberwachung in öffentlichen Verkehrsmitteln häufig nur auf die Aufzeichnung beschränkt, d.h. dass die laufenden Bilder nicht beobachtet werden. Dies hängt damit zusammen, dass es die Mehrzahl der Verkehrsbetriebe aus Gründen der Verkehrssicherheit ablehnt, den Fahrern die Beobachtung mehrerer Monitore (während der Fahrt!) abzuverlangen.

Dieser Frage kommt daher besondere Bedeutung zu. Ich bin zuversichtlich, dass im Ergebnis der weiteren Erörterungen die Verkehrsbetriebe in Deutschland in absehbarer Zeit eine verlässliche und handhabbare Empfehlung zum Einsatz von Videoüberwachung in ihren Bussen und Bahnen bekommen werden.

5.1.4 Webcams im Internet: Die Lust an der medialen (Selbst-)Darstellung

Erstaunlich ist es schon: Galt „Big Brother“ noch vor wenigen Jahren als Synonym des (glücklicherweise nur Fiktion gebliebenen) wissensdurstigen Überwachungsstaates, verbindet man heute damit die von privaten Medien inszenierte Selbstdarstellungsshow, die von einigen Medienkritikern sogar als (allerdings unbeabsichtigt) fortschrittliches Format anerkannt wird. Natürlich verstößt es nicht gegen das Recht auf informationelle Selbstbestimmung, wenn sich Menschen erklärtermaßen freiwillig und aus handfesten Motiven einer Dauerüberwachung stellen. Die Entwicklung zeigt aber, dass der Lebensalltag heute zunehmend durch die neuen Medien für jedermann weltweit abrufbar bereit gehalten und präsentiert wird.

Unternehmen und andere Private, aber auch öffentliche Stellen wie z. B. Kommunen, bilden immer häufiger Menschen bei ihren privaten Verrichtungen, so-

weit sie in der Öffentlichkeit stattfinden, in digitalen Aufnahmen ab. So werden im Internet zu Hunderttausenden Livebilder sog. Webcams angeboten.

Bei Webcams handelt es sich um digitale Kameras, die bewegte oder unbewegte Bilder in das Internet übertragen, die dort von jedem Internet-Nutzer abgerufen werden können. Gerade Unternehmen wie Hotels, Restaurants oder Kaufhäuser gehen immer mehr dazu über, ihre Internet-Auftritte durch solche Webcam-Übertragungen attraktiver zu gestalten und vorhandene Angebote zu visualisieren.

Solange die Webcam-Bilder Personen nicht erkennen lassen, verletzt dies keine datenschutzrechtlichen Belange. Gleiches gilt, wenn die Betroffenen damit einverstanden sind bzw. diese Selbstdarstellung sogar ausdrücklich wünschen. Das Recht des Einzelnen auf informationelle Selbstbestimmung ist aber spätestens berührt, wenn Personen erkennbar werden, die in die damit verbundene öffentliche Verbreitung und Zurschaustellung eben nicht eingewilligt haben, und ihnen - schlimmer noch - häufig überhaupt nicht bewusst ist, dass sie per Kamera beobachtet werden.

Bei mir fragen sowohl potenzielle Anwender solcher Bildübertragungen als auch Betroffene an, die meist erst zufällig auf solche Webcam-Übertragungen gestoßen sind, ob und unter welchen Voraussetzungen der Einsatz von Webcams zulässig ist oder nicht.

Ein Beispiel: Eine Kaufhauskette hat in mehreren ihrer Filialen Internetcafés eingerichtet, in denen die Kunden surfen und andere Online-Dienste in Anspruch nehmen können. Dabei werden sie (wie auch Kunden außerhalb des Internetcafés) von einer dort installierten Webcam erfasst, deren Bilder auf der Website des Unternehmens abgerufen werden können. Besonderer Clou dabei: Der Betrachter kann die Webcam von seinem PC aus nicht nur in alle Richtungen steuern, sondern das Bild auch so stark heranzoomen, dass einzelne Kunden formatfüllend dargestellt werden können. Zu allem Übel wären sich die Kaufhauskunden und Internetcafé-Nutzer dieser Beobachtungsmöglichkeit ihrer Person überhaupt nicht bewusst, da ein entsprechender Hinweis fehlte und man auch nicht typischerweise davon ausgehen muss, beim Einkaufen weltweit beobachtet werden zu können.

Aufgrund der Intervention des in diesem Fall zuständigen Hamburgischen Datenschutzbeauftragten ist die Webcam zwischenzeitlich im Einvernehmen mit dem Betreiber stillgelegt worden.

Dieses Beispiel wirft, wie der Einsatz von Webcams insgesamt, Fragen im Hinblick auf den Persönlichkeitsschutz auf, die vom geltenden Recht entweder gar nicht oder nur unzureichend beantwortet werden.

Das eigentliche Problem liegt dabei weniger in den Bildangeboten als solchen, sondern in der Tatsache der weltweiten Verbreitung und der nahezu unbegrenzten Möglichkeiten der Weiterverwendung durch jeden Internet-Nutzer. So ist inzwischen Software am Markt erhältlich, mit der (vergleichbar der konventionellen Zoomfunktion) einzelne Bilder stark vergrößert werden können. So kann aus der beiläufigen Darstellung eines Passanten eine formatfüllende Abbildung werden, die dann von jedem Nutzer gespeichert und - in welchem Zusammenhang auch immer - wieder in das Netz eingespeist werden kann.

Weder das für öffentliche Stellen in Niedersachsen geltende NDSG noch das für nichtöffentliche Stellen maßgebliche BDSG enthalten derzeit spezielle Regelungen zur Herstellung, Aufzeichnung oder Verbreitung digitaler Bildaufnahmen. Auch die im Zuge der BDSG-Novellierung vorgesehene Regelung zur Videoüberwachung würde keine wirksame Eingrenzung der sich aus den Verknüpfungsmöglichkeiten digitaler Bildaufnahmen ergebenden Gefährdungspotentiale

sicherstellen, wobei auch noch zu klären ist, ob und inwieweit Webcams überhaupt von der Regelung erfasst werden.

In diesem Zusammenhang ist häufig die Rede vom Recht am eigenen Bild. Tatsächlich schützt das im Jahr 1907 als Reaktion auf ein heimliches Pressefoto des toten Reichskanzlers Otto von Bismarck erlassene Kunsturhebergesetz vor einer Verbreitung oder öffentlichen Zurschaustellung von Bildern. Abgesehen davon, dass es sich hierbei um rein zivilrechtliche Normen handelt, die eben auch nur auf zivilrechtlichem Wege durch die Betroffenen selbst und nicht etwa durch eine öffentliche Stelle von Amts wegen durchgesetzt werden können, kann das Kunsturhebergesetz natürlich die heutigen technischen Möglichkeiten der Verbreitung und Weiterverarbeitung im weltweiten Netz nicht berücksichtigen.

Aus meiner Sicht muss daher die Frage der bildlichen Darstellung von Personen im Internet wie überhaupt die Einstellung von personenbezogenen Informationen in das Internet noch sehr intensiv diskutiert und die Geeignetheit bisheriger Regelungsansätze grundsätzlich überdacht werden.

Daher hat die 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 14./15. März 2000 eine Entschließung zu Risiken und Grenzen der Videoüberwachung gefasst (siehe Anlage 14). Die 60. Konferenz am 12./13. Oktober 2000 hat sich darauf verständigt, zur Aufarbeitung dieser Fragen und der Vorbereitung von notwendigen Rechtsetzungsmaßnahmen eine Arbeitsgruppe einzusetzen, die möglichst zeitnah ihre Ergebnisse vorlegen soll, um die Vorschläge in die zweite Stufe der BDSG-Novellierung einbeziehen zu können, die eine grundlegende Reform des deutschen Datenschutzrechts zum Ziel hat.

5.1.5 Videoüberwachung der Polizei

Im Anschluss an den Beschluss der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu den Risiken und Grenzen der Videoüberwachung am 15./16. März 2000 (Anlage 14), der für die öffentliche Erörterung dieses Themas wichtige rechtliche Rahmenvorgaben benannt hat, sowie den Beschluss der Ständigen Konferenz der Innenminister und -senatoren vom 5. Mai 2000 zum Videoeinsatz an Kriminalitätsschwerpunkten im öffentlichen Raum ist die Diskussion zu dieser Problematik weitergeführt worden.

Unter den Datenschutzbeauftragten des Bundes und der Länder besteht mittlerweile in den wesentlichen Punkten Übereinstimmung über die gesetzlich abzusichernden Forderungen aus datenschutzrechtlicher Sicht. Mit Schreiben vom 28. August 2000 habe ich diese Forderungen dem Präsidenten des Niedersächsischen Landtags und dem Niedersächsischen Innenministerium übermittelt, damit sie in das zurzeit laufende Novellierungsverfahren zum Niedersächsischen Datenschutzgesetz bzw. in eine erforderliche Novelle des Niedersächsischen Gefahrenabwehrgesetzes (NGefAG) einfließen können. Folgende Kernpunkte sind bei einer Regelung zur Videoüberwachung zu berücksichtigen:

- Jeder Einsatz von Videotechnik, bei dem eine Personenbeziehbarkeit tatsächlich besteht oder technisch möglich ist, ist als regelungsbedürftiger Eingriff in das Recht auf informationelle Selbstbestimmung anzusehen.
- Der Einsatz der Videotechnik muss im konkreten Fall verhältnismäßig sein, insbesondere dürfen keine überwiegenden schutzwürdigen Belange potenziell Betroffener entgegenstehen. Dies ist durch eine vorgeschaltete datenschutzrechtliche Vorabkontrolle zu belegen (Sonderregelungen z. B. in der StPO oder §§ 32 Abs. 2 und 35 Abs. 1 NGefAG bleiben unberührt).
- Der Einsatz der Videotechnik im öffentlichen Raum zur Kriminalitätsbekämpfung ist strikt auf solche Orte zu begrenzen, an denen wiederholt

Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort auch künftig weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und dass mit der Videoüberwachung neben der Beweissicherung eine Präventionswirkung erreicht werden kann. Ungezielte Verlagerungseffekte müssen vermieden werden.

- Eine bloße Störung der öffentlichen Ordnung rechtfertigt in keinem Fall einen Einsatz von Videotechnik auf öffentlichen Straßen und Plätzen.
- Der Einsatz der Videotechnik ist, falls nicht offenkundig, durch geeignete Maßnahmen erkennbar zu machen.
- Eine Aufzeichnung der Bilddaten ist nur ausnahmsweise bei konkretem Verdacht einer Straftat oder einer konkreten Gefahr für die öffentliche Sicherheit zulässig.
- Die Aufzeichnungen sind unverzüglich zu löschen, sobald sie für den vorausgesetzten Zweck nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.
- Videoüberwachungsmaßnahmen können kein Ersatz für polizeiliches Eingreifen sein. Es muss deshalb gewährleistet sein, dass polizeiliche Einsatzkräfte schnell auf erkannte Gefahrensituationen oder Straftaten reagieren können.
- Eine Mitbenutzung von videotechnischen Anlagen Dritter, die der Polizei einen Steuerungs- oder Speicherungszugriff ermöglicht, ist nur zulässig, wenn alle rechtlichen Voraussetzungen, die für den Einsatz polizeieigener Videotechnik gelten, erfüllt sind. Das Zweckbindungsgebot ist strikt einzuhalten.
- Die getroffenen Überwachungsmaßnahmen müssen in regelmäßigen Abständen auf ihre weitere Erforderlichkeit und auf ihre Wirksamkeit überprüft werden. Bei negativem Prüfergebnis sind die Überwachungsmaßnahmen unverzüglich einzustellen; um einen schleichenden Übergang in eine großflächige Überwachungsinfrastruktur nicht eintreten zu lassen, ist die eingesetzte Videotechnik zu entfernen.
- Zur Prüfung der Normeffizienz ist dem Parlament jährlich ein Erfahrungsbericht über die angeordneten Videoüberwachungsmaßnahmen und die mit ihnen erreichten Ergebnisse vorzulegen.

Zwar beziehen sich diese Forderungen in weiten Bereichen auf polizeispezifische Fallgestaltungen; soweit sie nicht durch diesen fachspezifischen Gesichtspunkt bestimmt sind, müssen sie jedoch auch ihren Niederschlag im NDSG finden, damit eine normenklare Regelung auch für den nicht-polizeilichen Einsatz der Videotechnik im öffentlichen Bereich geschaffen wird.

5.1.6 Videoüberwachung gegen illegale Abfallbeseitigung

Ich sehe mich in der letzten Zeit häufiger mit Anfragen von Städten und Landkreisen konfrontiert, die sich um Maßnahmen gegen ordnungswidrige Abfallbeseitigung bemühen.

Die unteren Abfallbehörden beklagen, dass zunehmend an den Wertstoff-Depotbehälterstandplätzen sowohl Abfall neben den Depotbehältern abgelagert wird als auch außerhalb der vorgesehenen Einwurfzeiten Wertstoffe entsorgt werden. Den Berichten nach kam es auch zu Depotbehälterbränden, deren Verursacher ebenfalls nicht ermittelt werden konnten. Dieses rechtswidrige Verhalten wollen die Behörden durch Videoüberwachung unterbinden.

Mit der Videoüberwachung ist die Erhebung, Speicherung und Übermittlung personenbezogener Daten als Eingriff in das Recht auf informationelle Selbstbestimmung verbunden. Einschränkungen dieses Rechts sind im überwiegenden Allgemeininteresse, zu dem auch die geordnete Entsorgung von Abfällen gehört, zulässig. Der Einsatz der Videotechnik bedarf einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entspricht und den Grundsatz der Verhältnismäßigkeit beachtet.

Gemäß § 45 Abs. 1 NAbfG dürfen die öffentlich-rechtlichen Entsorgungsträger u. a. zur Ausführung des Niedersächsischen Abfallgesetzes die erforderlichen personenbezogenen Daten verarbeiten. Während grundsätzlich die Erhebung, Speicherung, Übermittlung und Nutzung von Daten von § 3 NDSG in Verbindung mit § 45 Abs. 1 NAbfG gedeckt ist, erscheint zweifelhaft, ob diese Regelungen auch eine Videoüberwachung gestatten, da diese Vorschriften die Zulässigkeit der Datenverarbeitung (nur) generalklauselartig - lediglich durch das Kriterium der Erforderlichkeit - eingrenzen. Der Gesetzgeber wollte bei der Einbeziehung des NDSG in das NAbfG aber andere Verarbeitungsvorgänge als die Videoüberwachung erfassen. Wegen der besonderen Gefahren für die freie Entfaltung der Persönlichkeit erscheint eine spezielle Ermächtigungsgrundlage geboten, die jedenfalls für die reine Bildübertragung in § 45 Abs. 2 NAbfG i. V. m. § 32 Abs. 5 Niedersächsisches Gefahrenabwehrgesetz (NGefAG) zu finden sein dürfte.

Die Zulässigkeit der Bildaufzeichnung hingegen folgt nicht aus § 45 Abs. 2 NAbfG i. V. m. § 32 Abs. 2 NGefAG. Letztere Vorschrift erlaubt ausdrücklich nur den Polizeibehörden, nicht aber den Verwaltungsbehörden, Aufzeichnungen von einer Person zu fertigen, wenn sie sich in oder an einem sog. gefährdeten Objekt nach § 13 Abs. 1 Nr. 3 NGefAG befindet. Insoweit kann dahinstehen, ob es sich bei den Depotbehälterstandorten um solche Objekte handelt.

Eine Befugnis zur Bildaufzeichnung mittels Videokamera und Übermittlung der dabei gewonnenen Daten könnte sich daher lediglich aus den Regelungen des NDSG ergeben. Ich bin jedoch nicht der Meinung, dass die bestehenden Vorschriften des NDSG als bereichsspezifische und normenklare Ermächtigungsgrundlage für die mit der Videoüberwachung verbundenen Eingriffe angesehen werden können.

5.2 Landesgesetzliche Regelungen im Gesundheitswesen

Niedersachsen ist das einzige Bundesland, in dem die Datenverarbeitung durch Krankenhäuser nicht spezialgesetzlich geregelt ist. Diese Tatsache habe ich wiederholt kritisiert (z. B. XI. TB 21.2, 21.3).

Für Krankenhäuser in öffentlicher Trägerschaft gelten, weil sie öffentlich-rechtliche Wettbewerbsunternehmen sind, gemäß § 2 Abs. 2 Satz 1 Nr. 1 NDSG im Wesentlichen die auch auf Krankenhäuser in privater Trägerschaft anzuwendenden Vorschriften des Bundesdatenschutzgesetzes über den nichtöffentlichen Bereich.

Das novellierte Bundesdatenschutzgesetz wird in Umsetzung des Art. 8 der EU-Datenschutzrichtlinie spezielle Vorschriften über die Verarbeitung besonderer Arten personenbezogener Daten, zu denen Gesundheitsdaten gehören, enthalten. Gemäß § 28 Abs. 7 Satz 1 n.F. BDSG ist das Erheben von Gesundheitsdaten (über die Voraussetzungen des Abs. 6 hinaus) zulässig, wenn dies zum Zwecke der Gesundheitsvorsorge, medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung der Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Schweigepflicht unterliegen. Das Er-

heben personenbezogener Daten ist also recht ausführlich geregelt. Anders verhält es sich mit der in Satz 2 angesprochenen Verarbeitung und Nutzung, die sich zu den in Satz 1 genannten Zwecken nach den Geheimhaltungsvorschriften richten, die für ärztliches Personal oder sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, gelten. Das Bundesdatenschutzgesetz trifft also keine eigenen Regelungen, sondern verweist auf außerhalb des Gesetzes bestehende Geheimhaltungspflichten.

Festgelegt werden diese Geheimhaltungspflichten durch die Berufsordnungen, in Niedersachsen § 9 der „Berufsordnung der Ärztekammer Niedersachsen", und insbesondere durch § 203 Abs. 1 Satz 1 Nr. 1 StGB. § 9 der Berufsordnung trifft jedoch keine detaillierten Aussagen über die Datenverarbeitung durch Ärzte, sondern bestimmt nur einen Rahmen für eine befugte Offenbarung. Noch weniger ist § 203 Abs. 1 Satz 1 Nr. 1 StGB zu entnehmen, der nicht bestimmt, wann eine Offenbarung befugt erfolgt.

Diese Vorschriften bieten keine angemessene Grundlage für die Datenverarbeitung eines Krankenhauses, da sie den komplexen Abläufen und den damit verbundenen Datenverarbeitungen nicht gerecht werden. Es sind präzise Regelungen zu schaffen, unter welchen Voraussetzungen Patientendaten erhoben, gespeichert und zu welchen Zwecken und an wen sie übermittelt werden dürfen. Den Besonderheiten des Arzt-Patienten-Verhältnisses ist auch etwa bei der Frage des Zugriffs unterschiedlicher Abteilungen des Krankenhauses auf die Patientendaten, Art und Dauer der Aufbewahrung und der Auskunftserteilung Rechnung zu tragen.

Besonders dringlich ist eine klare Regelung der Auftragsdatenverarbeitung. Im Rahmen des sog. „Outsourcing" gewinnt sie zunehmend an Bedeutung. Sie umfasst die Archivierung und Vernichtung von Patientenunterlagen, die Mikroverfilmung und das Einscannen von Papierunterlagen, die Wartung von EDV-Anlagen und die Einschaltung von Rechenzentren etwa im Zusammenhang mit der Abrechnung von Krankenhausleistungen. Die Formen der Auftragsdatenverarbeitung sind also vielfältig. Der Datenschutz ist nicht berührt, wenn der Auftragnehmer keine Patientendaten zur Kenntnis nehmen kann, also etwa, wenn die zu archivierenden Unterlagen in einem mit einem Code versehenen Container verschlossen sind, den der Auftragnehmer nicht öffnen kann. Bei einer Mikroverfilmung hingegen ist eine Kenntnisnahme von Patientendaten kaum zu vermeiden. Auch hinsichtlich der für die ärztliche Schweigepflicht bedeutsamen Eigenschaft des Auftragnehmers als ärztlicher Gehilfe ist die Situation je nach Art und konkreter Ausgestaltung der Auftragsdatenverarbeitung unterschiedlich. In diesem unübersichtlichen Bereich mit einem bereichsspezifischen Gesetz eine umfassende Regelung zu schaffen, ist dringend geboten.

Die erforderlichen bereichsspezifischen Regelungen könnten, wie in den meisten anderen Bundesländern, Teil eines allgemeinen Krankenhausgesetzes sein. Denkbar ist aber auch, wie in Nordrhein-Westfalen, ein eigenes Gesundheitsdatenschutzgesetz zu schaffen.

Ein solches Gesundheitsdatenschutzgesetz sollte ebenfalls die Datenverarbeitung im öffentlichen Gesundheitsdienst erfassen. Hier sind zwar in den letzten Jahren einige bereichsspezifische Regelungen erfolgt, wie z. B. die §§ 31 Abs. 2, 56, 57 NSchG für Schuluntersuchungen und die §§ 32 ff. NPsychKG. Zudem gelten für die Gesundheitsämter eine Reihe bundesrechtlicher Gesetze wie das (bisherige) Bundesseuchengesetz und seit dem 1. Dezember 2000 das Infektionsschutzgesetz. Es werden jedoch nicht alle Tätigkeitsfelder eines Gesundheitsamtes erfasst. Zudem fehlen ebenso wie im Krankenhaus den Besonderheiten eines Gesundheitsamtes entsprechende Regelungen etwa zur Aufbewahrung von Unterlagen und zum Auskunftsrecht der Betroffenen.

5.3 Entschlüsselung des menschlichen Genoms

Die in den letzten Jahren zu verzeichnende Entwicklung der Genetik wird häufig mit der industriellen Revolution im 19. Jahrhundert verglichen. Ihren Anfang nahm diese Entwicklung 1953 mit der Entdeckung der DNS (Desoxyribonukleinsäure) durch Francis Crick und James Watson. Zu Beginn der 90-er Jahre begannen dann intensive Bemühungen, das menschliche Genom zu entschlüsseln, zunächst in einem öffentlichen Human Genomprojekt, dann in einem von Wirtschaftsunternehmen finanzierten Konkurrenzverfahren, für das der Name Craig Venter steht. In einem regelrechten Wettlauf erwies sich Venter als der Schnellere. Die Entschlüsselung des menschlichen Genoms wird bald als weitgehend abgeschlossen betrachtet werden können.

Die Erkenntnisse der Genetik werfen hochkomplexe medizinische, ethische und rechtliche Fragen auf. Jede verkürzte und vereinfachende Antwort, die in der öffentlichen Diskussion so nahe liegt, führt in die Irre. Deshalb kann nur versucht werden, in einem stetigen Prozess die Chancen und Probleme zu erfassen und gegeneinander abzuwägen. Die Datenschutzbeauftragten des Bundes und der Länder haben daher in ihrer 60. Konferenz am 12./13. Oktober 2000 unter Berücksichtigung einer Entschließung aus dem Jahre 1989 versucht, einige bedeutsame Fallgruppen herauszuarbeiten und Regeln zu benennen, die nach ihrer Ansicht einzuhalten sind (Anlage 25).

Ausgangspunkt der Entschließung ist die Tatsache, dass die Genomanalyse in einem bisher nicht genannten Ausmaß Einblick in den Kernbereich der Persönlichkeit ermöglicht, insbesondere in gesundheitliche Dispositionen. Das Recht auf informationelle Selbstbestimmung wird also massiv berührt. Zu diesem Recht gehört auch das Recht auf Nichtwissen. Es ist deshalb festzulegen, ob und wann genetische Untersuchungen vorgenommen werden dürfen und wer von den Ergebnissen Kenntnis erlangen soll.

Die Anforderungen an genetische Untersuchungen sind je nach den Bereichen, in denen sie erfolgen sollen, unterschiedlich.

Von besonderer Bedeutung sind genetische Untersuchungen in der Medizin. Sie ermöglichen wichtige Fortschritte bei der Diagnose, Therapie und Prävention genetisch bedingter Krankheiten. Die Entschlüsselung des Genoms eröffnet darüber hinaus die Chance, auch andere Krankheiten besser zu verstehen.

Voraussetzung einer genetischen Untersuchung ist grundsätzlich die Einwilligung der zur untersuchenden Person. Sie muss umfassend u. a. über Zweck und Aussagekraft der Untersuchung, der Risiken, die mit ihr verbunden sind, die Bedeutung festgestellter Anomalien und therapeutische Möglichkeiten unterrichtet werden. Die Einwilligung ist jederzeit widerruflich. Im Falle eines Widerrufs sind die Daten zu löschen oder an den Betroffenen herauszugeben. Bei genetischen Untersuchungen, deren Ergebnis die bisherige Lebenssituation des Betroffenen und seiner engeren Angehörigen radikal verändern kann, stellt sich die weitere Frage, ob und inwieweit Familienangehörige in das Unterrichtungs- und Einwilligungsverfahren einzubeziehen sind. Zu wählen sind in jedem Fall Verfahren, bei denen möglichst wenig Überschussinformationen gewonnen werden. Nicht benötigte Informationen sind zu löschen.

Besonders problematisch sind pränatale Genomanalysen. Es dürfen nur Informationen über Erbanlagen erhoben werden, bei denen eine Schädigung heilbar oder zumindest eine therapeutische Linderung eines Leidens möglich ist oder die zu einer so schwerwiegenden Gesundheitsbeeinträchtigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe. Nicht zulässig ist es daher, Eigenschaften zu ermitteln, die nicht die Gesundheit beeinträchtigen. Gerade bei der pränatalen Untersuchung ist eine umfassende Beratung der Eltern erforderlich.

Im Arbeitsverhältnis ist die Gefahr einer genetischen Diskriminierung besonders groß. Deshalb bedürfen genetische Untersuchungen einer gesetzlichen Grundlage. Die Einwilligung des Arbeitnehmers genügt in Anbetracht der Zwangssituation, in der er sich befindet, nicht.

Grundsätzlich unzulässig sind genetische Untersuchungen im Versicherungswesen. Für Pflichtversicherungen, insbesondere in der gesetzlichen Kranken- und Rentenversicherung stellt sich die Frage einer genetischen Untersuchung ohnehin nicht. Aber auch freiwillige Privatversicherungen sind Risikogemeinschaften, deren Aufgabe es nicht ist, Risiken auszuschließen, sondern sie gemeinsam zu tragen. Das Land Rheinland-Pfalz hat einen Antrag in den Bundesrat eingebracht (BR-Drs. 530/00), in dem die Bundesregierung aufgefordert wird, einen Gesetzentwurf mit spezifischen Regelungen vorzulegen, nach denen es Versicherungen verboten ist, eine Genomanalyse zur Voraussetzung der Annahme eines Versicherungsantrages zu machen. Die Frage nach genetischen Dispositionen, die dem Antragsteller bekannt sind, soll nur unter eng begrenzten Voraussetzungen, insbesondere zur Vermeidung der missbräuchlichen Ausnutzung des Versicherungssystems, zulässig sein. Der Bundesrat hat diese Empfehlung inzwischen beschlossen.

Am weitesten fortgeschritten ist die rechtliche Ausgestaltung von Genomanalysen im Bereich des Strafrechts, die ich in 26.3 ausführlich darstelle.

In einem Zivilverfahren, das der Feststellung der Abstammung dient, ist die genetische Untersuchung nur mit Einwilligung der betroffenen Personen oder auf richterliche Anordnung zulässig.

Die Konferenz ist sich der Tatsache bewusst, dass ihre Entschließung nur einen ersten Schritt darstellen kann und ihre Überlegungen zu überprüfen und anzupassen sind. Aus diesem Grunde hat sie die Einsetzung einer Arbeitsgruppe beschlossen, an der ich mich beteiligen werde.

5.4 Electronic Government

5.4.1 Datenschutz als Hemmnis?

Der Ruf nach serviceorientierter Verwaltung trägt sichtbare Früchte. Zahlreiche Städte und Gemeinden führen multifunktionale Servicebüros, Bürgerämter, Bürgerläden oder Kundencenter ein und ermöglichen so den Bürgerinnen und Bürgern, ihre verschiedenen Behördengänge zu reduzieren und zu beschleunigen. Dagegen scheint der Aufbau eines „Electronic Government“ eher schleppend voranzukommen. Zwar gibt es mittlerweile kaum noch eine Behörde, die nicht im Internet präsent ist. Die Präsenz beschränkt sich aber zumeist auf reine Informationsangebote, die in manchen Fällen sogar recht unprofessionell gestaltet sind und die Bürgerinnen und Bürger eher abschrecken als begeistern. Kommunikation und Transaktion zwischen Nutzern und Anbietern wie beim Electronic Commerce, also sozusagen das Salz in der Suppe, beschränken sich auf die Angabe einer E-Mail-Adresse und bei manchen Behörden auf das Angebot zum Download von Formularen. Dabei ist der Wunsch nach der Einführung von E-Government-Lösungen bei den Bürgerinnen und Bürgern sehr hoch. In verschiedenen Umfragen werden von den Nutzern die Behördenkontakte als wichtigste Anliegen genannt, die sie online erledigen möchten.

Woran liegt es, dass viele Behörden offenbar vor der Einführung transaktionsgebundener Internetanwendungen zurückschrecken? Der Grund hierfür, so hört man überall, seien die derzeitigen rechtlichen Regelungen, die dies nicht zuließen. Unter anderem würden Datenschutzbestimmungen ein weitergehendes E-Government-Engagement verhindern. Ich halte diese Einschätzung für unzu-

treffend. Es ist wohl eher so, dass das zögerliche Herangehen an transaktionsgebundene Internetanwendungen an der besonderen Situation liegt, in der sich die öffentliche Verwaltung nun einmal befindet. Sie handelt nicht gewinnorientiert und erfüllt ihre Aufgaben auch ohne Internet. Warum soll sie mühsam und aufwendig nach neuen Wegen suchen und sich dabei auch noch der Kritik von Datenschutzbeauftragten, Personalräten, Aufsichtsbehörden und anderen vermeintlichen Verhinderern aussetzen?

Ich bin der festen Überzeugung, dass die öffentliche Verwaltung die neuen Wege zum E-Government gehen muss. In dem im September 2000 veröffentlichten Memorandum des Fachausschusses Verwaltungsinformatik der Gesellschaft für Informatik e.V. und des Fachbereichs 1 der Informationstechnischen Gesellschaft im VDE wird die zentrale Bedeutung von E-Government für die Modernisierung von Staat und Verwaltung eindrucksvoll belegt. Erste Ansätze für datenschutzgerechte Lösungen lassen sich schon mit Hilfe vorhandener Technik und mit dem geltenden Recht verwirklichen, in beiden Feldern sind aber viel Einsatz und Einfallsreichtum erforderlich, um diese Ansätze weiter zu entwickeln. Mein besonderes Anliegen ist es, die öffentliche Verwaltung hierbei tatkräftig zu unterstützen. Ich biete meine Hilfe bei der Entwicklung und Einführung von E-Government-Lösungen an, die den Bürgerinnen und Bürgern einen verbesserten Service ohne eine Einschränkung des Rechts auf informationelle Selbstbestimmung ermöglichen.

Im Berichtszeitraum habe ich für verschiedene Vorhaben bereits Unterstützung in Form von umfassender Beratung und Prüfung geleistet. Dabei ging es mir nicht darum, neue Verfahren zu unterbinden, sondern diese durch angemessene Datenschutz-Leitplanken auf die richtigen Wege zu bringen.

Die Datenschutzleitplanken für E-Government

1. Datenvermeidung und Datensparsamkeit

Wo möglich, muss die Verarbeitung personenbezogener Daten vermieden werden (anonyme und pseudonyme Nutzung, datensparsame Protokollierung, Einschränkung der Recherchierbarkeit).

Grundsätzlich gilt: Bürgerdaten dürfen in Internet-Angeboten nur erscheinen, wenn diese Daten rechtmäßig veröffentlicht worden sind oder Bürgerinnen und Bürger eingewilligt haben. Mitarbeiterdaten dürfen auch erscheinen, wenn die Veröffentlichung für den Dienstverkehr erforderlich ist.

Die Notwendigkeit einer elektronischen Identität für die Abwicklung eines Einzelfalls darf nicht zu einer umfassenden Bürgerdatenbank führen (verteilte Trust Center usw.).

2. Hohe Sicherheit für die Bürgerinnen und Bürger

Unternehmen und Behörden müssen bei Kommunikationsangeboten (z B. E-Mail, elektronische Formulare, Transaktionen) den Bürgerinnen und Bürgern immer den Einsatz von Verschlüsselungen anbieten. Auch bei unsicheren Übertragungen im „back office"-Bereich ist eine Verschlüsselung erforderlich.

Behörden- und Unternehmensrechner müssen besonders gegenüber dem Internet geschützt werden (Firewalls, Intrusion-Detection-Systeme). Gerade in sicherheitskritischen Bereichen (z. B. bei Verschlüsselungstechnik) muss anerkannt sichere Software eingesetzt werden (Gütesiegel, Datenschutz-Audit).

Identifikation und Authentifikation von Bürgerinnen und Bürgern muss mit hohen technischen Standards erfolgen (z. B. digitale Signatur nach dem Signaturgesetz). Aber auch Behörden müssen sich gegenüber den Bürgerinnen und Bürgern eindeutig identifizieren.

3. Frühzeitiges Erkennen von Gefahren

Bei der Einführung neuer Techniken oder dem Umgang mit sensitiven Daten müssen rechtzeitig Technikfolgenabschätzungen durchgeführt werden.

In laufenden Systemen muss mit einem „Datenschutz-Controlling" sofort auf neue Gefahren reagiert werden.

4. Zugang für jedermann

E-Government-Lösungen müssen so gestaltet werden, dass sie jeder nutzen kann. Dies gilt im Hinblick auf den finanziellen Aufwand und auf die computertechnische Vorbildung.

5. Transparenz

Bürgerinnen und Bürger müssen auf Gefahren im E-Government hingewiesen werden. Das Sicherheitsniveau von E-Government-Lösungen muss offen gelegt werden. Bürgerinnen und Bürger müssen sich schnell, leicht und übersichtlich über die Verarbeitung ihrer Daten informieren können (auch elektronisch).

Die Datenschutzbeauftragten der Länder haben in einer Arbeitsgruppe, an der ich mitgewirkt habe, eine Orientierungshilfe "Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung" erstellt, die allen Verwaltungen in Deutschland zur Verfügung gestellt werden wird. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu der Orientierungshilfe am 12. Oktober 2000 eine Entschließung verabschiedet, in der sie ihre Bereitschaft erklärt, Entwicklungsprozesse zu einer stärker serviceorientierten Verwaltung konstruktiv zu begleiten (vgl. Anlage 22).

5.4.2 Die häufigsten Fragen

Was darf ins Internet?

Will eine öffentliche Stelle personenbezogene Daten im Netz bereitstellen, so gelten in vielen Fällen bereichsspezifische Regelungen (z. B. Sozialgesetzbuch, Meldegesetze). Fehlen solche Regelungen, so sind die jeweiligen Landesdatenschutzgesetze und bei Stellen des Bundes das Bundesdatenschutzgesetz einschlägig. Soweit die Bereitstellung von Daten im Internet ohne Einschränkungen erfolgt, also keine geschlossene Benutzergruppe durch z. B. ein Passwortverfahren gebildet wird, besteht weltweit die Möglichkeit eines Abrufs. Da es Staaten gibt, in denen keine oder sehr schwach ausgeprägte Datenschutzbestimmungen existieren, können durch die Einstellung ins Netz die datenschutzwürdigen Belange von Betroffenen beeinträchtigt sein. Ein Bereithalten personenbezogener Daten im Internet ist daher nur zulässig, wenn die betroffenen Personen eingewilligt haben oder dies aufgrund einer Rechtsvorschrift hinzunehmen haben.

Unabhängig hiervon ist der Grundsatz der Datenvermeidung zu beachten. Auch wenn die Verarbeitung von personenbezogenen Daten im Internet zulässig ist, sind alternative anonyme oder pseudonyme Verfahren zu wählen, wenn der Zweck der Verarbeitung so in gleicher Weise erreicht werden kann. Grundsätzlich zulässig ist die Bereitstellung von Informationen, die rechtmäßig veröffentlicht werden dürfen. Hierzu gehören u. a.

- Publikationen der Presse,
- Namen von Referenten und Gremienmitgliedern bei öffentlichen Veranstaltungen sowie
- amtliche Bekanntmachungen.

Dabei ist allerdings zu bedenken, dass auf diese Weise ein weltweiter Zugriff möglich ist und die bereitgestellten Daten automatisiert recherchierbar sind. Vor der Entscheidung über eine Veröffentlichung im Internet sollten daher mögliche negative Konsequenzen für die Betroffenen untersucht und berücksichtigt werden. Bereits bestehende Widerspruchsrechte sind zu beachten. Außerdem sollten die Möglichkeiten zur Reduzierung der Recherchierbarkeit in geeigneter Weise genutzt werden.

Ist die Zulässigkeit der Veröffentlichung nicht gesetzlich geregelt, ist die Einwilligung der Betroffenen Voraussetzung für eine Bereitstellung im Internet. Dabei sollten pseudonyme Verfahren gewählt werden, wenn dies möglich und sinnvoll ist. Auch beim Vorliegen einer Einwilligung sollten die Möglichkeiten zur Einschränkung der Recherchierbarkeit in geeigneter Weise genutzt werden. Besondere Regelungen gelten bei der Verarbeitung von Bedienstetendaten (vgl. 14.7).

Welche Nutzungsdaten dürfen wie verarbeitet werden?

Internet-Angebote öffentlicher Stellen sind entweder Teledienste, die im Teledienstegesetz (TDG) und im Teledienstedatenschutzgesetz (TDDSG) geregelt sind, oder Mediendienste, für die der Mediendienste-Staatsvertrag (MDStV) gilt. Die Verarbeitung von Daten der Nutzer, die für die Inanspruchnahme von Diensten erforderlich sind, also die sogenannten Nutzungsdaten, unterfallen diesen Regelungen.

Selbst wenn ein Nutzer im Internet keine Daten über seine Identität von sich aus offenbart (Ausfüllen von Formularen, E-Mail-Adressen usw.), fallen beim Anbieter Daten über den Nutzer an. Dazu gehören die IP-Adressen, über die der Datenaustausch vollzogen wird.

Während die Internet-Server feste Internetprotokoll-Adressen (IP-Adressen) haben, gilt dies für die Rechner der meisten Nutzer nicht. Vielmehr erhält der Nutzer von seinem Access-Provider für die jeweilige Session eine dynamische Adresse zugeteilt. Außer vom Accessprovider können dynamische Adressen auch von Außenstehenden (mit großem Aufwand) einem bestimmten Nutzer zugeordnet werden.

Es gibt außerdem Rechner, die über fest vergebene IP-Adressen verfügen. Dies können Rechner von Universitäten oder Firmen sein, die einen großen Bereich von IP-Adressen erworben haben, oder auch private Nutzer, die sehr früh im Internet präsent waren. In diesen Fällen lässt sich die IP-Adresse häufig auch ohne weitere Hilfsmittel einem bestimmten Nutzer zuordnen; sie ist deshalb als ein personenbezogenes Datum anzusehen. Allerdings ist nicht erkennbar, ob eine IP-Adresse statisch oder dynamisch ist. Daher müssen öffentliche Stellen darauf achten, dass vollständige IP-Nummern bei der Nutzung ihrer Informationsangebote nicht dauerhaft protokolliert werden, weil dies nach TDDSG bzw. MDStV nicht zulässig ist. Dies kann zum einen durch einen vollständigen Verzicht auf Protokollierungen erfolgen. Eine andere Möglichkeit besteht darin, nur die ersten drei Zahlen der IP-Adresse zu speichern. Auch ist es denkbar, schon während der Verbindung den Besuch des Internetangebots durch Zuordnung zu einer größeren Nutzergruppe zu erfassen, um so eine gewünschte, anonyme Statistik zu erhalten.

Welche Verwaltungsvorgänge können über das Internet abgewickelt werden?

Die Service-Orientierung der öffentlichen Verwaltung bedingt ein hohes Maß an Organisationsfreiheit der Verwaltung in der Ausgestaltung der Kommunikation mit den Bürgerinnen und Bürgern. Gerade auch Kommunen haben seit jeher auf ihre Organisationshoheit verwiesen, deren Grenzen lediglich in gesetzlichen Bestimmungen liegen. Kommunen wie andere Verwaltungen dürfen also - wenn nicht etwas anderes ausdrücklich festgelegt ist - ein Verwaltungsverfahren so durchführen, wie sie es für zweckmäßig halten. Das schließt auch die Wahl des Kommunikationsmediums ein.

Wie Internet-basierte Kommunikation mit der Verwaltung künftig aussehen könnte, zeigt folgendes Beispiel:

Die elektronische Anmeldung zum Volkshochschulkurs

Frau A möchte einen Volkshochschulkurs besuchen. Sie informiert sich auf der Homepage der Volkshochschule über die Angebote und entscheidet sich dort für den Kurs: „Aggressivität und aggressive Kinder - ein Wochenende für Betroffene". Auf der Homepage befindet sich der Hinweis, dass sie die Anmeldung auch online durchführen kann, wenn sie die erforderlichen Angaben per E-Mail übersendet. Da die Kommune ausdrücklich darauf hinweist, dass unverschlüsselte E-Mails auf ihrem Weg durch das Internet viele Stationen durchlaufen und unbemerkt gelesen oder verändert werden können, will sie das Angebot wahrnehmen, die E-Mail verschlüsselt zu übersenden. Hierzu installiert sie die erforderliche Software auf ihrem PC, lädt den öffentlichen Schlüssel der Kommune von der Homepage und überprüft ihn über den „Fingerprint". Anschließend verschlüsselt sie ihre Angaben mit dem heruntergeladenen Schlüssel und sendet sie an die Kommune. Diese kann die E-Mail entschlüsseln und die Anmeldung entsprechend weiter leiten. Auf dem gleichen Weg - verschlüsselt - erhält sie auch die Anmeldebestätigung und die Rechnung.

Da gesetzliche Vorgaben für die Anmeldung zu einem Volkshochschulkurs nicht bestehen, wäre in diesen Beispielsfällen eine Internet-basierte Kommunikation zulässig. Dagegen lässt sich eine ebenso eindeutige Aussage für einen anderen Beispielsfall - die Wohnsitzanmeldung - nicht treffen:

Die elektronische Wohnsitzanmeldung

Frau A ist umgezogen und möchte auf elektronischem Weg ihren Wohnsitz ummelden. Zu diesem Zweck ruft sie das elektronische Formular der entsprechenden Internetseite ihrer Kommune auf und gibt ihre Daten ein. Sie signiert das Meldeformular mit ihrem Signaturschlüssel und verschlüsselt das Dokument. Das Formular wird von den zuständigen Mitarbeiterinnen und Mitarbeitern geöffnet und mit einem elektronischen Eingangsstempel versehen. Eine Bestätigung ihrer Anmeldung wird ihr übersandt.

Das Melderechtsrahmengesetz enthält zurzeit keine Aussage darüber, wie die Meldepflicht konkret zu erfüllen ist. Regeln finden sich aber im Niedersächsischen Meldegesetz (NMG), das vorschreibt, dass die Meldepflichtigen einen Meldeschein auszufüllen, zu unterschreiben und bei der Meldebehörde abzugeben haben. Darüber hinaus sind durch Rechtsverordnung Form und Inhalt des Meldescheins detailliert festgelegt. Zwar kann vom Ausfüllen des Meldescheins abgesehen werden, falls das Melderegister automatisiert geführt wird. Dies gilt aber nur dann, wenn die meldepflichtige Person bei der Behörde erscheint, um die erforderlichen Angaben zu machen, und die Richtigkeit und Vollständigkeit der Daten durch Unterschrift bestätigt. Eine vollständig Internet-basierte Kommunikationsform ist in diesem Bereich derzeit nicht zulässig.

Wie ist die Internet-Kommunikation zwischen Bürgerinnen und Bürgern und der öffentlichen Verwaltung datenschutzrechtlich einzuordnen?

Bei der Internet-basierten Kommunikation zwischen den Bürgerinnen und Bürgern und der Verwaltung sind datenschutzrechtlich zwei Ebenen zu unterscheiden:

Auf der Inhaltsebene sind die Vorgaben für die einzelnen Gegenstandsbereiche zu beachten, die spezialgesetzlich normiert oder den allgemeinen Datenschutzgesetzen zu entnehmen sind.

Auf der Dienste-Ebene gibt es Vorgaben für das Angebot von Informations- und Kommunikationsdiensten, die Pflichten speziell für die Diensteanbieter enthalten. Hierzu gehören die oben erwähnten Nutzungsdaten.

Bei der Anmeldung zum Volkshochschulkurs über das Internet hat Frau A im Beispielsfall ihren Namen und ihre Adresse in das Formular eingegeben. Diese Angaben sind erforderlich, damit Frau A am Kurs teilnehmen kann. Die eingegebenen Daten unterliegen nicht der Diensteebene, weil sie unabhängig von der Art der Kommunikation sind. Sie gehören zur Inhaltsebene. Für die Zulässigkeit der Erhebung der personenbezogenen Inhaltsdaten gilt nichts anderes als bei dem Medium Papier. Fehlt es z. B. schon an der Erforderlichkeit der Angaben, dürfen sie nicht verarbeitet werden.

Bei der E-Mail-Kommunikation ist grundsätzlich zwischen dem Transport im Internet über die E-Mail-Server und dem Empfang bzw. Versand über die Endgeräte zu unterscheiden. Beim reinen Empfang bzw. Absenden einer E-Mail-Nachricht sind die Verwaltungen nicht Adressat der Regelungen des Teledienstedatenschutzgesetzes. Die Zulässigkeit der Speicherung der im Zusammenhang mit der E-Mail-Kommunikation entstandenen Datensätze richtet sich daher auch für die über den Inhalt einer E-Mail hinausgehenden Informationen nach den datenschutzrechtlichen Vorgaben auf der Inhaltsebene. Das bedeutet, dass personenbezogene Daten, wie etwa die Absenderadresse, das Sendedatum oder weitere Sendeinformationen zu löschen sind, wenn ihre Speicherung zur Erfüllung der jeweiligen Aufgabe nicht oder nicht mehr erforderlich ist.

Müssen die Verwaltungen Verschlüsselungsverfahren anbieten?

Anders als bei der Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem Informations- und Kommunikationsdienst E-Mail sind die Verwaltungen Diensteanbieter, wenn sie die Bürgerinnen und Bürger zu einer Internet-basierten Kommunikation etwa im Rahmen einer Homepage einladen. Nach § 4 Abs. 2 Nr. 3 TDDSG hat der Diensteanbieter durch technische und organisatorische Vorkehrungen sicherzustellen, dass Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch genommen werden können. Für die Nutzerinnen und Nutzer muss also die Möglichkeit - nicht die Verpflichtung - bestehen, sich durch technische Maßnahmen gegen unbefugte Kenntnisnahme und Verfälschung zu schützen (Schaar / Schulz in: Roßnagel, Recht der Multimediadienste, Stand: Januar 2000, RdNr. 91 ff. zu § 4 TDDSG).

Die abstrakte Verpflichtung nach § 4 Abs. 2 Nr. 3 TDDSG regelt allerdings nicht, wie die Verfahren zur Gewährleistung vertraulicher Kommunikation zu gestalten sind. Praktisch bedeutet diese Regelung jedoch, dass die Verwaltungen Verschlüsselungsverfahren anzubieten haben. Das gilt unabhängig vom Inhalt für beide oben genannten Beispielsfälle. Ein Warnhinweis kann zwar der nach § 3 Abs. 5 TDDSG erforderlichen Unterrichtung Rechnung tragen, vielleicht auch Grundlage einer Einwilligung sein. Einen wirksamen Schutz, wie er als technische oder organisatorische Maßnahme nach dem Teledienstedatenschutzgesetz gefordert ist, stellt der Warnhinweis aber nicht dar, weil er keine vor der Kenntnisnahme Dritter geschützte Kommunikation sicherstellen kann.

Die Auswahl des konkreten Verschlüsselungsverfahrens richtet sich nach den allgemeinen Datenschutzgrundsätzen. Danach hat die Verwaltung diejenigen Verschlüsselungsverfahren anzubieten oder zu verwenden, die erforderlich und angemessen sind, um die Vertraulichkeit zu gewährleisten.

Ist der Einsatz von Signaturverfahren erforderlich?

Weder das TDDSG noch das NDSG treffen konkrete Aussagen zu Signaturverfahren. Zum Schutz von Authentizität und Integrität ist der Einsatz von Signaturverfahren auf jeden Fall zu empfehlen. Ob ein Signaturverfahren auch zwingend erforderlich ist, muss im Einzelfall durch Gefahren- und Risikoanalyse festgestellt werden. Auch ist damit zu rechnen, dass Signaturverfahren in bestimmten bereichsspezifischen Regelungen für automatisierte Verfahren verbindlich vorgeschrieben werden. Zum Beispiel ist eine "elektronische Unterschrift" für das "maschinell geführte Grundbuch" in § 75 der Grundbuchverfügung (GBV) bereits vorgeschrieben (vgl. 5.4.3).

Manchmal erweist sich die Verwendung von Signaturverfahren auch aus anderen Erwägungen als sinnvoll. Die Signatur eines Dokumentes kann als obligatorische Voraussetzung für eine elektronische Anmeldung notwendig sein, um die Identität der Betroffenen zweifelsfrei festzustellen und einer Verbreitung unrichtiger Daten über die Betroffenen, wie etwa bei scherzhaften Massenbestellungen unter einem falschen Namen,

5.4.3 Schritte auf dem Weg zur digitalen Verwaltung

Auch wenn E-Government derzeit noch ganz am Anfang steht, so gibt es eine zunehmende Zahl von Projekten, die sich hiermit beschäftigen. Das wichtigste ist wohl das von der Bundesregierung ins Leben gerufene Projekt Media@Komm, in dem die nach einem Wettbewerb als Sieger hervorgegangenen Städte Bremen, Nürnberg und Esslingen E-Government-Modelle entwickeln. Aber auch in Niedersachsen gibt es Aktivitäten. Hierzu gehört die Multimedia-Initiative des Landes Niedersachsen und der Telekom, in der zahlreiche Projekte aus den Bereichen Telekooperation, Televerwaltung, Bildung, Medizin, Verkehr, Kultur und Wissenschaft angegangen werden, zum Teil mit E-Government-Bezug (www.niedersachsenonline.de). Vom Niedersächsischen Städte- und Gemeindebund ist das Portal gemeinde4u entwickelt worden, über das ein besserer Zugang zu Industrie und Gewerbe in den Regionen, aber auch zur kommunalen Verwaltung gefunden werden soll (www.gemeinde4u.de). Weiterhin sind gerade aus datenschutzrechtlicher Sicht von besonderer Bedeutung:

Das elektronische Grundbuch

In den niedersächsischen Grundbuchämtern sollen ab 2001 "maschinell geführte" Grundbücher eingeführt werden. Es ist vorgesehen, dass das elektronische Grundbuch nicht nur den Grundbuchämtern selbst, sondern z. B. auch Gerichten, Behörden und Notaren im Online-Verfahren zur Verfügung steht. Die rechtliche Zulässigkeit und die Ausgestaltung ist in der Grundbuchordnung (GBO) bereichsspezifisch geregelt worden. Für das Verfahren ist eine "elektronische Unterschrift" vorgesehen, die allerdings leider nicht die Qualität einer Signatur nach dem Signaturgesetz erreicht. Vor der Einführung des Verfahrens ist eine Technikfolgenabschätzung nach § 7 Abs. 3 des Niedersächsischen Datenschutzgesetzes erforderlich. Das Niedersächsische Justizministerium hat mir die Durchführung der Technikfolgenabschätzung und die Erstellung eines Datenschutz- und Datensicherungskonzepts zugesagt.

Die Immatrikulation über das Internet

An der Georg-August-Universität Göttingen ist seit dem Sommersemester 2000 eine Immatrikulation nur über das Internet oder über PC-Terminals in der Universität möglich. Dieses neue Einschreibungsverfahren berührt in besonderer

Weise den Datenschutz, weil eine elektronische Erhebung bei den angehenden Studierenden in den Verwaltungsvorgang einbezogen ist und ein herkömmliches Verfahren nicht mehr ermöglicht wird. § 33 Abs. des Niedersächsischen Hochschulgesetzes (NHG) legt fest, dass u. a. Verfahren, Formen und Fristen der Immatrikulation in einer Immatrikulationsordnung zu regeln sind. In der Immatrikulationsordnung der Georg-August-Universität Göttingen wird unter § 2 Abs. 4 festgelegt, dass Bewerber ihre persönlichen Daten per Internet zu übermitteln haben. Eine solche einseitige Festlegung auf ein elektronisches Einschreibungsverfahren halte ich ohne das Angebot von Alternativverfahren für unzulässig. Nach § 10 des Verwaltungsverfahrensgesetzes (VwVfG) sind Verwaltungsverfahren zwar nicht an eine bestimmte Form gebunden. Die Formfreiheit bedeutet jedoch keine Ermächtigung zu einer beliebigen Gestaltung. Vielmehr sind schutzwürdige Interessen der Betroffenen zu berücksichtigen. Hierzu zählt eine Datenverarbeitung, die Vertraulichkeit und Integrität der Daten sicherstellt. Auch muss jeder Bewerber die Möglichkeit haben, sich ohne einen unverhältnismäßigen Aufwand einzuschreiben. Dies ist bei einer reinen Internet-Immatrikulation nicht gegeben, weil zurzeit noch nicht davon auszugehen ist, dass jeder Bewerber über einen Internet-Zugang verfügt. In der Praxis hat die Universität dieses Problem durch die Aufstellung von PC-Terminals auf dem Universitätsgelände zu lösen versucht. Ich bin mit der Universität im Gespräch.

5.4.4 Datenschutzgerechtes E-Government der Stadt Hannover

Die in der Fachöffentlichkeit unter verschiedenen Etiketten wie „Electronic Government“ oder „Virtuelles Rathaus“ entwickelten Ideen kommunaler Dienstleistungen im Internet sollen in Hannover bald Wirklichkeit werden. Zu Beginn des Jahres 2000 wurden diese Überlegungen in einem dreistufigen Konzept zusammengefasst und in die politische Diskussion gegeben. Das Projekt will Wege zu mehr Bürgerfreundlichkeit aufzeigen und Perspektiven für effektive und effiziente Arbeitsabläufe in der Verwaltung entwickeln.

Da die technischen und rechtlichen Voraussetzungen für eine Umsetzung entsprechender Dienstleistungen eng mit Fragen des Datenschutzes und der Datensicherheit verbunden sind, habe ich eine Partnerschaft unter dem Arbeitstitel „Datenschutzgerechtes E-Government“ angeboten und inzwischen auch vereinbart. Ich habe mich verpflichtet, die den Datenschutz betreffenden Fragen und Probleme zu untersuchen und datenschutzfreundliche Lösungen mitzugestalten. Unterstützt werde ich hierbei von der Universität Kassel unter Leitung von Prof. Roßnagel, der das Projekt wissenschaftlich begleitet. Die Erkenntnisse sollen wegweisend für moderne Verwaltung sein; sie werden allen Interessierten zur Verfügung gestellt.

Bisher wurden die folgenden Bereiche genauer unter die Lupe genommen:

- das Einwohnermeldewesen,
- die Kfz-Zulassung.
- die Stadtbibliothek,
- das Bauantrags- und Bauanzeigeverfahren,

In allen Bereichen ist es das Ziel, auf der Grundlage des geltenden Rechts pragmatische E-Government-Lösungen zu entwickeln, die Informations- und Transaktionsangebote für die Bürgerinnen und Bürgern enthalten. Außerdem sollen Perspektiven für datenschutzgerechte Lösungen unter neuen rechtlichen Bedingungen geprüft und erarbeitet werden.

Aufbau einer Online-Melderegisterauskunft

Das Einwohnermeldeamt der Stadt Hannover stellt auf einem separaten, gegen unbefugten Zugriff gesicherten Server die Daten zur Verfügung, die für einfache Melderegisterauskünfte nach § 33 Abs. 1 des Niedersächsischen Meldegesetzes (NMG) erforderlich sind (Vor- und Familiennamen, Doktorgrad und Anschriften). Hiervon ausgeschlossen werden die Daten der Personen, für die nach § 35 Abs. 2 und 3 NMG eine Auskunftssperre besteht (Auskunftssperre wegen besonderer Gefährdungen usw.). Dasselbe gilt für Daten der Personen, die nach § 34 Abs. 5 NMG einen Widerspruch gegen die Weitergabe ihrer Daten eingelegt haben (z. B. gegen die Weitergabe an Adressbuchverlage).

Auf diese Daten soll in einem automatisierten Abrufverfahren über das Internet zugegriffen werden können. Hierzu müssen sich interessierte Personen eine digitale Signatur nach dem Signaturgesetz bei einem zertifizierten Trust-Center besorgen. Außerdem müssen sie sich zusätzlich gegenüber der Stadt Hannover identifizieren und die Zugriffsberechtigung beantragen. Die Stadt Hannover ermöglicht ihnen darauf hin, mit Hilfe der digitalen Signatur einfache Melderegisterauskünfte zu einzelnen, bestimmten Personen online einzusehen. Z. B. kann bei Angabe des Namens die zugehörige Anschrift automatisch abgerufen werden.

Auch nach Ansicht des Niedersächsischen Innenministeriums stehen dem geplanten Verfahren keine rechtlichen Bedenken entgegen. Das Verfahren wird demnächst bei der Stadt Hannover eingeführt.

Kfz-Zulassung

Im Bereich der Kfz-Zulassung sind tiefgreifende rechtliche Änderungen in Vorbereitung, die eine weitgehend elektronische Abwicklung des Zulassungsverfahrens möglich machen sollen. In einer ersten Entwicklungsstufe sollen die Händlerzulassung und die Vergabe von Wunschkennzeichen ermöglicht werden.

Hannovers Stadtbibliothek im Internet

Die Stadt Hannover setzt bereits ein modernes Bibliotheksverfahren ein, mit dem über Internettechnologien auf den Datenbestand zugegriffen werden kann. Mit dem Projekt wird der Online-Zugang nicht nur für die Bediensteten der Stadtbibliothek, sondern für jeden Nutzer der Bibliothek über das Internet möglich. Dabei soll nicht nur auf Informationen zu den ausleihbaren Medien zugegriffen werden können (Welche Bücher gibt es? Sind diese verfügbar?), sondern auch auf die eigenen persönlichen Nutzerdaten (Welche Bücher habe ich ausgeliehen und wann muss ich sie wieder zurückbringen? Welche Bücher habe ich vorgemerkt? Welche Gebühren muss ich noch bezahlen?). Ebenso sollen Nutzer möglichst viele Schritte des Ausleihverfahrens über das Internet ausführen können, z. B. die Verlängerung der Ausleihfrist oder eine Vorbestellung. Ein ähnliches Verfahren wird im Hochschulbereich bereits vom Gemeinsamen Bibliotheksverbund (GBV) durchgeführt, an dessen datenschutzgerechter Gestaltung ich beteiligt war (XIV. TB, 22.2).

Im Rahmen des Ausleihverfahrens werden umfangreiche personenbezogene Daten der Nutzer gespeichert. Der Umfang der Daten ist für die Abwicklung des Bibliothekbetriebes erforderlich und entspricht im Wesentlichen dem bisherigen. Durch die Internetanbindung werden die Daten jedoch nach außen weitergegeben. Im Gegensatz zu anderen Verfahren sollen hier aber nur die jeweils betroffenen Nutzer die Empfänger sein. Datenschutzrechtlich handelt es sich also nicht um eine Übermittlung, die eine Weitergabe an Dritte voraussetzt. Die Regelungen der §§ 12 und 13 des Niedersächsischen Datenschutzgesetzes sind daher nicht einschlägig.

Wichtig ist hier aber, dass Technik und Organisation des Verfahrens tatsächlich nur das zulassen, was gewollt ist. Der Zugriff der einzelnen Nutzer muss durch eine sichere Rechteverwaltung auf die eigenen Daten beschränkt werden. Hierzu ist eine eindeutige Identifikation erforderlich. Dies ist mit einem sicheren Passwortverfahren in angemessener Weise erreichbar. Auch hier ist allerdings die Einführung einer Signaturkarte wünschenswert, die eine besonders starke Berechtigungsprüfung ermöglicht. Die relativ hohen Kosten eines solchen Kartensystems (ca. 100 DM pro Nutzer) würde zurzeit aber nur von wenigen akzeptiert. Wenn in Zukunft die meisten Nutzer eine für diesen Zweck geeignete Karte besitzen werden, sollte das bisherige Passwortverfahren durch ein kartenbasiertes Verfahren abgelöst werden. Bereits jetzt ist es erforderlich, für die Übertragung von Daten über das Internet ein Verschlüsselungsverfahren einzurichten. Hierfür eignet sich der secure socket layer (SSL), den die gängigen Browser unterstützen. Die eingesetzte Schlüssellänge muss mindestens 128 bit betragen.

6 Informations- und Kommunikationstechnik

6.1 Es boomt ...

Das Internet boomt; „Goldgräberstimmung" macht sich breit. 28 Prozent der deutschen Haushalte „sind schon drin" im Internet. Das Internet ist nicht nur eine gewaltige, ständig wachsende Fundgrube für Informationen, es ist inzwischen auch ein rasant wachsender Marktplatz, auf dem viele Unternehmen Geld umsetzen wollen. 9 Millionen Menschen haben im vergangenen Jahr online gekauft und dabei ein Umsatzvolumen von 1 Milliarde DM geschaffen. Auch wenn dies - ähnlich wie das Graben nach Gold - noch nicht in jedem Fall profitabel ist, so erkennen viele, dass sie jetzt ihren Claim abstecken müssen, um später an den Gewinnen zu partizipieren. Es engagieren sich mittlerweile nicht nur „Dotcoms" - also reine international agierende Internet-Firmen - mit einfallsreichen Ideen und ungewöhnlichen neuen Ansätzen im Bereich von E-Commerce und E-Business. Auch die etablierten Unternehmen in nahezu allen Branchen führen zügig E-Commerce-Anwendungen ein, um neue Kunden zu gewinnen oder zumindest das Wegbrechen von vorhandenen Marktanteilen zu verhindern.

Diese neuen Entwicklungen im Internet, bei E-Commerce und E-Government halten die Datenschützer in Atem und verändern ihre Arbeit (vgl. 3.1 und 4.2). Eine weitere Herausforderung des Datenschutzes der Gegenwart ist die zunehmende Vernetzung der Datenverarbeitung in Wirtschaft und Verwaltung. Eine umfassende Datenschutzkontrolle ist weder von mir noch von anderen Datenschützern leistbar. Ich habe daher begonnen, meine Geschäftsstelle in ein Kompetenzcenter für die öffentliche Verwaltung und für die Wirtschaft umzuwandeln. Dabei setze ich auf Zusammenarbeit und Vernetzung der Datenschutzexperten aller Interessengruppen. Weiter versuche ich, Methoden des Datenselbstschutzes aufzuspüren. Ich suche die Kooperation mit Herstellern und Anbietern und biete allen mein Wissen und meine Erkenntnisse an. Bürgerinnen und Bürger berate ich im Auffinden und Anwenden von Maßnahmen zum Selbstschutz.

6.2 Selbstschutz tut Not

6.2.1 Selbsttest für Internet-Surfer

Seit August 2000 biete ich Internet-Surfern einen Selbsttest an, mit dem sie die Sicherheit ihres Rechners prüfen und verbessern können. Nutzerinnen und Nutzer können den Selbsttest mit ihrem Browser über meine Homepage

www.lfd.nieder-sachsen.de aufrufen. Der Selbsttest will und kann keine Sicherheitseinstellungen verändern. Diese muss der Nutzer selbst vornehmen. Der LfD-Server liefert ihm dazu die Ergebnisse des Tests als HTML-Seite zurück und gibt Hinweise und Tipps zur Behebung von Sicherheitslücken. Der Sicherheits-Check, vor dessen Beginn Hinweise zur Durchführung gegeben werden, besteht aus drei eigenständigen Phasen. Das Ergebnis der jeweiligen Phase erscheint umgehend auf dem Bildschirm. Die Kommunikation zwischen dem LfD-Server und dem zu testenden Rechner erfolgt verschlüsselt. Ein Abhören der Leitung durch Dritte ist somit zwecklos. Zur Verschlüsselung wird das Protokoll SSL (Secure Socket Layer) benutzt. Da das notwendige Zertifikat vom beauftragten Trust-Center nicht rechtzeitig zum Start des Selbsttests bereit gestellt werden konnte, wurde zunächst ein selbstgeneriertes Zertifikat verwendet. Dieses Zertifikat wurde von den Standard-Browsern als unsicher eingestuft. Das offizielle „Class 3-Server-Zertifikat" hat dieses Anfangsproblem inzwischen behoben.

Die Ergebnisse der drei Phasen des Selbsttests werden gespeichert und statistisch ausgewertet. Die abgelegten Daten enthalten dabei lediglich einen Zeitstempel sowie die ermittelten sicherheitsrelevanten Informationen. Angaben die Herkunft des Klienten (z. B. IP-Adresse oder Nutzername) werden nicht abgelegt. Die Auswertung wird für jede der drei Phasen getrennt durchgeführt. Interessierten werden die Ergebnisse aller durchgeführten Selbsttests zur Verfügung gestellt.

Der Selbsttest - als eine Datenselbstschutz-Maßnahme für Bürgerinnen und Bürgern in der Informationsgesellschaft gedacht - hat eine erfreuliche Resonanz gefunden. Bereits nach zwei Wochen wurden 30 000 Tests durchgeführt. Zahlreiche E-Mails und Anrufe haben mein Vorgehen bestätigt; selbst aus Amerika kam Lob. Natürlich gab es auch Kritik aus der „Netzcommunity", insbesondere über die Anlaufschwierigkeiten. Ich bin auch weiterhin an Äußerungen interessiert und bereit, Anregungen zur Verbesserung und Erweiterung - soweit möglich - in den Selbsttest einzuarbeiten.

6.2.2 Checklisten zur Selbstkontrolle

In die Reihe der Datenselbstschutz-Maßnahmen gehören auch meine Orientierungshilfen und Checklisten zu technischen Themen der automatisierten Datenverarbeitung. Geschäfts- und Behördenleitungen, Personalleitungen und Personalvertretungen, Datenschutzbeauftragte sowie Organisations- und DV-Leitungen werden mit den Orientierungshilfen in die Lage versetzt, die notwendigen Datensicherungskonzepte zu entwickeln, Technikfolgenabschätzungen vorzunehmen oder einfach ihr vorhandenes Sicherheitskonzept kritisch zu prüfen und zu verbessern. Ich selbst verwende die Prüfkataloge bei meinen Prüfungen im Bereich der öffentlichen Verwaltung und der Wirtschaft, stelle sie aber auch allen Interessierten zur Überprüfung ihrer Verfahren sowie der getroffenen technischen und organisatorischen Maßnahmen zur Verfügung.

Im Folgenden möchte ich meine neuen Broschüren in Kurzform vorstellen:

Datenschutz in Netzen

In Unternehmen und öffentlichen Verwaltungen gibt es kaum noch Computer, die nicht in ein Netzwerk eingebunden sind. Vielen Nutzern steht auch ein Zugang zum Internet mit elektronischer Post und dem Zugriff auf große Mengen personenbezogener Daten zur Verfügung. Mit der zunehmenden Vernetzung sind zahlreiche Datenschutz- und Datensicherheitsrisiken verbunden, die durch geeignete technische und organisatorische Maßnahmen abzusichern sind. Die

vorliegende Orientierungshilfe beschreibt Gefahren, benennt Lösungsansatze und stellt Checklisten zur Sicherheitsüberprüfung von Netzwerken zur Verfügung.

Im Einzelnen werden behandelt:

- Grundlagen der Netzsicherheit,
- Netz-Hardware,
- Übertragungsprotokolle,
- Netzwerk- und Transportprotokolle,
- Betriebssysteme,
- Netzwerkmanagement-Systeme,
- Verschlüsselungssysteme.

Datenschutz bei Tele- und Mediendiensten

Das Telekommunikations- und das Multimediarecht regeln für Anbieter und Nutzer den Umgang mit den Tele- und Mediendiensten. In der Bundesrepublik Deutschland sind hierfür rechtliche Rahmenbedingungen geschaffen worden, die richtungsweisende Regelungsansätze enthalten. Die Orientierungshilfe weist auf Gefahren und Risiken bei der Anwendung der Tele- und Mediendienste hin, beschreibt die Pflichten der Anbieter und die Rechte der Nutzer und gibt konkrete Empfehlungen für technische und organisatorische Sicherungsmaßnahmen. Die beigefügte Checkliste gibt Tele- und Mediendiensteanbietern Hilfen für die Konzeption ihrer Dienste und ermöglicht eine Kontrolle der getroffenen Sicherheitsmaßnahmen.

Passworte... aber richtig

Das Passwortverfahren ist gegenwärtig das am meisten verwendete Verfahren, um den unberechtigten Zugriff auf personenbezogene Daten zu verhindern. Jeder Benutzer sollte über eine Benutzerkennung und über ein persönliches Passwort verfügen, um sich so gegenüber dem IuK-System als Berechtigter ausweisen zu können. Meine Prüferfahrungen im Bereich der öffentlichen Verwaltung und der Wirtschaft zeigen jedes Jahr wieder deutlich auf, dass ein unsicheres Passwortverfahren nach wie vor zu den am häufigsten beanstandeten datenschutzrechtlichen Verstößen gehört. Die Checkliste für die Passwortgestaltung und -verwendung enthält konkrete Empfehlungen für technische und organisatorische Sicherungsmaßnahmen.

Protokollierung

Durch Protokollierung aller Verarbeitungsaktivitäten wird die IuK-Technik nachprüfbar und transparent. Zugleich wird damit einer missbräuchlichen Verwendung vorgebeugt, weil niemand darauf vertrauen kann, dass Verstöße unentdeckt bleiben. Mit der Protokollierung der Verarbeitung entstehen aber auch Sammlungen personenbezogener Daten über Nutzer bzw. über Betroffene. Damit wird es z. B. möglich, Nutzerprofile abzuleiten oder Listen über Auffälligkeiten zu erstellen. Für Art, Umfang und Aufbewahrung der Protokollierung gilt daher der Grundsatz der Erforderlichkeit. Die Checkliste beschreibt Art und Umfang der notwendigen Maßnahmen gegliedert nach:

- Allgemeine Rahmenbedingungen,
- Administration der IuK-Technik,
- Benutzung der IuK-Technik sowie
- Auswertung der Protokolle.

Verschlüsselung

E-Mails gehören zu den unsichersten Formen der elektronischen Kommunikation. Sie können von Unbefugten gelesen, manipuliert oder verändert werden. Gleiche Gefahren drohen auch bei der Speicherung von Daten auf dem PC oder auf mobilen Datenträgern. Wirksamstes Mittel gegen diese Gefahren ist die Verschlüsselung. Die zu schützenden Daten werden dabei so verändert, dass sie nur autorisierten Personen oder Geräten verständlich sind, für alle anderen aber sinnlos erscheinen. Grundprinzip ist die Veränderung (Vertauschung und Ersetzung) der Daten mit Hilfe von Rechenoperationen (Verschlüsselungsalgorithmus), der durch einen Parameter gesteuert wird. Wem Algorithmus und Schlüssel zur Verfügung stehen, kann die Daten ver- bzw. entschlüsseln. Ohne Kenntnis des Schlüssels lassen sich die Daten nur durch Ausprobieren aller möglichen Schlüssel zurückgewinnen ("brute force-Attacke"). Verschlüsselung steht heute jedem zur Verfügung, ihre Anwendung ist einfach. Die Orientierungshilfe zeigt den möglichen Einsatz von Verschlüsselungs- und Signaturverfahren auf und gibt praktische Hilfen zur Einführung.

Windows NT 4.0

Das Betriebssystem Windows NT 4.0 hat bei vielen Stellen der Privatwirtschaft und der öffentlichen Verwaltung die Version 3.51 abgelöst. Die aktuelle Version hat eine Reihe von neuen Funktionen, die für den Datenschutz und die Datensicherheit der Daten sowohl auf dem Server als auch auf den angeschlossenen Arbeitsplätzen genutzt werden können. Die Orientierungshilfe und Checkliste für den datenschutzgerechten Einsatz von Windows NT 4.0 geben Systemverwaltern Hilfestellung bei der Erarbeitung datenschutzgerechter Lösungen für den Einsatz von Windows NT. Für betriebliche und behördliche Datenschutzbeauftragte ist die Checkliste eine Kontrollhilfe. Sie ist auch zur Selbstkontrolle geeignet.

Systembetreuung, Wartung und Fernwartung

Die Checkliste kennzeichnet die Sicherheitsbereiche und beschreibt die notwendigen technischen und organisatorischen Maßnahmen. Um einen geordneten Betrieb von Informations- und Kommunikationssystemen zu ermöglichen, ist ein Systemadministrator erforderlich. Personen, die mit der Systemverwaltung betraut werden, sollten folgende Aufgaben erfüllen:

- Mitarbeit bei Organisation und Planung des IuK-Technikeinsatzes
- Systemadministration
- Netzwerkverwaltung und -überwachung
- Systemoperating und Wartung
- Kontroll-, Organisations- und Betreuungsmaßnahmen.

Die Checkliste beschreibt die Personalauswahl, die Aus- und Fortbildung sowie die technischen und organisatorischen Maßnahmen zur datenschutzgerechten Systemverwaltung und Wartung.

Zutrittskontrolle

Daten verarbeitende Stellen, die personenbezogene Daten automatisiert verarbeiten, sind gesetzlich verpflichtet, geeignete Maßnahmen zu treffen, um Unbefugten den Zutritt zu den Verarbeitungsanlagen zu verwehren („Zugangskontrolle"; § 7 Abs. 2 Nr. 1 des Niedersächsischen Datenschutzgesetzes bzw. Anla-

ge zu § 9 des Bundesdatenschutzgesetzes). Art und Umfang der notwendigen Sicherungsmaßnahmen richten sich dabei nach der Sensibilität der gespeicherten Daten. Die Checkliste gibt hierzu Hinweise und Empfehlungen.

6.3 Trojanische Pferde und anderes Ungetier

Viren haben erneut von sich reden gemacht; diesmal war es „LoveLetter", der den Mail-Verkehr in weiten Bereichen von Wirtschaft und Verwaltung zeitweise zum Erliegen brachte. Selbst große Unternehmen und Teile der öffentlichen Verwaltung hatten erhebliche Schwierigkeiten mit dem lawinenartig anwachsenden Mail-Aufkommen. Auch Melissa hat, wie schon viele Viren vor ihm, gezielt Schwachpunkte in weit verbreiteten Mail-Clients genutzt, um sich auszubreiten. Schon wenige Stunden nach dem ersten Auftritt des Virus standen Updates für die verbreitetsten Virenscanner bereit; dennoch können diese Updates immer erst entwickelt werden, wenn ein neuer Virus bekannt geworden ist.

Unter Viren wird Schadsoftware verstanden, die sich in anderen Programmen versteckt, von dort ihre Schadfunktion ausübt und sich darüber hinaus auch noch durch Infektion anderer geeigneter Programme vermehrt. Dagegen sind aktive Inhalte nicht per se Schadsoftware. Zunächst einmal handelt es sich schlicht um relativ kleine Programme, die mit Hilfe von E-Mail, Dokumentenaustausch oder beim Surfen im Internet auf den lokalen Rechner übertragen und dort abgearbeitet werden. Welche Funktion diese Programme ausführen, ist dabei technisch nicht festgelegt. Im positiven Fall helfen sie bei der Gestaltung einer Webseite oder der Darstellung des Ergebnisses einer Datenbank-Recherche; im negativen Fall sammeln sie alle Kennungen und Passwörter und versenden sie via E-Mail oder per File Transfer an einen Rechner irgendwo im weiten Internet. Und das alles ohne Kenntnis des rechtmäßigen Benutzers! Ob sie dann hinterher auch noch die Festplatte formatieren oder anderen Unsinn treiben, hängt von der Intention des Programmierers ab. Will er oder sein Programm unerkannt bleiben, wird wahrscheinlich zunächst keine spektakuläre Aktion erfolgen.

Während gegen (bekannte) Viren in aller Regel ein wirksames Kraut in Form eines aktuellen und gepflegten Virenscanners (zentral im Mail-Server und/oder dezentral auf den Clients) gewachsen ist, steht die Technik den aktiven Inhalten noch etwas hilflos gegenüber. Zwar gibt es einfache Möglichkeiten, die Gefährdung durch derartige Inhalte gegen null zu reduzieren; dies bedingt jedoch zwingend den Verzicht auf den Einsatz der entsprechenden Technik. Dieser Verzicht bewirkt inzwischen jedoch leider, dass eine sehr große Anzahl von Web-Seiten nur noch eingeschränkt oder auch überhaupt nicht mehr genutzt werden kann. Darüber hinaus gehen den Anwendern ganz wesentliche Komfort-Merkmale verloren, die ein sinnvolles Arbeiten und Zusammenwirken der Einzelkomponenten von Bürokommunikationssystemen überhaupt erst ermöglichen. Aus diesem Grund ist die technische Filterung dieser aktiven Komponenten nur schwierig zu realisieren und bleibt generell fehlerbehaftet.

So bleibt es im Grunde bei der altbekannten „Weisheit": nur aktuelle Virenscanner von namhaften Unternehmen einsetzen und nur mit „gesundem Misstrauen" an der elektronischen Kommunikation teilnehmen. Die Hersteller von Mailprogrammen bleiben aufgerufen, bereits bei der Programmentwicklung ein größeres Gewicht als bisher auf Sicherheit zu legen.

6.4 Sicherheit im Landesnetz

Die Landesverwaltung ist mit großem Eifer und hohem Mitteleinsatz dabei, die Dienststellen an das Internet anzuschließen und eigene Informationsportale auf-

zubauen. Sie will auf diese Weise eine moderne, bürgernahe Verwaltung fördern - so die politische Aussage. Dieses Konzept bietet jedoch nicht nur Vorteile. Bei möglichen Angriffen aus dem Netz könnten die Sicherheit der Informations- und Kommunikationstechnik des Landes und der gespeicherten personenbezogenen Daten gefährdet sein.

Das Landesnetz mit mehr als 60 000 Nutzern muss aufgrund seiner Größe, der physikalischen Ausdehnung und der Vielzahl administrativer Stellen als ein gefährdetes Netz angesehen werden. Daher habe ich zusammen mit der Universität Hannover - Lehrgebiet Rechnernetze und Verteilte Systeme - exemplarisch eine Bestandsaufnahme lokaler Netzkomponenten durchgeführt, mögliche Schwachstellen in lokalen Netzen analysiert und auf der Basis dieser Informationen für das LAN meiner Geschäftsstelle eine moderne Firewall-Installation zur Absicherung der Anbindung an das Landesnetz erarbeitet.

Diese Firewall schützt seither das lokale Netzwerk der Geschäftsstelle gegen Übergriffe aus dem iznNet oder dem Internet, indem alle Verbindungen zwischen den Netzen ausschließlich über die Firewall abgewickelt werden. Die eingesetzte Firewall ist gut geeignet, ein lokales Netzwerk einer Dienststelle sauber vom iznNet zu trennen und einen kontrollierten Datenverkehr zwischen beiden Netzen sicherzustellen. Damit kann ein unberechtigter und unkontrollierter Zugriff aus dem iznNet auf das interne LAN nach heutigem Kenntnisstand ausgeschlossen werden.

Die eingesetzte Firewall vereint in sich die Funktionalitäten von Packetfilter, Proxy und Network-Adress-Translation. Der Packetfilter ist in der Lage, den Zugriff auf der Basis von IP-Adressen und Port-Nummern zu überprüfen. Hierzu werden in erster Linie die Adressen von Absender und Empfänger eines IP-Packets auf Zulässigkeit an der Regelbasis überprüft. Der Packetfilter sichert weiter, dass nur die zulässigen Ports ansprechbar sind und somit keine Hintertüren in das Netzwerk der Geschäftsstelle führen. Über die Proxy-Prozesse können darüber hinaus Dienste spezifische Regelungen für die Nutzung getroffen werden. So können für bestimmte Dienste nur Teile des Befehlsvorrats freigegeben werden oder Einschränkungen in der Benutzungsrichtung (von außen nach innen/von innen nach außen) realisiert werden. Für die weitergehende Filterung bestimmter Webangebote etwa nach URL fehlen innerhalb des izn-Net derzeit allerdings die technischen Voraussetzungen; diese Filtermöglichkeiten benötigen zum Einsatz den Zugriff auf Namensauflösungen aus dem Internet (DNS-Server). Dieser Zugriff wird jedoch von der zentralen Firewall des Landes beim izn aus gutem Grund verhindert.

Allerdings kann keine Firewall - auch nicht die ausgewählte - alle bekannten und erst recht nicht die in der Entwicklung befindliche Schad-Software mit 100%iger Sicherheit kontrollieren und abblocken. So kann die Firewall weder die Einschleppung von Viren z. B. via E-Mail verhindern noch ist sie in der Lage, aktive Inhalte aller Art innerhalb von übertragenen Dokumenten oder im Zusammenhang mit Web-Seiten zu kontrollieren. Es gibt allerdings in neuerer Zeit Ansätze, die zusätzliche Sicherheit schaffen können. Einer dieser Ansätze ist die sog. Sandbox-Technik. Hierbei wird versucht, die aktiven Inhalte aller übertragenen Dateien zu filtern. Zunächst werden die Dateien auf bekannte Merkmale von Schadsoftware untersucht und anschließend in einer gesicherten Umgebung, eben der Sandbox, gestartet. Durch Verwenden dieser Sandbox steht der aktive Inhalt beim Ausführen sozusagen unter ständiger Beobachtung und es ist möglich, die Zugriffe des Programms auf Systemressourcen oder das Dateisystem gezielt zu unterbinden. Im Extremfall kann bei entsprechendem Verdacht die Programmausführung auch schlichtweg abgebrochen werden.

Es sind unterschiedliche Versionen entsprechender Sicherheitssoftware am Markt, die die Prüfungen und Überwachungen entweder zentral auf einem an die

Firewall „angedockten“ Server-System oder auch lokal auf den Arbeitsstationen der Benutzer durchführen. Der zentrale Einsatz kommt insbesondere für die beim Web-Surfen übertragenen aktiven Inhalte in Betracht, der lokale Einsatz deckt demgegenüber auch Programme ab, die von anderen Medien, über verschlüsselte E-Mails oder auf anderem Wege in das System gelangt sind. Ich habe mich zum optimalen Schutz für einen kumulativen Einsatz dieser Sicherheitssoftware entschieden; die Ergebnisse sind durchweg positiv.

Ich ermögliche so den Mitarbeiterinnen und Mitarbeitern der Geschäftsstelle einen direkten Zugang zum Landesnetz und zum Internet von ihrem Arbeitsplatzrechner aus. Ein zentraler Virenscanner sowie Virenscanner auf jedem APC sichern zudem den E-Mail-Verkehr gegen „unliebsame Gäste“. Darüber hinaus wird vor einem offiziellen Einsatz durch eine Vereinbarung mit den Mitarbeiterinnen und Mitarbeitern der Rahmen für die Nutzung der Internetanbindung verbindlich absteckt und das Verständnis für die Gefahrenlage bei der Nutzung der Internet-Anbindung gestärkt.

Meine Erkenntnisse aus dieser Untersuchung und der Installation habe ich dokumentiert. Mit der Veröffentlichung „Sicherheit im Landesnetz“ möchte ich allen Dienststellen des Landes Niedersachsen aufzeigen, wie eine sichere und kostengünstige Anbindung an das Landesnetz und an das weltweite Internet möglich ist. Die Ausführungen in der Orientierungshilfe enthalten konkrete Handlungsempfehlungen.

6.5 P 53 = Automatisierte Haushaltsmittelbewirtschaftung des Landes

6.5.1 Das Verfahren im Überblick

Seit dem 3. Januar 2000 betreibt das Land Niedersachsen ein automatisiertes Haushaltswirtschaftssystem mit den Funktionen Mittelverteilung, Mittelbewirtschaftung und Kasse. Das Verfahren soll an 12 000 Arbeitsplätzen in der niedersächsischen Landesverwaltung genutzt werden. Alle Buchungen der rund 700 Dienststellen werden nicht mehr in Papierform vorgenommen. Die alte schriftliche Kassenanordnung, die nach dem „Vier-Augen-Prinzip“ von zwei autorisierten Amtspersonen handschriftlich unterschrieben werden musste, gibt es nicht mehr. Solche Kassenanordnungen werden heute elektronisch umgesetzt und sofort vollzogen. Auf eine Funktion dieses Projekts ist die Landesregierung zurecht besonders stolz, nämlich auf die Einführung der Digitalen Signatur.

Jede Daten verarbeitende Stelle ist für den datenschutzgerechten Einsatz ihrer Anwendungen selbst verantwortlich. Sie hat daher eine den Vorschriften des NDSG entsprechende Verarbeitung personenbezogener Daten sicherzustellen.

6.5.2 Zentrale Softwareverteilung

Das Projekt P 53 sieht eine zentrale Softwareverteilung vor. Dezentrale Lösungen kämen aufgrund der Anzahl der betroffenen Arbeitsplätze nicht in Betracht, ist die Ansicht des federführenden Finanzministeriums. Einer Einführung der Softwareverteilung mit dem Produkt „ASDIS“ für das Projekt P 53 steht nach meiner Einschätzung nichts entgegen, wenn die folgenden Grundsätze eingehalten werden.

Die datenschutzgerechte Softwareverteilung wird durch folgende Maßnahmen gesichert:

– Art und Umfang der Verteilung werden schriftlich geregelt.

- Die Übermittlung erfolgt verschlüsselt.
- Verteilungspasswörter werden nur verschlüsselt übertragen.
- Alle Verteilungsaktivitäten werden protokolliert.
- Die Verteilung kann jederzeit durch den Auftraggeber abgebrochen werden.
- Der Auftraggeber überprüft die Einhaltung der vereinbarten Sicherungsmaßnahmen.

Die Einhaltung dieser Grundsätze haben die Projektverantwortlichen zugesagt.

6.5.3 Das Sicherheitskonzept

Mit der Einführung des automatisierten Haushaltswirtschaftssystems wird jeder PC-Arbeitsplatz mit einer persönlichen Sicherheitsumgebung (PSE) ausgestattet. Die Sicherheitsumgebung setzt sich aus folgenden Bestandteilen zusammen:

- Persönliche Chipkarte (PKS-Karte der Fa. TeleSec),
- Chipkartenlesegerät (Fa. UtiMaco),
- diverse Softwarekomponenten für den PC (PPM Digitale Signatur der Fa. BaaN, Signaturbibliothek, STP-Verschlüsselungskomponente u. PSE-Management der Fa. Secude, Treibersoftware).

Die Chipkarte wird zunächst dafür eingesetzt, Kassenanordnungen bei der Freigabe mit einer elektronischen Unterschrift (Digitale Signatur) zu versehen, durch die zum einen ein zweifelsfreier Identitätsnachweis des Anwenders geführt (Authentizität) und zum anderen die Unversehrtheit der Anordnungsdaten sichergestellt wird (Integrität). Das dafür entwickelte Verfahren entspricht den strengen Anforderungen des Signaturgesetzes (SigG) und der Signaturverordnung (SigVO) und ist in seiner technischen, an modernsten Standards ausgerichteten Ausgestaltung richtungsweisend.

Neben dem dafür notwendigen Signaturschlüsselpaar enthält die Chipkarte auch das Schlüsselpaar, durch das der für das Verfahren PPM betriebene Datenverkehr zwischen allen PC-Arbeitsplätzen und den Produktionsrechnern im izn einer starken Client-Server-Verschlüsselung unterzogen wird. Die Verschlüsselung wird auf einer anwendungsunabhängigen Transportschicht betrieben. All dies läuft automatisch im Hintergrund ab, ohne dass nennenswerte Nutzeraktivitäten erforderlich werden. Die Form der Datenverschlüsselung entspricht den modernsten Sicherheitsempfehlungen. Die Digitale Signatur basiert auf einem Public-Key-Kryptoverfahren (RSA-Verfahren) mit einem geheimen und einem öffentlichen Signaturschlüssel. In der Anwendung PPM greift die Funktionalität der digitalen Signatur auf eine hierfür entwickelte Komponentenbibliothek der Fa. Secude zurück. Die Vertraulichkeit der übertragenen Daten wird mittels einer Client-Server-Verschlüsselung sichergestellt. Zur Anwendung kommt ein hybrides symmetrisch-asymmetrisches Verschlüsselungsverfahren, bei dem die Daten mit einem zufällig unmittelbar vor dem Verschlüsselungsvorgang generierten Schlüssel im Wege des Private-Key-Verfahrens symmetrisch verschlüsselt werden. Dieser Schlüssel wird sodann im Public-Key-Verfahren verschlüsselt.

6.5.4 Was ist ein Trust-Center?

Die Aufgaben eines Trust-Centers, d. h. die Registrierung, Zertifizierung und personalisierte Schlüsselgenerierung nimmt die von der Regulierungsbehörde

für Telekommunikation und Post (RegTP) im Sinne des SigG zertifizierte Fa. TeleSec wahr. Die TeleSec bietet ferner einen Verzeichnis-, Sperr- und Zeitstempeldienst. Der Abschluss eines Rahmenvertrages zwischen dem Land Niedersachsen und der Fa. DeTeSystem wird allen künftigen Anwendern des Systems die dienstliche Nutzung der persönlichen Chipkarte und der erforderlichen Verzeichnisdienste des Trust-Centers ermöglichen. Das Land Niedersachsen hat seine Bediensteten von sämtlichen Haftungsansprüchen der Deutschen Telekom AG sowie von sämtlichen Ansprüchen freistellt, die durch die Zertifizierungsstelle verursacht werden. Die Kosten der Nutzung des Verfahrens werden vom Land Niedersachsen getragen.

Nach Maßgabe des Signaturgesetzes muss die Chipkarte von jedem Anwender unter Vorlage eines ausgefüllten zweiseitigen Formulars und eines Identitätsnachweises persönlich beantragt werden. Die Anträge nimmt jeder T-Punkt der Deutschen Telekom AG entgegen. Daneben ist mit der Fa. DeTeSystem vereinbart worden, dass bei größeren Dienststellen sog. mobile T-Punkte eingerichtet werden können, um die Antragsaufnahme zu beschleunigen und die Abläufe für die Beschäftigten komfortabler zu gestalten. Nach Bearbeitung der Anträge wird die Fa. TeleSec die Chipkarten unmittelbar an die Nutzer an deren dienstliche Adresse versenden. Der Empfang der Chipkarte ist vom Anwender durch eine Empfangsbestätigung zu quittieren. Nachdem die Empfangsbestätigung der Zertifizierungsstelle wieder vorliegt und dort der Nutzer in ein Verzeichnis eingetragen worden ist, kann die Chipkarte eingesetzt werden. Beim erstmaligen Gebrauch der Chipkarte ist diese vom Benutzer mittels einer speziellen Software (PSE-Management) zu initialisieren und mit einem geheimen Passwort (PIN) zu versehen.

6.5.5 Die digitale Unterschrift zum Dienstgebrauch

Im Rahmen des Signaturverfahrens werden personenbezogene Daten der betroffenen Bediensteten verarbeitet. Die Verarbeitung erfolgt auf den Rechnern der einzelnen Dienststellen, beim izn und bei der Telesec. Dabei verarbeitet die Telesec diese Daten im Auftrag für das Land Niedersachsen. Die Einführung von P 53 setzte zwingend voraus, dass Unterschriften, z. B. auf Kassenanordnungen, nicht mehr auf Papier, sondern elektronisch geleistet werden. Die Verarbeitung der Bedienstetendaten ist daher für die organisatorische Umsetzung des Projekts P 53 erforderlich gewesen. Die Zulässigkeit beurteilt sich nach § 101 Abs. 2 des Niedersächsischen Beamtengesetzes.

Dabei waren folgende Punkte zu beachten:

Eine private Nutzung des Signaturverfahrens ist untersagt. Telesec darf personenbezogene Daten der Zertifikate nicht zum Abruf bereit stellen. Für das Verfahren sind die erforderlichen technischen und organisatorischen Maßnahmen getroffen worden, um eine den Vorschriften des NDSG entsprechende Verarbeitung sicherzustellen (Sicherheitskonzept). Dabei war der Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten.

Die personenbezogenen Daten sind bei Speicherung und Übertragung gegen die Kenntnisnahme Unbefugter zu schützen und die Bediensteten über Risiken und notwendige Gegenmaßnahmen ausreichend zu unterrichten. Für das Verfahren wurde eine Vereinbarung nach § 81 des Niedersächsischen Personalvertretungsgesetzes (NPersVG) abgeschlossen.

6.5.6 Weiterer Gewinn durch andere Nutzung

Ein weiterer wesentlicher Ansatz der Projektidee besteht darin, mit der Einführung des neuen Systems sowohl die Grundlage für die datentechnische Anbindung einer Vielzahl von Behörden an das Landesdatennetz zu schaffen als auch eine erweiterte Inhouse-Vernetzung und verbesserte Ausstattung eines erheblichen Anteils der insgesamt ca. 55 000 Büroarbeitsplätze zu ermöglichen. Die Ausstattung der PC-Arbeitsplätze berücksichtigt daher neben dem Haushaltsverfahren auch andere Büroanwendungen sowie Anbindungen an Bürokommunikationsdienste, Verzeichnis- und Informationsdienste (E-Mail, MS-Outlook, X-500, Internet). Es ist vorgesehen, die für das Haushaltssystem entwickelten Sicherheitskomponenten auch für die Nutzung von Standard- und Fachanwendungen einzusetzen (z. B. gesicherter E-Mail-Dienst, verschlüsselter Datenverkehr für beliebige Fachanwendungen).

6.6 Technikfolgenabschätzung heißt jetzt Vorabkontrolle

Das Niedersächsische Datenschutzgesetz verpflichtet öffentliche Stellen, vor Einsatz oder wesentlicher Änderung von automatisierten Verfahren die hiermit verbundenen Gefahren und deren Beherrschung durch geeignete Maßnahmen zu untersuchen (§ 7 Abs. 3 NDSG). Mit dieser Regelung hat Niedersachsen vor der EU-Datenschutzrichtlinie und früher als andere Länder ein wichtiges Verfahren eingeführt, um den Gefahren neuer Technologien im Informations- und Kommunikationsbereich zu begegnen. Die inzwischen siebenjährigen Erfahrungen in Niedersachsen zeigen, dass dieses Verfahren bei richtigem Einsatz sehr erfolgreich sein kann.

Technikfolgenabschätzung oder Vorabkontrolle - wie sie die EU-Datenschutzrichtlinie bezeichnet - ist eine Chance. Die Methode bietet die Möglichkeit, auf effiziente Weise notwendige Sicherungsmaßnahmen in automatisierten Verfahren zu berücksichtigen. Technikfolgenabschätzung ist ein Prozess; nicht die Ablieferung eines Papiers steht im Vordergrund, sondern die datenschutzgerechte Gestaltung des Verfahrens. Die Gefahren- und Risikoanalysen sind nur Mittel zum Zweck. Die Substanz der Technikfolgenabschätzung sind die erarbeiteten Sicherungsmaßnahmen, aus denen hervorgeht, unter welchen Rahmenbedingungen das automatisierte Verfahren eingeführt werden kann. Die Bereitschaft zur frühzeitigen Untersuchung möglicher Gefahren und zur Erstellung von Sicherungskonzepten vor dem Einsatz neuer automatisierter Vorhaben hat erfreulich zugenommen. Insbesondere das izn leistet dabei wertvolle Unterstützung für die Daten verarbeitenden Stellen des Landes. Auch ich bin in vielen Projekten frühzeitig beteiligt worden und konnte so meine unentgeltliche Beratungskompetenz einbringen. Eine unrühmliche Ausnahme stellt allerdings das Niedersächsische Justizministerium dar, das es bisher vorgezogen hat, über die gesetzliche Notwendigkeit der Vorabkontrolle zu diskutieren, anstatt sich auf eine nutzbringende Kooperation einzulassen. Ein Beispiel ist die Einführung des maschinellen Mahnverfahrens in der niedersächsischen Justiz, für das nach fast zweijähriger vergeblicher Anforderung einer Vorabkontrolle im Oktober 1999 schließlich ein Datenschutz- und Datensicherungskonzept versprochen wurde. Auch dieses Sicherungskonzept liegt mir bis heute nicht vor.

Im Folgenden sind die wichtigsten Technikfolgenabschätzungen der letzten beiden Jahre aufgeführt.

6.6.1 iznNet

Das iznNet umfasst gegenwärtig drei verschiedene Netze, die technisch nicht zusammengeschlossen sind. Auf ihnen werden unterschiedliche, inkompatible Protokolle eingesetzt. Die Teilnetze sollen im Laufe der Zeit zusammengeführt werden. Zudem liegen Anträge aus dem kommunalen Bereich vor, an das Landesnetz angeschlossen zu werden. Für den Aufbau des iznNet wurden in einer Technikfolgenabschätzung die Schutzbedürftigkeit der im Netz zu transportierenden Daten und eine Gefahren- und Risikoanalyse der Infrastruktur durchgeführt. Danach trägt das izn Verantwortung nur für das technische Netz bis zur Schicht 3 des ISO/OSI-Modells. Zumindest in den Anwendungen der Polizei und der Finanzverwaltung sind jedoch hochsensible Daten zu transportieren, für die einfache Grundschutzmaßnahmen nicht ausreichen. Daraus folgt, dass jede Daten verarbeitende Stelle eigene Datensicherungs- und Datenschutzuntersuchungen anstellen und gegebenenfalls gesonderte Technikfolgenabschätzungen durchführen muss. Meine zusätzlichen Forderungen an die Projektbetreiber und die Sicherheit im Landesnetz sind:

- Die Gefahren der Netzübergänge (Gateways) nach außen müssen besonders untersucht und ihre Absicherungen dargestellt werden.
- Es ist sicherzustellen, dass Fremdnetze nur über zentral kontrollierte Stellen an das iznNet angebunden werden.
- Es muss verbindlich geregelt werden, dass Nutzer des iznNet keine eigenen Verbindungen nach außen herstellen dürfen.
- Die Abschottung der Bereiche Polizei- und Finanzverwaltung muss auch in Zukunft auf unterer Ebene sichergestellt werden.
- Es müssen beim Nutzer ausreichende Absicherungen gegen Virengefahren getroffen werden.
- Für Anwendungen mit personenbezogenen Daten haben Daten verarbeitende Stellen eigene Sicherheitskonzepte, ggf. auch Technikfolgenabschätzungen zu erstellen; das iznNet selbst kann dafür keine ausreichende Sicherheit gewährleisten.

6.6.2 Projekt P 53

Die Technikfolgenabschätzung für das Projekt P 53 wurde im Auftrag des Niedersächsischen Finanzministeriums vom izn erstellt. Das Sicherungskonzept, an dem ich aktiv mitgearbeitet habe, schreibt zum datenschutzgerechten Einsatz der Anwendung BaaN neben dem Grundschutz folgende Maßnahmen verbindlich vor:

- Jede Dienststelle erstellt ein Sicherheitskonzept. Die Maßnahmen des IT-Grundschutzhandbuches (Bundesamt für Sicherheit in der Informationstechnik) sind zu beachten.
- Auf allen Ebenen ist ein Berechtigungs- und Zugriffskonzept (Rechteverwaltung) festzulegen.
- Alle Kassenanordnungen sind digital zu signieren.
- Die Datenübermittlung erfolgt verschlüsselt.
- Alle Clients sind mit dem Betriebssystem Windows NT 4.0 einschließlich Service Pack 3 oder ggf. mit Folgeversionen auszustatten.

- Für die BaaN-Software ist ein Berechtigungskonzept zu erstellen und zu dokumentieren. Regelmäßige Kontrollen des Konzeptes sind vorzusehen.
- Auf Anwendungs- und Administrationsebene sind geeignete Protokollierungen vorzunehmen. Kontrollen sind festzulegen.
- Eine Fernwartung bzw. -administration der Server im izn durch externe Stellen ist auszuschließen.
- Zentrale IuK-Komponenten sind in gesicherten Systembetriebsräumen unterzubringen.
- Zur Beachtung der organisatorischen und technischen Maßnahmen sind in die Dienstanweisungen entsprechende Regelungen zum Datenschutz aufzunehmen.
- Die datenschutzgerechte Softwarefernverteilung erfolgt entsprechend meinen Empfehlungen.
- Bei Änderungen der BaaN-Software muss ein formelles Freigabeverfahren durchgeführt werden.

6.6.3 X.500 Verzeichnisdienste

Auch in der öffentlichen Verwaltung wird zunehmend elektronisch kommuniziert. Hierbei werden elektronische Mitarbeiterverzeichnisse benutzt, auf die von verschiedenen Stellen direkt zugegriffen werden kann. Die elektronischen Verzeichnisse enthalten Informationen und Funktionen, die weit über die bisherigen Möglichkeiten eines in Papierform vorliegenden Adress- und Telefonverzeichnisses hinausgehen. Der Interministerielle Arbeitskreis für Informations- und Kommunikationstechnik (IMA-IuK) hat über den Umfang der erforderlichen Daten und den datenschutzgerechten Einsatz des Verzeichnisdienstes diskutiert und entschieden. Für den X.500-Verzeichnisdienst der niedersächsischen Landesverwaltung wurde nach Beschluss des IMA-IuK eine Technikfolgenabschätzung durchgeführt. Die erforderlichen Daten und die Anforderungen an Erhebung, Speicherung und Nutzung wurden festgelegt. Es wurde die Empfehlung ausgesprochen, das Verfahren durch eine Vereinbarung gemäß § 81 PersVG oder durch eine Rahmendienstvereinbarung abzusichern.

Meine Forderungen zum datenschutzgerechten Einsatz von elektronischen Verzeichnissen wurden erfüllt:

- Der Verzeichniseintrag ist auf die erforderlichen Angaben: Name, Telefon, Telefax, E-Mail-Adresse, Öffentlicher Schlüssel beschränkt. Angaben über Zuständigkeiten, Aufgabenbereiche, Tätigkeitsfelder, Arbeitszeiten sowie Bilder oder persönliche Interessen werden nicht in Verzeichnisdienste aufgenommen.
- Die Zugriffsregelungen für Verzeichnisdienste sind so eng wie möglich zu fassen und durch eine hierfür verantwortliche Stelle vorzunehmen.
- Der Zugriff auf Basisinformationen ist über die jeweilige Dienststelle hinaus für dienstliche Zwecke innerhalb der Landesverwaltung zulässig. Eine darüber hinausgehende Zugriffsmöglichkeit für andere Länderverwaltungen, die Bundesverwaltung oder für die Allgemeinheit (z. B. über das Internet) ist im Einzelfall zu prüfen. Dabei ist entscheidend, ob der Zugriff zur Kontaktaufnahme oder -pflege erforderlich ist; bei dieser Bewertung ist zu berücksichtigen, dass sich die moderne Verwaltung als Dienstleister versteht und eine nachhaltige Öffnung gegenüber Bürgerinnen und Bürgern anstrebt (vgl. 14.7). Als Grundeinstellung sollte die stärkste Beschränkung

(nur landesintern innerhalb der öffentlichen Verwaltung) vorgegeben werden.

- In Zweifelsfällen sollte die Zustimmung des Betroffenen eingeholt werden. Hierzu muss er über die Speicherung und Nutzung seiner Daten sowie die damit verbundenen Risiken angemessen informiert werden (z. B. Übersicht über das Directory, Beschreibung der gespeicherten Daten, Empfänger übermittelter Daten, Beschreibung des Zugriffsschutzverfahrens, Hinweis auf mögliche Risiken, Hinweis auf Freiwilligkeit und Folgenlosigkeit einer Ablehnung, Ansprechpartner in Problemfällen). Die Einwilligung ist zu dokumentieren.
- Die Administration der Verzeichnisse wird durch ein starkes Authentifizierungsverfahren (digitale Signatur, Chipkarte) abgesichert. Die Funktionen für eine Neueintragung und Veränderung von Einträgen werden verbindlich festgeschrieben und nur einem kleinen Kreis von Administratoren zugänglich gemacht. Durch angemessene Protokollierung und regelmäßige Revision werden die Aktivitäten der Administratoren überwacht.
- Die Einträge in elektronischen Verzeichnissen sind zeitnah zu aktualisieren. Vor „Veröffentlichung" des Eintrags im Verzeichnis müssen den Betroffenen die Daten des Eintrags zur Einsichtnahme und / oder Korrektur vorgelegt werden. Betroffenen muss es jederzeit möglich sein, Auskunft über ihre persönlichen Daten zu erhalten.
- Das Neueinrichten, Ändern und Löschen von Verzeichniseinträgen sowie das Erstellen und Verbreiten von Repliktionen ist zu protokollieren.
- Bei der Übertragung von Verzeichnissen (z. B. zur netzweiten Aktualisierung) sollten kryptographische Verfahren eingesetzt werden.

6.6.4 Telearbeit

Im Auftrag des Niedersächsischen Innenministeriums hat das izn mit meiner Unterstützung eine Technikfolgenabschätzung für das Pilotprojekt Telearbeit erstellt. Da im Testfeld nur ausnahmsweise personenbezogene Daten bearbeitet werden, die zudem auch nur den Schutzstufen A, B und C zuzuordnen sind, genügten für die Pilotarbeitsplätze neben IT-Grundschutzmaßnahmen folgende Festlegungen:

- die Schaffung und Nutzung von Telearbeitsplätzen erfolgen nur im Einverständnis der speichernden Stelle und der Arbeitnehmer,
- Kontrollrechte des Dienstherrn/Arbeitgebers werden entsprechend den in einer Dienstanweisung festgelegten Regelungen ausgeübt,
- alle erforderlichen arbeitsrechtlichen, organisatorischen, technischen und datenschutzrechtlichen Regelungen zu Telearbeitsplätzen werden schriftlich verbindlich festgelegt,
- die erforderlichen Sicherheitskonzepte werden dem Stand der Technik entsprechend angepasst und ergänzt.

Ausgenommen von der Telearbeit wurden Bedienstetendaten und personenbezogene Daten der Schutzstufen D und E.

6.6.5 Firewall für Landesdienststellen

Mit dem Anschluss von Landesdienststellen an das Internet und Landes-Intranet sind Gefahren für das Recht auf informationelle Selbstbestimmung Betroffener verbunden, die wirksam beherrscht werden müssen. Der IMA-IuK hat eine temporäre Arbeitsgruppe mit dem Auftrag eingesetzt, Fragen der erforderlichen technischen und organisatorischen Absicherungen, der Berechtigungen, eines Sicherungskonzepts und des verbleibenden Restrisikos zu untersuchen und einen Vorschlag für eine Dienstvereinbarung mit den Betroffenen zu erarbeiten. Neben einer Technikfolgenabschätzung wurde eine Rahmendienstanweisung für die Nutzung des Internetzugangs der Landesverwaltung erarbeitet und vom IMA-IuK beschlossen.

Danach darf das Internet nur zu dienstlichen Zwecken genutzt werden. Beim izn ist ein zentraler Internetzugang für die Landesverwaltung einzurichten. Das Internet darf auf Rechnern in mit dem iznNet verbundenen lokalen Netzen nur über den Internetzugang des izn und damit über die zentrale Firewall des Landes genutzt werden. Andere Internetzugänge sind nur auf Einzelplatz-PC zulässig. Vor der Einrichtung eines Internetzugangs hat jede Dienststelle festzulegen, welche Internet-Dienste in welcher Weise für den Dienstverkehr erforderlich sind. Sie veranlasst die entsprechende Konfiguration der izn-Firewall durch einen schriftlichen Auftrag an das izn. Soweit nicht ausschließlich Einzelplatz-PC zum Einsatz kommen, ist ein lokales Sicherungssystem (Router, Proxy-Server, Firewall) zusätzlich zur Landes-Firewall einzurichten. Leistungsfähigkeit und Konfiguration des Sicherungssystems müssen so beschaffen sein, dass insbesondere unberechtigte Zugriffe auf das lokale Netz wirksam verhindert werden.

Internet-Dienste sollten nur Nutzern zugänglich sein, die in die Internetnutzung eingewiesen sind. In der Einweisung müssen die Gefahren der Internetnutzung, Art und Umfang der Kontrollen, die Speicherung personenbezogener Daten und das Verhalten bei Fehlfunktionen des Arbeitsplatzrechners (APC) angesprochen werden. Die Einweisung sollte von den Nutzern schriftlich bestätigt werden. Administratoren des lokalen Sicherungssystems müssen ausreichend geschult werden. Sie sind anzuweisen, die Sicherungsmaßnahmen regelmäßig zu überprüfen und dem Stand der Technik anzupassen.

6.6.6 Enterprise-Management-System

Das Niedersächsische Finanzministerium ist entschlossen, zur IuK-Optimierung eine Fernsteuerung der Systemadministration und eine Software-Verteilung über dezentrale Software-Depots unter der Bezeichnung „Enterprise-Management-System (EMS)“ landesweit einzuführen. Das Konzept wird seit dem 1. Dezember 1999 mit dem Landesarbeitsgericht, den Arbeitsgerichten, dem Landesgesundheitsamt, dem Finanzministerium und dem izn als Pilotteilnehmern getestet. Damit sollen messbare Ergebnisse für die Entscheidung über den landesweiten Einsatz gefunden werden. Eingesetzt wird das Produkt Unicenter TNG Remote Control Option auf Systemen mit dem Betriebssystem Windows NT. Da gerade im Bereich Windows NT der Administrator Möglichkeiten zum unbemerkten Zugang zu Daten auf Servern und Benutzer-PC hat, sind sowohl alle softwareseitigen Konfigurationsvorgaben zu nutzen als auch Handlungsanweisungen zu treffen, um eine datenschutzgerechte Lösung zu finden.

Meine nachfolgenden Forderungen für einen datenschutzgerechten Einsatz der geplanten Softwareverteilung wurden akzeptiert:

- Art und Umfang der Verteilung werden schriftlich geregelt.
- Die Übermittlung erfolgt verschlüsselt.

- Verteilungspasswörter werden nur verschlüsselt übertragen.
- Alle Verteilungsaktivitäten werden protokolliert.
- Die Verteilung kann jederzeit durch den Auftraggeber abgebrochen werden.
- Der Auftraggeber überprüft die Einhaltung der vereinbarten Sicherungsmaßnahmen.

Der Erfahrungsbericht über die Pilotierung und die Entscheidung des IMA-IuK über den landesweiten Einsatz von EMS stehen aus.

6.7 Data Warehouse und Data Mining

Data Warehouse und Data Mining sind zu interessanten Werkzeugen in Wirtschaft und Verwaltung geworden. Sie ermöglichen die Entdeckung von verborgenen Informationen aus großen Datenbeständen und ein ökonomisches und zeitgerechtes Datenmanagement. Diese Technologien gelten vor allem im Unternehmensbereich als die Schlüsseltechnologien des modernen Marketings.

Durch vielfältige Verknüpfungen und Auswertungen der systematisch zusammengeführten Kundendaten im Data Warehouse können neue personenbezogene Erkenntnisse gewonnen werden, die vorher gänzlich unbekannt waren. Mit Data Mining können aus vorhandenen Kundendaten neue personenbezogene Informationen erzeugt werden. Diese neu hinzugewonnenen Personendaten werden für die unterschiedlichsten Zwecke verwendet, so z. B. für das Direktmarketing oder den kommerziellen Datenhandel. Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren. Meine Fragen an Betreiber entsprechender Lösungen sind daher:

- Werden potentielle Kunden und Vertragspartner informiert, dass ihre persönlichen Daten ausgewertet und mit Hilfe der Data Warehousing- und Data Mining-Technologien nach versteckten Beziehungen, auffälligen Mustern und vor allem nach neuen personenbezogenen Informationen durchsucht werden?
- Wissen die Personen, deren Daten ausgewertet werden, dass mit Data Mining weitere personenbezogene Merkmale in einem Umfang gewonnen werden können, wie er ohne diese Technologie und anhand der einzelnen bekannt gegebenen Personendaten nicht möglich wäre?
- Sind Kunden und Vertragspartner darüber im Bilde, dass fortlaufend Daten über ihre Reaktionen aufgrund von Direktmarketingaktionen für das Data Warehouse oder den Data Mart gesammelt werden? Und darüber, dass diese zusammen mit den bereits vorhandenen Personendaten (und gegebenenfalls betriebsextern beschafften Personendaten) mit Data Mining ausgewertet werden, um über die betreffenden Personen neue nützliche Informationen zu gewinnen, wie z. B. Kaufgewohnheiten, Verhaltensmuster, persönliche Eigenheiten und Interessenprofile, Vorlieben sowie Kauf- und Auftragswahrscheinlichkeiten für bestimmte Produkte und Dienstleistungen?
- Liegen von Betroffenen, deren Daten ausgewertet werden, Einwilligungen für Data Mining vor?
- Wird in Verträgen, Allgemeinen Geschäftsbedingungen, Kreditkarten- und Versicherungsanträgen usw., mit denen eine Einwilligung für die Datenverarbeitung eingeholt wird, explizit darauf hingewiesen, dass mit den Metho-

den des Data Mining noch viele weitere Informationen über den künftigen Vertragspartner oder Kunden in Erfahrung gebracht werden können?

- Ist die Einwilligungsklausel für Data Mining und Data Warehousing klar und umfassend?
- Wissen potentielle Kunden, vorhandene Kunden, Vertragspartner, Lieferanten usw., über die personenbezogene Informationen im Data Warehouse (oder Data Mart) gespeichert werden, dass diese Daten einer großen Anzahl von Mitarbeitern unternehmensweit zum Abruf oder zur Datenauswertung zur Verfügung gestellt werden?

Die Schlussfolgerung, ein Data Warehouse dürfe aus datenschutzrechtlicher Sicht grundsätzlich nicht betrieben werden, wäre sicher voreilig. Nach meinen bisherigen Erkenntnissen können Data Warehouse-Systeme unter Nutzung datenschutzfreundlicher Technologien, insbesondere durch Anonymisierung und Pseudonymisierung, so konzipiert werden, dass sie den datenschutzrechtlichen Anforderungen genügen. Natürlich sind dann technische und organisatorische Maßnahmen erforderlich, die eine Deanonymisierung verhindern bzw. die Zuordnung eines Pseudonyms zu einer Person nur unter vorher festgelegten, rechtlich zulässigen Bedingungen ermöglichen. Die 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierfür erste „Datenschutzleitplanken" erarbeitet (vgl. Anlage 16).

Datenschutzleitplanken für ein Data Warehouse

- Personenbezogene Daten dürfen nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem „Daten-Lagerhaus" gesammelt werden.
- Eine Zweckänderung ist in den gesetzlich vorgesehenen Fällen oder mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden sind. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist unwirksam.
- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.
- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zu widerrufen.
- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern" rechtswidrig.
- Keiner darf einer belastenden automatisierten Einzelentscheidung unterworfen werden (Art. 15 EU-Datenschutzrichtlinie).

7 Datenschutz beim Landtag

In der Vergangenheit haben sich Bürgerinnen und Bürger verschiedentlich wegen ihrer Namensnennung im Zusammenhang mit Petitionen an den Niedersächsischen Landtag sich an mich gewandt (s. XI. TB 5.1, 16.5). Obwohl diese Vorstöße zu einer Änderung des Petitionsverfahrens geführt haben, ist dieses - wie ich zuletzt im XIV. TB 5 - dargelegt habe, unter Datenschutzgesichtspunkten immer noch nicht befriedigend ausgestaltet. Anders als im Bund und in anderen Bundesländern kommt es in Niedersachsen nach wie vor zu einer personenbezogenen öffentlichen Diskussion von Petitionen im Parlament.

Ich habe dem Landtag im XIV. TB 5 empfohlen, die von der Konferenz der Präsidentinnen und Präsidenten der Deutschen Landesparlamente angenommene Entschließung zum parlamentspezifischen Datenschutzrecht vom 8./11. Mai 1995 auch in Niedersachsen umzusetzen. Hierzu werde ich in der nächsten Berichtsperiode intensive Gespräche mit dem Landtag führen.

8 Statistik

8.1 Gesetz zur Vorbereitung eines registergestützten Zensus

Die heftigen Auseinandersetzungen um die Volkszählung, die 1983 stattfinden sollte, ist nicht nur Statistik- und Datenschutzexperten in lebhafter Erinnerung. Zahlreiche Verfassungsbeschwerden richteten sich damals gegen das Volkszählungsgesetz, das vom Bundesverfassungsgericht in dem berühmten, auch in diesem Tätigkeitsbericht mehrfach erwähnten „Volkszählungsurteil“ vom 15. Dezember 1983 für teilweise nicht mit dem Grundgesetz vereinbar erklärt wurde. Diese Entscheidung darf als ein Meilenstein in der Geschichte des Datenschutzes bezeichnet werden. Erst 1987 konnte dann die Volkszählung aufgrund eines geänderten Gesetzes durchgeführt werden.

Für das Jahr 2001 ist in der Europäischen Union eine gemeinschaftsweite Volks- und Wohnungszählung vorgesehen. Nach langen Diskussionen hat die Konferenz der Innenminister und -senatoren 1998 aufgrund des Vorschlags einer Arbeitsgruppe beschlossen, für die anstehende Volkszählung einen Methodenwechsel von einer primärstatistischen Vollerhebung zu einer hauptsächlich registergestützten Erhebung vorzunehmen. Vom Deutschen Bundestag wurden die Bemühungen der Bundesregierung, von einer Totalerhebung abzusehen, und ihre Überlegungen, eine stichtagsbezogene Auswertung der Melderegister vorzunehmen, in einem Beschluss begrüßt (BT-Drs. 13/1168 vom 26. Juni 1998).

Grund für diesen Wechsel von einer Vollerhebung zu einer registergestützten Erhebung ist in erster Linie die Aussicht, durch Nutzung von Daten aus Verwaltungsdateien, insbesondere den Melderegistern, erhebliche Kosten zu sparen. Daneben erhofft man sich jedoch auch durch Verzicht auf eine Befragung der Bevölkerung die Vermeidung der bei der vorhergehenden Volkszählung aufgetretenen Akzeptanzprobleme.

Die mit dem Methodenwechsel verbundenen neuen Verfahren müssen vorbereitet und in Tests erprobt und weiterentwickelt werden. Von den Datenschutzbeauftragten ist wiederholt darauf hingewiesen worden, dass auch Datenerhebungen, die zu solchen Erprobungszwecken erfolgen, mit einem Eingriff in das Recht auf informationelle Selbstbestimmung verbunden sind und daher einer Rechtsgrundlage bedürfen.

Diese Rechtsgrundlage soll durch das „Gesetz zur Vorbereitung eines registergestützten Zensus (Zensusvorbereitungsgesetz - ZensVorG)“ geschaffen werden, dessen Entwurf mit Stand vom 4. September 2000 vorliegt. Vorgesehen sind

Testerhebungen zur Prüfung der Qualität der Melderegister und der Dateien der Bundesanstalt für Arbeit sowie weiterhin die Überprüfung statistischer Verfahren und methodische Untersuchungen. Der Entwurf ordnet daher Testerhebungen auf Stichprobenbasis bei Meldebehörden und der Bundesanstalt für Arbeit sowie eine Gebäude- und Wohnungsstichprobe in ausgewählten Gemeinden an. Daneben erfolgt eine Befragung von Personen, die in den für die Stichprobenerhebungen ausgewählten Gebäuden wohnen, um die Qualität und Validität der aus Registern gewonnenen Daten und der dabei angewandten statistischen Verfahren zu überprüfen. Diese Befragung ist nur für die Erprobungsphase vorgesehen und wird bei einem künftigen registergestützten Zensus entbehrlich.

Von den Datenschutzbeauftragten wurden keine grundsätzlichen Einwände vorgetragen. Zugleich wurde jedoch darauf hingewiesen, dass ein registergestützter Zensus nicht einen per se milderen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, es vielmehr auf die konkrete Ausgestaltung ankommt. Kritik wurde insbesondere an dem sehr umfangreichen Katalog der Hilfsmerkmale, die teilweise kaum von Erhebungsmerkmalen abzugrenzen sind, und ihrer langen Speicherung geübt.

Nach Auffassung des Bundesministeriums des Innern sind alle vorgesehenen Hilfsmerkmale für die Erprobungsphase unentbehrlich. Nach ihrem Abschluss wird geprüft werden, welche dieser Hilfsmerkmale bei einem künftigen Zensus entfallen können. Hinsichtlich der Speicherungsdauer berücksichtigte das Ministerium die Kritik der Datenschutzbeauftragten und setzte den Löschungstermin für die nicht die Meldebehörden betreffenden Hilfsmerkmale auf spätestens fünf Jahre nach dem Stichtag fest.

Die Datenschutzbeauftragten werden das weitere Verfahren wie bisher konstruktiv begleiten.

8.2 Was kosten den Staat seine arbeitsunfähigen Beamten?

Es ist unbestritten, dass der Staat Planzahlen für seine gesetzlich festgelegten Leistungen braucht. Das gehören auch verlässliche Zahlen über Versorgungsleistungen für dienstunfähige Mitarbeiterinnen und Mitarbeiter. Solange dies anonym geschieht, ist eine solche Auswertung sensibler Mitarbeiterdaten datenschutzrechtlich unbedenklich. Gegen das von der Bundesregierung geplante Erhebungs- und Verarbeitungsverfahren durch das Statistische Bundesamt, mit dem personenbeziehbare Informationen über Dienstunfähigkeit, Reaktivierung, Teildienstunfähigkeit und Versorgungsansprüche von den personalbewirtschaftenden Stellen und Amtsärzten übermittelt und zentral gespeichert sowie ausgewertet werden sollen, habe ich in Übereinstimmung mit dem für das Statistikrecht zuständigen Niedersächsischen Innenministerium frühzeitig Bedenken erhoben.

Anders als von den Entwurfserstellern des Bundes angenommen, handelt es sich bei der geplanten Erhebung um eine Sekundärstatistik, deren Durchführung einer gesetzlichen Grundlage bedarf. In Anbetracht der geringen Zahl der Fälle in bestimmten Personalbereichen und der differenzierten Erhebung kann zumindest nicht ausgeschlossen werden, dass in Einzelfällen die Daten deanonymisierbar sind. So können z. B. bei Richterinnen und Richtern durch Personalnachrichten in der „Niedersächsischen Rechtspflege“ oder Veröffentlichung im Handbuch der Justiz Name und Alter entnommen und den statistischen Daten zugeordnet werden. Hinzu kommt, dass mit den detaillierten Angaben zu Erkrankungen personenbeziehbare Daten erhoben und übermittelt werden, deren Verarbeitung nach der EU-Datenschutzrichtlinie grundsätzlich verboten ist. Eine Verarbeitung von Gesundheitsdaten setzt eine spezialgesetzliche Ermächtigung voraus.

Das für diese Angelegenheit zuständige Niedersächsische Finanzministerium hat sich meinen Bedenken zwischenzeitlich angeschlossen. Die Weitergabe der Daten zu den Dienstunfähigkeitsgründen wurde ausgesetzt, bis eine bundeseinheitliche statistikrechtliche Regelung getroffen ist. Allerdings wurden die Daten im Niedersächsischen Landesamt für Statistik - mit Blick auf eine noch ausstehende Stellungnahme des Bundes -- vorsorglich zusammengestellt.

Eine nach geltendem Recht datenschutzrechtlich unbedenkliche Lösung müsste sich auf die bei den Daten verarbeitenden Stellen vorhandenen Daten beschränken. Die Daten müssten von diesen Stellen ausgewertet und so zusammengestellt werden, dass Rückschlüsse auf einzelne Betroffene ausgeschlossen sind.

9 Neue Medien

9.1 Tele- und Mediendienste auf dem Prüfstand

9.1.1 Datenschutz im globalen Zusammenhang

Die Internet-Begeisterung in Deutschland nimmt zu; 7,7 Millionen Haushalte in Deutschland haben inzwischen einen Internet-PC, ein Zuwachs von 30 Prozent innerhalb des letzten halben Jahres. Allerdings besteht bei ihnen große Skepsis gegenüber der Internet-Sicherheit, wie Umfragen beweisen. Über 50% befragter Internet-Nutzer fordern mehr Datenschutz im weltweiten Netz. Es hat sich herumgesprochen, dass jede Kommunikation eine Vielzahl von personenbeziehbaren Spuren hinterlässt. Daraus lassen sich dann leicht Nutzerprofile ableiten; entsprechende interessante Daten und kostenfreie Recherche-Software werden im Internet feilgeboten. Elektronische Kommunikation kann zudem belauscht und ausgewertet, E-Mails können mitgelesen und verändert werden. Die vernetzte Datenverarbeitung im Internet mit seinen vielen Beteiligten ist kaum mehr durchschaubar, geschweige denn kontrollierbar. Kaum jemand weiß, wo seine Daten eingesehen, gespeichert, verändert oder auf sonstige Weise genutzt werden.

Dabei haben das deutsche Teledienste- und das Mediendiensterecht für die datenschutzfreundliche Internetnutzung einige neue Regelungen geschaffen, die für das weltweite Internet richtungsweisend sein könnten. Für das sensible Verhältnis von Anbietern und Nutzern wurden dabei für Multimedia Datenschutzleitplanken gebaut. Das Tele- und Medienrecht versucht, einen Ausgleich zwischen den Interessen des freien Wettbewerbs, den berechtigten Nutzerinteressen sowie den öffentlichen Ordnungsinteressen zu schaffen. Es enthält Ansätze zum Systemdatenschutz und Wahlmöglichkeiten anonymer und pseudonymer Nutzung. Damit wurden Regelungsansätze zum Schutz personenbezogener Daten und zur Gewährleistung des Rechts auf informationelle Selbstbestimmung aufgegriffen, die Datenschützer seit längerem vorschlagen. Die in Deutschland agierenden Diensteunternehmen haben insbesondere die folgenden Regelungen zum Schutz personenbezogener Daten zu beachten:

- für das geschäftsmäßige Erbringen von TK-Diensten das Telekommunikationsgesetz - TKG vom 25. Juli 1996 (BGBl. I S. 1120), geändert durch Begleitgesetz zum Telekommunikationsgesetz vom 17. Dezember 1997 (BGBl. I S. 3108),
- für die individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Tönen das Teledienstegesetz - TDG und das Teledienstedatenschutzgesetz - TDDSG vom 22. Juli 1997 (BGBl. I S. 1870),
- für das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten in Text, Ton oder Bild den Me-

diendienstestaatsvertrag - MDStV vom 20. Januar 1997/12. Februar 1997 (Nds. GVBl S. 253) sowie

– die allgemeinen Datenschutzvorschriften im Bundesdatenschutzgesetz und in den Datenschutzgesetzen der Länder.

Bei der Einrichtung entsprechender Informations- und Kommunikationssysteme ist es daher wichtig, genau zu unterscheiden, welche gesetzlichen Grundlagen zu beachten sind. Doch bei aller Zufriedenheit über das deutsche Multimediarecht bleibt angesichts des weltweiten Internets die traurige Erkenntnis, dass diese länderspezifischen Regelungen nur bedingt dem Datenschutz nutzen. Notwendig wären internationale Festlegungen über Mindeststandards, um die Interessen von wirtschaftlicher Nutzung und individuellem Schutz angemessen auszugleichen. Die internationale Diskussion ist im Gange, Lösungen sind noch nicht verabredet (vgl. Dix in Bäumler: E-Privacy, Verlag Vieweg, 2000, S. 93).

9.1.2 Datenschutzgrundsätze bei Multimedia

Das neue Multimediarecht führt Maßnahmen zum Systemdatenschutz ein, betont den Grundsatz des Datenselbstschutzes, sieht die Möglichkeit einer elektronischen, also nicht schriftlichen Einwilligung vor und fordert Transparenz der Datenverarbeitung. Im Einzelnen sind folgende Datenschutzgrundsätze hervorzuheben:

Wahlfreiheit der Betroffenen

Aus dem Recht der informationellen Selbstbestimmung folgt der Anspruch, dass jedermann grundsätzlich selbst darüber entscheidet, wem er Informationen über seine Person für welche Zwecke zugänglich macht. Dies gilt auch für die Nutzer von Multimediadiensten. Die Umsetzung des Selbstbestimmungsrechts des Nutzers bei der Verarbeitung seiner Daten findet sich in dem „Datenselbstschutz" und dem „Systemdatenschutz" wieder.

Datenvermeidung

Die Fülle von Einzeldaten eröffnet die Möglichkeit, Nutzerprofile zu erstellen. Wo keine personenbezogenen Daten anfallen, sind auch keine besonderen Anstrengungen des Anbieters zum Schutz der Privatsphäre der Nutzer erforderlich. Das neue Tele- und Medienrecht verpflichtet daher die Diensteanbieter, ihre technischen Einrichtungen am Ziel der Datenvermeidung auszurichten und anonyme oder zumindest pseudonyme Nutzungs- und Bezahlverfahren anzubieten.

Systemsicherheit

Der Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten der Nutzer von Multimediadiensten verlangt ein hohes Niveau an technischen und organisatorischen Maßnahmen zur Datensicherheit. Vor der Implementierung von Maßnahmen zur Datensicherheit ist eine Technikfolgenabschätzung der Verarbeitung personenbezogener Daten durchzuführen. Dabei sind Schwachstellen und Risiken zu analysieren und ist ein Sicherheitskonzept zu erstellen. Das Sicherheitskonzept muss regelmäßig auf seine Effektivität und Effizienz hin untersucht und dem Stand der Technik angepasst werden. Sicherungsziele sind:

Vertraulichkeit der personenbezogenen Daten

Verfügbarkeit der personenbezogenen Daten und

Integrität der personenbezogenen Daten.

Selbstschutz

Die gesetzlich vorgeschriebenen Schutzmaßnahmen reichen nicht aus, ausreichende Sicherheit im Internet zu schaffen. Deshalb sollte sich jeder Nutzer durch selbstbestimmte Instrumente zusätzlich schützen. Hierfür bieten die Informations- und Kommunikationstechnik vielfältige Möglichkeiten an. Verschlüsselung und Steganografie, digitale Signatur, Pseudonyme, Certified Electronic Mail und Sicherheitsprogramme sind solche Technologien eines Teilnehmer kontrollierten Selbstschutzes. Hierüber sollten Diensteanbieter ihre Kunden aufklären und Hilfen zum Einrichten anbieten.

Transparenz der Datenverarbeitung

Nutzer von Multimediadiensten sollen wissen können, wer welche personenbezogenen Daten für welche Zwecke erhebt und wie diese Daten genutzt werden (Transparenz der Datenverarbeitung). Diese Transparenz muss sowohl beim Zugang zu den Multimediadiensten als auch bei der Nutzung der Multimediadienste bestehen. Zur vollständigen Transparenz der Datenverarbeitung gehört auch, dass sich das Wissen um die Verarbeitung personenbezogener Daten auch auf eine eventuelle Nutzung außerhalb des Multimediadienstes erstreckt.

Datenübermittlung

Die Nutzung weltweiter und offener Informations- und Kommunikationsnetze führt zu einer für den Nutzer von Multimediadiensten häufig nicht mehr erkennbaren Weitergabe seiner Daten an Dritte. Dabei hat der Nutzer gegenüber dem Anbieter Anspruch auf Mitteilung über Umfang und Zweck der Datenverarbeitung und Angabe weiterer Empfänger der Daten. Ein Anbieter von Multimediadiensten, der Daten des Nutzers nicht nur vorübergehend verarbeitet, hat dem Nutzer auf Verlangen Auskünfte zu erteilen.

Gewährleistung der Integrität

Soweit der Anbieter eines Multimediadienstes personenbezogene Daten eines Nutzers speichert, ist er verpflichtet, organisatorische und technische Vorkehrungen zu treffen, die eine korrekte Datenhaltung gewährleisten. Diese Maßnahmen müssen dem jeweiligen Stand der Technik entsprechen. Die Sicherung wird durch unternehmens- und dienstespezifische Gegebenheiten (Größe, Branche, Organisation, Technik) geprägt. Ein unabhängiges Beratungs-, Schulungs- und Kontrollorgan (z. B. der betriebliche Datenschutzbeauftragte) bietet die Gewähr dafür, dass die Datenschutzgrundsätze umgesetzt werden.

Datenschutzaudit

Anbieter von Tele- und Mediendiensten können ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen. Inhaltliche Anforderungen und Ausgestaltung des Auditverfahrens sollen in einem Ausführungsgesetz geregelt werden. Die Einführung des Datenschutzaudits wird sowohl von der Wirtschaft als auch der Politik unterstützt. Datenschutzgerechte Technik hat sich als Wettbewerbsvorteil erwiesen.

9.1.3 Aufsicht mit Augenmaß

Mit Wirkung vom 1. August 1997 wurde mir die Datenschutzaufsicht über Tele- und Mediendienste-Unternehmen übertragen. Die Aufsicht über die Diensteanbieter erfolgt routinemäßig; sie ist als Regelaufsicht gestaltet. Sie kann somit

auch durchgeführt werden, wenn keine Anhaltspunkte für eine Verletzung von Datenschutzvorschriften vorliegen. Die Aufsicht ist nicht davon abhängig, ob die personenbezogenen Daten in Dateien verarbeitet werden. Neben meiner Datenschutzaufsicht bei Tele- und Mediendienste-Unternehmen besteht weiter eine Aufsichtskompetenz des Bundesbeauftragten für den Datenschutz für die zugrunde liegenden Telekommunikationdienste.

Um mir einen Überblick über die meiner Aufsicht unterstehenden Unternehmen und den bestehenden Handlungsbedarf zu verschaffen, habe ich ca. 70 Diensteanbieter angeschrieben und über das anzuwendende Datenschutzrecht aufgeklärt; hierzu gehörten auch Fragen der Verschlüsselung, Anonymisierung und Pseudonymisierung. In Form eines Fragenkatalogs habe ich die Anwendungspraxis und die aufgetretenen Probleme aufzuklären versucht. Schließlich habe ich eine konstruktive und kooperative Zusammenarbeit angeboten. In mehreren Vortragsveranstaltungen, u. a. zusammen mit der Industrie- und Handelskammer Hannover-Hildesheim, habe ich mich um einen konfliktfreien Start junger Diensteunternehmen bemüht.

Die folgende Aufstellung beinhaltet die wichtigsten Erkenntnisse aus der Auswertung der Fragebogen-Aktion und den von mir geführten Beratungsgesprächen.

Forderung	Praxis	Meine Empfehlungen!
Anbieterkennzeichnung (§ 6 TDG und § 6 MDStV): Diensteanbieter haben für ihre (geschäftsmäßigen) Angebote Name und Anschrift, bei Personenvereinigungen und Personengruppen Name und Anschrift des Vertretungsberechtigten anzugeben.	– Nennung des Verantwortlichen ohne Anschrift – Firmennamen ohne Nennung des Vertretungsberechtigten und ohne dessen Anschrift	– Impressum auf der Homepage – Besser wäre: – Impressum auf jeder Web-Seite, Verweis auf Impressum auf jeder Web-Seite, bei sonstigen interaktiven Angeboten Hinweis zu Beginn des Dialogs
Datensparsamkeit (§ 3 TDDSG und § 13 MDStV): Diensteanbieter haben Nutzern alternative Nutzungsformen anzubieten, soweit dies technisch möglich und zumutbar ist.	– Bisher nicht vorhanden – Obligatorische Personalisierung – Nachträgliche Zuordnung eines Pseudonyms – Verwendung statischer IP-Nr. als Pseudonym – Unzureichende Unterrichtung über anonyme oder pseudonyme Nutzung – Erstellung von Nutzungsprofilen unter Verwendung der Identität der Nutzer	– Wahl des Nutzers, den Dienst entweder personalisiert, pseudonymisiert oder anonym zu nutzen – Besser wäre: – Angebote grundsätzlich ohne Personalisierung – Freie Vergabe der Kennung durch den Nutzer ohne Identifikation
Unterrichtung des Nutzers (§ 3 Abs. 5 TDDSG und § 12 Abs. 6 MDStV): Der Nutzer ist vor der Erhebung über Art, Umfang, Ort und Zwecke der Verwendung seiner Daten zu unterrichten.	– Allgemeiner Hinweis auf AGB oder Nutzungsbedingungen – Pauschaler Hinweis, dass dem Datenschutz Rechnung getragen wird – Allgemeiner Hinweis, dass personenbezogene Daten verarbeitet werden – Information erst nach erfolgter Datenerhebung	– Unterrichtung vor Beginn der Erhebung – Unterrichtung auf Homepage des Anbieters – Ausdrücklicher Verweis (Link) auf die Unterrichtung in der Homepage – Unterrichtung im elektronischen Erhebungsformular – Schriftliche Information vor der ersten Erhebung von Daten

Forderung	Praxis	Meine Empfehlungen!
Auskunftsrechte (§ 7 TDDSG, § 16 MDStV): Nutzer hat ein umfassendes Recht auf Auskunft über die Daten, die der Anbieter über ihn gespeichert hat.	– Allgemeiner Hinweis auf Arten der Daten anstatt Auskunft über seine Daten – unvollständiger Zugriff des Nutzers auf seine Daten	– Online-Auskunft nach Authentifizierung des Nutzers – Auskunft per E-Mail an die E-Mail-Adresse des Nutzers – bei Auskunft über Internet sollte Auskunft verschlüsselt erfolgen, ansonsten Hinweis auf Risiko
Einwilligung (§ 3 Abs. 7 TDDSG, § 12 Abs. 8 MDStV): Personenbezogene Daten dürfen erhoben, verarbeitet und genutzt werden, soweit dies eine Rechtsvorschrift erlaubt oder der Nutzer eingewilligt hat. Die Einwilligung darf grundsätzlich nicht zur Voraussetzung der Nutzungsmöglichkeit des Dienstes gemacht werden. **Zulässig Datenverarbeitung mit Einwilligung:** – Bestandsdaten für Zwecke der Beratung, Werbung, Marktforschung und zur bedarfsgerechten Gestaltung der Dienste – Aufnahme in Teilnehmerverzeichnisse – E-Mail-Adresse für Zusendung von Newslettern – Zugangsdaten, die für Nutzung geschlossener Dienste erforderlich sind	– Bloße Information statt ausdrücklicher Einwilligung – Erklärung wird nur eingeblendet, nicht bestätigt – Fehlender Hinweis auf Freiwilligkeit – Unterbrechung der Anmeldung zu einem Dienst, wenn Nutzer nicht seine Einwilligung zur DV für andere Zwecke erteilt (§ 3 Abs. 3 TDDSG, § 12 Abs. 4 MDStV).	– Anbieter sendet Text der Einwilligung per E-Mail, Nutzer bestätigt durch Rücksendung. – Einwilligungserklärung wird dem Nutzer in einem Bildschirmfenster angezeigt, der Nutzer bestätigt durch Anklicken eines eindeutig beschrifteten Auswahlfeldes. – Der Nutzer erhält in einem Formular verschiedene Wahlmöglichkeiten.

Forderung	Praxis	Meine Empfehlungen!
Die Einwilligung kann in Schriftform und, unter bestimmten Bedingungen, auch elektronisch erfolgen. Die elektronische Einwilligung setzt voraus, dass: – sie durch eindeutige und bewusste Handlung erfolgt – sie nicht unerkennbar verändert werden kann – ihr Urheber erkannt werden kann – die Einwilligung protokolliert wird und – der Inhalt der Einwilligung jederzeit vom Nutzer abgerufen werden kann		
Protokollierung der Einwilligung: Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein. Der Nutzer kann auf Unterrichtung verzichten. Die Unterrichtung und der Verzicht sind zu protokollieren.	– Die Protokollierung der Einwilligung beim Anbieter ohne Abrufmöglichkeit des Inhalts der Unterrichtung – auf das Widerrufsrecht wird nicht hingewiesen – Abrufmöglichkeit nur der neuesten Version der Einwilligungserklärung	– Möglichkeiten der Protokollierung und des Abrufs: – Speicherung der Einwilligung oder des Verzichts der Unterrichtung beim Anbieter – Speicherung der Einwilligung auf Rechner des Nutzers – bei Änderung der Unterrichtung sind auch ältere Versionen zu speichern
Cookies: Das Setzen eines Cookies ist ein unerlaubter Eingriff in den Nutzer-PC. Der Nutzer ist vor dem Setzen eines Cookies, das über die aktuelle Sitzung hinaus gespeichert bleiben soll, zu unterrichten.	– allgemeiner Hinweis auf Konfigurationsmöglichkeiten im Browser – pauschaler Hinweis, dass Cookies verwendet werden – Unterrichtung erst im Nachhinein	– Unterrichtung auf der Homepage – ausdrücklicher Verweis (Link) auf die Unterrichtung in der Homepage – Unterrichtung bei Links mit Cookies

9.1.4 Einzelfälle der Aufsicht

Weitergabe von Kundendaten

Ein Bürger hat mich informiert, dass ein Tele- und Mediendienste-Anbieter Kundendaten an verbundene Unternehmen weitergibt, ohne die explizite Einwilligung seiner Kunden einzuholen. Nach dem TDDSG sowie dem MDStV ist der Diensteanbieter entgegen den allgemeinen Regelungen des Bundesdatenschutzgesetzes (BDSG) und des Telekommunikationsrechts verpflichtet, den Nutzer um seine ausdrückliche Einwilligung zu bitten und, falls dieser nicht reagiert, die Zweckentfremdung seiner Bestandsdaten zu unterlassen. Es genügt nicht, dem Nutzer ein Widerspruchsrecht einzuräumen. Eine Übermittlung von Nutzungs- und Abrechnungsdaten an Dritte ist unzulässig.

Links zu personenbezogenen Datensammlungen

Ein Tele- und Mediendienste-Anbieter verwies auf einer Seite seines Internet-Angebotes mit einem Link auf eine Zip-Datei, die personenbezogene Daten hauptamtlicher Mitarbeiter des Staatssicherheitsdienstes der ehemaligen DDR enthielt. Nach meinen Recherchen handelte es sich dabei um eine Liste aller Personen, die zu einem bestimmten Zeitpunkt aus dem Haushalt des MfS bezahlt wurden.

Nach § 5 Abs. 2 TDG sowie § 5 Abs. 2 MDStV ist der Diensteanbieter für fremde Inhalte, die er zur Nutzung bereithält, verantwortlich, wenn er von diesen Inhalten Kenntnis hat und es ihm technisch möglich ist, deren Nutzung zu verhindern. Durch die inhaltliche Aufbereitung des Themas „100 000 Stasi-Mitarbeiter im Netz“ und dem Setzen des oben genannten Links, der direkt auf die Zip-Datei verweist, ist die Verantwortlichkeit nach TDG/MDStV gegeben und der Anbieter so zu behandeln, als würde er die personenbezogenen Daten selbst veröffentlichen. Damit sind die Bestimmungen des Bundesdatenschutzgesetzes anzuwenden. Im vorliegenden Fall ist die Verarbeitung und Nutzung nach § 29 BDSG zu bewerten, da keine erkennbaren eigenen Zwecke durch die speichernde Stelle verfolgt wurden. Bereits das Speichern der Liste zum Zwecke der Übermittlung war unzulässig, da Gründe zu der Annahme bestehen, dass Betroffene ein schutzwürdiges Interesse am Ausschluss der Speicherung haben (§ 29 Abs. 1 Satz 1 Nr. 1 BDSG). Somit ist nach § 29 Abs. 2 Satz 1 Nr. 2 BDSG auch eine Übermittlung in jeglicher Form über das Internet nicht zulässig, da wiederum die gleichen Gründe für die Annahme bestehen, dass Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung haben. Die zusammenfassende Bewertung ergab, dass sowohl die Speicherung als auch jede nachfolgende Übermittlung rechtswidrig waren. Damit greift die Strafvorschrift des § 43 Abs. 1 BDSG. Darüber hinaus kann die Veröffentlichung auch zivilrechtliche Ansprüche der Betroffenen auf Schadensersatz und Schmerzensgeld (§§ 823 Abs. 1, 847 Abs. 1 BGB) bzw. Unterlassung (§ 1004 BGB) auslösen.

Inhaltskontrollen von E-Mails

Ein Bürger hat sich darüber beschwert, dass seine privaten E-Mails vom Anbieter inhaltlich überprüft worden seien. Die Pflichten der Telekommunikationsunternehmen und die Rechte von Nutzern sind im Telekommunikationsgesetz (TKG) geregelt. Für die Verarbeitung von Kommunikationsinhalten im Rahmen der Telekommunikation sind § 89 Abs. 4 und 5 TKG von Bedeutung. Telekommunikationsunternehmen haben das Fernmeldegeheimnis zu wahren. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur zum Erbringen des Telekommunikationsdienstes verwenden. Danach sind geheim zu halten der Inhalt der Telekommunikation und ihre näheren Umstände, insbeson-

dere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war.

9.2 Neue Medienordnung

Die Ministerpräsidenten der Länder haben ihre Rundfunkreferenten beauftragt, Modelle für eine neue Medienordnung zu erarbeiten. Durch die E-Commerce-Richtlinie der Europäischen Kommission ist eine Neuordnung des deutschen Tele- und Mediendiensterechts notwendig geworden. Die Richtlinie muss bis zum 17. Januar 2002 in nationales Recht umgesetzt werden. Dies macht eine Novellierung des Informations- und Kommunikationsdienstegesetzes und des Mediendienstestaatsvertrages erforderlich. Es ist zu hoffen, dass die Umsetzung der E-Commerce-Richtlinie zum Anlass genommen wird, die Trennung der Regelungen für Mediendienste und Teledienste aufzugeben und stattdessen ein einheitliches Regelwerk zu schaffen. Die horizontalen Regelungen von Bund und Ländern würden damit entzerrt und parallele Regelungen vermieden. Nur für den Rundfunk wären dann noch spezifische Länderregelungen erforderlich. Auf Bundesseite wird überlegt, das Teledienstegesetz und das Teledienstdatenschutzgesetz aufzugeben und die besondere Regelungen für die elektronischen Dienste in die 2. Stufe des neuen BDSG zu überführen.

Zunächst jedoch soll mit einem ersten Gesetz zur Änderung des Gesetzes über den Datenschutz bei Telediensten der unmittelbare gesetzgeberische Handlungsbedarf erfüllt werden. Die Bundesregierung hat dazu in ihrem Bericht über Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des Informations- und Kommunikationsdienstegesetzes (BT-Drs. 14/1191) Vorschläge gemacht. Auch ich habe mich an einer Stellungnahme der Datenschutzaufsichtsbehörden zur Evaluierung des IuKDG beteiligt. Zahlreiche der dort angesprochenen Punkte sind von der Bundesregierung in ihrem Bericht berücksichtigt worden. Inzwischen liegt auch ein Entwurf für ein Erstes Gesetz zur Änderung des Gesetzes über den Datenschutz bei Telediensten (1. TDDSGÄndG) vor, der den gesetzgeberischen Handlungsbedarf umsetzen soll. Dabei geht es um die Abstimmung des allgemeinen und des bereichsspezifischen Datenschutzrechts und um die Verbesserung der Transparenz. Der Entwurf verdeutlicht, dass das TDDSG nur im Verhältnis von Anbietern und Nutzern von Telediensten gilt. Es enthält als Spezialregelungen die besonderen Grundsätze, Pflichten und Erlaubnistatbestände für Anbieter von Telediensten. Diese speziellen Regelungen sind abschließend, sie ergänzen somit das traditionelle Datenschutzkonzept des BDSG. Wesentliche Grundsätze und Pflichten des geltenden TDDSG zum Systemdatenschutz (Datenvermeidung, Datensparsamkeit, Anonymisierung und Pseudonymisierung) und zur Anlass unabhängigen Datenschutzaufsicht werden jedoch in das BDSG-neu aufgenommen und machen dann spezielle Regelungen im TDDSG überflüssig. Mit dem Änderungsgesetz wird weiterhin eine Optimierung der Vorschriften des TDDSG angestrebt. So sollen die Einwilligungslösung präzisiert, eine breitere Anwendung der elektronischen Einwilligung ermöglicht, die Bestimmungen zur Verhinderung des Missbrauchs von Telediensten verschärft und Sanktionsinstrumente eingeführt werden.

9.3 Telekommunikations-Datenschutzverordnung

Die Bundesregierung hat am 17. Mai 2000 nach langer, zäher Vorarbeit eine neue Telekommunikations-Datenschutzverordnung beschlossen, die zwar einige Verbesserungen enthält, dennoch den Schutz von Telefonkunden in wichtigen Punkten verschlechtert. Durch die Verordnung soll die bisher geltende TDSV aus dem Jahre 1996 abgelöst werden. Mit der Neufassung würde die Frist zur

Speicherung von Verbindungsdaten drastisch von bisher 80 Tagen auf sechs Monate ab Versendung der Rechnung ausgedehnt werden. Das Wahlrecht von Kundinnen und Kunden, ob sie ihre Verbindungsdaten insgesamt nach Ende der Verbindung gelöscht oder im Gegenteil vollständig gespeichert haben wollen, wird in der Weise eingeschränkt, dass diese Option nur noch gegenüber dem Anbieter ausgeübt werden kann, der die Rechnung schickt. Auf die Speicherung der Daten bei anderen Dienstleistern (z. B. im Call-by-Call-Verfahren) haben die Kundinnen und Kunden keinen Einfluss mehr. Schließlich werden die Möglichkeiten der Anbieter, ihre Datenbestände zur Missbrauchsbekämpfung zu durchrastern, deutlich erweitert. Sie können die Verbindungsdaten der zurückliegenden sechs Monate analysieren; bisher galt dafür ein Zeitraum von einem Monat. Außerdem dürfen die so erhobenen Daten auch ins Ausland übermittelt werden, selbst wenn dort kein angemessenes Datenschutzniveau herrscht.

Ich bin mir mit meinen Kolleginnen und Kollegen einig, dass das Recht der Kundinnen und Kunden auf unbeobachtete Telekommunikation wirksamer geschützt werden muss. Dem Niedersächsischen Ministerium für Wirtschaft, Technologie und Verkehr habe ich zu den Kritikpunkten detaillierte Änderungsvorschläge unterbreitet. Doch erst eine konzertierte Pressearbeit der Datenschutzbeauftragten, so z. B. meine Pressemitteilung vom 4. Juli 2000 „Datenschutz von Telefonkunden verschlechtert", scheint das gewünschte Echo gefunden zu haben. In einer kleinen Runde mit den Telekommunikationsreferenten der Wirtschaftsministerien wurden tragfähige Lösungen der strittigen Punkte erzielt.

Der Bundesrat hat sich am 29. September 2000 mit der TDSV abschließend befasst. Bis zuletzt war datenschutzrechtlich umstritten, wie lange TK-Unternehmen die von ihnen erhobenen Verbindungsdaten zu speichern haben. Die nunmehr vom Bundesrat verabschiedete Regelung, wonach Verbindungsdaten grundsätzlich sechs Monate nach Versendung der Rechnung aufzubewahren sind, muss als datenschutzrechtlich bedenklich angesehen werden. Der Bundesrat bezweckt mit dieser Speicherpflicht, Datenmaterial für mögliche künftige Abfragen von Strafverfolgungsbehörden zu erhalten. Da auch die Verbindungsdaten dem Fernmeldegeheimnis unterfallen, stellt diese Vorratsdatenspeicherung einen unnötigen Eingriff in das grundrechtlich geschützte Fernmeldegeheimnis dar. Mit dieser Regelung werden alle Nutzer von Telekommunikationsdiensten als potentielle Kriminelle behandelt. Hiergegen haben sich die Datenschutzbeauftragten in einer erneuten Pressemitteilung gewandt. Das Bundeskabinett hat sich in seiner abschließenden Entscheidung über die TDSV leider dem Votum des Bundesrates angeschlossen.

9.4 Rundfunkgebühren

9.4.1 Datensparsamkeit bei der Erhebung von Rundfunkgebühren

Meine Pressemitteilung vom 3. April 2000 „Abschaffung der Rundfunkgebühren - ein Beitrag zum Datenschutz" hat ein lebhaftes, bundesweites Echo gefunden. Hatten die einen Sorge um den Fortbestand des öffentlich-rechtlichen Rundfunks, so ging den anderen mein Vorschlag einer datenschutzfreundlichen Rundfunkfinanzierung nicht weit genug; sie forderten ihre Abschaffung. Beide Parteien wollten mich gründlich missverstehen. Mit meiner Stellungnahme habe ich lediglich die gegenwärtige Diskussion der Medienreferenten der Länder aufgegriffen, die ebenfalls nach Lösungen zur Weiterentwicklung des Verfahrens der Rundfunkfinanzierung suchen.

Der öffentlich-rechtliche Rundfunk in Deutschland wird derzeit in erster Linie durch Gebühren finanziert. Die Gebühren werden im Auftrage der Landesrund-

funkanstalten durch die Gebühreneinzugzentrale (GEZ) abgerechnet. Gebührenpflichtig sind grundsätzlich alle Bürgerinnen und Bürger sowie Unternehmen und Behörden, die Rundfunkgeräte zum Empfang bereithalten. Die Gebührenpflicht soll sich nach Forderungen der Rundfunkanstalten auch auf alle PC mit Internet-Zugang erstrecken. Darüber hinaus sind weitere Technologien durch den neuen UMTS-Standard zu erwarten, die ebenfalls einen Rundfunkempfang ermöglichen und damit gebührenpflichtig würden.

Das GEZ-Register umfasst schon jetzt personenbezogene Daten von über 30 Millionen Haushalten. Es kommt damit praktisch einem Bundesmelderegister gleich, das rechtlich nicht zulässig und politisch auch nicht gewollt ist. Die in den meisten Ländern - so auch in Niedersachsen - festgelegte regelmäßige Übermittlung von Meldedaten der Einwohnermeldeämter an die Rundfunkanstalten ist aus meiner Sicht ein Systembruch im Melderecht. Diese Übermittlung wird damit begründet, dass viele Rundfunkempfänger trotz Meldepflicht die Geräte nicht bei den öffentlich-rechtlichen Rundfunkanstalten anmelden. Deshalb müssten die Rundfunkanstalten große Anstrengungen unternehmen, um Kostenpflichtige aufzuspüren. Doch gerade dieses „Aufspüren" empfinden viele Bürgerinnen und Bürger als Schnüffelei und führen bei mir häufig Beschwerde.

Die Datenschutzbeauftragten des Bundes und der Länder kritisieren schon seit längerem die auf dem jetzigen Modell der Rundfunkfinanzierung beruhende Verarbeitung personenbezogener Daten. In ihrer Entschließung vom 13. Oktober 2000 (vgl. Anlage 24) fordern sie die Bundesländer auf, bei der anstehenden Weiterentwicklung des Systems der Rundfunkfinanzierung ein Modell zu Grunde zu legen, das sich stärker an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Auf diese Weise könnte auch ein Beitrag zur Erhöhung der Wirtschaftlichkeit bei der Rundfunkfinanzierung geleistet werden.

9.4.2 Befreiung von der Rundfunkgebühr

Bei mir sind besorgte Anfragen und Beschwerden von Studierenden über das Antragsverfahren zur Befreiung von der Rundfunkgebührenpflicht eingegangen. Der Fragebogen wird als Ausforschung intimer Lebensbereiche angesehen; zumindest seine Fragen nach den Ausgaben für die Nutzung von Telefon/Handy und Internet, Studienmaterial, PKW-Unterhaltung und Versicherungen werden als unverhältnismäßig und nicht erforderlich für die Befreiungsentscheidung angesehen. Auf wenig Verständnis stieß mein Vorschlag, die Beschwerden an den Datenschutzbeauftragten des NDR weiterzugeben, denn seine Antwort war meist der Grund der Beschwerden.

Nach der Niedersächsischen Verordnung über die Befreiung von der Rundfunkgebührenpflicht vom 3. September 1992 (Nds. GVBl. S. 239) entscheidet grundsätzlich der NDR. Außer bei einer Gebührenbefreiung aus sozialen Gründen ist der Antrag unmittelbar an die Landesrundfunkanstalt zu richten. Im Falle einer Gebührenbefreiung von Personen, die bestimmte Leistungen nach dem Lastenausgleichsgesetz erhalten (§ 1 Abs. 1 Nr. 5), ist der Antrag an das zuständige Ausgleichsamt, in den übrigen Fällen einer Gebührenbefreiung aus sozialen Gründen an den örtlichen Träger der Sozialhilfe bzw. an Gemeinden/Samtgemeinden zu richten. Der NDR entscheidet über derartige Anträge auf Vorschlag dieser Behörden. Er kann die Behörden zur Aushändigung des Befreiungsbescheides ermächtigen. Die Sozialämter erteilen nur positive Bescheide nach Vorlage des jeweiligen Befreiungsantrags und der erforderlichen Belege. Unklare und abzulehnende Fälle werden an den NDR weitergeleitet, der die Ablehnung erklärt. Die Rechtswirkungen des Handelns der zur Entgegennahme des Antrags vorgesehenen Stellen treffen ausschließlich den NDR.

Nach dem Verordnungstext liegt zwar die Entscheidungskompetenz in Gebührenbefreiungsverfahren ausschließlich bei der Landesrundfunkanstalt. Tatsächlich entscheiden die Sozialämter in den Positiv-Fällen abschließend unter dem Briefkopf des NDR mit eigener Unterschrift und mit eigenem Stempel. Dies entspricht jedoch nicht der Vorgabe der VO; danach ist lediglich vorgesehen, dass das Sozialamt dem NDR einen Entscheidungsvorschlag unterbreitet und ermächtigt werden kann, den Bescheid auszuhändigen. Die Sozialämter sind auch nach Ansicht aller beteiligten Datenschutzbeauftragten durchaus die richtigen Stellen für die Bearbeitung sensibler Daten. Sie dürfen allerdings bei der Antragsbearbeitung keine Daten verwenden, von denen sie bei der Durchführung des BSHG oder anderer Sozialleistungsgesetze Kenntnis erhalten haben, es sei denn, die Antragsteller willigen zu ihrer eigenen Entlastung ausdrücklich in die Verwendung ein.

Für die Kontrolle eigener Datenverarbeitung des NDR ist nach § 41 NDR-Staatsvertrag der Datenschutzbeauftragte der Rundfunkanstalten zuständig. Dessen Zuständigkeit erstreckt sich nach der ausdrücklichen staatsvertraglichen Regelung auch auf den Fall, dass Dritte im Auftrag des NDR tätig werden. Meine Zuständigkeit neben der des Datenschutzbeauftragten des NDR sehe ich dennoch aus folgenden Gründen:

- Bei der Aufgabenwahrnehmung durch die Sozialämter besteht die Gefahr, dass auf personenbezogene Daten, die beim Sozialamt bei Wahrnehmung anderer Aufgaben (insbes. Bearbeitung von Sozialhilfeangelegenheiten) anfallen, zugegriffen wird. Diese Gefahr hat sich in einigen Ländern bereits realisiert, weil dort ganz offen derartige Daten in die Bearbeitung der Befreiungsanträge einbezogen werden.
- Die bei den Sozialämtern im Zusammenhang mit der Bearbeitung von Befreiungsanträgen stattfindende Verarbeitung personenbezogener Daten muss daher umfassender in die Aufsicht einbezogen werden. Diese weitergehende Aufsicht wird von der Regelung des NDR-Staatsvertrages nicht erfasst.
- Gleichzeitig kommt insoweit dem Umstand Bedeutung zu, dass der Datenschutzbeauftragte des NDR vom NDR selbst berufen worden ist und für seine Tätigkeit gegenüber Dienststellen des Landes oder des kommunalen Bereichs nicht die gleiche parlamentarische Legitimation wie der LfD besitzt.

Als Lösung bietet sich daher eine gemeinsame Aufsicht des NDR-Datenschutzbeauftragten und der staatlichen Datenschutzaufsicht im Sinne eines Kondominiums an.

Eine pragmatische Entflechtung dieses Problems deuten Gespräche der Landesbeauftragten für Datenschutz der NDR-Länder Hamburg, Mecklenburg-Vorpommern, Schleswig-Holstein und Niedersachsen mit dem NDR an. Der NDR plant die Übernahme eines ARD-Projekts zur automatisierten Antragsbearbeitung, mit dem die Zuständigkeit der Antragsentscheidung auf die Sozialämter übergehen soll. Das neue Verfahren soll mit einigen Städten bereits im Jahr 2000 erprobt werden. Auch die Landeshauptstadt Hannover zählt zu den Pilotstädten. Diesen Versuch werde ich aufmerksam verfolgen und datenschutzrechtlich begleiten.

10 Ausweis- und Melderecht

10.1 Niedersächsische Meldedatenübermittlungsverordnung

Mit einer Verordnung zur Änderung der Niedersächsischen Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (NMeldDÜV) beabsichtigt

das Innenministerium, die bisherigen Datenübermittlungen zu erweitern. Soweit es gemäß § 3 Abs. 3 NMeldDÜV um die Übermittlung der Daten „ Doktorgrad, Geschlecht, Sterbetag und -ort“ an die Polizei geht, ist dies unproblematisch, auch die Übermittlung von Daten an den Landkreis als Führerscheinbehörde und in Staatsangehörigkeitsangelegenheiten stößt nicht auf Bedenken. Soweit der Änderungsentwurf für die Polizeidienststellen jedoch als Übermittlungszweck ganz allgemein die Fortschreibung „ihrer polizeilichen Informationssysteme“ vorsieht, halte ich dies angesichts der Vielzahl solcher polizeilichen (zentralen und dezentralen) Informationssysteme für zu unbestimmt. Meinem Vorschlag, das bundesweite Informationssystem der Polizei (INPOL) und das landesweite Polizeiliche Auskunftssystem (POLAS) in der Verordnung zu benennen, soweit es sich um diese handelt, mochte das Innenministerium mit der Begründung nicht folgen, dass diese Bestimmung fortlaufend zu ändern sei, wenn sich die Bezeichnung des Auskunftssystems ändere. Schließlich hat das Ministerium auch meinen Vorschlag einer Formulierung wie „Fortschreibung ihres landesweiten polizeilichen Informationssystems“ abgelehnt und erklärt, für welchen Zweck die Polizei die ihr übermittelten Daten rechtmäßig nutzen dürfe, richte sich vielmehr nach den für die Polizeiaufgabenerfüllung maßgebenden Vorschriften. Zu berücksichtigen sei, dass die Regelung im Entwurf im Vergleich zur geltenden Fassung des § 3 Abs. 3 NMeldDÜV bereits bestimmter gefasst sei. Im Hinblick auf die vom Bundesverfassungsgericht im Volkszählungsurteil vom 15. Dezember 1983 geforderte Normenklarheit sehe ich dennoch keinen Anlass, von meiner Forderung nach Konkretisierung der Regelung abzuweichen.

10.2 Melderechtsrahmengesetz

Das Innenministerium hat mir den Arbeitsentwurf eines Dritten Gesetzes zur Änderung des Melderechtsrahmengesetzes (MRRG) des Bundesministeriums des Innern, Stand: 27. Juni 2000, übersandt. Die Gesetzesbegründung liegt mir bislang noch nicht vor.

Unter datenschutzrechtlichen Gesichtspunkten sind die geplanten Regelungen in dem Entwurf, wonach a) durch Landesrecht bestimmt werden kann, dass zur Unterstützung der melderechtlichen Aufgaben Melderegister mehrerer Meldebehörden gemeinsam genutzt werden dürfen, b) hinsichtlich des Namens, der Vornamen, des Doktorgrads und der Anschrift eines Einwohners das Melderegister nach Maßgabe des MRRG jedermann zugänglich sein und c) Auskünfte aus dem Melderegister nach § 21 Abs. 1 MRRG (einfache Melderegisterauskünfte) auch durch elektronischen Abruf zulässig sein sollen, besonders relevant.

Während nach den derzeit geltenden Bestimmungen die Meldebehörden zur Wahrnehmung ihrer Aufgaben befugt und verpflichtet sind, Daten zu übermitteln (§ 28 NMG), besteht offenbar in der Praxis zur Erfüllung meldebehördlicher Aufgaben weiterer Unterstützungsbedarf in der Form der Nutzung von Melderegistern auch anderer Meldebehörden. Datenschutzrechtlich ist diese Befugniserweiterung, deren Gründe ich noch nicht kenne, nur hinnehmbar, wenn hierzu ein zwingendes Bedürfnis besteht. Zudem muss klar erkennbar sein, von wem bzw. von welchen Behörden und Einrichtungen, zu welchen Zwecken und unter welchen Voraussetzungen diese Möglichkeit genutzt werden soll.

Die Absicht, das Melderegister jedermann zugänglich zu machen, bedeutet eine Öffnung des Registers, ähnlich den Regelungen zum Handelsregister (§ 9 Abs. 1 HGB). Nach der derzeitigen Rechtslage ist das Melderegister kein öffentliches, sondern ein für behördliche Zwecke bestimmtes Register, das die Meldebehörden zur Erfüllung ihrer Aufgaben führen. Ein Auskunftsersuchen kann jedoch auch nach geltendem Recht von jeder Person voraussetzungslos - also ohne Angabe von Gründen - gestellt werden. Die Öffnung des Melderegisters für jeder-

mann und vor allem der elektronische Abruf bei der einfachen Melderegisterauskunft haben aber Änderungen des Verfahrens zur Folge, durch die bisherigen Schutzmechanismen der Boden entzogen wird.

Bei dem derzeitigen Auskunftsverfahren erfolgt die Auskunftserteilung unter Prüfung durch die Meldebehörde, ob die Angaben des Auskunftssuchenden ausreichen, um beispielsweise Personenverwechslungen auszuschließen. Auch bei der Erteilung einer einfachen Melderegisterauskunft, die an keine besonderen Voraussetzungen gebunden ist, hat sie zu prüfen, ob schutzwürdige Interessen der Betroffenen beeinträchtigt werden (§ 6 MRRG i. V. m. § 4 NMG und Nr. 4 der Allgemeinen Verwaltungsvorschriften zum NMG).

Der Arbeitsentwurf enthält eine - bislang nicht begründete -Abkehr vom bisherigen Verfahren. Das Melderegister soll hinsichtlich der Grunddaten wie Namen, Vornamen, Doktorgrad und Anschrift der Einwohner auch durch Online-Abruf zugänglich sein. Auch Behörden und sonstigen öffentlichen Stellen des In- und Auslands soll der elektronische Abruf möglich sein. Bei einer solchen Rechtslage habe ich Zweifel, dass schutzwürdige Interessen Betroffener hinreichend gewahrt werden können, denn die derzeit vorhandenen Prüfungsmöglichkeiten unbefugter Verwendung der Daten durch die Meldebehörde werden bei einem elektronischen Abruf, der ohne Einschaltung der Meldebehörde abläuft, nicht mehr gegeben sein.

Wie mir von einigen Meldeämtern bekannt wurde, vollzieht sich die Prüfung, ob schutzwürdige Belange gewahrt werden, dadurch, dass in Zweifelsfragen und bei Vorliegen von Hinweisen über Auskunftssuchende / Betroffene, bei denen eine unbefugte Verwendung der Auskunft anzunehmen oder zu befürchten ist, die Auskunft erst dann erteilt wird, wenn Zweifel oder Unstimmigkeiten ausgeräumt sind. Diese Möglichkeit der Einflussnahme ist beim elektronischen Abruf (bei dem allerdings, wie schon jetzt, Übermittlungssperren und Auskunftssperren durch technische Vorkehrungen berücksichtigt werden können) nicht mehr gegeben.

Die Datenschutzbeauftragten des Bundes und der Länder waren auf ihrer Herbstkonferenz im Oktober 2000 einmütig der Auffassung, dass der elektronische Abruf von Daten Dritter aus dem Melderegister durch Privatpersonen (jedermann) abzulehnen ist. Inzwischen gibt es Anzeichen, dass die Regelungsabsichten im Bundesinnenministerium noch einmal überdacht werden.

Datenschutzrechtlich begrüßenswert ist indes, das für erweiterte Melderegisterauskünfte nach dem Entwurf künftig ein rechtliches Interesse glaubhaft zu machen ist. Gleiches gilt für die vorgesehene Regelung, dass Melderegisterauskünfte in besonderen Fällen (zum Beispiel Auskünfte an Parteien, Wählergruppen vor Wahlen, an Presse und Rundfunk bei Alters- und Ehejubiläen usw.) nur zulässig sein sollen, wenn der Betroffene schriftlich eingewilligt hat. Allerdings nehmen sich diese datenschutzrechtlichen Verbesserungen neben den oben dargestellten nachteiligen Regelungen eher bescheiden aus.

10.3 Hotelmeldescheine für den Fremdenverkehrsbeitrag

Den meisten ist bekannt, dass sie als Gast in einem Hotel, einem Ferienappartement oder auf einem Campingplatz nicht der allgemeinen Meldepflicht unterliegen. Weniger bekannt ist dagegen, dass sich Feriengäste in einem vereinfachten Verfahren anzumelden haben. Diese „Besonderen Meldescheine für Beherbergungsstätten“, umgangssprachlich wohl eher als Hotelmeldescheine bekannt, sind von allen Gästen mit Name, Anschrift, Geburtstag, Staatsangehörigkeit und dem Anreise- und Abreisetag auszufüllen. Diese Angaben dürfen nach dem Niedersächsischen Meldegesetz nur von den Meldebehörden (Städten und Gemein-

den) und Sicherheitsbehörden (also insbesondere Polizei, Staatsanwaltschaften und Verfassungsschutz) für Zwecke der Gefahrenabwehr oder der Strafverfolgung sowie zur Aufklärung des Schicksals von Vermissten und Unfallopfern ausgewertet und verarbeitet werden.

Ein Unternehmer aus einem niedersächsischen Erholungsort hatte sich an mich gewandt, der Ferienhäuser an Urlaubsgäste vermietet. Gegenstand seiner Kritik war insbesondere, dass die Gemeinde diese Hotelmeldescheine für andere Zwecke, nämlich zur Festsetzung des örtlichen Fremdenverkehrsbeitrages nutzt und in diesem Zusammenhang auch Kontrollanrufe bei Gästen erfolgt seien. Außerdem seien die Meldescheine weder - wie es das Melderecht vorsieht - zurückgegeben noch nach der gesetzlichen Aufbewahrungsfrist vernichtet worden.

Meine Prüfung hat Folgendes ergeben: Die fragliche Gemeinde erhebt auf der Grundlage einer kommunalen Satzung Fremdenverkehrsbeiträge, die u. a. von den örtlichen Beherbergungsbetrieben wie dem des Einsenders zu entrichten sind. Zur Festsetzung des Fremdenverkehrsbeitrages wurden zum damaligen Zeitpunkt die von den Gästen ausgefüllten und bei den Hotelbetreibern bzw. Vermietern aufbewahrten Meldescheine bei der Gemeinde eingereicht und die Fremdenverkehrsbeiträge nach Anzahl und Aufenthaltsdauer der Gäste festgesetzt. Die Meldescheine sind (erst dann) vernichtet worden, wenn die Beitragsbescheide unanfechtbar geworden waren. Dabei wurde zweierlei deutlich: Auf der einen Seite stieß dieses relativ unbürokratische Verfahren auf große Akzeptanz bei den örtlichen Betrieben und privaten Vermietern, auf der anderen Seite war die damit verbundene Nutzung personenbezogener Daten Dritter - nämlich der der Feriengäste - jedoch nicht durch die Vorschriften des Melderechts gedeckt.

Das Niedersächsische Meldegesetz setzt der Nutzung dieser Hotelmeldescheine nämlich völlig zu Recht enge Grenzen. So dürfen sie nur Sicherheits-, Strafverfolgungs- und Meldebehörden zugänglich gemacht und ausschließlich zu Zwecken der Gefahrenabwehr, der Strafverfolgung und der Aufklärung des Schicksals von Vermissten und Unfallopfern ausgewertet werden. Außerdem dürfen sie nicht länger als bis zum Ende des auf die Abreise des Gastes folgenden Jahres aufbewahrt werden.

Die in der Gemeinde praktizierte Nutzung der in den Meldescheinen enthaltenen personenbezogenen Angaben der Feriengäste zu abgabenrechtlichen Zwecken ging über diese gesetzliche Zweckbestimmung hinaus. Hinsichtlich der Vernichtungsregelung konnte es zu einer längeren Aufbewahrungsfrist kommen, wenn - wie in dem Fall des Einsenders - die Beitragsbescheide angefochten worden waren.

Das von der Gemeinde praktizierte Verfahren war daher in datenschutzrechtlicher Hinsicht unzulässig. Von meinem Recht, dies förmlich zu beanstanden, habe ich gleichwohl keinen Gebrauch gemacht und der Gemeinde vielmehr Alternativen aufgezeigt, die auch den datenschutzrechtlichen Belangen Rechnung tragen.

Diese Vorschläge sind von der Gemeinde mit Beginn der Saison 2000 in der Weise umgesetzt worden, dass seitdem auf die Übermittlung der in den Meldescheinen enthaltenen personenbezogenen Daten der Feriengäste verzichtet wird, zumal diese für die Beitragsberechnung ohnehin irrelevant sind. Dies geschieht in der Weise, dass das Original des Meldescheins beim Vermieter verbleibt und die Abrechnungsstelle der Gemeinde hiervon nur noch eine Durchschrift erhält, auf der lediglich die Personenzahl und die Aufenthaltsdauer der (namentlich nicht genannten) Gäste erkennbar sind.

Auf diese Weise werden seitdem keine personenbezogenen Daten der Feriengäste mehr übermittelt. Diese Verfahrensweise trägt sowohl datenschutzrechtli-

chen Belangen als auch den Erfordernissen der Praxis in angemessener Weise Rechnung.

11 Polizei

11.1 Nutzung von SPUDOK-Daten (Brandanschlag auf das Arbeitsamt Göttingen)

Nach einem Brandanschlag auf das Arbeitsamt Göttingen am 7. November 1997 kam es infolge der Auswertung eines Selbstbezichtigungsschreibens zu einem Ermittlungsverfahren des Generalbundesanwaltes beim Bundesgerichtshof (GBA). Das Verfahren richtete sich gegen Unbekannt u. a. wegen des Verdachts auf Bildung einer terroristischen Vereinigung (Autonome im Bereich Göttingen). Der GBA beauftragte das Landeskriminalamt Niedersachsen (LKA) mit der Wahrnehmung der polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung. Im Rahmen der Ermittlungen erstellte das LKA im Februar 1998 auch eine Liste mit 105 Datensätzen (105-Liste). Die Angaben umfassen Namen, Vornamen, Geburtstag und -ort. Gemeinsames Merkmal dieses Personenkreises war nach den polizeilichen Unterlagen die Zurechnung zur linksextremistischen bzw. autonomen Szene Göttingens überwiegend in den 80er Jahren oder auch später. Die Einbeziehung des Personenkreises in die laufenden Ermittlungen beruhte auf der Annahme, dass es sich bei den Tätern des Brandanschlages um Angehörige dieser Szene handeln könne, weil das aktuelle Selbstbezichtigungsschreiben deutliche Ähnlichkeiten mit Bekennerschreiben der „revolutionären Zellen" aus dem Jahre 1980 aufwies. Zweck der „105-Liste" war es, die Namen mit Daten des Arbeitsamtes Göttingen abzugleichen. Dem lag die Arbeitshypothese zu Grunde, dass nach dem Selbstbezichtigungsschreiben Angehörige der älteren autonomen Szene selbst von Maßnahmen des Arbeitsamtes betroffen sein konnten, was als mögliches Tatmotiv angesehen wurde. Die Verpflichtung des Arbeitsamtes zur Auskunftserteilung wurde durch einen Beschluss des Ermittlungsrichters des Bundesgerichtshofes angeordnet. Hinweise auf einen Tatvorwurf gegen einzelne Personen ergab der Datenabgleich nicht. Das LKA hat den polizeilichen Ermittlungsvorgang zwischenzeitlich an den GBA abgegeben. Das Ermittlungsverfahren ist noch nicht abgeschlossen.

Bei den auf der Liste aufgeführten Personen handelt es sich um solche, die heute u. a. als Journalisten, Rechtsanwälte, Pfarrer, Politiker, Direktoren, Dezernenten oder Ministerialbeamte tätig sind, vgl. Fraktion Bündnis 90/Die Grünen, LT-Drs. 14/866. Unter dem Stichwort „105 Göttinger Dauerverdächtige" kam es zu einer kritischen Medienberichterstattung und zu parlamentarischen Beratungen, in denen u. a. die Meinung vertreten wurde, dass sich die Nutzung der vor langer Zeit gespeicherten Namen für aktuelle Ermittlungen nicht mit dem Recht auf informationelle Selbstbestimmung und dem Grundsatz der Verhältnismäßigkeit vertrage. Das Niedersächsische Innenministerium wies namens der Landesregierung dies wie auch den Vorwurf zurück, es handele sich bei der Namensauflistung um Namen aus einer alten SPUDOK-Datei (SPUDOK Nr. 74), deren Löschung im Februar 1983 die Landesregierung zwei Jahre später bestätigt hatte. Vielmehr sei die „105-Liste" durch kriminalistische Auswertung manuell erstellt worden. Die Liste wurde mir von einer Abgeordneten des Niedersächsischen Landtages mit der Bitte um datenschutzrechtliche Überprüfung übergeben. Prüfungsgegenstand sollte die durch die Ermittlungstätigkeit zur Aufklärung des Brandanschlages auf das Arbeitsamt Göttingen ausgelöste polizeiliche Datenverarbeitung hinsichtlich der Erstellung und Nutzung von Personenlisten bei der Polizeiinspektion Göttingen und dem LKA sein.

Beim Polizeiamt für Technik und Beschaffung (PATB NI) besteht eine Auflistung sämtlicher SPUDOK-Anwendungen mit Informationen über Einrich-

tung/Löschung der Datei, Dateiname, Dateinummer, sachbearbeitende Dienststelle und Anzahl der Datensätze zum Zeitpunkt der Löschung. Ausweislich der Auflistung wurde die SPUDOK-Datei Nr. 74 am 4. Februar 1983 physikalisch gelöscht. Ein Reaktivieren der Daten ist technisch nicht möglich. Nach dem dortigen Erinnerungswissen wurde auch eine Kopie der Datei nicht gezogen. Für die Existenz dieser Datei sprechende Anhaltspunkte habe ich ebenso wenig gefunden wie eine der Datei entsprechende Liste in Papierform. Nach intensiven Erörterungen vor Ort besteht für mich kein Grund, an der Darstellung des LKA zu zweifeln, nach der es eine solche Liste nicht gegeben hat und dass ermittelnde Beamte eine solche Liste somit auch nicht für die Erstellung der „105-Liste" benutzt haben.

Ausgangspunkt der „Namenssuche" war - wie eingangs angesprochen - die Annahme, dass einer der Verfasser des Selbstbezichtigungsschreibens selbst von Maßnahmen des Arbeitsamtes Göttingen betroffen war und dass die Diktion des Selbstbezichtigungsschreibens auf die „ältere autonome Szene" hindeutete. Nach meinen Feststellungen erfasst die Liste Daten von 104 Menschen; zwei Datensätze betreffen ein und dieselbe Person. Eine Dokumentation der Arbeitsschritte zum Auffinden der Namen für die Liste gab es nicht, sie ist auch rechtlich nicht geboten. Die nachfolgende Darstellung beruht auf einer nachvollziehbaren Rekonstruktion der Quellen für die Namen auf der Liste. Danach stammen die Datensätze (Namen) aus drei Arten von Unterlagen, nämlich einem anderen strafrechtlichen Ermittlungsvorgang, zwei Sachakten (Staatsschutz) des LKA und einer Kriminalakte. Aus der Kriminalakte rühren ca. 4/5 der Namen auf der „105-Liste". Das übrige 1/5 verteilt sich auf die Quellen Sachakten (Staatsschutz) des LKA und den anderen Ermittlungsvorgang. Die Speicherung der Namen in den genannten Akten habe ich stichprobenartig überprüft. Die Namen auf der „105-Liste" kamen durch eine manuelle Auswertung der genannten Unterlagen zustande. Anhaltspunkte für eine nachträgliche Veränderung der Liste habe ich nicht festgestellt.

Die Polizei verzichtete seinerzeit auf eine Überprüfung der Aktualität der durch die Auswertung erhaltenen Personalien. Dies hätte nach Meinung des LKA weitere personenbezogene Ermittlungen nach sich gezogen, obwohl bereits zu Beginn feststand, dass, wenn überhaupt, nur ein Bruchteil des betroffenen Personenkreises für weitere Ermittlungen in Betracht gekommen wäre; insoweit wäre überflüssigerweise in großem Umfang in Rechte Nichtbetroffener eingegriffen worden.

Grundsätzlich bestehen keine rechtlichen Bedenken gegen die Auswertung der Akten zur Aufklärung des Brandanschlages auf das Arbeitsamt Göttingen. Die Zusammenstellung der „105-Liste" war jedoch nur rechtmäßig, wenn die darin enthaltenen Daten zulässigerweise in den herangezogenen Unterlagen - dem strafrechtlichen Ermittlungsvorgang, den beiden Sachakten (Staatsschutz) des LKA und der Kriminalakte - gespeichert waren. Das ist bezüglich der Kriminalakte nicht der Fall.

Die Kriminalakte wird zu einem Wiederholungsstraftäter geführt, der der Göttinger autonomen Szene zugerechnet wird. Die Kriminalakte besteht seit 1975 und umfasst zwei volle Leitzordner. Ich habe bei drei Namen (Betroffene) die Rechtmäßigkeit ihrer Erfassung in dieser Kriminalakte überprüft. Nach meinen Feststellungen sind Schriftstücke zur Kriminalakte genommen worden, in denen der Name des Wiederholungsstraftäters genannt wurde. Soweit darin auch Daten der Betroffenen aus der ersten Hälfte der 80er Jahre enthalten waren, sind diese mit übernommen worden. Es kann dahinstehen, ob - wie das LKA meint - eine Speicherung von Daten Dritter schon seit Inkrafttreten des NGefAG (1994) erlaubt ist und insofern die erst mit dem Änderungsgesetz von 1997 gesetzlich neu aufgenommene Befugnis in § 39 Abs. 3 nur eine klarstellende Bedeutung hatte. Zu bewerten ist hier die Zulässigkeit einer Zuspeicherung von Daten Dritter in

einer Kriminalakte aus der ersten Hälfte der 80er Jahre, für die allenfalls der Übergangsbonus fruchtbar gemacht werden kann. Die Inanspruchnahme dieses Übergangsbonus setzt jedoch voraus, dass ohne die Zuspeicherung der Daten in der Kriminalakte die Funktionsfähigkeit der polizeilichen Arbeit nicht gewährleistet gewesen wäre.

Dies ist zumindest zweifelhaft, braucht hier aber nicht abschließend entschieden zu werden, denn zumindest die Speicherungsdauer der noch heute in den Akten enthaltenen Daten der Betroffenen ist rechtswidrig. Die in Rede stehenden Daten sind für keinen der in den §§ 38 und 39 NGefAG genannten Verwendungszwecke erforderlich. Die Speicherung von Daten Dritter in einer Kriminalakte erfolgt - auch nach Auffassung des Niedersächsischen Innenministeriums - zu dem Zweck, Informationen vorzuhalten, die einen Erkenntniswert für die Vorsorge zur Verfolgung von Straftaten oder die Verhütung einer künftigen Straftat derjenigen Person haben, zu der die Kriminalakte geführt wird. Diese Bedeutung haben die Zuspeicherungen von Daten Dritter hier nicht. Sie beinhalten Aussagen über nicht strafbewehrte Handlungen. Sie zeigen lediglich, dass die Betroffenen ebenso wie der Wiederholungsstraftäter an einer nicht verbotenen Demonstration teilgenommen haben. Eine darüber hinausgehende Verbindung mit dem Wiederholungsstraftäter dokumentieren sie nicht. Aus dieser - inzwischen mehr als 15 Jahre zurückliegenden - Tatsache lassen sich heute keinerlei Erkenntnisse über das künftige Verhalten des Wiederholungsstraftäters herleiten, die für eine Gefahrenvorsorge von Belang sein könnten. Die fortdauernde Speicherung dieser Daten ist deshalb nicht erforderlich. Nach § 39 a NGefAG sind personenbezogene Daten zu löschen, die zu einem der in den §§ 38 und 39 NGefAG genannten Zwecke nicht mehr erforderlich sind. Diese Vorschrift ist durch das Änderungsgesetz vom 28. November 1997 in das NGefAG eingefügt worden, um ein in sich geschlossenes System der Datenverarbeitungsvorschriften zu erreichen. Zuvor musste hinsichtlich der Frage der Löschung auf § 17 NDSG zurückgegriffen werden, soweit nicht an anderer Stelle die Löschung in speziellen Bestimmungen ausdrücklich angeordnet wurde. Materiell unterscheidet sich die Regelung im § 39 a NGefAG von der zuvor geltenden Rechtslage dadurch, dass die Löschungsverpflichtung nunmehr bereits dann eintritt, wenn die weitere Datenspeicherung zu einem der in den §§ 38 und 39 NGefAG genannten (konkreten) Verwendungszwecke nicht mehr erforderlich ist. Vor der Einfügung des § 39 a in das Gesetz trat die Löschungsverpflichtung gem. §§ 48 und 17 Abs. 2. Nr. 2 NDSG hingegen erst ein, wenn die weitere Datenspeicherung zur Aufgabenerfüllung der Daten verarbeitenden Stelle nicht mehr erforderlich war.

Die Vorschrift des § 38 Abs. 1 S. 4 NGefAG kann nicht zu einer anderen Bewertung führen. Hiernach dürfen neben den zur Zweckerreichung erforderlichen Daten ausnahmsweise auch solche Daten gespeichert werden, die zwar zur Zweckerreichung nicht benötigt werden, deren an sich gebotene Abtrennung aber aus tatsächlichen Gründen entweder nicht oder nur mit einem unverhältnismäßigen Aufwand möglich ist. Die Regelung bezieht sich nur auf den Vorgang der (Erst-)Speicherung von personenbezogenen Daten, nicht aber auf das weitere Vorhalten gespeicherter Daten. Damit sind z. B. auf Foto- oder Filmaufnahmen miterfasste Daten über unvermeidbar mitbetroffene Dritte angesprochen, die aus technischen Gründen nicht oder nur mit einem unvertretbaren Aufwand abgetrennt werden könnten (vgl. Böhrenz/Franke, NGefAG, 5. Aufl., § 38, Erl. 6). Die hier in Rede stehende Frage, wie lange bereits gespeicherte Daten aufbewahrt werden dürfen bzw. wann sie gelöscht werden müssen, beurteilt sich nach dem eindeutigen Wortlaut der Vorschrift hingegen nicht nach § 38 Abs. 1 S. 4 NGefAG, sondern nach § 39 a des Gesetzes. Im Falle einer von vornherein unzulässigen Speicherung würde sich die Löschungsverpflichtung aus § 48 NGefAG i. V. m. § 17 Abs. 2 Nr. 1 NDSG ergeben.

Ich habe daher gemäß § 23 Abs. 1 NDSG das Vorhalten der Unterlagen zu den Betroffenen beanstandet und deren Löschung gefordert. Darüber hinaus ist die Notwendigkeit der Löschung der übrigen Zuspeicherungen in dieser Kriminalakte zu überprüfen, soweit es um Namen aus der „105-Liste“ geht. Ich halte es für notwendig, für die Zukunft klare Vorgaben zur Zuspeicherung von Daten Dritter - einschließlich der Dauer der Speicherung - in der „Richtlinie für das Führen von Kriminalakten" zu schaffen.

Die eingesehenen beiden Sachakten des LKA werden zu Gruppierungen aus dem linksextremen Spektrum geführt. Nach Darstellung des LKA ist Zweck der auf § 38 NGefAG beruhenden Speicherungen, Auskunft über die Historie einer Organisation zu erhalten. Hierbei kommt es naturgemäß auch zur Speicherung personenbezogener Daten. Die Informationen sind chronologisch abgeheftet. Es handelt sich u. a. um Hinweise auf Kontakte im Terrorismusbereich oder um strafrechtlich relevante Aktivitäten.

Bei vier Namen (Betroffene) habe ich die Rechtmäßigkeit ihrer Erfassung in diesen beiden Sachakten überprüft. Die Erforderlichkeit der seinerzeitigen Speicherung ist für mich nachvollziehbar. Für die Beurteilung der Frage, ob auch die weitere Speicherung dieser Daten erforderlich ist, fehlen mir derzeit geeignete Bewertungsmaßstäbe, mit deren Hilfe ich unter Berücksichtigung des zuvor beschriebenen Zweckes einer Sachakte zu einer eindeutigen Stellungnahme kommen könnte.

Die Angaben in den Staatsschutzakten haben - wie der vorliegende Prüfvorgang zeigt - erhebliche grundsätzliche Datenschutzrelevanz.

Auffällig ist, dass es für Sachakten dennoch keine konkrete Regelung über die Speicherungsdauer personenbezogener Daten gibt.

Für Kriminalakten wurden in der „Richtlinie für das Führen von Kriminalakten" (KA-Richtlinie) vom 6. Februar 1998 in Ziffer 10.1 Prüffristen - bei Erwachsenen - von in der Regel fünf Jahre, in besonderen Fällen von zehn Jahre vorgeschrieben. Ein besonderer Fall ist in der Regel anzunehmen, wenn aufgrund der Persönlichkeit des Betroffenen, nach Art der Tatausführung bzw. der Art des begangenen Delikts oder der hervorgerufenen Gefahr die Annahme gerechtfertigt ist, dass ein einschlägiges Verhalten der Person auch nach einer Frist, die fünf Jahre übersteigt, erwartet werden kann. In Fällen geringerer Bedeutung ist eine kürzere Frist vorzusehen.

Ziffer 15.3 der Richtlinie bestimmt, dass personenbezogene Daten gemäß § 39 a NGefAG zu löschen sind, wenn sich bei der Überprüfung ergibt, dass die Daten nicht mehr erforderlich sind. Ergibt sich die Notwendigkeit einer weiteren Speicherung der Daten, so ist eine neue Prüffrist von höchstens drei Jahren vorzusehen. Diese Prüffrist ist zu begründen.

Bei Sachakten hingegen fehlen derartige Prüffristen. Es wird in keiner Weise zwischen „Schlüsselpersonen“, Mitgliedern, Mitläufern und Randpersonen sowie nur zufällig Betroffenen hinsichtlich der Speicherungsdauer ihrer Daten differenziert. Zweck einer Sachakte ist - wie dargelegt - das Vorhalten von Auskünften zur Historie einer Organisation. Dabei liegt es auf der Hand, dass Erkenntnisse über z. B. Gründungsmitglieder oder Vorstandsmitglieder der Organisation, also über Personen, die die Organisation in wesentlichen Bereichen (mit-)gestalten, anders zu beurteilen sind als beispielsweise Erkenntnisse über Mitglieder ohne besondere Einflussmöglichkeiten oder sogar über reine Mitläufer und Randpersonen, die sich lediglich im Umfeld der Organisation bewegen.

Nach Ansicht des LKA richtet sich die Speicherungsdauer nach der Aufbewahrungsfrist der Niedersächsischen Aktenordnung (30 Jahre), die auch für diese Vorgänge gelte, wobei diese Frist erst nach Schließung der Akte beginnt. Der

Zweck, die Entwicklung der betreffenden Gruppe nachvollziehen zu können, rechtfertige diese Speicherungsdauer. Eine zusätzliche Prüfung, wie lange die Daten von Personen gespeichert bleiben können, die irgendwann mit der Gruppe in Verbindung gestanden haben, sei nicht erforderlich. Nach dieser Betrachtungsweise dürften Daten über alle Personen, die in einem bis zu 30 Jahre zurückliegenden Zeitraum in Beziehung zu der Gruppe gestanden haben, ohne jede Überprüfung und Differenzierung so lange gespeichert und genutzt werden, wie die Unterlagen über die Gruppe selbst.

Dass eine solche Verfahrensweise schon bei Personen, die in einer eher seltenen Beziehung zur Gruppe gestanden haben, rechtlich zweifelhaft ist, liegt, wie vorstehend dargelegt, auf der Hand, da solche Informationen kaum zur Charakterisierung der Gruppe und als Information über ihre Historie dienen können. Eindeutig rechtswidrig ist diese Handlungsweise jedenfalls, wenn die betroffenen Personen eine inhaltlich bedeutungslose Berührung mit der Gruppe hatten, ohne dass sonstige konkrete Hinweise eine nähere Verbindung belegen. So sagt z. B. die bloße Teilnahme an einer nicht verbotenen Demonstration, womöglich zu einem aktuellen politischen Thema, im Regelfall noch nichts Wesentliches über die Gruppe aus, insbesondere wenn auch Vertreter der Gruppe lediglich als Demonstrationsteilnehmer, nicht aber als Veranstalter auftreten. Selbst wenn die erstmalige Speicherung eines solchen Datums im Hinblick auf die möglicherweise noch nicht abschätzbare künftige Entwicklung der Gruppe im Einzelfall noch als zulässig angesehen würde, ist eine undifferenzierte Weiterführung der Speicherung für einen Zeitraum von mindestens 30 Jahren keinesfalls erforderlich. Die Regelung der Aufbewahrungsdauer von Akten in der NdsAktO aus dem Jahre 1970 orientiert sich an heute nicht mehr tragfähigen Vorstellungen. Datenschutzgesichtspunkte spielten dabei keine Rolle. Ich habe in anderen Zusammenhängen mehrfach darauf hingewiesen, dass diese Regelungen überarbeitungsbedürftig sind. Zudem übersieht die polizeiliche Praxis, dass die NdsAktO hier ohnehin nicht anwendbar ist. Nach § 39 a NGefAG - die Vorschrift gilt auch nach Auffassung des Niedersächsischen Innenministeriums auch für Sachakten, solange diese zu Zwecken der Gefahrenabwehr angelegt werden und in ihnen personenbezogene Daten gespeichert sind - sind personenbezogene Daten zu löschen, die zu einem der in den §§ 38 und 39 NGefAG genannten Zwecke nicht mehr erforderlich sind. Diese Regelung erfordert - im bewussten Gegensatz zu § 17 NDSG - eine Einzelfallbewertung. Sie kann nicht durch die Festlegung einer generellen Aufbewahrungsfrist ersetzt werden.

Hinsichtlich der in den Sachakten enthaltenen personenbezogenen Daten ist daher zumindest eine Prüfung der Löschungsnotwendigkeit gemäß den genannten Vorschriften in regelmäßigen Abständen auf der Grundlage einer Einzelfallbewertung unerlässlich.

Da es sich um Prüffristen für die jeweilige gesamte Sachakte handelt, ist ein Register über die in den Sachakten enthaltenen personenbezogenen Daten nicht erforderlich Die Gefahr des Entstehens weiterer/neuer Dateien mit personenbezogenen Daten, die zu personenbezogenen Selektionsmöglichkeiten in Sachakten führen würden, besteht somit nicht. Eine aus Gründen der Arbeitserleichterung ggf. vorzunehmende Kennzeichnung derjenigen Sachakten, die personenbezogene Daten beinhalten, ist aus datenschutzrechtlicher Sicht unproblematisch. .

Die generelle Speicherung personenbezogener Daten für die Zeitdauer von mindestens 30 Jahren ist mit § 39 a NGefAG also nicht vereinbar.

Ich habe daher gemäß § 23 Abs. 1 NDSG diese Verfahrensweise beanstandet und deren Änderung gefordert. Die genannten Sachakten sind daraufhin zu überprüfen, ob sie Daten von Personen aus der „105-Liste“ enthalten, die zur Aufgabenerfüllung nicht (mehr) erforderlich und somit zu löschen sind. Darüber hinaus muss eine Regelung getroffen werden, wie künftig die Beachtung des

§ 39 a NGefAG auch bei personenbezogenen Daten in Sachakten in der Verwaltungspraxis sichergestellt werden soll.

Eine datenschutzrechtliche Überprüfung der Zulässigkeit des vom Ermittlungsrichter des Bundesgerichtshofes per Beschluss angeordneten Auskunftsverpflichtung des Arbeitsamtes Göttingen zu den Namen auf der „105-Liste" (Datenabgleich) ist mir verwehrt. Gemäß § 2 Abs. 1 NDSG unterliegen gerichtliche Entscheidungen nicht der Prüfkompetenz des Landesbeauftragten für den Datenschutz.

Das Innenministerium hat zu meinem Prüfbericht und den Beanstandungen Stellung genommen. Im Kern läuft die Argumentation darauf hinaus, dass sich im Bereich der polizeilichen Ermittlungstätigkeit die Relevanz bestimmter Daten oft erst nach Jahren herausstelle. Deshalb seien die zugespeicherten Daten Dritter erforderlich im Sinne des NGefAG und somit erst zusammen mit der jeweiligen Kriminal- oder Sachakte zu löschen. Würde eine vorherige Löschung vorgenommen, seien die Akten unvollständig und daher wertlos. Zudem wäre eine Löschung nur mit einem unvertretbar hohen Aufwand möglich, sodass sie gemäß § 38 Abs. 1 Satz 4 NGefAG nicht gelöscht werden müssten.

Ich befinde mich zur Zeit im Gespräch mit dem Innenministerium, um zu einer datenschutzrechtlich einwandfreien Lösung zu gelangen, die andererseits die polizeilichen Belange praxisnah berücksichtigt.

11.2 Verdachtsunabhängige Kontrolle („Schleierfahndung")

Den Beispielen Baden-Württembergs, Bayerns und Niedersachsens folgend haben inzwischen zahlreiche Länder sowie der für den BGS zuständige Bund in ihren Polizeigesetzen die Möglichkeit sog. verdachtsunabhängiger Kontrollen geschaffen, andernorts als Schleierfahndung bekannt. Auch wenn Voraussetzungen und Eingriffsbefugnisse in den Polizeigesetzen der Länder und des Bundes durchaus unterschiedlich geregelt sind, geht es im Kern immer um die der Polizei eröffnete Möglichkeit, polizeiliche Personenkontrollen auch ohne Vorliegen eines konkreten Verdachts oder einer Gefährdungssituation gegen jedermann durchführen zu können. In Niedersachsen gilt seit der letzten Novellierung des Niedersächsischen Gefahrenabwehrgesetzes, dass die Polizei zur Vorsorge für die Verfolgung oder zur Verhütung von Straftaten von erheblicher Bedeutung mit internationalem Bezug jede im öffentlichen Verkehrsraum angetroffene Person kurzfristig anhalten, befragen, mitgeführte Ausweispapiere prüfen und mitgeführte Sachen in Augenschein nehmen kann (vgl. auch XIV. TB 10.3). Eine räumliche Beschränkung, etwa auf Grenzgebiete oder bestimmte Straßenkategorien, kennt die niedersächsische Regelung nicht. Sie ist insoweit flächendeckend.

In einem Aufsehen erregenden, aber doch nicht unerwarteten Urteil hat das Landesverfassungsgericht Mecklenburg-Vorpommern im Oktober 1999 die Verfassungswidrigkeit von Teilen der dort geltenden Regelung zur Schleierfahndung festgestellt, nicht aber die grundsätzliche Befugnis des Staates zur Einführung solcher Jedermannkontrollen in Frage gestellt (LVerfG MV, Urteil vom 21. Oktober 1999 - LVerfG 2/98, NJW 2000, 2016). Ich möchte an dieser Stelle nur kurz auf diese Entscheidung eingehen, weil sich die ihr zugrundeliegende Rechtslage in Mecklenburg-Vorpommern wesentlich von der in Niedersachsen unterscheidet. Zwar umfasst die Schleierfahndung dort einen deutlich engeren räumlichen Bereich als in Niedersachsen (nämlich das Grenzgebiet bis zu einer Tiefe von 30 km, Durchgangsstraßen, öffentliche Einrichtungen des internationalen Verkehrs und das Küstenmeer), dafür sind die polizeilichen Befugnisse aber weitaus stärker ausgestaltet: Während sich das niedersächsische Recht im Wesentlichen auf ein Befragungs- und Inaugenscheinnahmerecht der Polizei beschränkt, sieht das mecklenburg-vorpommerische Recht insbesondere die Ver-

pflichtung zur Offenbarung der Identität vor, die auch mit polizeilichen Zwangsmaßnahmen bis hin zur Durchsuchung und Durchführung erkennungsdienstlicher Maßnahmen durchgesetzt werden kann bzw. konnte.

Das Verfassungsgericht sieht einen Verstoß gegen das Recht auf informationelle Selbstbestimmung u. a. darin, dass eine gesetzliche Eingriffsbefugnis ohne Differenzierung gegen jede Person eingeräumt werde, die sich auf Durchgangsstraßen außerhalb des Grenzgebietes aufhält. Der Freiheitsanspruch des Einzelnen verlange, dass er von polizeilichen Maßnahmen verschont bleibt, die nicht durch eine hinreichende Beziehung zwischen ihm und einer Gefährdung eines zu schützenden Rechtsgutes oder eine entsprechende Gefahrennähe legitimiert sind. Es sei daher erforderlich, die Eingriffsschwellen im Gesetz präzise zu bestimmen, wobei für Eingriffe, die über das Anhalten und die Aufforderung, sich auszuweisen, hinausgehen, die Schwellen höher gelegt werden müssten.

Mit dem Niedersächsischen Innenministerium habe ich die Frage eingehend erörtert, ob und inwieweit sich aus dieser verfassungsrechtlichen Bewertung auch gesetzgeberischer Handlungsbedarf in Niedersachsen ergibt. Vor dem Hintergrund der unterschiedlichen, nicht vergleichbaren Rechtslage in beiden Ländern sieht das Innenministerium einen solchen Handlungsbedarf nicht. Wie an anderer Stelle ausgeführt, werde ich mit dem Innenministerium demnächst Gespräche über den Novellierungsbedarf beim NGefAG führen und dabei auch das Urteil des Landesverfassungsgerichts Mecklenburg-Vorpommern zur sog. Schleierfahndung mit ansprechen. Aus meiner Sicht geht es dabei vor allem um die Frage, ob es geboten ist, den bisherigen räumlichen Anwendungsbereich (nämlich den gesamten öffentlichen Verkehrsraum des Landes) zu beschränken.

11.3 „Fahndungsehe“ zwischen Polizei und Arbeitsamt?

Der nachfolgende Fall mag belegen, dass meine Befürchtung, verdachtsunabhängige Kontrollen der Polizei könnten gleichsam als „Türöffner“ für andere, mit der Bekämpfung erheblicher Straftaten mit internationalem Bezug in keinerlei Zusammenhang stehende Kontrollen benutzt werden, zumindest nicht ganz unbegründet ist.

Was war geschehen? Unter der Überschrift „Kontrollen quer durch die Gesetze“ berichtete eine Zeitung aus dem Oldenburgischen über eine verdachtsunabhängige Kontrolle der Polizei auf der Autobahn A 28 in Zusammenarbeit mit dem Arbeitsamt, bei der - so die Zeitung weiter - reihenweise Sozialbetrüger ins Netz gegangen seien. Der Ablauf stellte sich so dar, dass die Polizei auf dem Gelände einer Autobahnraststätte eine großflächige verdachtsunabhängige Kontrolle durchgeführt hatte. Auf der Grundlage eines entsprechenden polizeilichen Lagebildes - nur dies ist Voraussetzung für die ansonsten voraussetzungsfreien Kontrollen - sollte mit der Maßnahme gezielt Einbruchskriminalität osteuropäischer Tätergruppen bekämpft werden. Nach Abschluss der Polizeikontrolle wurden dann bestimmte Fahrzeuge (überwiegend Kleinlastwagen und -transporter, wie sie allgemein von Kurierdiensten eingesetzt werden) zu einer Kontrollstelle des Arbeitsamtes „weitergereicht“. Ziel dieser nächtlichen Arbeitsamts-Kontrolle war es insbesondere, Fälle von Leistungsmissbrauch aufzudecken.

Der Verdacht lag nahe, dass sich das Arbeitsamt hier an die nur der Polizei zustehende Befugnis zur Jedermannkontrolle „angehängt“ und sich auf diese Weise die des Leistungsmissbrauchs und der Schwarzarbeit verdächtigen Klein- und Kleinstunternehmer hatte zuführen lassen. Diese Verknüpfung verdachtsunabhängiger Kontrollen der Polizei mit Außenprüfungen des Arbeitsamtes (auf der Grundlage des SGB III) habe ich daher mit den zuständigen Landes- und Bundesbehörden erörtert, da deren Zulässigkeit auch im Hinblick auf die gesetzliche Zielrichtung verdachtsunabhängiger Kontrollen zumindest fraglich erschien.

Die beteiligten Stellen haben darauf hingewiesen, dass beide Kontrollen in der jeweils eigenen Zuständigkeit durchgeführt worden seien und insbesondere die Polizei auch nicht in unterstützender Weise für das Arbeitsamt tätig geworden sei (was auch unzulässig gewesen wäre). Vielmehr habe die Polizei eine eigene Kontrollaktion durchgeführt und dazu Fahrzeuge angehalten und eingewiesen. Das Arbeitsamt, dem ein Anhalterecht selbst nicht zusteht, habe lediglich diesen tatsächlichen Umstand genutzt.

In datenschutzrechtlicher Hinsicht ist es tatsächlich nicht zu beanstanden, wenn die Polizei die ihr eingeräumte Befugnis zu einer verdachtsunabhängigen Kontrolle nutzt und zu diesem Zweck alle Fahrzeuge anhält und kontrolliert. Für mich bleibt aber nach wie vor offen, aufgrund welcher Rechtsgrundlage das Arbeitsamt seinerzeit die im Anschluss an die Polizeikontrolle zu überprüfenden Fahrzeuge angehalten hatte. Ich habe diese Frage letztlich auf sich beruhen lassen, da das fehlende Anhalterecht der Arbeitsverwaltung keine datenschutzrechtliche Frage ist und die Zuständigkeit für die Arbeitsverwaltung ohnehin dem Bundesbeauftragten für den Datenschutz obliegt, den ich natürlich entsprechend informiert habe.

Im Ergebnis ist festzuhalten, dass die beschriebene „Fahndungsehe" zwischen Polizei und Arbeitsamt zwar in datenschutzrechtlicher Hinsicht zulässig war, die tatsächlichen Umstände aber gleichwohl die Vermutung nahe legen, dass das besondere Instrument der verdachtsunabhängigen Kontrollen hier auch für ganz andere als die gesetzlich festgelegten Zielen genutzt worden ist. Ich werde diese Entwicklung weiterhin aufmerksam beobachten.

11.4 INPOL-neu

Bereits in meinem letzten Tätigkeitsbericht hatte ich mich mit Problemen der Neukonzeption der INPOL-Datenbank auseinandergesetzt. Da sich herausgestellt hat, dass die Mehrzahl der Länder aus unterschiedlichen Gründen nicht in der Lage sein wird, rechtzeitig zur Inbetriebnahme von INPOL-neu beim Bundeskriminalamt (BKA) eigene INPOL-neu-kompatible Datenbanken bereitzustellen, hat sich das BKA auf der Grundlage des § 2 Abs. 5 des Bundeskriminalamtgesetzes (BKAG) bereit erklärt, im Wege der Auftragsdatenverarbeitung die Daten der Länderpolizeien zu verarbeiten. Nach dieser Vorschrift kann das BKA die Länder auf Ersuchen bei deren Datenverarbeitung unterstützen. Allerdings folgt aus § 2 Abs. 1 BKAG, dass die Länder grundsätzlich eigene Datenspeicher zu betreiben haben. Die Hilfeleistung des BKA kann also nur zeitlich befristet erfolgen. Mittlerweile mehren sich die Anzeichen dafür, dass das BKA und die Polizeien der Länder zunehmend eine dauerhafte Datenhaltung der Länder beim BKA anstreben.

Bereits Mitte Juni und nochmals Ende September 2000 habe ich mich an das Niedersächsische Innenministerium gewandt und darauf hingewiesen, dass ich in Übereinstimmung mit den anderen Datenschutzbeauftragten eine dauerhafte Auslagerung der Verarbeitung wesentlicher Teile der Datenbestände der Landespolizeien zum BKA auf der Grundlage des § 2 Abs. 5 BKAG für unzulässig halte. Diese Haltung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einem Umlaufbeschluss vom 10. Oktober 2000 gegenüber dem Bundesinnenministerium nochmals bekräftigt (vgl. Anlage 20).

Gleichwohl möchte ich mich zwingenden Erforderlichkeiten, im Wege einer zeitlich begrenzten Übergangslösung einen termingerechten Anschluss an INPOL-neu sicherzustellen, nicht verschließen und eine datenschutzkonforme Ausgestaltung der vertraglichen Grundlagen für eine übergangsweise Auftragsdatenverarbeitung erreichen. Der Termin- und Kostendruck, unter dem der Anschluss der Datenverarbeitung der Länder an INPOL-neu steht, darf aber weder

die rechtliche Interpretation des Regelungsgehaltes des § 2 Abs. 5 BKAG steuern noch als Begründung für eine neuerliche faktische Ausdehnung des wechselseitigen Zugriffs von BKA und Länderpolizeien auf Daten dienen, ohne dass die durch § 2 Abs. 1 BKAG bezeichnete Grenze beachtet würde. Aus § 2 Abs. 1 BKAG folgt, dass die Länderpolizeien grundsätzlich eigene Datenspeicher zu betreiben haben. Die Hilfskonstruktion per Auftragsdatenverarbeitung ist nur als vorübergehende Notmaßnahme zur Gewährleistung eines termingerechten Anschlusses der Länder an INPOL-neu tragbar. Die Datenbestände der Länder sind beim BKA so zueinander abzuschotten, wie es bei einer dezentralen Haltung der Landesdaten der Fall wäre.

Zu dem mittlerweile vorliegenden Entwurf einer Rahmenvereinbarung zur Auftragsdatenverarbeitung durch das BKA habe ich gegenüber dem Niedersächsischen Innenministerium umfangreich Stellung genommen. Ich habe eine eindeutige Trennung der Landesdatenbestände untereinander sowie gegenüber dem Bundesbestand verlangt. Die gegenwärtige Rechtslage fordert eine solche eindeutige Verpflichtung zur Wahrung einer absoluten Zweckbindung sowohl gegenüber dem BKA als auch den anderen Teilnehmern am INPOL-neu-Verbund.

Als ein weiteres Problem stellt sich die Übernahme von Daten aus INPOL-aktuell in das neue System INPOL dar. Hierzu hat die Arbeitsgruppe INPOL-neu der Datenschutzbeauftragten des Bundes und der Länder darauf hingewiesen, dass die Datenbestände unter Erforderlichkeitsgesichtspunkten vor einer Übernahme zu selektieren seien. Dies trifft insbesondere für die PIOS-Dateien zu, in denen Daten über „Dritte" gespeichert sind, die nach geltender Rechtslage nicht mehr Bestandteil von INPOL sein dürfen. Die Projektgruppe INPOL-neu des BKA hat hierzu dargelegt, Plausibilitäten entwickelt zu haben, um die erforderlichen Selektionen durchführen zu können. Die Prüfung, ob in PIOS Daten gespeichert sind, die gemäß BKAG nicht nach INPOL-neu übernommen werden können, werde in Abstimmung mit den Bundesländern nach Abschluss der fachlichen Vorarbeiten erfolgen. Ich habe beim Niedersächsischen Innenministerium angefragt, ob für den Bereich der niedersächsischen Polizei bereits Kriterien für die Selektion der Datenbestände entwickelt worden sind, und gebeten, mir diese ggf. mitzuteilen. Eine Antwort steht noch aus.

Weiterhin ist nach meinem Kenntnisstand geplant, in INPOL-neu im Rahmen eines sogenannten DNA-Merkers die Möglichkeit zur Speicherung eines Hinweises über eine bereits stattgefundene Entnahme von Körperzellen zu schaffen. Diese Information soll den polizeilichen Anwendern von INPOL-neu bei jeder Personenabfrage zur Verfügung gestellt werden. Hiergegen bestehen meinerseits erhebliche Bedenken, weil durch die Erfassung dieses Merkmales eine stigmatisierende Wirkung im Kontakt zwischen Polizei und Bürger erzeugt werden könnte, die u. U. dazu führt, dass der Bürger weitergehenden Kontrollen unterzogen wird. Rechtlicher Ansatzpunkt für diese Überlegungen sind die engen Zweckbestimmungsregelungen im DNA-Identitätsfeststellungsgesetz und der Errichtungsanordnung für die DNA-Analyse-Datei beim BKA. Da ich jedoch die grundsätzliche Zulässigkeit der Speicherung des DNA-Merkers nicht bestreite, sehe ich eine mögliche Lösung dieses Konflikts darin, dass der DNA-Merker erforderlichenfalls nur über eine zweite Abfrage zur Verfügung gestellt wird. Diese zweite Abfrage sollte durch flankierende Maßnahmen (Protokollaufzeichnung o. Ä.) für Zwecke datenschutzrechtlicher Kontrollen abgesichert werden. Ich habe das Innenministerium gebeten, sich beim BKA für eine solche Lösung einzusetzen.

11.5 Mitteilungen der Polizei an Presse, Hörfunk und Fernsehen

Das Niedersächsische Innenministerium genehmigte einem Fernsehteam, zwecks Erstellung einer mehrteiligen Serie über Polizeiarbeit zum Thema „Mordkommission" die polizeilichen Ermittlungen nach dem Mord zum Nachteil eines Kindes vor Ort zu begleiten. Es war ausdrücklich vereinbart, gefertigte Aufnahmen nicht für eine aktuelle Berichterstattung, sondern lediglich für die im darauffolgenden Jahr geplante Serie zu verwenden. Des Weiteren stand die Genehmigung unter dem ausdrücklichen Vorbehalt, Persönlichkeitsrechte der Betroffen zu wahren sowie Bilder erst nach Freigabe durch Polizei bzw. Staatsanwaltschaft zu senden. Abgestimmt war diese Maßnahme zudem mit dem Niedersächsischen Justizministerium und der Generalstaatsanwaltschaft.

Das Kamerateam begleitete die Arbeit der eingerichteten Mordkommission über den Zeitraum von mehr als einem Jahr. Dabei nahmen Mitarbeiter des Fernsehsenders auch an internen Besprechungen teil.

Am Tag der Festnahme des mutmaßlichen Täters begleitete das Fernsehteam zunächst die vorausgehende Einsatzbesprechung und schließlich den Zugriff auf den heranwachsenden Tatverdächtigen auf dem Gelände einer Schule, bei dem Filmaufnahmen gefertigt wurden.

Entgegen den Vereinbarungen wurden diese Aufnahmen des nicht unkenntlich gemachten Festgenommen am gleichen Tag in den Mittagsnachrichten ausgestrahlt. Darüber hinaus wurde das Material anderen interessierten Fernsehsendern zur Verfügung gestellt.

Die Begleitung von polizeilichen Maßnahmen durch Fernsehteams ist in dem Erlass über „Mitteilungen der Polizei an Presse, Hörfunk und Fernsehen im Rahmen ihrer Öffentlichkeitsarbeit" (RdErl. d. MI v. 17. Dezember 1993, II Nr. 7, Nds. MBl. Nr. 9/1993) geregelt. Darin ist ausdrücklich festgelegt, dass die Weitergabe personenbezogener Daten an die Medien die Ausnahme sein soll. Besondere Zurückhaltung ist außerdem bei Jugendlichen zu üben.

Dieser Erlass wurde im vorliegenden Fall nicht hinreichend beachtet. Für die Zukunft sagte das Niedersächsische Innenministerium zu, im Rahmen von Dienstbesprechungen und auf andere geeignete Weise auf die Einhaltung des Erlasses hinzuwirken. Datenschutzrechtliche Maßnahmen gegen den Fernsehsenderwegen der nicht vereinbarungsgemäßen Vorgehensweise waren bereits wegen des sich aus § 41 BDSG ergebenden Medienprivilegs ausgeschlossen. Der Sender entschuldigte sich jedoch ausdrücklich für die verabredungswidrige Vorgehensweise beim Niedersächsischen Innenministerium.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer 60. Sitzung in Braunschweig am 12./13. Oktober 2000 dieses Problem insbesondere vor dem Hintergrund des Reality-TV intensiv erörtert und einer Arbeitsgruppe den Auftrag erteilt, Mindestbedingungen zu formulieren, die datenschutzrechtliche Verstöße bei der Zusammenarbeit zwischen den Medien und der Polizei verhindern sollen.

11.6 Umsetzung des sog. BND-Urteils des Bundesverfassungsgerichts

Das BVerfG hat aus Anlass von drei Verfassungsbeschwerden, die sich gegen die Änderung des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Art. 10 GG [G10-Gesetz]) durch das Verbrechensbekämpfungsgesetz vom 28. Oktober 1994 (BGBl. I S. 3186) gewandt haben, bestimmte Regelungen der §§ 3 und 9 G10-Gesetz für verfassungswidrig erklärt, weil sie mit Art. 10 und 19 Abs. 4 GG nicht zu vereinbaren sind, und dem Gesetzgeber auferlegt, bis zum 30. Juni 2001 einen verfassungsgemäßen Zustand

herzustellen. Die Entscheidung hat nicht nur weit tragende Bedeutung für den auf § 3 G10-Gesetz gestützten Bereich der Überwachung der Telekommunikation durch den Bundesnachrichtendienst (BND) und die Weitergabe erlangter Daten u. a. an die Strafverfolgungsbehörden. Wegen ihrer grundsätzlichen Aussagen, die sich auch auf die Gewährleistung des allgemeinen Persönlichkeitsrechts erstrecken, hat sie in gleicher Weise Bedeutung für die staatliche Erhebung und Verarbeitung von Daten in anderen Bereichen

Art. 10 GG gehört zu dem Gewährleistungsbereich des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), das die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen umschreibt, „grundsätzlich selbst zu bestimmen, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“ (siehe BverfGE 65, 1, 41 f.). Aus diesem Gesamtgewährleistungsbereich schützt Art. 10 GG als Ausschnitt die freie Entfaltung der Persönlichkeit durch den vor der Öffentlichkeit verborgenen Austausch von Nachrichten, Gedanken und Meinungen - mithin von Informationen - mittels Fernmeldeeinrichtungen. Soweit sich einzelne Ausprägungen des allgemeinen Persönlichkeitsrechts auf Informationen beziehen, werden sie zu Aspekten des Rechts auf informationelle Selbstbestimmung. Als Konsequenz beanspruchen bei allen Informationseingriffen - nicht nur beschränkt auf das Fernmeldegeheimnis - einheitliche Grundsätze für die Prüfung der Zulässigkeit einer Grundrechtsbeschränkung Geltung. Diese finden ihren Niederschlag im Verhältnismäßigkeitsgrundsatz, der die Anforderungen an die Zielerreichung, die Zweckbindung und das Verfahren unabhängig von dem jeweiligen Gewährleistungsbereich vorgibt (vgl. BVerfG, NJW 2000, 55, 60 f.). Auch kommt der Überwachung des Fernmeldeverkehrs - ebenso wie dem Recht auf informationelle Selbstbestimmung - ein über das Individualinteresse hinausgehender Gemeinwohlbezug zu (vgl. BVerfG, NJW 2000, 55, 63), der eine gleichförmige Bewertung notwendig macht. Art. 19 Abs. 4 GG gewährt dem Bürger Anspruch auf eine wirksame gerichtliche Kontrolle in Fällen, in denen eine Verletzung seiner Rechte durch die öffentliche Gewalt möglich erscheint. Diese Rechtsschutzgarantie gilt wiederum unabhängig davon, ob staatliche Stellen in das allgemeine Persönlichkeitsrecht oder in dessen spezielle Gewährleistungen eingreifen (vgl. BVerfG, NJW 2000, 55, 58). Daher müssen die in dem Urteil des BVerfG formulierten Anforderungen an die Zulässigkeit von Eingriffen in das allgemeine Persönlichkeitsrecht auch auf die polizeilichen Maßnahmen gemäß §§ 30 ff. NGefAG übertragen werden.

Einzelne Vorschriften der §§ 30 ff. NGefAG, die eine polizeiliche Datenerhebung und -verarbeitung erlauben, sind - soweit bislang ersichtlich - mit den Anforderungen an die Zulässigkeit von Eingriffen in das allgemeine Persönlichkeitsrecht nicht vereinbar und bedürfen einer gesetzlichen Neuregelung.

11.6.1 Kenntnis des Betroffenen von der Maßnahme

Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG vermittelt den Betroffenen einen Anspruch auf Kenntnis von polizeilichen Maßnahmen. Das ist ein Erfordernis effektiven Rechtsschutzes. Denn ohne eine solche Kenntnis können sie weder die Unrechtmäßigkeit der Erfassung und Kenntnisnahme ihrer Daten noch etwaige Rechte auf Löschung oder Berichtigung geltend machen. Dieser Anspruch verengt sich nicht sogleich auf den gerichtlichen Rechtsschutz aus Art. 19 Abs. 4 GG. Zunächst handelt es sich um ein spezifisches Datenschutzrecht, das gegenüber der informations- und datenverarbeitenden Stelle geltend gemacht werden kann. Wie die Kenntnisgewährung im Einzelnen auszugestalten ist, gibt das Grundgesetz dabei nicht vor (vgl. BVerfG, NJW 2000, 55, 57). Eine Benachrichtigung ist nur geboten, wenn die Datenerhebung heimlich erfolgt, Auskunftsansprüche aber nicht eingeräumt worden sind oder den Rechten der Be-

troffenen nicht angemessen Rechnung tragen (vgl. BverfGE 30, 1, 21, 31 f.). Soweit die Kenntnis des Eingriffs dazu führen würde, dass dieser seinen Zweck verfehlt, ist es nicht zu beanstanden, die Kenntnisgewährung entsprechend einzugrenzen. Unter Umständen genügt es, den Betroffenen erst später von dem Eingriff zu benachrichtigen (vgl. BVerfGE 49, 329, 342 f.).

Art. 19 Abs. 4 GG gewährt den Betroffenen Anspruch auf eine wirksame gerichtliche Kontrolle in Fällen, in denen eine Verletzung seiner Rechte durch die öffentliche Gewalt möglich erscheint. Soll die Rechtsschutzgarantie auch die Möglichkeit zur Wahrnehmung anderweitig bestehender materieller Rechte sicherstellen, kann auch sie neben dem allgemeinen Persönlichkeitsrecht eine Benachrichtigung gebieten, wenn diese Form der Kenntnisgewährung Voraussetzung der Inanspruchnahme gerichtlichen Rechtsschutzes ist (vgl. BVerfGE 65, 1, 70). Diese Regelung ist auch bei der grundsätzlich bestehenden Pflicht zur Vernichtung nicht mehr erforderlicher Daten zu berücksichtigen. Die Rechtsschutzgarantie des Art. 19 Abs. 4 GG verbietet Maßnahmen, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln (vgl. BVerfGE 69, 1, 49). Daher muss die Vernichtungspflicht für die Fälle, in denen der Betroffene die gerichtliche Kontrolle staatlicher Informations- und Datenverarbeitungsmaßnahmen anstrebt, mit der Rechtsschutzgarantie so abgestimmt werden, dass der Rechtsschutz nicht unterlaufen oder vereitelt wird (vgl. BVerfG, NJW 2000, 55, 58).

Die Regelung im NGefAG zur Unterrichtungspflicht ist damit nicht vereinbar. Sie erfolgt gemäß § 30 Abs. 4 Satz 1 NGefAG lediglich in den besonders gravierenden Fällen der Datenerhebung mit besonderen Mitteln und Methoden gemäß § 30 Abs. 2 Satz 2 Nr. 2 NGefAG, nicht aber in den übrigen Fällen der verdeckten Datenerhebung gemäß § 30 Abs. 2 Satz 2 Nr. 1, 3 und 4 NGefAG. Auch in diesen Fällen hat der Betroffene ein Interesse an der Kenntnis der Maßnahmen, um deren Zulässigkeit nach §§ 32 Abs. 2, 34 bis 37 NGefAG gerichtlich überprüfen lassen und ggf. Löschungs- oder Berichtigungsansprüche geltend machen zu können. Ein Anspruch auf Auskunft ist ihm insoweit nicht eingeräumt. Soweit die Unterrichtung über die Erhebung personenbezogener Daten mit besonderen Mitteln gemäß § 30 Abs. 4 Satz 3 NGefAG erfolgt, „sobald dies möglich ist, ohne die Maßnahme zu gefährden", ist das mit dem Erfordernis effektiven Rechtsschutzes zu vereinbaren.

Bedenken bestehen auch gegen die Regelung des § 30 Abs. 5 Nr. 4 NGefAG, nach der eine Unterrichtung der betroffenen Person stets unterbleibt, wenn die Frist für die Löschung der Daten abgelaufen ist, spätestens jedoch nach Ablauf von zehn Jahren. Gleiches gilt, soweit angenommen wird, dass eine Benachrichtigung auch dann nicht in Betracht kommt, wenn die Daten sofort gelöscht werden. Art. 19 Abs. 4 GG verbietet Maßnahmen, die den Rechtsschutz vereiteln könnten (vgl. BVerfGE 69, 1, 49). Die Vernichtung nicht mehr benötigter Daten muss daher für die Fälle, in denen eine gerichtliche Kontrolle der Maßnahmen in Frage kommt, mit der Rechtsschutzgarantie so abgestimmt werden, dass diese nicht unterlaufen wird (vgl. BVerfG, NJW 2000, 55, 68). Da bereits die Erhebung von Daten einen Eingriff darstellt, muss auch diese überprüfbar sein. Das wird vereitelt, wenn eine Unterrichtung nur deshalb unterbleibt, weil die Daten unverzüglich vernichtet worden sind. Auch nach dem Ablauf von zehn Jahren kann ein schutzwürdiges Interesse der betroffenen Person daran bestehen, eine Datenverarbeitung gerichtlich überprüfen zu lassen und ggf. Berichtigungsansprüche geltend zu machen. Die Anknüpfung an die in Rechts- oder Verwaltungsvorschriften geregelten und u. U. kürzeren Löschungsfristen mag für die Praxis praktikabel sein, kann aber nicht einen Ausschluss der Unterrichtungspflicht rechtfertigen. Der bloße Zeitablauf genügt nicht, weil er keinerlei Schluss darauf erlaubt, dass die erfassten Daten innerhalb dieser Zeit keiner weiteren Verwendung zugeführt worden sind. Gerade diese wirkt sich aber in der Regel

als besonders belastend für den Betroffenen aus (vgl. BVerfG, NJW 2000, 55, 67).

11.6.2 Kennzeichnungs- und Protokollierungspflichten

Art. 10 GG schützt das Fernmeldegeheimnis. Es umfasst zunächst den Kommunikationsinhalt. Die öffentliche Gewalt soll grundsätzlich nicht die Möglichkeit haben, sich Kenntnis vom Inhalt des über Fernmeldeanlagen abgewickelten mündlichen oder schriftlichen Informations- und Gedankenaustauschs zu verschaffen. Das Fernmeldegeheimnis umfasst aber ebenso die Kommunikationsumstände. Dazu gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist (vgl. BVerfGE 67, 157, 172; 85, 386, 396). Auch insoweit kann der Staat grundsätzlich keine Kenntnis beanspruchen. Die Nutzung der Kommunikationsmedien soll insgesamt vertraulich möglich sein (vgl. BVerfG, NJW 2000, 55, 56 f.).

Beschränkungen des Fernmeldegeheimnisses sind zwar gemäß Art. 10 Abs. 2 GG möglich. Sie bedürfen aber nicht nur einer gesetzlichen Regelung, die einen legitimen Gemeinwohlzweck verfolgt und im Übrigen den Grundsatz der Verhältnismäßigkeit wahrt. Zudem ergeben sich aus Art. 10 GG auch besondere Anforderungen an den Gesetzgeber, die gerade die Verarbeitung personenbezogener Daten betreffen, welche mittels Eingriffen in das Fernmeldegeheimnis erlangt worden sind. Zu diesen Anforderungen gehört, dass sich Voraussetzungen und Umfang der Beschränkungen klar und für den Einzelnen erkennbar aus dem Gesetz ergeben. Insbesondere müss der Zweck, zu dem Eingriffe in das Fernmeldegeheimnis vorgenommen werden dürfen, bereichsspezifisch und präzise bestimmt werden, und das erhobene Datenmaterial muss für diesen Zweck geeignet und erforderlich sein. Speicherung und Verwendung erlangter Daten sind daher grundsätzlich an den Zweck gebunden, den das zur Kenntnisnahme ermächtigende Gesetz festgelegt hat. Die Zweckbindung lässt sich nur dann gewährleisten, wenn auch nach der Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher geboten (vgl. BVerfG, NJW 2000, 55, 57). Erforderlich sind auch Vorkehrungen zum Schutz des Fernmeldegeheimnisses. Diese sind in der Verpflichtung der Daten erhebenden Stelle zu sehen, die Übermittlung wie auch deren Durchführung sowie die Vernichtung und Löschung der Daten, die aus Eingriffen in Art. 10 GG stammen, zu protokollieren. Nur unter diesen Umständen kann eine hinreichende nachträgliche Kontrolle stattfinden (vgl. BVerfG, NJW 2000, 55, 67). Schließlich müssen die Daten, die aus Eingriffen in das Fernmeldegeheimnis stammen, vernichtet werden, sobald sie für die den Eingriff rechtfertigenden Zwecke nicht mehr erforderlich sind (vgl. BVerfG, NJW 2000, 55, 68). Auch diese Löschungsverpflichtung muss mit der Rechtschutzgarantie des Art. 19 Abs. 4 GG abgestimmt werden.

§ 33 Abs. 1 NGefAG erlaubt die Aufzeichnung des Zeitpunktes und des Fernmeldeanschlusses, nicht aber des Gesprächsinhaltes. Gleichwohl handelt es sich um einen Eingriff in das Fernmeldegeheimnis, da dieses auch die Umstände der Kommunikation schützt. Die Regelung des § 33 NGefAG enthält weder eine besondere Zweckbindung für die Daten noch spezifische Kennzeichnungs-, Protokollierungs- oder Löschungspflichten. Aus diesem Grund besteht die Gefahr, dass die Daten im Rahmen der Verarbeitung in einer Weise abgespeichert werden oder sich mit anderen Daten und Informationen vermischen, dass ihre Herkunft aus einer Maßnahme zur Überwachung des Fernmeldeverkehrs nicht mehr erkennbar ist. Eine Kontrolle, zu welchem Zweck die Daten gespeichert, übermittelt oder sonst genutzt worden sind, ist ebenfalls nicht möglich. Gegenüber dem Anschlussinhaber und/oder Gesprächsteilnehmer, gegen den sich die poli-

zeiliche Maßnahme richtet, handelt es sich um die Erhebung personenbezogener Daten ohne seine Kenntnis, mithin um eine verdeckte Datenerhebung im Sinne von § 30 Abs. 2 Satz 1 NGefAG. Notwendig ist daher eine Unterrichtungspflicht, die sich aus Art. 19 Abs. 4 GG sowie aus Art. 10 GG ergibt. §§ 30 Abs. 4, 33 NGefAG sehen eine solche - u. U. erst nachträgliche - Benachrichtigung des Anschlussinhabers bzw. Gesprächsteilnehmers nicht vor.

11.6.3 Einsatz von Richtmikrofon und Videokamera

§ 35 Abs. 1 Satz 3 NGefAG stellt klar, dass aufgrund dieser Vorschrift u. a. nicht in das Fernmeldegeheimnis eingegriffen werden darf. Gleichwohl wird es für zulässig gehalten, die Äußerungen eines Teilnehmers am Fernmeldeverkehr mit dem Richtmikrofon abzuhören oder mit einer Videokamera aufzuzeichnen, welche Nummer eine Person am Telefon anwählt. Wie dargelegt, erschöpft sich der Schutzbereich des Art. 10 GG nicht in der Abschirmung des Kommunikationsinhalts gegen staatliche Kenntnisnahme, sondern umfasst auch die äußeren Kommunikationsumstände. Dazu gehört vor allem, ob, wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist (vgl. BVerfG, NJW 2000, 55, 56 f.). Die Aufzeichnung der gewählten Nummer per Videokamera sowie das Abhören eines Teilnehmers sind damit Eingriffe in das Fernmeldegeheimnis. Die Observation der näheren Umstände der Kommunikation oder die Aufzeichnung der Kommunikation sind ziel- und zweckgerichtete staatliche Maßnahmen und nicht nur mittelbare Folgen eines anderen zielgerichteten Eingriffs. Insoweit ist die Aussage des § 35 Abs. 1 Satz 3 NGefAG unzutreffend, da sehr wohl in das Fernmeldegeheimnis eingegriffen wird. § 38 Abs. 2 NGefAG enthält für die aufgrund besonderer Mittel und Methoden erlangten Daten eine Kennzeichnungspflicht, beschränkt diese aber unzulässig auf die Speicherung von personenbezogenen Daten in Akten. Die Zweckbindung wird aber nur gewahrt, wenn sich die Kennzeichnung auch auf die Speicherung in Dateien erstreckt. Es fehlen auch besondere Protokollierungs- und Löschungspflichten, die dem Schutz des Fernmeldegeheimnisses gerecht werden. Die Benachrichtigungspflicht gemäß § 30 Abs. 4, 5 NGefAG bedarf für Maßnahmen nach § 35 NGefAG der Abstimmung mit Art. 19 Abs. 4 GG.

11.6.4 Datenübermittlung

Gemäß § 3 Abs. 5 i. V. m. Abs. 3 Satz 1 G 10 ist der Bundesnachrichtendienst verpflichtet, aus der Fernmeldeüberwachung erlangte Daten anderen Behörden zur Erfüllung ihrer Aufgaben zu übermitteln. Zu diesen Behörden gehören auch die Polizeibehörden, soweit dies zur Erfüllung der Aufgaben des Empfängers - Verhinderung, Verfolgung und Aufklärung bestimmter in § 3 Abs. 3 Satz 1 G 10 genannter Straftaten - erforderlich ist. Die Schwere des Eingriffs ergibt sich daraus, dass in der Übermittlung der personenbezogenen Daten eine erneute Durchbrechung des Fernmeldegeheimnisses liegt, die größere Beeinträchtigungen als der Ersteingriff zur Folge haben kann. Die Wirkung der Datenübermittlung erschöpft sich nicht in der Ausweitung des Personenkreises, der von den Telekommunikationsumständen und -inhalten Kenntnis erhält. An die Kenntnisnahme können sich vielmehr Maßnahmen gegen die von der Überwachung Betroffenen anschließen. So werden die Behörden, denen die Daten nach § 3 Abs. 5 Satz 1 G 10 zu übermitteln sind, regelmäßig Ermittlungen gegen die Betroffenen einleiten, die zu weiteren Nachforschungen und gegebenenfalls zur Einleitung von Strafverfahren führen können (vgl. BVerfG, NJW 2000, 55, 65 f.).

Werden Daten vom Bundesnachrichtendienst gemäß § 3 Abs. 5 i. V. m. Abs. 3 Satz 1 G 10-Gesetz an die niedersächsischen Polizeibehörden übermittelt, dürfen sie gemäß § 39 Abs. 5 NGefAG nur unter den - engen - Voraussetzungen des Absatz 4 gespeichert, verändert oder genutzt werden, da es sich bei den Methoden, derer sich der Bundesnachrichtendienst bedient, um solche handelt, die nach Art und Schwere des Eingriffs den besonderen Mitteln und Methoden vergleichbar sind. Die Polizei hat gemäß § 41 Abs. 2 NGefAG zu prüfen, ob die Zweckbindungen des § 39 Abs. 4 NGefAG vorliegen. Ist das nicht der Fall, sind sie unverzüglich zu löschen. Auch insoweit fehlt es an einer Verpflichtung, die Übermittlung - wie auch deren Durchführung sowie die Vernichtung und Löschung der Daten - zu protokollieren und besonders zu kennzeichnen. Diese Regelungen sind aber zum Schutz des Fernmeldegeheimnisses und einer nachträglichen Kontrolle der Maßnahmen unerlässlich.

Ich werde zu allen angesprochenen Punkten nach Abschluss meiner Prüfung mit dem Niedersächsischen Innenministerium Gespräche aufnehmen. Hierbei werde ich auch die Urteile des Landesverfassungsgerichts Mecklenburg-Vorpommern zum so genannten Großen Lauschangriff im präventiven Bereich (LVerfG 5/98 vom 18. Mai 2000) und zur so genannten Schleierfahndung (LVerfG 2/98 vom 21. Oktober 1999, NJW 2000, 2016) mit einbeziehen.

11.7 Deutsch-russisches Regierungsabkommen über polizeiliche Zusammenarbeit

„Bonn/Moskau: Daten für die Mafia?" - so titelte 1999 der SPIEGEL. Es geht um das noch nicht in Kraft getretene Abkommen zwischen der deutschen und der russischen Regierung über die Zusammenarbeit bei der Bekämpfung von Straftaten von erheblicher Bedeutung. Es dient dem Ziel, gemeinsame Maßnahmen deutscher und russischer Sicherheitsbehörden zur Bekämpfung von unter Einbeziehung organisierter krimineller Strukturen begangenen Straftaten zu ergreifen, insbesondere zur Bekämpfung des Handelns mit Menschen, Waffen und Drogen, Erpressung, Geldwäsche, Falschgeldkriminalität und Terrorismus. Inhalt des Abkommens ist im Wesentlichen der Datenaustausch zwischen deutschen und russischen Behörden zur Verhütung, Ermittlung und Aufklärung derartiger Straftaten. Zur Erleichterung der Zusammenarbeit ist auch vorgesehen, Verbindungsbeamte in den jeweils anderen Staat zu entsenden.

Auch aus meiner Sicht ist es richtig, grenzüberschreitende Kriminalität grenzüberschreitend zu bekämpfen. In datenschutzrechtlicher Hinsicht ist jedoch zu berücksichtigen, dass das Abkommen die Weitergabe hochsensibler personenbezogener Daten sowie eine sehr umfangreiche polizeiliche Zusammenarbeit zwischen beiden Staaten zum Inhalt hat.

Ich hatte der Landesregierung zunächst empfohlen, gegenüber der Ständigen Vertragskommission der Länder ihre Zustimmung zu diesem Abkommen nicht zu erklären, und zwar aus folgenden Gründen:

Das Bundeskriminalamtgesetz (BKAG) regelt in § 14 die Befugnisse bei der Zusammenarbeit im internationalen Bereich und enthält insbesondere das sog. Zweckbindungsgebot, das als eines der tragenden Grundprinzipien des Datenschutzes verlangt, dass Daten nur zu dem Zweck genutzt werden dürfen, zu dem sie erhoben bzw. übermittelt worden sind. Zwar enthält das Abkommen einige datenschutzrechtliche Standards, wie beispielsweise die Prüfung der Erforderlichkeit, Verhältnismäßigkeit oder die Unzulässigkeit der Datenübermittlung bei Beeinträchtigung schutzwürdiger Betroffeneninteressen. Zum Zweckbindungsprinzip und der ausreichenden Kontrollmöglichkeit durch unabhängige Datenschutzbeauftragte enthält das Abkommen jedoch nur den sehr allgemeinen Hinweis, dass die angelieferten Daten nur zu den im Abkommen bezeichneten Zwe-

cken verwendet werden dürfen, die ihrerseits wiederum sehr allgemein beschrieben sind. In diesem Zusammenhang sei nur erwähnt, dass als Datenempfänger auf russischer Seite auch der Föderale Sicherheitsdienst vorgesehen ist, der im Wesentlichen als Inlandsgeheimdienst tätig ist.

Es ist auch nicht ersichtlich, wie die datenschutzrechtlichen Vorgaben des Abkommens in der Russischen Föderation überwacht werden sollen. Auch wenn Russland seit 1996 Mitglied des Europarats ist, bleiben doch erhebliche Zweifel, ob in diesem Staat bereits ein angemessener Datenschutzstandard gewährleistet ist, wie ihn das BKAG fordert.

Zwischenzeitlich hat die Ständige Vertragskommission der Länder dem Abkommen nicht zugestimmt, sondern es lediglich zur Kenntnis genommen. Sie sieht insbesondere aus datenschutzrechtlichen Erwägungen weiteren Beratungsbedarf und hat die Bundesregierung u. a. um Beantwortung der Frage gebeten, wie ein Missbrauch von an den russischen Föderalen Sicherheitsdienst übermittelten Daten etwa für nachrichtendienstliche Zwecke ausgeschlossen werden kann und ob das Abkommen die Änderung bundes- oder landesrechtlicher Regelungen erforderlich macht.

Inzwischen ist man auch im Bundesinnenministerium zu der Einschätzung gelangt, dass das Abkommen nicht als Regierungsabkommen und damit ohne parlamentarische Beratung verabschiedet werden kann, sondern dass es der Ratifizierung durch den Deutschen Bundestag bedarf. Mit den Arbeiten an einem entsprechenden Gesetzentwurf ist bereits begonnen worden.

Diesen Sinneswandel der Bundesregierung begrüße ich, da der mit dem Abkommen verbundene Eingriff in das Recht auf informationelle Selbstbestimmung eine parlamentarische Behandlung zwingend erforderlich macht.

11.8 Veröffentlichung von DNA-Profilen im Internet

Nach Überführung eines Mörders anhand von DNA-Profilen besuchte ein Fernsehsender eine Polizeibehörde, um zur Thematik „genetischer Fingerabdruck" Recherchen vorzunehmen. Im Rahmen der Erläuterungen zur Thematik wurden den Mitarbeitern des Fernsehsenders zur Veranschaulichung drei Datenblätter ausgehändigt, die die ausgewerteten DNA-Profile einer Probe des Täters, der beim Opfer gesicherten Spur sowie eines Mitarbeiters der Polizeidienststelle zeigten. Des Weiteren wurde ihnen gestattet, ein Vergleichsdiagramm zu filmen.

Aufgrund einer vorangegangenen telefonischen Rücksprache mit der zuständigen Staatsanwaltschaft vor Übergabe der Datenblätter war den Mitarbeitern des Fernsehsender bekannt, dass die Probe und die Spur von dem Täter stammten.

In einer nachfolgenden Sendung des Senders wurde die Thematik anhand der übergebenen Datenblätter erläutert. Die DNA-Profile wurden in Form von Tabellen dargestellt.

Außerdem wurden die abgebildeten DNA-Sequenzen- ohne vorherige Absprache mit der Polizeibehörde - im Internet unter Hinweis auf die bereits ausgestrahlte Sendung veröffentlicht.

Auch wenn die veröffentlichten Werte lediglich die Länge bestimmter DNA-Sequenzen bezeichnen und keine Informationen über bestimmte Eigenschaften der Person ablesbar sind, so handelt es sich doch um Einzelangaben, die geeignet sind, einen Bezug zu einer natürlichen Person - dem Täter - herzustellen. Insbesondere vor dem Hintergrund, dass die Erbinformationen zu den intimsten personenbezogenen Daten eines Menschen gehören, war die Weitergabe an den Sender trotz Zustimmung der Staatsanwaltschaft nicht zulässig.

Die Übermittlung der Daten des Mitarbeiters der Dienststelle war wegen seiner Einwilligung unproblematisch.

Die Polizeibehörde hat eingeräumt, hier einen Fehler begangen zu haben. Für die Zukunft will man dadurch, dass man Medien gegenüber losgelöst von konkreten Ermittlungsverfahren lediglich auf Daten von Mitarbeitern - mit deren Einwilligung - bzw. auf erfundene Sequenzen zurückgreift, eine Wiederholung verhindern. Der Sender hat zwischenzeitlich die im Internet dargestellten Sequenzen auf meine Bitte hin durch Einsetzen anderer Werte verfremdet. Für den Fall, dass die entsprechende Fernsehsendung nochmals ausgestrahlt werden sollte, habe ich ebenfalls um Abänderung der Profile gebeten.

12 Ausländerangelegenheiten

12.1 Aufzeichnung von Telefongesprächen mit Ausländern

Von meinem Kollegen aus Bremen wurde ich darauf aufmerksam gemacht, dass ein Unternehmen aus Oldenburg ein von einer Mitarbeiterin einer Meldestelle in Bremen mit einem ausländischen Mitbürger geführtes Telefongespräch aufgezeichnet habe. Zudem sei die Mitarbeiterin um Einwilligung gebeten worden, dass dieses Gespräch auf CD-ROM übertragen und veröffentlicht wird. Weiter war der Eindruck entstanden, dass die Firma im Rahmen des vorgenannten Vorhabens weitere Telefongespräche mit anderen Meldestellen und Sozialbehörden aufzeichnen bzw. veröffentlichen wolle.

Bei meiner Prüfung habe ich festgestellt, dass das Telefongespräch im Rahmen eines Projekts zur Erstellung von Lehrmaterialien stattfand, das von einer Sprach- und Kommunikationsberatungsgesellschaft entwickelt und von der Carl von Ossietzky Universität Oldenburg betreut wird.

Zweck des Projekts ist die Entwicklung von Lehrmaterialien für Ausländer, die in das hiesige Berufsleben integriert werden sollen und dazu eine sprachliche Weiterqualifizierung im Deutschen benötigen. Als Aufgabe wurde das Telefonieren in folgenden Situationen gestellt: Terminabsprache mit einer Arztpraxis, Auskunft zur Eröffnung eines Bankkontos, Wohnungssuche, Anfrage zwecks Jobsuche, Anfrage bei einer Behörde.

Für das Gespräch waren folgende Regelungen getroffen worden:

- Alle Anrufer wussten vorher vom Mitschnitt des Gesprächs und hatten ihr Einverständnis dazu gegeben.
- Alle Angerufenen wurden unmittelbar nach Beendigung des Gesprächs über die Tatsache des Mitschnitts informiert und gefragt, ob sie zur Weiterverwendung der Aufnahme ihre Genehmigung geben wollen.
- Alle Mitschnitte mit Angerufenen, die diese Genehmigung nicht gaben, wurden sofort gelöscht.
- Kein Gesprächsmitschnitt, der aus diesem Grunde gelöscht wurde, ist vorher abgehört oder Dritten zur Verfügung gestellt worden. Kein Gesprächsmitschnitt, zu dessen Weiterverwendung das Einverständnis fehlte, wurde kopiert.
- Es existieren daher keine Mitschnitte von Gesprächen, zu denen kein Einverständnis vorliegt.
- Alle Namen von Personen, Firmen oder Institutionen in den Gesprächen, zu deren Verwendung das Einverständnis der Betreffenden vorliegt, werden sowohl in den Tondokumenten als auch in den Transkripten dieser Doku-

mente anonymisiert. Das geschieht u. a., indem auf elektronischem Weg die Namen geändert werden.

Die Aufnahme von Gesprächen ist nunmehr abgeschlossen und weitere Aufnahmen von Telefonaten sind nicht geplant. Es wurden für die Lehrmaterialien insgesamt 15 Aufnahmen verwendet. Die Gesamtzahl der Gesprächsmitschnitte lag nicht wesentlich höher (ca. 20). Eine genaue Zahl konnte nicht benannt werden, da über die gelöschten Aufnahmen keinerlei Aufzeichnungen angefertigt wurden.

Aufgrund der vollständigen informierten Einwilligung der anrufenden Person, der sofortigen Löschung des Gesprächs bei der Ablehnung einer Genehmigung und der Anonymisierung der Daten Dritter habe ich das Verfahren hingenommen.

12.2 Prüfung von Einbürgerungsverfahren

Die Reform des Staatsangehörigkeitsrechts war eines der bestimmenden innenpolitischen Themen im Jahr 1999. Noch vor der zum 1. Januar 2000 umgesetzten Reform hatte ich das Verfahren zur Einbürgerung (nach altem Recht) in datenschutzrechtlicher Hinsicht bei einem großen Landkreis und dessen übergeordneter Bezirksregierung überprüft.

Prüfungsgegenstand waren 20 Einbürgerungsverfahren, die aus der Gesamtmenge der im Jahre 1998 bei dem Landkreis abgeschlossenen Verfahren nach dem Zufallsprinzip ausgewählt worden waren. Wie die nachfolgenden Zahlen verdeutlichen, handelt es sich bei diesen 20 Fällen natürlich nur um einen Bruchteil der in dem Jahr insgesamt abschließend bearbeiteten Fälle: So wurden insgesamt 2 064 Einbürgerungen vollzogen, davon 1 224 durch den Landkreis selbst (Anspruchseinbürgerungen privilegierter Personengruppen) und 840 durch die Bezirksregierung (Anspruchs- und Ermessenseinbürgerungen nach dem Reichs- und Staatsangehörigkeitsgesetz und dem Ausländergesetz), in denen der Landkreis vor- und nachbereitend tätig war. Die 20 überprüften Fälle stammten ausschließlich aus letzterem Bereich, jeweils zur Hälfte auf der Grundlage des Reichs- und Staatsangehörigkeitsgesetzes und des Ausländergesetzes.

Die überprüften Verfahren endeten in zwölf Fällen mit der Einbürgerung, in sieben Fällen mit der Antragsrücknahme und in einem Fall mit der Ablehnung des Einbürgerungsantrages. Der Verfahrensablauf stellte sich im Allgemeinen so dar, dass die Einbürgerungsbewerberin oder der Einbürgerungsbewerber (nachfolgend: Bewerber) die Einbürgerung beim Landkreis beantragte und die geforderten Unterlagen vorlegte. Der Landkreis holte danach weitere Auskünfte und Stellungnahmen ein und legte den Vorgang anschließend mit einem Hinweis, ob die Einbürgerungsvoraussetzungen vorliegen oder nicht, und mit einem Votum der Bezirksregierung zur Entscheidung vor. Diese stellte dann weitere Ermittlungen an, die sich in den geprüften Fällen im Wesentlichen darauf beschränkt hatten, eine Auskunft aus dem Bundeszentralregister (das sog. Führungszeugnis) einzuholen. Nach abschließender Prüfung unterrichtete die Bezirksregierung den Landkreis über das Ergebnis; sofern der Einbürgerung entsprochen werden sollte, erhielt der Landkreis die Einbürgerungsurkunde zur Aushändigung an den Bewerber.

Zweck der Prüfung war insbesondere festzustellen, wie die Verfahren im Einzelnen ausgestaltet sind und ob (ggf. inwieweit) die Bewerber eine „Durchleuchtung" ihrer Persönlichkeit hinzunehmen hatten.

Um das wesentliche, schon in der Überschrift anklingende Ergebnis vorwegzunehmen: Die in den 20 Prüffällen festgestellte Datenverarbeitung gab keinen

Anlass zu datenschutzrechtlichen Beanstandungen. In den erleichterten Einbürgerungsverfahren nach dem Ausländergesetz war zudem festzustellen, dass trotz der Tragweite des hoheitlichen Aktes - die Verleihung einer neuen Staatsbürgerschaft - die von mir insgeheim befürchtete Durchleuchtung der Bewerber, also die systematische Erhebung aller wesentlichen Lebensumstände des Einzelnen, nicht festzustellen war. Diese Tendenz bewerte ich datenschutzpolitisch als positiv und habe dies gegenüber den geprüften Stellen und deren Aufsichtsbehörde, dem Niedersächsischen Innenministerium, auch deutlich zum Ausdruck gebracht.

Daneben war leider festzustellen, dass der Bundesgesetzgeber die vom Bundesverfassungsgericht in seinem sog. Volkszählungsurteil aus dem Jahr 1983 erhobene Forderung nach bereichsspezifischen Regelungen zur Datenverarbeitung auch in diesem Bereich noch immer nicht umgesetzt hat. Dies führt bei den beteiligten Stellen zu erheblichen Rechtsunsicherheiten, insbesondere was den Umfang der Datenerhebung in den Verfahren nach dem Reichs- und Staatsangehörigkeitsgesetz betrifft. Ich habe daher empfohlen, den Bund bei der Erarbeitung solcher bereichsspezifischer Regelungen zur Datenverarbeitung bei Einbürgerungen zu unterstützen, insbesondere was den Umfang der Beschaffung von Informationen über die Bewerber angeht.

Auffällig war auch das seinerzeit noch praktizierte zweigestufte Verfahren zwischen den Landkreisen, kreisfreien Städte und großen selbstständigen Städten einerseits und den Bezirksregierungen andererseits. In der Praxis stellte sich dies so dar, dass es wesentliche Aufgabe der kommunalen Körperschaften war, Anträge und Erklärungen von Bewerbern entgegenzunehmen, die Entscheidung vorzubereiten und letztlich zu vollziehen, während die Entscheidung als solche in der Regel der Bezirksregierung oblag. Allen Prüffällen war gemeinsam, dass die Bezirksregierung - als eigentliche Entscheidungsbehörde - im Gegensatz zum Landkreis nur wenig eigene Datenerhebungen durchgeführt hatte. Dies ist eine Folge des beschriebenen zweigestuften Verfahrens, das systembedingt zu Doppelspeicherungen und Datenübermittlungen zwischen den Behörden führt, die bei einer Aufgabenwahrnehmung durch eine Behörde nicht erforderlich wären. Ich habe daher - auch wenn dies im Kern sicher kein überwiegend datenschutzrechtliches Problem ist - empfohlen, auch die Entscheidungszuständigkeit über die Einbürgerung auf die bislang nur mitwirkend tätigen Kommunen zu übertragen, um ein Verfahren in einer Hand zu gewährleisten.

Wenn auch nicht als Folge meiner Empfehlung, sondern eher aus verwaltungsökonomischen Gründen hat die niedersächsische Landesregierung inzwischen die einschlägige „Allgemeine Zuständigkeitsverordnung für die Gemeinden und Landkreise zur Ausführung von Bundesrecht“ in diesem Sinne geändert, so dass nun die Verfahren tatsächlich in einer Hand betreut werden können.

13 Verfassungsschutz

13.1 Umsetzung des sog. BND-Urteils des Bundesverfassungsgerichts

Unter Ziffer 11.6 dieses Tätigkeitsberichts habe ich mich bereits mit der Frage auseinander gesetzt, inwieweit aufgrund der Urteile des Bundesverfassungsgerichts vom 14. Juli 1999 1 BvR 2226/94, 2420/95 und 2437/95 (sog. BND-Urteil) zur Telefonüberwachung durch den Bundesnachrichtendienst (BND) - unter Einbeziehung der Urteile des Landesverfassungsgerichts Mecklenburg-Vorpommern zum so genannten Großen Lauschangriff (LverfG 5/98 vom 18. Mai 2000) und zur sog. Schleierfahndung (LverfG 2/98 vom 21. Oktober 1999, NJW 2000, 2016) - eine Überarbeitung des NGefAG erforderlich ist.

Den sich daraus für das Niedersächsische Verfassungsschutzgesetz (NVerfSchG) ergebenden Regelungsbedarf werde ich mit dem Innenministerium erörtern.

13.2 Erweiterung der Überwachungsbefugnisse nach dem G 10-

Durch eine Bundesratsinitiative vom 26. September 2000 (BR-Drs. 577/00) versucht das Land Brandenburg eine Erweiterung des G 10-Gesetzes dahingehend zu erreichen, dass der Straftatenkatalog des Art. 1 § 2 Nr. 1 G 10-Gesetz um den § 130 StGB (Volksverhetzung) erweitert wird. Die dahinter stehende Absicht, nämlich die wirkungsvolle Bekämpfung des (Rechts)-extremismus, ist zu begrüßen. Allerdings hätte diese Änderung zur Folge, dass künftig die Überwachung der Telekommunikation von Bürgerinnen und Bürgern durch den Verfassungsschutz auch dann erfolgen kann, wenn es sich (nur) um Einzeltäter handelt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich auf ihrer Sitzung am 12./13. Oktober 2000 in Braunschweig sehr intensiv mit diesem Thema beschäftigt. Dabei ergab sich als einhellige Meinung der Konferenzteilnehmer heraus, dass die Ausweitung der Überwachungsbefugnisse des Verfassungsschutzes nach dem G 10-Gesetz auf extremistische Einzeltäter abgelehnt wird. Der Rechtsstaat ist gekennzeichnet durch die verfassungsrechtlich gewährte gerichtliche Kontrolle der öffentlichen Gewalt, die den prozessualen Grundpfeiler des Grundrechtsschutzes unserer Verfassung bildet. Zum Schutz der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes kann der gerichtliche Grundrechtsschutz aufgehoben und durch eine Nachprüfung außergerichtlicher Organe ersetzt werden (Art. 10 Abs. 2 Satz 2 GG). Diese Regelung des Grundgesetzes stellt einen Bruch im System der Verfassung dar und ist deshalb äußerst zurückhaltend zu handhaben. Eine Erweiterung der Überwachungsbefugnisse nach dem G 10-Gesetz würde den Rechtsschutz gegenüber der öffentlichen Gewalt weiter einschränken.

Abgesehen von den datenschutzrechtlichen Problemen ist diese Entwicklung deshalb auch verfassungsrechtlich äußerst bedenklich und verfassungspolitisch abzulehnen. Eine effiziente Strafverfolgung muss gerade im Bereich des Rechtsextremismus Sache der Polizei bleiben.

14 Personalangelegenheiten

14.1 Regelungslücken im Niedersächsischen Beamtengesetz

Mit dem Dritten Gesetz zur Änderung dienstrechtlicher Vorschriften vom 17. Dezember 1997 (Nds. GVBl. S. 528) hat Niedersachsen die gesetzlichen Regelungen zur Verarbeitung von Daten aller Beschäftigtengruppen im öffentlichen Dienst im Anschluss an das Beamtenrechtsrahmengesetz des Bundes neu geordnet. Ich habe diese Rechtsänderung in meinem XIV. Tätigkeitsbericht (vgl. 13.1) ausdrücklich begrüßt. Bei der Anwendung der neuen Vorschriften haben sich mittlerweile jedoch Probleme ergeben.

§ 101 Abs. 2 Satz 1 NBG enthält eine umfassende Regelung für die Verarbeitung von personenbezogenen Daten über Bewerber, Beamte, frühere Beamte und Hinterbliebene; zudem ist über § 261 Abs. 1 Nr. 2 des Gesetzes das Tarifpersonal mit erfasst. Nach dem im Gesetzentwurf (LT-Drs. 13/3220) zum Ausdruck gebrachten Willen der Landesregierung sollte sich die Vorschrift in ihrer ursprünglichen Konzeption sowohl auf Personaldaten wie auch auf Personalaktendaten beziehen. Eine Verarbeitung von Personalaktendaten wäre danach in

Betracht gekommen, wenn sie für Zwecke der Personalverwaltung oder der Personalwirtschaft erforderlich gewesen wäre. Im Laufe des Gesetzgebungsverfahrens ist jedoch in § 101 Abs. 2 Satz 2 NBG ergänzend festgelegt worden, dass Personalaktendaten nur nach den für Personalakten geltenden Vorschriften verarbeitet werden dürfen. Die Regelung setzt voraus, dass die Vorschriften über Personalakten alle für die Verwaltungspraxis notwendigen Verarbeitungsfälle erfassen. Aus meiner Sicht ist dies nicht der Fall. Insbesondere für die behördeninterne Verarbeitung von Personalaktendaten enthält das NBG keine ausreichenden Rechtsgrundlagen.

Keine Gesetzeslücke besteht allerdings für die Erhebung solcher Daten, die wegen ihres unmittelbaren inneren Zusammenhangs mit dem Dienstverhältnis zur Personalakte gehören (§ 101 a Abs. 1 Satz 2 NBG), aber noch nicht Bestandteil dieser Akte geworden sind. Diese Daten haben im Zeitpunkt ihrer Beschaffung noch keine Personalaktenqualität, ihre Erhebung richtet sich deshalb nach § 101 Abs. 1 Satz 1 NBG. Dagegen fehlt jede Rechtsgrundlage für die Erhebung und weitere Verarbeitung personenbezogener Daten, die bereits als Personalaktendaten anzusehen sind.

Die Notwendigkeit einer solchen Datenverarbeitung ergibt sich vor allem dann, wenn einzelne Organisationseinheiten der Beschäftigungsbehörde für ihre Aufgabenerledigung auf bestimmte Personalaktendaten zurückgreifen müssen. Ein solches Erfordernis tritt in der Verwaltungspraxis häufig auf, u. a. dann, wenn im Zuge von Verwaltungsreformenüberlegungen Teilaufgaben der Personalstelle dezentralisiert werden. Werden einzelnen Organisationseinheiten außerhalb der Personalstelle Befugnisse für bestimmte Personalverwaltungsmaßnahmen (z. B. zur Urlaubsgewährung) übertragen, setzt diese Aufgabenerledigung in der Regel eine Kenntnis von Personalaktendaten voraus. Eine Rechtsgrundlage für die Anforderung dieser Daten bei der Personalstelle und die Datenweitergabe an die anfordernde Organisationseinheit fehlt. Das NBG enthält keine dem § 11 Abs. 4 NDSG entsprechende Vorschrift über die innerbehördliche Weitergabe dieser Daten. Einen Rückgriff auf diese Bestimmung für die Verarbeitung von Personalaktendaten schließt § 101 Abs. 2 Satz 2 NBG aus.

Auch die Vorschriften zur Datenübermittlung an dritte Stellen werfen wegen ihrer zum Teil unklaren Fassung Probleme auf. So übermittelt z. B. das Niedersächsische Landesamt für Bezüge und Versorgung (NLBV) unter bestimmten Voraussetzungen (vgl. 14.6) Daten über Pfändungen etc. an die Personalstellen. Als Rechtsgrundlage hierfür kommt nur § 101 e NBG in Betracht. Die Vorschrift lässt eine Übermittlung von erforderlichen Personalaktendaten an eine oberste Dienstbehörde oder eine im Rahmen der Dienstaufsicht weisungsbefugte Behörde zu. Außerdem dürfen diese Daten an eine Behörde desselben Geschäftsbereichs übermittelt werden, wenn dies zur Vorbereitung oder Durchführung einer Personalentscheidung notwendig ist. An Behörden eines anderen Geschäftsbereichs dürfen die erforderlichen Daten jedoch nur übermittelt werden, wenn diese Stellen an einer Personalentscheidung mitzuwirken haben. Dieser Wortlaut ist zu eng gefasst. Denn eine Personalstelle außerhalb des Geschäftsbereichs des Finanzministeriums, zu dem das NLBV gehört, wirkt im Zusammenhang mit der Mitteilung von Pfändungs- und Überweisungsbeschlüssen nicht an einer Personalentscheidung dritter Stellen mit, sondern entscheidet selbst, ob und welche Maßnahmen aufgrund dieser Mitteilung zu treffen sind. Durch entsprechende Auslegung kann zwar im Wege eines Erst-Recht-Schlusses (wenn die Personalaktendaten einer Stelle übermittelt werden dürfen, die an einer Personalentscheidung mitzuwirken hat, dürfen sie erst recht an eine Stelle weitergegeben werden, die die Entscheidung selbst zu treffen hat) kann zwar ein sachgerechtes Ergebnis erzielt werden. Im Interesse der Rechtsanwender wäre es jedoch zu begrüßen, wenn der Regelungsgehalt der Vorschrift durch eine klare

Gesetzesfassung, zumindest jedoch durch Erläuterungen in den Verwaltungsvorschriften zum NBG verdeutlicht würde.

Unklar ist auch, auf welcher Rechtsgrundlage im Falle eines Rechtsstreits in dienstlichen Angelegenheiten Personalaktendaten einem die Behörde vertretenden Rechtsanwalt zur Prozessführung zur Verfügung gestellt werden dürfen. Auf § 101 Abs. 5 Satz 3 NBG lässt sich diese Datenverarbeitung schon deshalb nicht stützen, weil - wie sich aus § 101 e Abs. 2 Satz 2 NBG, aber auch aus § 101 Abs. 5 Satz 4 des Gesetzes ergibt - an Dritte lediglich Auskünfte aus der Personalakte erteilt, nicht aber Personalaktenbestandteile übermittelt werden dürfen. Zudem wäre die Anknüpfung der Datenübermittlung an ein glaubhaft gemachtes rechtliches Interesse verfehlt.

Um das jedem praktischen Bedürfnis zuwiderlaufende Ergebnis zu vermeiden, dass einem Prozessvertreter der Behörde die erforderlichen Personalakten nicht zur Verfügung gestellt werden dürfen, geht das Innenministerium davon aus, dass bei dieser Fallkonstellation keine Datenverarbeitung vorliegt. Der Rechtsanwalt vertrete im Prozess im Rahmen eines Mandantschaftsverhältnisses die Personalstelle mit der Folge, dass seine Datenverarbeitung unmittelbar der Personalstelle zugerechnet werde. Datenschutzbelange würden bereichsspezifisch durch die Bundesrechtsanwaltordnung gewährleistet.

Dieser Einschätzung vermag ich nicht zu folgen. Dabei braucht die Frage, welcher Phase der Datenverarbeitung die Weitergabe einer Personalakte an einen Rechtsanwalt zuzuordnen ist, hier nicht weiter vertieft zu werden. Verneint man eine Datenübermittlung, so fällt die Aktenweitergabe jedenfalls unter den Auffangtatbestand des Nutzens personenbezogener Daten (§ 3 Abs. 2 Nr. 7 NDSG). Auch hierfür ist eine Rechtsgrundlage nicht vorhanden.

Um keine Missverständnisse aufkommen zu lassen, möchte ich ausdrücklich betonen, dass in dieser wie in den zuvor genannten Fallkonstellationen für mich außer Zweifel steht, dass die bisherige Vorgehensweise der Verwaltung notwendig ist. Das Innenministerium sieht dies nicht anders. Es hat jedoch bislang im Ergebnis versucht, aus dem praktischen Bedürfnis der genannten Datenverarbeitungen deren rechtliche Zulässigkeit abzuleiten. Meiner Forderung, umgehend die notwendigen rechtlichen Korrekturen zu schaffen, hat es sich bisher verschlossen.

Diese Vorgehensweise muss auf Kritik stoßen. Wenn das Innenministerium umgehend Schritte zur Änderung des NBG einleitet, um die aufgetretenen rechtlichen Probleme zu lösen, halte ich es für vertretbar, für die Übergangszeit die bisher ohne geeignete Rechtsgrundlage erfolgenden Datenverarbeitungen hinzunehmen. Wenn eine konkrete, in die Tat umgesetzte Bereitschaft zur Schaffung der notwendigen Rechtsgrundlagen allerdings nicht besteht, müssen die in Rede stehenden Datenverarbeitungen eingestellt werden.

14.2 Regelungsdefizit im Schwerbehindertenrecht

Eine Rechtsgrundlage fehlt auch für die Einsicht der Schwerbehindertenvertretung in Bewerbungsunterlagen und die Teilnahme an Vorstellungsgesprächen. Die Schwerbehindertenvertretung wird aufgrund der vom Innenministerium erlassenen Schwerbehindertenrichtlinie (Nds. MBl. 1993 S. 361) in Personalauswahlverfahren auch über die persönlichen und leistungsbezogenen Daten der nicht schwerbehinderten Mitbewerberinnen und Mitbewerber unterrichtet. Sie hat außerdem das Recht, an Vorstellungsgesprächen teilzunehmen, sofern sich auch eine schwerbehinderte Person um die Stelle beworben hat.

Ich habe dieses Problem bereits in meinem XIII. Tätigkeitsbericht (14.16) angesprochen und darauf hingewiesen, dass diese Praxis, die die Datenschutzbelange der Bewerber tangiert, nur beibehalten werden kann, wenn hierfür eine gesetzliche Grundlage geschaffen wird. Dies ist bislang nicht geschehen.

Das Ministerium für Frauen, Arbeit und Soziales (MFAS) hat sich zwar gegenüber dem Bundesministerium für Arbeit und Sozialordnung für eine entsprechende Ergänzung des Schwerbehindertengesetzes ausgesprochen, seine Forderung ist allerdings nicht aufgegriffen worden. Nachdem inzwischen mehrere Jahre ergebnislos verstrichen sind, ohne dass sich eine konkrete Lösung des Problems abzeichnet, kann die bisherige rechtswidrige Verwaltungspraxis nicht unverändert fortgeführt werden. Ich habe das Innenministerium deshalb aufgefordert, den Schwerbehindertenerlass unverzüglich zu überarbeiten. Das Ressort hat mir daraufhin mitgeteilt, kurzfristig wolle man die „eingespielte Praxis" nicht aufgeben, vielmehr wolle das MFAS erneut den Versuch unternehmen, eine entsprechende Änderung des Schwerbehindertengesetzes des Bundes zu erreichen.

Für den Fall, dass auch dieser Versuch scheitert, führt an einer Änderung der bisherigen Verfahrensweise kein Weg vorbei. Ich weise für die dann zu treffende Erlassregelung schon jetzt darauf hin, dass ich eine Beteiligung der Schwerbehindertenvertretung an Vorstellungsgesprächen aufgrund einer Einwilligung für problematisch halte. Bei einem Bewerber, der bei einer Verweigerung seiner Einwilligung Nachteile im Bewerbungsverfahren befürchten muss, ist die Freiwilligkeit dieser Entscheidung zu bezweifeln.

14.3 Einführung der Neuen Steuerungsinstrumente

14.3.1 Kosten- und Leistungsrechnung

Bei der Einführung der „Neuen Steuerungsinstrumente" (s. XIV. TB 9) kommen der Kosten- und Leistungsrechung (KLR) einschließlich der Produktbildung sowie dem Controlling, dem Berichtswesen und der Budgetierung eine wesentliche Bedeutung zu.

Die Landesregierung hat mit den Spitzenorganisationen der Gewerkschaften und Berufsvertretungen eine Vereinbarung zur Einführung von betriebswirtschaftlichen Steuerungsinstrumenten in der niedersächsischen Landesverwaltung, insbesondere zur Kosten- und Leistungsrechnung, abgeschlossen (Nds. MBl. 1999 S. 342). Die Verhandlungspartner haben sich im September 2000 zu einem ersten Erfahrungsaustausch getroffen. Meine Beteiligung am Austausch habe ich begrüßt, da dies zu einer Stärkung meiner Beratungskompetenz gegenüber Projektgruppen und Personalvertretungen führen wird.

Ausgangssituation

In Niedersachsen wurden seit 1995 in vielen KLR-Projekten umfangreiche Erfahrungen gesammelt. Insgesamt befinden sich derzeit 32 Behörden und 27 Landesbetriebe in Pilotprojekten zur Umsetzung von neuen Steuerungsinstrumenten. An einem zentralen Verfahren mit der integrierten Standsoftware BaanPPM für das Haushalts-, Kassen- und Rechnungswesen einschließlich einer Kosten- und Leistungsrechnung nehmen 7 Behörden in einem Pilotversuch teil, mit dem alle im Haushaltsvollzug anfallenden Zahlungen in die KLR übernommen werden.

Personalvertretungen und Datenschutzbeauftragte der betroffenen Behörden haben mich um Beratung gebeten, da akzeptanzsteigernde Maßnahmen und eine Kommunikation mit den Dienststellen nicht stattgefunden haben.

Rechtliche Betrachtung der Kosten- und Leistungsrechnung

Datenschutzrechtliche Belange sind bei Einführung der Neuen Steuerungsinstrumente nur dann zu berücksichtigen, wenn personenbezogene Daten verarbeitet werden. Eine automatisierte Verarbeitung ausschließlich anonymisierter Daten wäre datenschutzrechtlich unbedenklich.

Sofern personenbezogene Daten von Bediensteten bei der Einführung der neuen Steuerungsinstrumente verarbeitet werden, sind - je nach Beschäftigungsgruppe - § 101 Abs. 2 Satz 1 bzw. § 261 Abs. 1 Nr. 2 i. V. m. § 101 Abs. 2 Satz 1 NBG als bereichsspezifische datenschutzrechtliche Ermächtigungen anzusehen. Danach dürfen Personaldaten - nicht aber Personalaktendaten - nur dann verarbeitet werden, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, eine Vereinbarung nach § 81 NPersVG oder eine Dienstvereinbarung dies vorsieht.

Ziel und Zweck der zwischen der Landesregierung und den Spitzenorganisationen der Gewerkschaften und Berufsvertretungen abgeschossenen Vereinbarung ist es, nur die für die Aufgabenerledigung unabdingbar erforderlichen Daten zu verarbeiten und anonyme Verarbeitungsformen vorzusehen.

Personenbezogene Daten in den Teilen der Kosten- und Leistungsrechnung Kostenartenrechnung - Welche Kosten sind entstanden?

Die Kostenarten lassen sich unterteilen in:

- Personalkosten
- Sachkosten
- Investitionen
- Dienstleistungskosten

In einer reinen Kostenartenrechnung treten keine personenbezogenen Daten auf (in seltenen Ausnahmen Tabelleneinsen).

Kostenstellenrechnung - Wo sind die Kosten entstanden?

Sobald die Kostenartenrechnung auf kleine Kostenstellen aufgeteilt wird, können zumindest personenbeziehbare Daten entstehen. Dabei ergibt sich folgende Situation:

Anlagenwirtschaft: keine personenbezogenen Daten,
Sachkosten: teilweise personenbezogene Daten (z. B. Telefonkosten, Kopierkosten),
Personalkosten: überwiegend personenbezogene Daten.

Kostenträgerrechnung - Wofür sind die Kosten entstanden?

Die Kostenträgerrechnung ordnet die Kosten den erbrachten Leistungen zu. Dies führt - je nach Tiefe der Rechnung - von einer Leistungskontrolle von Dienststellen insgesamt bis zu einer Leistungskontrolle jedes einzelnen Bediensteten (z. B. Fallzahlen). U. U. werden auch personenbeziehbare Daten Dritter in die Kostenträgerrechnung einfließen (z. B. Daten studentischer Hilfskräfte).

Meine Empfehlungen

Die Prinzipien der Datenvermeidung und Datensparsamkeit verlangen eine frühestmögliche Löschung bzw. Anonymisierung der personenbezogenen Ausgangsdaten. Bei der Einführung der Kosten- und Leistungsrechnung dürfen personenbezogene Daten nur im erforderlichen Umfang verarbeitet werden. Folgende Maßnahmen sind denkbar:

- Für die Personalkosten sind grundsätzlich nur Durchschnittswerte zu verwenden. Eine Ist-Kosten-Berechnung ist für die Ergebnisse der KLR in der Regel nicht erforderlich. Evtl. sind die von der Kommunalen Gemeinschaftsstelle (KGST) ermittelten Personalkosten oder die aus der Gesamtheit der Personalkosten einer Vergütungsgruppe errechneten Mittelwerte zu verwenden. Sofern es Bereiche gibt, in denen eine sinnvolle KLR nur eingeführt werden kann, wenn Personal-Ist-Daten verwendet werden, müssen diese Ausnahmen in einer Dienstvereinbarung mit der Personalvertretung geregelt werden. In diesen Fällen sollte jeder Beschäftigte eine Identifikationsnummer (IDN) erhalten. Diese wird als Bezugsgröße für die Personalkosten mit der Besoldungs-, Vergütungs- oder Lohngruppe, der Arbeitszeit, ggf. dem Kapitel und der Kostenstelle bei einer Vertrauensstelle hinterlegt.

- Konkrete Angaben zu Beihilfen dürfen nicht verwendet werden. Evtl. sind die aus der Gesamtheit der Beihilfekosten einer Dienststelle errechneten Mittelwerte zu nutzen.

- Bei den Sachkosten sind die größten Einheiten zu wählen, mit denen die Ziele erreicht werden.

- Eine Auswertung der Leistungsdaten darf für das Controlling nur anonymisiert erfolgen. Dies ist z. B. bei der Steuerung über Produkte (z. B. mit Hilfe von Kennzahlen) problematisch, wenn ein Rückschluss auf einzelne Beschäftigte möglich ist. Es ist darauf zu achten, dass diese Kennzahlen nicht personenbezogen konkretisiert werden. Dieses lässt sich nur dadurch erreichen, dass der Personenbezug der Angaben bei der Auswertung beseitigt ist. Folgende Maßnahmen sind denkbar: Die Kosten- und Leistungsstellen werden zu größeren dienstlichen Einheiten geführt, sodass eine Zuordnung zu einer Person nicht möglich ist. Sobald ein Personenbezug nicht mehr erforderlich ist, hat eine vollständige Anonymisierung zu erfolgen (z. B. Aggregierung, Löschung von Referenzlisten usw.).

- Arbeits- und dienstrechtliche Maßnahmen bzw. Entscheidungen dürfen nicht auf Informationen gestützt werden, die aus der Kosten- und Leistungsrechnung gewonnen werden. Organisatorische und personalwirtschaftliche Maßnahmen aufgrund aggregierter Ergebnisse bleiben davon unbenommen.

- Der behördliche Datenschutzbeauftragte und die Personalvertretung sollten Einblick in das Gesamtsystem erhalten, um überprüfen zu können, ob ggf. durch Datenverknüpfungen oder andere technische Möglichkeiten datenschutzrelevante Informationen missbräuchlich abgerufen werden können.

Die Zugriffsrechte der Controlling-Stelle sind auf den erforderlichen Umfang zu beschränken. In der Aufbauphase erscheint jedoch ein genereller Zugriff auf die Buchungsbelege hinnehmbar. Nach Abschluss der Aufbauphase sollte der Zugriff nicht weiter oder nur temporär zugelassen werden. Bei der Einführung der Kosten- und Leistungsrechnung sind außerdem besondere technische und organisatorische Maßnahmen zu treffen, um eine datenschutzgerechte Verarbeitung der Daten sicherzustellen.

14.3.2 Projekt Personalmanagementverfahren in Niedersachsen (PMV)

Ausgangslage

In der unmittelbaren Landesverwaltung werden in unterschiedlichsten Aufgabenbereichen ca. 130 000 Beamtinnen und Beamte und ca. 70 000 Angestellte, Arbeiter und Arbeiterinnen beschäftigt. Die für die Personalverwaltung und Stellenbewirtschaftung erforderlichen personenbezogenen Daten der Beschäftigten werden zu vielfältigen Zwecken durch eine nicht mehr überschaubare Anzahl von Bediensteten erhoben, in Akten verarbeitet oder Dateien gespeichert. Nach meiner Einschätzung dürfte es nur wenige Bedienstete geben, die eine exakte Vorstellung davon haben, durch wen in welchen Akten und Dateien die eigenen personenbezogenen Daten vorgehalten und verarbeitet und an welche Stellen sie zu welchen Zwecken übermittelt werden.

So werden neben den Verfahren für die Bezüge- und Beihilfezahlung (KIDICAP und Samba) in der Landesverwaltung derzeit nach meiner Kenntnis mehr als 20 unterschiedliche Softwareprodukte für die verschiedensten Aufgaben der Personalverwaltung, der Stellenbewirtschaftung und der Personalkostenbudgetierung eingesetzt. Zu nennen sind hier die in den größeren Personalkörpern eingeführten Verfahren ASTEB (Kultusministerium), DISPO (Finanzministerium), izn-Personal, TRISTAN (Justizministerium), HISSVA-GX (Ministerium für Wissenschaft und Kultur), PePPSi und RPS (MI-Polizei) sowie PUMA für den Bereich der Personalkostenbudgetierung. Diese Verfahren sind ausschließlich auf Bedürfnisse bestimmter Ressorts mit ihren jeweiligen Fachaufgaben zugeschnitten und decken zudem in ihrem Leistungsspektrum nur Teilbereiche der von einem modernen Personalmanagementverfahren zu erfüllenden Anforderungen ab.

Auf der Grundlage eines Projektvorschlages des Beauftragten für die Staatsmodernisierung wurde im Herbst 1999 unter Federführung des MF eine Koordinierungsgruppe aus Mitarbeitern der Ressorts, des Beauftragten für die Staatsmodernisierung, eines Vertreters der Gewerkschaften und der Arbeitsgemeinschaft der Hauptpersonalräte gebildet. Diese Koordinierungsgruppe hat den Auftrag, den Auswahlprozess für eine einheitliche und wirtschaftliche Software für die Personalverwaltung einschließlich der Personalbewirtschaftung und Personalentwicklung, der Personalkostenbudgetierung und der Stellenbewirtschaftung zu organisieren und zu koordinieren. Auch vor dem Hintergrund der Dimension des Vorhabens habe ich mich im Sinne meines Aufgabenverständnisses schon in der Frühphase der Projektarbeit an den Sitzungen der Koordinierungsgruppe beteiligt, um so bereits im Vorfeld einer möglichen Ausschreibung aktiv an datenschutzgerechten und datenschutzfreundlichen Lösungen mitwirken zu können.

Zielsetzung des Projektes

Das Projekt verfolgt folgende Ziele:

- Einführung eines einheitlichen Personalmanagementverfahrens (PMV) für alle Dienststellen der unmittelbaren Landesverwaltung bei gleichzeitiger Migration der bereits gespeicherten Daten
- Reduzierung von Medienbrüchen durch die Bearbeitung aller einschlägigen Personalvorgänge in einem PMV-Verfahren oder durch Schaffung von automatisierten Schnittstellen. Besondere Bedeutung haben die Schnittstellen zum Verfahren für die Haushaltsaufstellung, zum Bezügeverfahren, zur Haushaltsrechnung und zur Unterrichtsversorgung.
- Abbau von Redundanzen bei der Datenerfassung, Erfassung der Daten, wo sie zuerst anfallen.

Darüber hinaus soll

- eine Bearbeitung personalbezogener Vorgänge auf einer weitestgehend einheitlichen Datenstruktur sichergestellt werden,
- eine Effizienzsteigerung der personal - und stellenwirtschaftlichen Aktivitäten stattfinden,
- eine Verbesserung der Informationsbasis und Grundlagen für Entscheidungsträger erreicht werden,
- eine Steigerung der Effizienz für Personalbetreuung, Personalentwicklung, Personalplanung etc. gesichert werden,
- der Schriftverkehr im Zusammenhang mit der Personalsachbearbeitung unterstützt werden,
- die manuelle Tätigkeit im Personalbereich minimiert werden.

Meine Einschätzung der Chancen und Risiken

Die Notwendigkeit für die Einführung eines effizienten Personalmanagementverfahrens liegt auch vor dem Hintergrund der sich stetig verknappenden finanziellen Ressourcen auf der Hand. Es wird auch künftig mehr denn je erforderlich sein, die Kapazitäten der Personalstellen in die Bereiche zu lenken, die für eine moderne Personalentwicklung und -bewirtschaftung wirklich bedeutsam sind. Das setzt voraus, dass einerseits bei den rein administrativen Aufgaben der Personalstellen die verfahrensmäßigen Abläufe durch eine einheitliche Programmsteuerung erleichtert werden, um damit Entlastungen zu erreichen, und andererseits die Datenbasis für Personalentscheidungen deutlich verbessert und vereinheitlicht wird.

Ein Blick in die Privatwirtschaft zeigt, dass in vielen Großunternehmen die im Bereich der Personalverwaltung administrativ anfallenden Aufgaben schon seit längerem durch leistungsfähige und flexible Personalmanagementsysteme unterstützt werden. Die Mitarbeiterinnen und Mitarbeiter der Personalabteilungen werden dort von ebenso routinemäßigen wie zeitintensiven Verwaltungstätigkeiten und Datenerhebungen entlastet und somit die Arbeitsvorgänge insgesamt wesentlich effektiver gestaltet. Der Unternehmensführung können die Personalinformationen je nach Erfordernis entscheidungsbezogen und zeitgerecht vorgelegt werden. Die von reinen Verwaltungstätigkeiten entlasteten Personalabteilungen können sich verstärkt den Feldern der Personalwirtschaft widmen, denen auch zur Erhaltung der Wettbewerbsfähigkeit eine immer größere Bedeutung zukommt, so etwa der Personalauswahl und der Personalentwicklung unter Einschluss der Aus- und Fortbildung. Dieser Entwicklung darf sich die niedersächsische Landesverwaltung nicht verschließen.

Aus Sicht des Datenschutzes bietet das Projekt zur Einführung eines landeseinheitlichen Personalmanagementverfahrens die Chance, die Vielzahl der eingeführten, auch mir nicht in allen Einzelheiten bekannten Systeme durch ein modernen technologischen Standards entsprechendes landeseinheitliches Verfahren abzulösen, das auch die gerade bei den überwiegend sensiblen Personaldaten so wichtigen Anforderungen des Datenschutzes und der Datensicherheit erfüllt und außerdem für die Bediensteten wesentlich mehr Transparenz bei dem Umgang der Personalstellen mit ihren Personaldaten schafft.

Ebenso wie bei der Einführung der Kosten- und Leistungsrechnung und anderer technischer Systeme, etwa zur Arbeitszeiterfassung, ist zu erwarten, dass eine Vielzahl von Bediensteten und Personalvertretungen der Einführung eines landeseinheitlichen Personalmanagementverfahrens aus Sorge um die Entstehung des „gläsernen" Bediensteten zunächst mit Skepsis begegnen wird. Diese Be-

sorgnisse nehme ich sehr ernst und werde daher umso mehr bemüht sein, durch meine Mitwirkung an dem Projekt zu gewährleisten, dass eine in jeder Hinsicht datenschutzgerechte Lösung erreicht wird. Dazu gehört es auch, im Sinne der Datensparsamkeit die bisherigen Redundanzen beim Vorhalten von Personaldaten deutlich zurückzuführen und dem Gebot der Zweckbindung durch eine sehr exakte Steuerung der Zugriffberechtigungen Rechnung zu tragen.

Ich begrüße es daher, dass ich Gelegenheit habe, bei diesem Projekt an der Erarbeitung eines an den künftigen Erfordernissen einer modernen Personalverwaltung ausgerichteten Datenkataloges und eines dem Stand der Technik entsprechenden Datenschutz- und Datensicherheitskonzeptes gestaltend mitzuwirken.

Bei Einführung eines Verfahrens sollten zur Sicherstellung einer datenschutzgerechten Verarbeitung der personenbezogenen Daten meiner Auffassung nach im Rahmen einer Technikfolgenabschätzung die folgenden technischen, organisatorischen und datenschutzrechtlichen Gesichtspunkte berücksichtigt werden:

Administration

Die Betriebsverantwortung für das Gesamtsystem soll einer zentralen Stelle übertragen werden (zentrale Administration). Die jeweilige Ortsdienststelle kann Administrationsaufgaben selbst übernehmen, wobei die Option für eine zentrale Administration gesichert sein muss. Die Datenhaltung wird zentral erfolgen.

Gefahren und Risiken

Mit dem PMV können in automatisierter Weise aus einer Datensammlung durch vielfältige Datenverknüpfungen und -kombinationen sowie durch die Erstellung von Hypothesen und deren Überprüfung bisher völlig unbekannte Informationen gewonnen werden. Insbesondere die gezielte Zusammenführung von Daten über Landesbedienstete aus unterschiedlichen Datenquellen und ihre Auswertung erfolgt überwiegend ohne Kenntnis der Bediensteten.

Diese Entwicklung schafft neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Datenschutzverantwortung

Jede Daten verarbeitende Stelle ist für den datenschutzgerechten Einsatz ihrer Anwendungen selbst verantwortlich. Da personenbezogene Daten von Bediensteten bei der Einführung des PMV verarbeitet werden, sind - je nach Beschäftigungsgruppe - § 101 Abs. 2 Satz 1 bzw. § 261 Abs. 1 Nr. 2 i. V. m. § 101 Abs. 2 Satz 1 NBG als bereichsspezifische datenschutzrechtliche Ermächtigungen anzusehen. Danach dürfen Personaldaten - nicht aber Personalaktendaten - nur dann verarbeitet werden, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

Datenschutzleitplanken

Konkrete Forderungen zum datenschutzgerechten Einsatz der Anwendung PMV:

– Bei der Verarbeitung dürfen nur Personaldaten im erforderlichen Umfang verarbeitet werden (Datenvermeidung und Datensparsamkeit).

- Die Betroffenen sind zu unterrichten (Transparenzgebot).
- Eine zentrale Auswertung der Personaldaten sollte nur unter Einsatz von datenschutzfreundlichen Technologien möglich sein (Anonymisierung oder Pseudonymisierung).
- Für die Betriebssystemebene und für die Anwendung sowie für die Auswertung und die Statistiken des Datenbestandes ist ein Berechtigungs- und Zugriffskonzept festzulegen. Protokollierungen und regelmäßige Kontrollen sind vorzusehen (Rechteverwaltung).
- Die Datenübermittlung erfolgt verschlüsselt. Der Einsatz einer digitalen Signatur ist zu prüfen.
- Eingangs- und Ausgangsschnittstellen zu anderen Verfahren sind inhaltlich und technisch zu dokumentieren.
- Wartung der Datenverarbeitungsanlagen und der Anwendungssoftware durch externe Personen oder Stellen sollte nur dann gewählt werden, wenn eine eigene Wartung nur eingeschränkt oder gar nicht möglich ist.
- Für die weitere Ausgestaltung der Datenschutz- und Datensicherungsmaßnahmen ist ein Sicherheitskonzept und eine Dienstanweisung erforderlich

14.3.3 Übermittlung von Beihilfesummen für haushaltswirtschaftliche Zwecke

Das u. a. für die Bearbeitung von Beihilfeangelegenheiten zuständige NLBV fordert nach der Berechnung und Auszahlung der Beihilfebeträge an die Berechtigten die Erstattung der geleisteten Zahlungen als Gesamt- oder Teilsumme von dem Kostenträger. In diesem Verfahren haben Landesbetriebe eine Aufgliederung der Gesamtsumme auf jeden Einzelfall und damit die Weitergabe personenbezogener Beihilfedaten zu Abrechnungszwecken im Rahmen der Personalkostenbudgetierung, zur Durchführung der Kosten- und Leistungsrechnung sowie zu Kostenberechnungen im Zusammenhang mit aus Drittmitteln finanzierten Projekten gefordert.

Ein solches Verfahren ist nach geltendem Recht nicht zulässig.

Beihilfedaten dürfen als Personalaktendaten (vgl. § 101 a NBG) nur nach den für Personalaktendaten geltenden Vorschriften verarbeitet werden. Schon die Übermittlungsvoraussetzungen für Personalaktendaten sind nicht erfüllt. Nach § 101 e Abs. 2 Satz 1 i. V. m. Abs. 1 NBG dürfen Auskünfte aus der Personalakte ohne Einwilligung des Beamten nur der obersten Dienstbehörde oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde für Zwecke der Personalverwaltung oder Personalwirtschaft erteilt werden. Eine Auskunft an Behörden desselben Geschäftsbereichs kommt in Betracht, soweit sie zur Vorbereitung oder Durchführung einer Personalentscheidung notwendig ist. Eine Übermittlung an Behörden eines anderen Geschäftsbereichs desselben Dienstherrn ist zulässig, soweit diese Behörden an einer Personalentscheidung mitzuwirken haben und die jeweils in Rede stehenden Daten hierfür erforderlich sind. Diese Voraussetzungen sind nicht gegeben. Landesbetriebe sind zum einen weder oberste Landesbehörden noch im Rahmen der Dienstaufsicht weisungsbefugte Behörden gegenüber dem NLBV, zum anderen sind die Angaben über erbrachte Beihilfeleistungen an die Berechtigten nicht für die Vorbereitung, Mitwirkung oder Durchführung von Personalentscheidungen notwendig.

Hinzu kommt, dass Beihilfedaten wegen ihrer besonderen Sensibilität einen gegenüber den übrigen Personalaktendaten erhöhten Schutz genießen. Sie unterliegen deshalb nach § 101 b Satz 1 NBG einer strikten Zweckbindung. Für Beihilfezwecke ist eine Übermittlung von auf den Einzelfall bezogenen Beihilfedaten

an die Landesbetriebe nicht erforderlich. Auch eine Zweckdurchbrechung kommt hier nicht in Betracht. Für andere als Beihilfezwecke darf die Beihilfeakte nach § 101 b Satz 4 NBG nur verwendet werden, wenn entweder eine Einwilligung des Beihilfeberechtigten sowie der betroffenen Angehörigen für jeden Einzelfall vorliegt oder wenn ein im Zusammenhang mit dem Beihilfeantrag stehendes behördliches oder gerichtliches Verfahren dies erfordert. Um ein solches Verfahren handelt es sich nicht, wenn personenbezogene Daten für Zwecke der Personalkostenbudgetierung, der Kosten- und Leistungsrechnung oder für Kostenberechnungen im Zusammenhang mit aus Drittmitteln finanzierten Projekten verwendet werden sollen. Schließlich verstößt die Verwendung von personenbezogenen Abrechnungsdaten zu Zwecken der Kosten- und Leistungsrechnung auch gegen die „Vereinbarung zur Einführung von betriebswirtschaftlichen Steuerungsinstrumenten in der niedersächsischen Landesverwaltung insbesondere zur Kosten- und Leistungsrechnung zwischen der Landesregierung und den Spitzenorganisationen der Gewerkschaften und Berufsverbände“ vom 4. Juni/1. Juli 1999 (Nds. MBl. S. 342). In Nr. 2 Abs. 1 Satz 2 dieser Vereinbarung ist festgelegt, dass Personalkosten zweckorientiert nach Durchschnittswerten berechnet werden. Eine Zugrundelegung von Ist-Werten ist nicht vorgesehen. Sie wäre aus datenschutzrechtlicher Sicht zur Aufgabenerfüllung auch nicht erforderlich (s. auch XIV. TB 4.9). Die Landesregierung hat deshalb - nicht zuletzt, um eine möglichst breite Akzeptanz unter den Beschäftigten zum Einsatz der Neuen Steuerungsinstrumente zu erlangen - mehrfach erklärt, dass die Personalkostenberechnungen auf der Grundlage pauschalierter Durchschnittssätze vorzunehmen sei.

Gegen eine Übermittlung nur von Angaben zur Summe der aufgrund entsprechender Anträge gezahlten Beihilfen an die für die finanzielle Abwicklung zuständigen Stellen bestehen keine Bedenken, da es sich hierbei nicht um personenbezogene Daten handelt.

14.4 Datenerhebung bei Dritten / Übermittlung von Personalaktendaten

In einer Vielzahl von Fällen ist deutlich geworden, dass in der Verwaltungspraxis das Ineinandergreifen der datenschutzrechtlichen Regelungen des NBG und des NDSG Schwierigkeiten bereitet. Dabei hat der Gesetzgeber die Regelungsbereiche der Vorschriften klar voneinander abgegrenzt. Nach § 101 Abs. 1 NBG gehen die Bestimmungen dieses Gesetzes den Regelungen des allgemeinen Datenschutzrechts vor. Soweit das NBG allerdings keine Regelung enthält, muss auf das NDSG zurückgegriffen werden. Für die Rechtsanwendung im Personalbereich sind deshalb Kenntnisse des allgemeinen Datenschutzrechts unerlässlich. Diese sind nach meinen Erfahrungen (vgl. hierzu meine Ausführungen in früheren Tätigkeitsberichten) häufig immer noch nicht in ausreichendem Maße vorhanden.

Probleme haben sich in der Verwaltungspraxis besonders bei der Erhebung von Daten über Mitarbeiterinnen und Mitarbeiter bei Dritten ergeben. Als Beispiel für ein häufiger von mir festgestelltes fehlerhaftes Vorgehen bei solchen Problemkonstellationen mag folgender Fall dienen:

Ein Beamter erlitt auf einer Dienstfahrt mit seinem anerkannten privaten Pkw einen Unfall. Den entstandenen Sachschaden machte er gegenüber seiner Beschäftigungsbehörde geltend. Die Reparatur des Fahrzeugs ließ er mehrere Monate nach dem Schadensfall vornehmen. Die anschließend vorgelegte Rechnung erweckte bei der Beschäftigungsbehörde Zweifel, dass alle darin aufgeführten beseitigten Schäden auf den gemeldeten Unfall zurückzuführen seien. Zur Aufklärung des Sachverhalts wandte sich die Behörde an die Kfz-Werkstatt und an die Versicherungsgesellschaft des Beamten. Dabei erläuterte sie telefonisch und

schriftlich den Hintergrund ihrer Anfragen und teilte Einzelheiten des geltend gemachten Schadensersatzanspruchs mit. Der Versicherungsgesellschaft übersandte die Behörde eine Ablichtung des Sachschadensantrags des Beamten und weitere kopierte Unterlagen des von ihr bearbeiteten Vorgangs.

Meine ausführlich erläuterte Kritik an diesem Verfahren stieß bei der Behörde nicht auf Verständnis. Sie legte den Vorgang ihrer obersten Dienstbehörde vor. Diese konnte ich schließlich von der Unzulässigkeit der dargestellten Verfahrensweise überzeugen.

Nach § 101 Abs. 2 Satz 1 NBG dürfen Daten über Beamte u. a. verarbeitet werden, wenn dies zur Durchführung des Dienstverhältnisses erforderlich ist. Zur Datenverarbeitung gehört auch das Erheben von personenbezogenen Daten (§ 3 Abs. 2 Satz 1 NDSG). Gemäß § 9 Abs. 1 Satz 2 NDSG sind die Daten grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben. Die Beschäftigungsbehörde musste also den Sachverhalt zunächst durch Befragen des Beamten aufklären. Eine Datenerhebung bei Dritten - hier: der Kfz-Werkstatt und der Kfz-Versicherung des Beamten - kommt nur in Betracht, wenn eine der hierfür in § 9 Abs. 1 Satz 3 NDSG genannten Voraussetzungen vorliegt. Im geschilderten Fall wäre dies zu bejahen, wenn Angaben des Betroffenen überprüft werden mussten (Nr. 3 der genannten Vorschrift). Dies ist jedoch nur der Fall, wenn konkrete Anhaltspunkte für die Unrichtigkeit der Angaben des Betroffenen vorhanden sind. Es reicht nicht aus, wenn die Behörde lediglich vage Zweifel an der Richtigkeit der Angaben hat und sich durch die Datenerhebung die nötigen Anhaltspunkte für diese Einschätzung erst verschaffen will.

Die frühere Gesetzesfassung brachte diesen Regelungsgehalt der Vorschrift deutlich zum Ausdruck, aus Gründen der „Gesetzesverschlankung" hat der Gesetzgeber diese Fassung jedoch leider verändert (vgl. XIV. TB 6.1.4).

Mit einer Datenerhebung ist in der Regel auch eine Datenübermittlung verbunden. Eine bei anderen Stellen anfragende Behörde wird keine Antwort erwarten dürfen, wenn sie diesen Stellen nicht den Hintergrund ihrer Anfrage erläutert und damit eine Einschätzung ihres Auskunftsbegehrens ermöglicht. Unter diesem Gesichtspunkt ist es nachvollziehbar, wenn die Beschäftigungsbehörde der Kfz-Werkstatt und der Versicherung des Beamten bestimmte Daten mitteilen wollte. Datenschutzrechtlich liegt jedoch in der Weitergabe dieser personenbezogenen Angaben eine Datenübermittlung, die nur zulässig ist, wenn die hierfür geltenden rechtlichen Voraussetzungen erfüllt sind.

Im vorliegenden Falle wurden u. a. Personalaktendaten übermittelt. Personalaktendaten dürfen nach § 101 Abs. 2 Satz 2 NBG nur nach den für diese Daten geltenden Vorschriften verarbeitet werden. Die Übermittlung dieser Daten hat der Gesetzgeber wegen ihres besonderen Schutzbedürfnisses nur unter engen Voraussetzungen zugelassen. Personalaktendaten dürfen nach § 101 Abs. 5 Satz 3 NBG an Dritte nur übermittelt werden, wenn der Empfänger ein rechtliches Interesse an der Kenntnisnahme der Daten glaubhaft macht und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an der Geheimhaltung überwiegt. Wie sich aus dem Erfordernis der Geltendmachung des rechtlichen Interesses sowie dem Folgesatz ergibt, lässt das Gesetz eine Datenübermittlung aus Personalakten nur auf entsprechendes Verlangen eines Dritten und nur in Form einer Auskunft zu (vgl. auch § 101 e Abs. 2 Satz 2 NBG). Über Inhalt und Empfänger der Auskunft ist der Betroffene schriftlich zu unterrichten. Eine Übermittlung von Kopien aus der Personalakte an private Dritte kommt nicht in Betracht.

Da die mit der Datenerhebung untrennbar verbundene Datenübermittlung vom NBG nicht gedeckt ist, ist der Gesamtvorgang der Datenbeschaffung bei der Kfz-Werkstatt und der Kfz-Versicherung als rechtswidrig zu bewerten.

Dieses vom Gesetzgeber gewollte Ergebnis führt auch - anders als es ein erster Anschein nahe legen mag - nicht zu unvertretbaren Hindernissen für die Verwaltungspraxis. Im vorliegenden Falle war es Sache des geschädigten Beamten, die Voraussetzungen für einen Schadensersatzanspruch nachzuweisen. Er hätte deshalb bei entsprechendem Aufklärungsbedarf von der Beschäftigungsbehörde aufgefordert werden können, notwendige Unterlagen und Nachweise von der Kfz-Werkstatt bzw. Versicherung beizubringen. Ein anderer Weg hätte darin bestanden, ihn um seine schriftliche Einwilligung (§ 4 NDSG) zur vorgesehenen Verfahrensweise zu bitten. Hätte der Beamte seine Mitwirkung verweigert und wäre aus diesem Grund eine Erklärung der Voraussetzungen für den geltend gemachten Anspruch nicht möglich gewesen, hätte der Antrag insoweit abgelehnt werden können.

14.5 Korruptionsbekämpfung

Die Landesregierung misst der Korruptionsbekämpfung besondere Bedeutung zu. Sie hat deshalb ein Bündel von Maßnahmen vorgesehen, die darauf abzielen, Korruptionserscheinungen auf allen staatlichen Ebenen sowohl repressiv wie präventiv verstärkt entgegenzutreten. Für die Koordinierung und Umsetzung ressortübergreifender Maßnahmen wurde unter Federführung des Innenministeriums eine Arbeitsgruppe „Korruptionsbekämpfung" eingesetzt. Diese hat den Entwurf einer Verwaltungsvorschrift zu dieser Problematik erarbeitet. Die Vorschrift soll Regelungen zur Korruptionsbekämpfung zusammenfassen und vereinheitlichen und eine Handreichung für Vorgesetzte und Beschäftigte geben.

Jede Dienststelle soll künftig für ihren Bereich einen sog. „Gefährdungsatlas" erstellen. Dieser soll einen Überblick darüber geben, ob und in welchen Bereichen Korruptionsgefährdungen bestehen. Um dieses zu ermitteln, sollen sämtliche Arbeitsplätze anhand eines Kriterienkataloges überprüft werden, ob eine allgemeine Korruptionsgefährdung vorliegt. Der vorgesehene Kriterienkatalog ist weit gefasst: Schon wenn Prüfungen, Kontroll- oder Aufsichtstätigkeiten mit Außenwirkung durchgeführt oder Entscheidungen getroffen werden, die für Dritte aus materiellen oder immatriellen Gründen von besonderer Bedeutung sind, wird von einer allgemeinen Korruptionsgefährdung ausgegangen. Wird diese allgemeine Korruptionsgefährdung nach dem jeweiligen Aufgabenbereich festgestellt, ist anhand eines weiteren Kriterienkatalogs zu prüfen, ob darüber hinaus von einer gesteigerten Korruptionsgefährdung des Arbeitsplatzes auszugehen ist. Dies soll z. B. der Fall sein, wenn häufig Außenkontakte zum gleichen Personenkreis bestehen. Die zusammengefasste Bewertung der einzelnen Arbeitsplätze bildet den Gefährdungsatlas der Behörde. Die Voraussetzungen zur Feststellung einer allgemeinen oder gesteigerten Korruptionsgefährdung sind zwar recht weit gefasst, aus datenschutzrechtlicher Sicht bestehen gegen die Aufstellung eines solchen Gefährdungsatlas jedoch keine Bedenken, solange die Bewertung ausschließlich an die Aufgaben des jeweiligen Arbeitsplatzes anknüpft und keinerlei Bezug zur Person des Arbeitsplatzinhabers vorhanden ist.

In einer weiteren Stufe des Verfahrens sollen die Arbeitsplätze, bei denen eine gesteigerte Korruptionsgefährdung festgestellt worden ist, einer Risikoanalyse unterzogen werden. Soweit sich die Risikoanalyse auf Aufgabenbestand und Arbeitsabläufe des einzelnen Arbeitsplatzes beschränkt, bestehen gegen das Verfahren ebenfalls keine Bedenken. Nach dem Entwurf der Verwaltungsvorschrift soll jedoch für die Risikoanalyse auch von Bedeutung sein, ob bei den Bediensteten oder in ihrem persönlichen Umfeld Umstände vorliegen, die als Anknüpfungspunkte für eine auf korruptives Verhalten hinauslaufende Ansprache dienen könnten. Als Beispiel hierfür werden u. a. Schulden, Krankheit, besondere Hobbys und Neigungen, persönliche oder geschäftliche Beziehungen, auch von

Personen des sozialen Nahbereichs, genannt. Die im Rahmen der Risikoanalyse anfallenden Daten sollen zu einer „Unterakte" genommen werden, über deren rechtlichen Charakter (Personalakte, Sachakte?) die Verwaltungsvorschrift nichts aussagt.

Die Verarbeitung dieser Daten halte ich nicht für zulässig. Nach § 101 Abs. 2 Satz 1 NBG dürfen Daten von Beschäftigten u. a. verarbeitet werden, wenn sie zur Durchführung des Dienstverhältnisses erforderlich sind. Das ist hier nicht ersichtlich. Erforderlich ist eine Datenverarbeitung nur, wenn ohne sie die betreffende Verwaltungsaufgabe nicht, nicht vollständig oder nur unter unverhältnismäßig großen Schwierigkeiten erfüllt werden könnte. Aus meiner Sicht kann keine Rede davon sein, dass eine wirksame Korruptionsbekämpfung ausgeschlossen wäre, wenn diese Daten nicht verarbeitet würden. Die Verarbeitung ist also nicht erforderlich. Die beispielhaft genannten Daten geben in der Regel nicht einmal ein Indiz für eine Korruptionsgefährdung. Weder aus einer Kreditaufnahme für einen Hausbau, aus Bandscheibenproblemen des Beschäftigten, einer Sammelleidenschaft für Briefmarken oder anderen Hobbys lassen sich Schlüsse auf eine persönliche Korruptionsanfälligkeit von Mitarbeiterinnen und Mitarbeitern ziehen. Fragen nach solchen „Umständen" an die Bediensteten sind deshalb unzulässig. Eine Befragung dritter Personen kommt erst recht nicht in Betracht (§ 9 NDSG i. V. m. § 101 Abs. 1 NBG). Eine Erhebung von Daten über „Personen des sozialen Nahbereichs", wie sie die Verwaltungsvorschriften nahe legen, scheiden von vornherein aus.

Meine entsprechende Stellungnahme stieß bei der Arbeitsgruppe nicht auf Begeisterung. Sie fühlte sich missverstanden. Die Vorsitzende betonte, an eine Datenerhebung habe die Arbeitsgruppe nicht gedacht. Man habe vielmehr nur auf vorhandene Daten zurückgreifen wollen.

Aus dem Wortlaut der Verwaltungsvorschrift ergibt sich dies allerdings nicht. Aber auch wenn zusätzliche Datenerhebungen von der Verwaltungsvorschrift nicht beabsichtigt sein sollten, macht dies die Angelegenheit aus Datenschutzsicht nicht besser. Die genannten Daten sind in der Personalakte nicht vorhanden und haben dort auch nichts zu suchen. Sie dürften darüber hinaus mangels entsprechender Rechtsgrundlage (vgl. 14.1) auch nicht von der Personalstelle weitergegeben werden.

Die Arbeitsgruppe wird ihre Überlegungen zur Ausgestaltung der Risikoanalyse überdenken. Über datenschutzrechtliche Erwägungen hinaus sollte sie sich auch die Frage stellen, ob es gerechtfertigt ist, in einem derartigen Umfang, wie er bisher beabsichtigt ist, von Arbeitsplätzen mit gesteigerter Korruptionsgefährdung auszugehen.

14.6 Mitteilung von Gehaltspfändungen

Im XIV. Tätigkeitsbericht (13.5) habe ich die Verfahrensweise kritisiert, dass die Besoldungsstellen des Landes der jeweiligen Personal verwaltenden Stelle ohne jede Beschränkung Kopien von Pfändungs- und Überweisungsbeschlüssen, die gegen Bedienstete erwirkt worden sind, sowie Abtretungserklärungen übersenden. Diese Vorgehensweise wurde auf einen 1995 außer Kraft getretenen Runderlass des Finanzministeriums gestützt. Sie ist in dieser Form nicht zulässig.

Eine Unterrichtung der Personal verwaltenden Stellen darf nur vorgenommen werden, wenn die Durchführung des Dienstverhältnisses dies erfordert. Dies setzt voraus, dass die Mitteilung Anlass zu einer fürsorgerischen oder dienstrechtlichen Maßnahme sein kann. Als Fürsorgemaßnahme kommt insbesondere eine Beratung der/des Bediensteten in Betracht, als dienstrechtliche Maßnahme

in gravierenden Fällen die Prüfung und ggf. Einleitung eines Disziplinarverfahrens wegen leichtfertigen Schuldenmachens. Dabei ist zu berücksichtigen, dass der Gesetzgeber die außerdienstlichen Pflichten von Beamten 1994 eingeschränkt hat. Danach stellt ein außerdienstlichen Verhalten nur dann ein Dienstvergehen dar, wenn es im Einzelfall geeignet ist, das Vertrauen in die pflichtgemäße Amtsführung nachhaltig zu beeinträchtigen.

Ich habe mich deshalb für eine differenzierte Regelung eingesetzt, die für eine Übermittlung der Daten an die Beschäftigungsstellen insbesondere auf die Höhe und die Häufigkeit der gegenüber den Bediensteten geltend gemachten Forderungen abstellt. Mit Runderlass vom 26. April 2000 (Nds. MBl. S. 313) hat das Finanzministerium das Verfahren in datenschutzgerechter Weise neu geregelt. Im Kern werden danach die Personal verwaltenden Stellen vom NLBV nur noch über zu vollstreckende Forderungen, die das Zweifache der regelmäßigen monatlichen Bruttobezüge überschreiten, oder über Fälle, in denen innerhalb eines Jahres - unabhängig von der Forderungshöhe mehr als drei Pfändungs- und Überweisungsbeschlüsse oder in drei aufeinander folgenden Kalenderjahren mindestens ein Pfändungs- und Überweisungsbeschluss ergangen sind, unterrichtet. Wegen weiterer Einzelheiten verweise ich auf den Runderlass.

14.7 Mitarbeiterdaten im Internet

Der zunehmende Einsatz des Internet hat vermehrt Fragen aufkommen lassen, ob und welche Beschäftigtendaten in das Internet eingestellt werden dürfen. Für den Hochschulbereich hat das Ministerium für Wissenschaft und Kultur diese Problematik durch Runderlass vom 8. Juni 1998 (Nds. MBl. S. 984) eingehend geregelt. Der Erlass ist mit mir abgestimmt worden (vgl. XIV. TB 22.1). Die darin dargestellte Rechtslage gilt auch für andere Verwaltungsbereiche.

Eine Übermittlung von Bedienstetendaten an Personen und Stellen außerhalb des öffentlichen Bereichs ist nur zulässig, wenn die Empfänger ein rechtliches Interesse darlegen oder der Dienstverkehr es erfordert (§ 101 Abs. 5 Satz 1 NBG). Für einen automatisierten Abruf - wie z. B. im Internet - dürfen personenbezogene Daten nur bereitgehalten werden, wenn die Daten jeder Person offen stehen und ihr Inhalt veröffentlicht werden darf (§ 12 Abs. 5 NDSG). Eine Veröffentlichung von Daten der Bediensteten im Internet oder vergleichbaren Medien kommt deshalb nur in Betracht, wenn der Dienstverkehr eine solche Veröffentlichung erfordert.

Erforderlich ist eine Datenverarbeitung nur, wenn ohne das in Rede stehende Datum eine Aufgabe nicht, nicht vollständig, nur unter unverhältnismäßig großen Schwierigkeiten oder verspätet erfüllt werden könnte (vgl. Gesetzesbegründung zu § 9 NDSG - LT-Drs. 12/3210).

Durch eine Einstellung ins Internet werden die Daten weltweit zur Verfügung gestellt. Sie können in unterschiedlichster Weise mit anderen Daten verknüpft und ausgewertet werden. In diesem Zusammenhang ist auch zu berücksichtigen, dass es nach den derzeitigen Planungen künftig möglicherweise erleichtert werden soll, die Anschriften von Bürgerinnen und Bürgern in Erfahrung zu bringen. Der Bund erwägt zurzeit eine Änderung des Melderechtsrahmengesetzes, die aus dem Melderegister ein öffentliches Register macht, das jedermann zugänglich sein soll. Der Zugriff auf die Grunddaten des Melderechts (Name, Titel, Vorname, Anschrift) wäre danach - auch für ausländische Stellen - durch elektronischen Abruf möglich (vgl. 10.2).

Die Veröffentlichung von Mitarbeiterdaten soll einer schnellen und servicefreundlichen Kommunikation dienen. Die Frage der Zulässigkeit entscheidet sich danach, ob die Veröffentlichung zur Kontaktaufnahme und -pflege (ein an-

derer Aspekt des Dienstverkehrs kommt hier nicht in Betracht) erforderlich ist. Bei dieser Bewertung ist zu berücksichtigen, dass sich die moderne Verwaltung als Dienstleister versteht und eine nachhaltige Öffnung gegenüber Bürgerinnen und Bürgern anstrebt.

Aus der Kommunikationsfunktion folgt, dass Daten über Mitarbeiterinnen und Mitarbeiter, die nach ihrem Aufgabenbereich nicht an der Außenkommunikation ihrer Behörde teilnehmen und mit anderen öffentlichen oder privaten Stellen dienstlich nicht in Kontakt treten (wie dies z. B. bei Schreibkräften oder anderen Angehörigen des Inneren Dienstes der Fall sein kann), nicht an Dritte übermittelt werden dürfen. Neben dem Personenkreis begrenzt das Erforderlichkeitsprinzip den Umfang der Beschäftigtendaten, die übermittelt werden dürfen. Er muss sich auf die zur Kontaktaufnahme notwendigen Angaben beschränken. Dazu zählen jedenfalls Name, Angaben zur Funktion des Bediensteten, Dienstadresse, Tätigkeitsbereich, Telefon- und Fax-Nummer sowie E-Mail-Adresse. Ob Vorname und Amtsbezeichnung zu den zulässigerweise zu übermittelnden Daten gerechnet werden können, ist umstritten. Der Vorname ist bei Namensgleichheit als Unterscheidungsmerkmal von Bedeutung. Nach meinen Erfahrungen hat es sich inzwischen auch weitgehend eingebürgert, in amtlichen Telefonverzeichnissen, die an Dritte weitergegeben werden, die Vornamen der Bediensteten anzuführen. Schließlich kann nicht außer Acht gelassen werden, dass Bedienstete in zunehmendem Maße im dienstlichen Verkehr - wenn auch aufgrund eigener Entscheidung - nicht nur mit ihrem Namen, sondern auch dem Vornamen zeichnen. Angesichts dieser Entwicklung halte ich auch die Angabe des Vornamens für vertretbar. Bezüglich der Amtsbezeichnung ist darauf hinzuweisen, dass der Beamte im Dienst die Amtsbezeichnung führt (§ 89 Abs. 3 Satz 1 NBG). Eine Übermittlung der Amtsbezeichnung berührt jedoch in weitaus stärkerem Maße als die übrigen genannten Daten die Interessensphäre des Beamten, da sich aus ihr mit Hilfe von Besoldungstabellen u.Ä. Schlussfolgerungen auf die erhaltenen Bezüge ziehen lassen. Solche Angaben sind vor allem für Werbezwecke von besonderem Interesse. Von der Einstellung der Amtsbezeichnung in das Internet sollte deshalb abgesehen werden.

Nach dem Erforderlichkeitsprinzip ist auch zu beurteilen, wie weit der Kreis der Empfänger der genannten Daten gezogen werden darf. Er muss sich auf die Behörden, privaten Stellen und Personen beschränken, mit denen Kommunikationsbeziehungen bestehen oder von den behördlichen Aufgaben her in Betracht kommen. Es versteht sich von selbst, dass diese Abgrenzung nicht nach einzelnen Stellen und Personen erfolgen kann, sondern in einem nachvollziehbaren Maße eine schematisierende Betrachtung erfolgen darf.

Da durch eine Einstellung von Daten ins Internet Angaben über die Beschäftigten weltweit zur Verfügung gestellt werden, kann ein dienstliches Erfordernis nur bejaht werden, wenn die behördliche Aufgabenerledigung entsprechende Kommunikationsbeziehungen notwendig macht. Für den Hochschulbereich hat dies das Ministerium für Wissenschaft und Kultur bezüglich der in Forschung und Lehre tätigen Bediensteten für mich nachvollziehbar bejaht. In anderen Verwaltungsbereichen bedarf dies jeweils einer näheren Prüfung.

Im Zweifelsfall sollte die Einstellung von Mitarbeiterdaten ins Internet auf eine Dienstvereinbarung mit dem Personalrat gestützt werden. Die Dienstvereinbarung stellt eine eigenständige Rechtsgrundlage für die Verarbeitung von Personaldaten dar.

Daneben kommt eine Übermittlung auf der Grundlage einer Einwilligung der Betroffenen in Betracht. Sie muss schriftlich erfolgen und die übrigen Voraussetzungen des § 4 NDSG erfüllen. Ein besonderes Problem bei der Einwilligung zur Einstellung von Daten ins Internet ist die erforderliche Aufklärung. Sie muss so umfassend erfolgen, dass die Bediensteten die möglichen Folgen und Risiken,

die sich aus dieser Datenverarbeitung ergeben, sachgerecht abschätzen können. Zudem sind sie darauf hinzuweisen, dass sie ihre Einwilligung mit Wirkung für die Zukunft jederzeit widerrufen können.

Eine Veröffentlichung von Abbildungen der Bediensteten ist nur mit deren Einwilligung rechtlich zulässig.

14.8 Aufbewahrungsfristen für Personalvorgänge im Justizbereich

Durch AV vom 1. Oktober 1997 (Nds. Rpfl. S. 2177) hat das Justizministerium Bestimmungen über die Aufbewahrungsfristen für Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden getroffen. Die AV, die bundesweit abgestimmt sind, enthalten auch Vorschriften für den Personalbereich. Sie legen die Aufbewahrungsfristen für Vorgänge über erfolglose Bewerbungen auf fünf Jahre fest, die Aufbewahrungsfristen für Personalakten der Angestellten und Arbeiter werden auf 20 Jahre nach Abschluss der Akte festgesetzt.

Soweit die Regelungen den Personalbereich betreffen, sind sie überholt und nicht mehr anzuwenden. Kurz nach Erlass der AV hat der Niedersächsische Landtag durch das Dritte Gesetz zur Änderung dienstrechtlicher Vorschriften vom 17. Dezember 1997 (Nds. GVBl. S. 528) die Aufbewahrungsfristen für die Personalakten von Beamten geregelt (§ 101 g NBG). Die Vorschrift gilt nach § 261 Abs. 1 Nr. 2 NBG für Angestellte und Arbeiter entsprechend, sofern keine tarifvertragliche Regelung besteht. Für Richter ergibt sich die Geltung aus § 4 Abs. 1 Niedersächsisches Richtergesetz. Für alle Beschäftigtengruppen im Justizbereich gelten somit einheitlich die Aufbewahrungsvorschriften des NBG.

Dies hat zur Folge, dass Bewerbungsunterlagen unverzüglich zu löschen sind, sobald feststeht, dass ein Dienstverhältnis nicht zu Stande kommt (§ 101 Abs. 4 NBG). Dies ist erst dann der Fall, wenn die Auswahlentscheidung unanfechtbar geworden ist (vgl. XIV. TB 13.1). Personalakten sind nach § 101 g NBG fünf Jahre nach ihrem Abschluss (anstelle der in der AV vorgesehenen 20 Jahre) aufzubewahren.

Das Justizministerium hat zugesagt, die AV zu überarbeiten

15 Kommunalverwaltung

Im September 2001 werden in den Gemeinden und Landkreisen die Mitglieder der Räte und Kreistage gewählt. Viele Bürgerinnen und Bürger werden in den Vertretungskörperschaften und Ausschüssen erstmals ehrenamtlich mit kommunalen Verwaltungsaufgaben befasst sein. In der Ausübung ihres Mandats werden sie in vielen Fällen mit personenbezogenen Daten in Berührung kommen, so etwa bei Bau- und Vertragsangelegenheiten und in Personalangelegenheiten der Bediensteten. Vertraulich zu behandelnde Informationen finden sich in Sitzungsunterlagen, Niederschriften und sonstigen Materialien, die den Mitgliedern der kommunalen Organe, vereinzelt schon heute auf elektronischem Wege, zur Vorbereitung der Beratung und Beschlussfassung von der Verwaltung zur Verfügung gestellt werden. Die den Mitgliedern der Räte und Kreistage zur ihrer Information und zur Ausübung ihrer Kontrollfunktion gegenüber der Verwaltung zustehenden Auskunfts- und Akteneinsichtsrechte wurden im Zuge der umfassenden Novellierung des Kommunalverfassungsrechts erheblich ausgeweitet und erleichtert. Seither ist jedem einzelnen Ratsmitglied das Recht eingeräumt, in allen Angelegenheiten, sofern sie nicht der Geheimhaltung unterliegen, die zu seiner Unterrichtung erforderlichen Auskünfte zu verlangen.

Auch für die ehrenamtliche Mandatstätigkeit gelten die allgemeinen datenschutzrechtlichen Regelungen, so etwa das Niedersächsische Datenschutzgesetz. Den Belangen des Datenschutzes wird kommunalverfassungsrechtlich in besonderer Weise durch das Gebot der Amtsverschwiegenheit und Regelungen über den Ausschluss der Öffentlichkeit Rechnung getragen. Die bei mir eingehenden Anfragen und Eingaben zeigen jedoch, dass sowohl in der Verwaltung als auch bei den ehrenamtlichen Mandatsträgerinnen und Mandatsträgern häufig Unsicherheiten über den Umgang mit schützenswerten Daten bestehen. So werden nicht selten vertrauliche Daten in der „politischen Auseinandersetzung" verwendet, in der lokalen Presse veröffentlicht und somit ungeschützt jedermann zugänglich.

Ich halte es daher für geboten, im Zusammenwirken mit dem Innenministerium und den kommunalen Spitzenverbänden Handreichungen für den Umgang mit personenbezogenen Daten im Bereich der kommunalen Mandatstätigkeit zu veröffentlichen. Diese jeweils vor Ort in den Kommunen umzusetzenden Empfehlungen und Hinweise dürften gerade für die neugewählten Mandatsträgerinnen und Mandatsträger eine wertvolle Orientierungshilfe darstellen.

16 Bau-, Wohnungs- und Vermessungswesen

Liegenschaftskataster im Internet

Die Daten des amtlichen Vermessungswesens umfassen öffentlich zugängliche Angaben zum Landesbezugssystem und zur Topographie sowie eingeschränkt zugängliche Angaben zu Liegenschaften und Hinweise auf öffentlich-rechtliche Festlegungen. Das Liegenschaftskataster ist amtliches Verzeichnis im Sinne des § 2 Abs. 2 Grundbuchordnung und enthält Angaben über sachliche Verhältnisse von bestimmbaren Personen. Das Liegenschaftskataster besteht aus dem Liegenschaftsbuch, das flächendeckend in automatisierter Form geführt wird, und aus der Liegenschaftskarte, die in großen Teilen automatisiert, in Teilen auch analog geführt wird. Es ist erklärte Absicht, den berechtigten Nutzern die Angaben in einem automatisierten Abrufverfahren über das Internet zur Verfügung zu stellen.

In einer Technikfolgenabschätzung, an der ich mitgearbeitet habe, wurde für das geplante Abrufverfahren geprüft, ob bei Nutzung des Kommunikationsnetzes Internet die Gefahr einer Verletzung datenschutzrechtlicher Bestimmungen beherrscht wird. Das Datensicherungskonzept sieht vor, dass der Abruf im Client-Server-Verfahren über einen im Grenznetz des iznNet („demilitarisierte Zone") installierten Server realisiert wird. Der Originaldatenbestand soll dort als Kopie bereitgestellt und im online-Verfahren aktualisiert werden. Vor einer flächendeckenden Bereitstellung des Angebots wird zunächst mit einer begrenzten Anzahl berechtigter Nutzer für einen örtlich begrenzten Raum das Client-Server-Verfahren im iznNet getestet. Mit der Neufassung des Niedersächsischen Vermessungs- und Katastergesetzes sollen die rechtlichen Voraussetzungen für eine erweiterte Abrufbefugnis geschaffen werden; für die organisatorischen und technischen Maßnahmen gilt weiterhin das NDSG.

17 Finanzverwaltung

17.1 Fristenüberwachung bei den Steuerberatern

Bereits in meinem letzten Tätigkeitsbericht habe ich unter Nummer 17.2 die geplante Einführung einer sogenannten Steuerberaterdatei in Niedersachsen darge-

stellt. Diese Datei ist zum einen eine Adressdatenbank der Angehörigen der steuerberatenden Berufe und dient damit der automatisierten Adressierung der Steuerbescheide. Als weiterer Zweck soll die gesetzliche Aufgabenerfüllung des § 80 Abs. 5 AO und der §§ 5 Abs. 2 und 7 StBerG, nämlich die Zurückweisung von Personen, die unerlaubt Hilfe in Steuersachen leisten, besser überwacht werden. Auf datenschutzrechtliche Bedenken stieß im Wesentlichen die geplante Überwachung der fristgerechten Abgabe der Steuererklärungen durch die Steuerberater. Es wurde in Gesprächen mit Vertretern des Finanzministeriums eine einvernehmliche Lösung gefunden, wonach bei der Auflistung der noch abzugebenden Steuererklärungen bei Fristverlängerungen über den 30. September. bzw. den 28. Februar hinaus lediglich eine Abstimmung mit den von den Steuerberatern eingereichten Listen der noch abzugebenden Steuererklärungen erfolgen soll, um so diejenigen Fälle auszuscheiden, bei denen zwar eine Steuerberatung vermerkt wurde, allerdings das Mandat nicht mehr besteht und somit die Steuererklärung unverzüglich angefordert werden muss. Bei der Ermessensentscheidung über die Gewährung einer Fristverlängerung über den 28. Februar des zweiten auf das Veranlagungsjahr folgenden Kalenderjahres hinaus soll lediglich ein anonymes Zahlenwerk der bereits abgegebenen Steuererklärungen mit Fristverlängerung und eine namentliche Nennung der noch offenen Steuerfälle eines bestimmten Steuerberaters ausgewiesen werden, sodass hierbei nur die personenbezogenen Daten von Steuerpflichtigen, die ihrer Erklärungspflicht noch nicht nachgekommen sind und vom Steuerberater ohnehin benannt werden müssen, ausgewiesen werden.

17.2 EDV-Zugriff der Betriebsprüfer

Der Regierungsentwurf eines Gesetzes zur Senkung der Steuersätze und zur Reform der Unternehmensbesteuerung (Steuersenkungsgesetz) sah die Einführung eines Absatzes 6 im § 147 Abgabenordnung (AO) vor. Inhalt dieses neuen Absatzes war u. a. die Ermächtigung der Finanzverwaltung, im Rahmen der Außenprüfung die Datenverarbeitungssysteme des Betriebes einzusehen und diese Systeme für die steuerliche Überprüfung zu nutzen, sofern hiermit eine Buchführung oder Einnahme-Überschuss-Rechnung erstellt worden ist. Diese Regelung sollte bereits ab dem 1. Januar 2001 gelten. Da in dem Datenverarbeitungssystem des Betriebes auch sehr sensible Daten wie z. B. die personenbezogenen Daten der Mitarbeiter, von Kunden und Geschäftspartnern abgespeichert werden, muss der Zugriff des Betriebsprüfers auf diese Bereiche technisch ausgeschlossen werden, da diese Daten nicht für seine Aufgabenerfüllung erforderlich sind. Die damit verbundene Umstellung der Datenverarbeitungssysteme ist nicht kurzfristig leistbar und erfordert daher eine spätere Inkraftsetzung der neuen Regelung. Auf vielfaches Drängen, insbesondere auch von Datenschutzbeauftragten des Bundes und der Länder, wurde dann auch die Einführung der Neuregelung auf den 1. Januar 2002 verschoben.

Forderungen nach einer Protokollierung der Zugriffe durch den Betriebsprüfer konnten bisher allerdings nicht durchgesetzt werden. Diese Protokollierung der Dateizugriffe ermöglicht eine Kontrolle von Datenabfragen, wie sie in anderen Gesetzen (vgl. u. a. § 133 Grundbuchordnung i. V. m. § 83 Grundbuchverfügung, § 915 h Abs. 1 Nr. 2 ZPO i. V. m. § 18 Abs. 6 Schuldnerverzeichnisverordnung und § 13 Ausländerzentralregistergesetz i. V. m. § 16 AZRG-Verordnung) seit langem vorgesehen ist. Sie dient sowohl dem Schutz der Personen, deren Daten in dem Datenverarbeitungssystem gespeichert sind, als auch des Betriebsprüfers vor falschen Anschuldigungen. So könnte dann im Einzelfall ermittelt werden, ob die Ermittlungen von steuerlich relevanten Sachverhalten im Rahmen der Prüfungsanordnung durchgeführt worden sind. Eine solche Protokollierung sollte ohnehin im Interesse des Betriebsinhabers liegen, um auch

den Zugriff von Mitarbeitern auf schützenswerte Daten erkennen zu können. Ich werde mich weiterhin für diese Protokollierung einsetzen.

17.3 Fahrtenbücher für steuerliche Zwecke

Ab dem 1. Januar 1998 müssen die Ärzte bei Führung eines Fahrtenbuches für steuerliche Zwecke neben dem Datum und Kilometerstand zu Beginn und Ende jeder einzelnen beruflichen Fahrt auch den Reisezweck und den Namen des aufgesuchten Patienten angeben. Diese Regelung hat der Bundesbeauftragten für den Datenschutz förmlich beim Bundesfinanzministerium beanstandet mit der Begründung, dass die Ärzte dem Auskunftsverweigerungsrecht des § 102 Abs. 1 Nr. 3 c Abgabenordnung unterliegen. Das Auskunftsverweigerungsrecht bezieht sich auch auf den Namen des aufgesuchten Patienten. Im Übrigen verstößt der Arzt mit der Angabe des Patientennamens in seinem Fahrtenbuch gegen die Strafvorschrift des § 203 Abs. 1 Strafgesetzbuch (ärztliche Schweigepflicht). Die ärztliche Schweigepflicht umfasst neben einschlägigen medizinischen Daten auch den Namen und die Anschrift des Patienten.

Ein vom Bundesbeauftragten für den Datenschutz und dem Bundesfinanzministerium inzwischen erarbeiteter Konsens, der sowohl die ärztliche Schweigepflicht wie auch steuerliche Belange ausreichend berücksichtigt, sieht nun vor, dass im Fahrtenbuch des Arztes als Reiseziel lediglich eine Nummer angegeben wird, über die sich mit einem gesondert zu führenden Verzeichnis der Name des Patienten ermitteln lässt. Die Finanzverwaltung soll dieses Verzeichnis nur einsehen, wenn Umstände vorliegen, die Zweifel an der Richtigkeit oder Vollständigkeit der Eintragungen begründen und diese Zweifel nicht anders auszuräumen sind. Diese Verfahrensweise wurde u. a. auch der Bundesärztekammer mitgeteilt. Das Bundesfinanzministerium hat die Länder mit der Umsetzung dieser Anweisung beauftragt.

Die Oberfinanzdirektion Hannover hat daraufhin das Karteiblatt zur "ertragsteuerlichen Erfassung der Nutzung eines betrieblichen Kraftfahrzeugs zu Privatfahrten..." der Einkommensteuerkartei mit Datum vom 8. Juli .2000 geändert; eine Sonderregelung für Ärzte, wie sie die Absprache auf Bundesebene vorsieht, lässt diese Karteikarte allerdings vermissen. Auf meine Nachfrage beim Niedersächsischen Finanzministerium, wann denn nun mit der Umsetzung in Niedersachsen zu rechnen sei, wurde mir mitgeteilt, dass eine entsprechende Regelung in Kürze ergehen werde. Man sei bisher davon ausgegangen, dass das geschilderte Verfahren in den Finanzämtern mit Rücksicht auf etwaige Berufsgeheimnisse bereits angewendet werde.

Ich werde die Umsetzung im Auge behalten.

17.4 Zweitwohnungssteuer

Gleich durch mehrere Petenten wurde ich auf einen Fragebogen zur Festsetzung der Zweitwohnungssteuer einer Samtgemeinde aufmerksam gemacht. Ziel dieses Fragebogens ist die Klärung des tatsächlichen Hauptwohnsitzes des Bürgers bei einem Widerspruch gegen eine festgesetzte Zweitwohnungssteuer. Dabei ist nicht von dem melderechtlichen Erst- und Zweitwohnsitz auszugehen, sondern die Satzung der Samtgemeinde stellt auf den tatsächlichen Lebensmittelpunkt des Betroffenen ab. Um diesen Lebensmittelpunkt bestimmen zu können, muss der Betroffene entsprechende Nachweise aufgrund objektiv nachprüfbarer Kriterien erbringen.

Die Samtgemeinde stellt für diese Festsetzung eine Vielzahl von Fragen, deren Berechtigung den Petenten und auch mir zum Teil nicht einleuchtet. So wird u. a. nach dem Arbeitgeber der Betroffenen, nach der Schuldenfreiheit der eigenen Häuser oder Wohnungen und nach dem Wohnort der "näheren Verwandten" gefragt. Außerdem sollen die vollständigen Einkommensteuererklärungen der letzten Jahre vorgelegt werden.

Die Samtgemeinde beruft sich darauf, dass sie gem. § 88 Abgabenordnung beim Verfahren zur Festsetzung der Zweitwohnungssteuer Art und Umfang der Ermittlungen bestimmt. Dies kann allerdings nur im Rahmen pflichtgemäßen Ermessens geschehen. Dazu gehört insbesondere, dass nur solche Fragen gestellt werden, die zur Aufklärung, ob ein steuerpflichtiger Tatbestand vorliegt, erforderlich sind. Dies ist bei einer Frage nach dem Arbeitgeber, mit der zunächst nur eine Angabe über den Beschäftigungsort angestrebt wird, nicht der Fall. Eine Aussage über die Verschuldung der einzelnen als Hauptwohnsitz in Betracht kommenden Objekte hat ebenso wenig eine Aussagekraft für den Hauptwohnsitz wie der Wohnort "näherer Verwandter". Auch die Forderung nach Vorlage vollständiger Einkommensteuererklärungen verletzt den datenschutzrechtlichen Erforderlichkeitsgrundsatz. Zwar kann es notwendig sein, bestimmte Daten auch aus der Steuererklärung (z. B. Mieteinkünfte, Fahrten zwischen Wohnung und Arbeitsstätte) zu erheben; diese Notwendigkeit muss jedoch im Einzelfall begründet sein. Entsprechende Aufklärungsfragen dürfen deshalb nicht generell jedem Betroffenen vordruckmäßig ohne Berücksichtigung des jeweiligen Sachverhalts gestellt werden.

Eine einvernehmliche datenschutzgerechte Lösung konnte bisher nicht gefunden werden; die Gespräche mit der Samtgemeinde dauern an.

17.5 Feststellung des Hundebestandes durch private Dritte

Mir wurde mitgeteilt, dass einige Gemeinden und Städte in Niedersachsen zur Ermittlung des Hundebestandes Fremdfirmen beauftragt haben, diejenigen Hundehalter festzustellen, die ihren Hund bisher nicht angemeldet haben und deswegen auch keine Hundesteuer entrichten. Die Mitarbeiter dieses Unternehmens nehmen Befragungen von Grundstückseigentümern nach vorgefertigten Listen vor und übergeben sie den Städten und Gemeinden, die die Hundesteuer daraufhin festsetzen.

Dieses Verfahren entbehrt einer gesetzlichen Grundlage und ist damit unzulässig. Gem. § 12 des Niedersächsischen Kommunalabgabengesetzes (NKAG) können Gemeinden und Landkreise in Satzungen bestimmen, dass die Ermittlung von Berechnungsgrundlagen, die Abgabenberechnung, die Ausfertigung und Versendung von Abgabebescheiden sowie die Entgegennahme der zu entrichtenden Abgabe von einem damit beauftragten Dritten wahrgenommen werden können. Diese Ermächtigung ist allerdings auf den Bereich der Gebühren und Beiträge beschränkt und umfasst nicht die Erhebung von Daten zur Festsetzung der Hundesteuer. Nach § 12 Abs. 1 Satz 2 NKAG wird ausdrücklich klargestellt, dass die Ermächtigung nicht für den Bereich der Steuern gilt. Auch die Befragung der Haushalte durch Angehörige der Kommunalverwaltung ist nicht zulässig. Zwar haben die Beteiligten nach § 93 Abgabenordnung die erforderlichen Auskünfte im Besteuerungsverfahren zu erteilen, allerdings gilt diese Auskunftspflicht erst dann, wenn die Steuerpflicht feststeht und nicht schon in dem Vorverfahren, in dem erst geprüft wird, ob eine Steuerpflicht überhaupt besteht. Der Bundesfinanzhof (BFH) hat u. a. in seinen Urteilen vom 23. Oktober 1990 (BStBl. 199 II S. 277) und vom 29. Oktober 1986 (BStBl 1988 II S. 359) erklärt, "ins Blaue hinein" dürfe die Finanzbehörde Auskunftsverlangen nicht stellen; Auskunftsersuchen im Rahmen von Rasterfahndungen oder ähnlichen

Ermittlungen seien unzulässig. Auf die Unzulässigkeit dieser Erhebungsmethoden der Kommunen habe ich sowohl die betroffenen Kommunen als auch den Städte- und Gemeindebund aufmerksam gemacht. Dennoch hat die Stadt Salzgitter nach einer Pressemitteilung vom 29. August 2000 eine Befragung aller Haushalte durch Mitarbeiter einer privaten Firma angekündigt. Dieses Verhalten werde ich förmlich beanstanden.

18 Soziales

18.1 Gesundheitsreform 2000

Mitte 1999 hat die Bundesregierung den Entwurf eines Gesetzes zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 (GKV-Gesundheitsreform 2000) beschlossen. Die Datenschutzbeauftragten des Bundes und der Länder haben hierzu am 25. August 1999 eine Entschließung verabschiedet (s. Anlage 6). Dem Niedersächsischen Ministerium für Frauen, Arbeit und Soziales habe ich diese Entschließung versehen mit einer umfangreichen Stellungnahme im September 1999 übersandt. Aufgrund der Vorschläge der Datenschutzbeauftragten wurden von dem zuständigen Bundesministerium für Gesundheit wesentliche Änderungen des Verfahrens erarbeitet, die datenschutzrechtliche Belange sehr weitgehend berücksichtigten. Der Gesetzentwurf sah u. a. die Pseudonymisierung des gesamten Abrechnungsverfahrens bei den gesetzlichen Krankenkassen vor. Hierin liegt nicht nur eine entscheidende datenschutzrechtliche Verbesserung. Gefunden wurde vielmehr ein für die medizinische Datenverarbeitung allgemein wegweisendes technisches und rechtliches Verfahren, mit dem weitgehende Auswertungsinteressen bezüglich medizinischer Daten mit den Belangen des Patientengeheimnisses in Einklang gebracht werden können.

Die Vorstellung dieses Konzepts im Rahmen der Sachverständigenanhörung des Bundestagsausschusses für Gesundheit am 22. September 1999 und die Diskussion hierüber ergaben, dass nicht nur die Vertreter sämtlicher Bundestagsfraktionen, sondern auch die Interessenverbände den Vorschlägen zustimmten.

Im Nachgang zu dieser Diskussion geäußerte Bedenken wegen zusätzlicher, durch die Pseudonymisierung entstehender Kosten konnten in Zusammenarbeit mit dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) ausgeräumt werden.

Die 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer Sitzung am 7./8. Oktober 1999 die Ergebnisse der Verhandlungen in einer Entschließung begrüßt (Anlage 11).

Im weiteren Gesetzgebungsverfahren ist dann jedoch der Gesetzentwurf in einen zustimmungspflichtigen und einen nicht zustimmungspflichtigen Teil gesplittet worden. Da die Mehrzahl der datenschutzrechtlichen Regelungen zu dem zustimmungspflichten Teil gehören, sind sie aufgrund seiner Ablehnung durch den Bundesrat nicht in Kraft getreten.

Zurzeit wird im Bundesgesundheitsministerium ein Gesetzentwurf erarbeitet, dessen Ziel es ist, Regelungen zu schaffen, die die in der gesetzlichen Krankenversicherung vorhandenen Abrechnungs- und Leistungsdaten unter Wahrung des Rechts auf informationelle Selbstbestimmung der Versicherten für das Gesundheitswesen verfügbar machen.

18.2 Krankenhausentlassungsberichte an Krankenkassen

Im Berichtszeitraum häuften sich Anfragen, ob es zulässig sei, dass von Krankenkassen angeforderte Krankenhausentlassungsberichte oder andere Arztberichte diesen direkt übersandt werden dürfen. Hierzu stelle ich fest, dass gemäß §§ 275 ff. SGB V es grundsätzlich Aufgabe des Medizinischen Dienstes der Krankenversicherung (MDK), nicht aber der Krankenkassen ist, Prüfungen durchzuführen und Gutachten zu erstellen. Die Krankenkassen dürfen diese Sozialdaten zwar bei den Leistungserbringern erheben, soweit es für die Beteiligung des MDK erforderlich ist (§ 276 Abs. 1 i. V. m. § 284 Abs. 1 Nr. 7 SGB V). Der den Leistungserbringern gegenüber anzugebende Erhebungszweck ist jedoch ausschließlich auf die Weitergabe der Daten an den MDK begrenzt und erlaubt keine Kenntnisnahme der Patientenunterlagen durch die Krankenkassen. Die Krankenhäuser sollten diese Unterlagen entsprechend kennzeichnen (verschlossener Briefumschlag mit Aufdruck „Nur für den MDK bestimmt").

Der Bundesbeauftragte für den Datenschutz hat gegenüber den Spitzenverbänden der Krankenkassen demgemäß Datenerhebungen der Krankenkassen beim Krankenhaus, die über den Umfang der nach § 301 SGB V vom Krankenhaus zu übermittelnden Daten hinausgehen, nur in Ausnahmefällen für zulässig angesehen. Zu den Voraussetzungen, die nach Auffassung des Bundesbeauftragten erfüllt sein müssen, gehört u. a., dass die Datenerhebung nur erfolgen darf, wenn die Krankenkasse über die Einschaltung des Medizinischen Dienstes zu entscheiden hat. Zudem muss bereits vor der Übermittlung die Einwilligung des Betroffenen vorliegen.

18.3 Auskunftspflichten der Leistungserbringer gegenüber den Versicherten

Gemäß § 305 Abs. 2 SGB V unterrichten die an der vertragsärztlichen Versorgung teilnehmenden Ärzte/Zahnärzte und ärztlich geleiteten Einrichtungen die Versicherten schriftlich über die zu Lasten der Krankenkassen abgerechneten Leistungen und die von den Krankenkassen zu zahlenden Entgelte innerhalb von vier Wochen nach Ablauf des Quartals, in dem die Leistungen in Anspruch genommen worden sind. Das Nähere regeln die Vertragspartner in den Bundesmantelverträgen. Obwohl diese Vorschrift bereits am 1. Juli 1997 in Kraft getreten ist, sind diese Verträge immer noch nicht abgeschlossen worden. Nach Auffassung der Kassenärztlichen Bundesvereinigung ist die Information erst dann möglich, wenn für ärztliche Leistungen feste Punktwerte vereinbart sind. Die Krankenkassen sind der Auffassung, dass eine Unterrichtung auch anhand des letzten bekannten Abrechnungswertes erfolgen kann.

Ich messe der Unterrichtung seitens der Leistungserbringer einen hohen Stellenwert bei. Sie vermittelt dem Versicherten einen Überblick über die von ihm in Anspruch genommenen Leistungen und die dadurch entstandenen Kosten. Ich halte es für dringend geboten, eine entsprechende Vereinbarung abzuschließen.

18.4 Angaben zu Patienten bei Überweisungen durch Sozialleistungsträger

Die Ärztekammer Niedersachsen hat mich darauf aufmerksam gemacht, dass Sozialleistungsträger bei Überweisungen an Ärzte, die Untersuchungen für diese Stellen durchgeführt haben, auf den Überweisungsträgern sowohl den Namen des untersuchten Patienten als auch den Grund für die Überweisung angeben. Diese Angaben erscheinen dann auf den Kontoauszügen der Bank des Arztes. Der Arzt muss zwar in der Lage sein, die Überweisung einer von ihm erbrachten Leistung sachgerecht zuordnen zu können, hierfür ist es jedoch nicht erforderlich, den Patientennamen und den Gegenstand des Auftrages anzugeben. Das

Niedersächsische Ministerium für Frauen, Arbeit und Soziales hat sich in einem Schreiben an die Arbeitsgemeinschaft der kommunalen Spitzenverbände und die AOK dieser Auffassung angeschlossen und auf die Möglichkeit der Anonymisierung/Pseudonymisierung, etwa durch Angabe von Rechnungsdatum und Rechnungsnummer bzw. Patientennummer, hingewiesen. Das Ministerium hat zudem auf das Urteil des BVerwG vom 23. Juni 1994 - 5 C 16.92 (DVBl. 1994 S. 1313) verwiesen, in dem ausgeführt wird, dass es nicht mit dem Sozialdatenschutz zu vereinbaren ist, wenn auf Überweisungsträgern personenbezogene Daten des Leistungsempfängers Dritten zugänglich gemacht werden.

18.5 Datenabgleich zwischen Sozialamt und Kfz-Zulassungsstelle

Zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe sind die Träger der Sozialhilfe befugt, Daten von Personen, die Leistungen beziehen, bei anderen Stellen zu überprüfen.

Gemäß § 117 Abs. 3 Satz 4 Buchst. f) BSHG darf deshalb die Kfz-Zulassungsstelle die „Eigenschaft als Kraftfahrzeughalter" übermitteln. Aus diesem Wortlaut lässt sich ableiten, dass nicht nur mitgeteilt werden darf, ob jemand Kfz-Halter ist oder nicht, sondern auch, in wie vielen Fällen (für wie viele Kfz) diese Eigenschaft besteht. Darüber hinausgehende Auskünfte werden von dieser Vorschrift nicht gedeckt.

Wenn weitere Daten erforderlich sind, sind diese beim Betroffenen zu erheben, falls für die Überprüfung des fraglichen Sachverhalts nicht ausnahmsweise eine Erhebung bei anderen Stellen in Betracht kommt (§ 67 a Abs. 2 SGB X). Daten über die Art des Kraftfahrzeuges können nur unter dieser Voraussetzung von der Zulassungsstelle erlangt werden.

18.6 Einmalige Beihilfe zum Lebensunterhalt durch Verpflichtungsschein

Zu der Frage der Zulässigkeit der Ausgabe eines Verpflichtungsscheins (Wertgutschein) anstelle von Bargeld durch den Träger der Sozialhilfe zur Beschaffung eines größeren Haushaltsgeräts durch den Hilfeempfänger hat mich das Niedersächsische Oberverwaltungsgericht um Stellungnahme gebeten. Der Verpflichtungsschein besteht in dem konkreten Fall aus einem Schreiben des Sozialhilfeträgers an den Hilfeempfänger. Er enthält dessen Vornamen, Namen und Anschrift. Gegen Rückgabe des Scheins verpflichtet sich der Sozialhilfeträger, bis zur Höhe des angegebenen Betrages die Kosten für die angegebene Ware/Leistung zu übernehmen. Der Hilfeempfänger händigt den Schein einer von ihm ausgewählten Firma aus. Zusammen mit der Rechnung wird der Verpflichtungsschein, auf dem der Leistungsempfänger den Empfang der Ware bzw. die Ausführung der Dienstleistung bestätigt, dem Sozialhilfeträger zur Begleichung übersandt.

Mit der Aushändigung des Verpflichtungsscheins offenbart der Hilfeempfänger der Lieferfirma die im Schein genannten Daten sowie den Sozialhilfebezug. Diese Sozialdaten dürfen vom Sozialleistungsträger aber nur unter den Voraussetzungen der §§ 67 ff. SGB X verarbeitet werden. Nach § 69 Abs. 1 Nr. 1 1. Fall SGB X ist die Bekanntgabe der im Verpflichtungsschein enthaltenen Sozialdaten zulässig, wenn die Aushändigung des Scheins an die Lieferfirma eine Datenübermittlung darstellt, die für die Erfüllung der Zwecke erforderlich ist, für die die Daten erhoben worden sind.

Ich bin in meiner umfangreichen Stellungnahme gegenüber dem OVG zu dem Ergebnis gelangt, dass bei einer rechtmäßigen Ermessensentscheidung über die

Gewährung einer Sachleistung in der Form eines Verpflichtungsscheins die Erforderlichkeit der Datenübermittlung nach dieser Vorschrift zu bejahen ist. Datenschutzrechtliche Gesichtspunkte, die bereits in die Ermessungsabwägung eingeflossen sind, können im Falle einer rechtmäßigen Verwaltungsentscheidung die Erforderlichkeit einer Übermittlung, die sich an fachspezifischen Gesichtspunkten orientiert, nicht infrage stellen. Bei Vorliegen eines überwiegenden Allgemeininteresses und der Auswahl eines Mittels, das für den angestrebten Zweck geeignet und erforderlich ist, muss insofern auch das Recht auf informationelle Selbstbestimmung zurücktreten. Ein Verpflichtungsschein, der wie im vorliegenden Fall nur Name und Anschrift des Hilfeberechtigten enthält, stellt ein für die Aufgabenerfüllung geeignetes Mittel dar.

18.7 Anforderung von Kontoauszügen durch Sozialhilfeträger

Anlässlich von Beschwerden hatte ich mich mit der Frage zu befassen, inwieweit es datenschutzrechtlich zulässig ist, dass Sozialhilfeträger und Wohngeldstellen zur Verhinderung von Leistungsmissbrauch die lückenlose Vorlage von Kontoauszügen für einen bestimmten Zeitraum fordern, ohne dass Anhaltspunkte für einen Leistungsmissbrauch vorliegen.

Ich bin zu dem Ergebnis gekommen, dass in den folgenden Fallgruppen die Vorlage von Kontoauszügen grundsätzlich gefordert werden kann:

- Erstmalige Beantragung von laufenden Leistungen der Hilfe zum Lebensunterhalt,
- Beantragung von einmaligen Beihilfen gemäß § 21 Abs. 2 BSHG,
- bei lfd. Hilfebezug nach Ablauf eines Zeitraums von mindestens 12 Monaten,
- bei Zweifeln an der Vollständigkeit oder Richtigkeit der Angaben oder zur Klärung einer konkreten Frage zu der Einkommens- und Vermögenssituation.

Im Hinblick auf § 67 a Abs. 3 Satz 1 SGB X muss der Sozialhilfeträger angeben, warum der Nachweis nicht mit anderen Unterlagen erbracht werden kann bzw. akzeptiert wird. Für welchen Zeitraum Kontoauszüge vorgelegt werden müssen, bestimmt sich nach der Erforderlichkeit im jeweiligen Einzelfall.

Die Verpflichtung zur Vorlage von Kontoauszügen darf aber nicht automatisch zu einer Speicherung der darin enthaltenen Daten führen. Gemäß § 67 c Abs. 1 SGB X dürfen Sozialdaten nur gespeichert werden, soweit dies für die Erfüllung der jeweiligen Aufgabe erforderlich ist. Kontoauszüge enthalten oft eine Vielzahl von Kontobewegungen, die für die Feststellung des Sozialhilfebedarfs nicht relevant sind. Ihre Speicherung ist somit unzulässig. Es darf jedoch in der Akte vermerkt werden, für welchen Zeitraum Kontoauszüge eingesehen worden sind. Wurden bei der Einsichtnahme sozialhilferechtlich relevante Daten festgestellt, so kann dies ebenfalls in der Akte vermerkt werden. Es kann auch eine Kopie zu den Akten genommen werden, wenn zuvor die nicht erforderlichen Daten geschwärzt worden sind.

Das MFAS hat sich dieser Rechtsauffassung angeschlossen.

Bezüglich der Anforderung von Bankauskünften verweise ich in diesem Zusammenhang auf den Beschluss des Hessischen Verwaltungsgerichtshofs vom 7. Februar 1995 (DVBl. 1995 S. 702), in dem u. a. ausgeführt wird, dass „allein die Tatsache der Beantragung von Sozialhilfe als solche grundsätzlich nicht ausreicht, um den Angaben des Antragstellers im schriftlichen Antrag auf Gewährung von Sozialleistungen keinen Glauben zu schenken". „Ohne Vorliegen kon-

kreter Anhaltspunkte ist das Verlangen, der Einholung von Bankauskünften zuzustimmen, aber eine überflüssige Ermittlungstätigkeit des Sozialhilfeträgers und somit nicht erforderlich i. S. von § 60 Abs. 1 Nr. 1 SGB I".

18.8 Hilfe bei Schwangerschaftsabbrüchen

Ich hatte bereits in meinem XIV. TB unter 18.14 dargestellt, dass ich gemeinsam mit dem MFAS der Auffassung bin, dass das Abrechnungsverfahren künftig nicht mehr personen-, sondern fallbezogen erfolgen sollte. Hierzu hatte ich Vorschläge unterbreitet. Bis heute ist es weder dem MFAS noch mir gelungen, die Krankenkassen zu einer Änderung des Verfahrens zu bewegen. Sie sperren sich gegen eine Anonymisierung des Kostenerstattungsverfahrens und machen hierfür in erster Linie den finanziellen Mehraufwand (der keiner ist) geltend. Nach meinem Eindruck geht es ihnen allerdings wohl eher darum, vom Land ein höheres pauschaliertes Entgelt zu erhalten.

19 Gesundheit

19.1 Übermittlung von Angaben über Patienten eines psychiatrischen Krankenhauses an eine Besuchskommission

Das MFAS ernennt gemäß § 30 Abs. 1 des Niedersächsisches Gesetzes über Hilfen und Schutzmaßnahmen für psychisch Kranke (NPsychKG) einen Ausschuss für Angelegenheiten der psychiatrischen Krankenversorgung, dessen Aufgabe darin besteht, zu prüfen, ob psychisch Kranke oder behinderte Menschen entsprechend den Vorschriften des Gesetzes betreut und behandelt werden.

Um diese Aufgabe erfüllen zu können, bildet der Ausschuss für psychiatrische Krankenhäuser und sonstige psychiatrische Einrichtungen eines jeden Regierungsbezirks eine oder mehrere Besuchskommissionen, die in der Regel einmal im Jahr die Krankenhäuser und Einrichtungen aufsuchen, dem Ausschuss über festgestellte Mängel berichten und Vorschläge zur Verbesserung der Behandlung und Betreuung unterbreiten (§ 30 Abs. 3 NPsychKG).

Zur Vorbereitung eines solchen Besuches bat eine Besuchskommission ein psychiatrisches Krankenhaus um Übersendung einer Liste mit den Namen von Patienten und deren Betreuern. Das Krankenhaus äußerte dagegen datenschutzrechtliche Bedenken.

Diese waren jedoch nicht begründet. Gemäß § 30 Abs. 5 NPsychKG sind die Krankenhäuser und Einrichtungen sowie ihre Träger verpflichtet, den Ausschuss und die Besuchskommission bei ihrer Arbeit zu unterstützen. Sie haben dem Ausschuss und der Besuchskommission, soweit zu deren Aufgabenerfüllung erforderlich, Auskünfte zu erteilen, Akteneinsicht zu gewähren und Gespräche mit Patienten und Bediensteten zu ermöglichen. Krankenunterlagen dürfen allerdings nur mit Einwilligung des Patienten bzw. seines Personensorgeberechtigten oder Betreuers vorgelegt werden.

Die Namenliste war erforderlich, damit die Besuchskommission, die überprüfen wollte, ob Patienten länger als erforderlich untergebracht waren, die Möglichkeit erhielt, diese und ihre Betreuer um die Einwilligung zur Einsichtnahme in die Krankenunterlagen zu bitten. Die Voraussetzungen des § 30 Abs. 5 NPsychKG waren daher erfüllt.

19.2 Übermittlung von Ärztelisten durch die Ärztekammer Niedersachsen

Die Ärztekammer Niedersachsen bat um Auskunft, unter welchen Voraussetzungen eine Übermittlung von Ärztelisten an andere Stellen oder Personen zulässig ist.

Die gesetzlichen Regelungen sind sehr differenziert, sodass ich sie auch im Hinblick auf andere Stellen ausführlich darstellen möchte.

§ 5 Heilberufekammergesetz (HKG) regelt die Übermittlung von Verzeichnissen der Kammermitglieder im Rahmen des Katastrophenschutzes. Weitere in Betracht kommende Vorschriften enthält das Gesetz nicht.

Es gilt daher das Niedersächsische Datenschutzgesetz. Zu unterscheiden ist zwischen einer Übermittlung an öffentliche Stellen und einer Übermittlung an Stellen oder Personen außerhalb des öffentlichen Bereichs.

Übermittlung an öffentliche Stellen

Gemäß § 11 Abs. 1 NDSG ist die Übermittlung personenbezogener Daten an öffentliche Stellen nur zulässig, wenn sie zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist.

Eine Übermittlung wird nur in Ausnahmefällen für die Erfüllung der Aufgaben der Landesärztekammer erforderlich sein. Im Regelfall werden die Daten für die Aufgabenerfüllung des Empfängers bestimmt sein. Für die Frage der Erforderlichkeit kommt es darauf an, ob er seine Aufgaben ohne diese Daten nicht oder nicht vollständig, nicht rechtzeitig oder nur unter unverhältnismäßigen Schwierigkeiten erfüllen könnte. Wenn also z. B. Daten von Ärzten mit einer bestimmten Teilgebietsbezeichnung ausreichen, wäre es nicht erforderlich, eine vollständige Arztliste zu übersenden.

Hinsichtlich der weiteren Voraussetzungen verweist § 11 Abs. 1 NDSG auf § 10 NDSG. Gemäß § 10 Abs. 1 Satz 1 NDSG ist die Übermittlung zulässig, wenn die Landesärztekammer die Daten zu dem Zweck, für den sie erhoben wurden, übermittelt. In der Regel wird die Übermittlung jedoch eine Zweckänderung darstellen, deren Zulässigkeit § 10 Abs. 2 NDSG regelt. Danach ist eine zweckändernde Übermittlung zulässig mit Einwilligung der Betroffenen (§ 10 Abs. 1 Satz 1 Nr. 1 NDSG). Es ist also zu überlegen, ob zumindest für bestimmte, absehbare Standardsituationen die Einwilligung der Ärzte eingeholt wird. Dies könnte z. B. bei der Kammeranmeldung erfolgen.

Ohne Einwilligung darf die Übermittlung unter den Voraussetzungen des § 10 Abs. 2 Satz 1 Nr. 2 NDSG, der auf § 9 Abs. 1 Satz 3 Nrn. 1 bis 5 verweist, vorgenommen werden. Von Bedeutung ist insbesondere § 9 Abs. 1 Satz 3 Nr. 5 NDSG. Danach ist die Übermittlung zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können. Zu diesen Quellen gehören Telefonbücher und Branchenverzeichnisse. Zwar besteht die Möglichkeit, einer Eintragung zu widersprechen. Diese Möglichkeit ändert jedoch nichts daran, dass es sich hinsichtlich der in den Telefonbüchern und Branchenverzeichnissen genannten personenbezogenen Daten um solche allgemein zugängliche Quellen handelt. Zu nennen sind ebenfalls Ärztehandbücher. Die Übermittlung ist also nach dieser Vorschrift zulässig, soweit sie sich auf die in den Verzeichnissen enthaltenen Daten beschränkt.

In Ausnahmefällen werden die Voraussetzungen des § 9 Abs. 1 Satz 3 Nr. 1 NDSG erfüllt sein, weil eine Rechtsvorschrift eine Übermittlung vorsieht oder zwingend voraussetzt. Möglicherweise kommt im Einzelfall auch eine Anwendung des § 9 Abs. 1 Satz 3 Nr. 3 NDSG (Überprüfung der Angaben eines Betroffenen) oder des § 9 Abs. 1 Satz 3 Nr. 4 NDSG (Offensichtlichkeit, dass die

Übermittlung im Interesse der Betroffenen liegt und dass sie in die Übermittlung einwilligen würden) in Betracht.

Es hängt also von der jeweiligen Fallgestaltung ab, ob eine Übermittlung zulässig ist.

Die Landesärztekammer muss nur in eingeschränktem Umfang die Zulässigkeit des Ersuchens prüfen. Wenn die Übermittlung aufgrund eines Ersuchens erfolgt, hat die übermittelnde Stelle nämlich lediglich zu prüfen, ob sich das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden Stelle hält. Die Rechtmäßigkeit des Ersuchens prüft die übermittelnde Stelle nur, wenn im Einzelfall hierzu Anlass besteht; die empfangende Stelle hat der übermittelnden Stelle die für die Prüfung erforderlichen Angaben zu machen (§ 11 Abs. 3 NDSG).

Die übermittelnde Stelle muss also eine Art Schlüssigkeitsprüfung vornehmen, ob die ersuchende Stelle generell für die betreffende Aufgabe zuständig ist und ob ein solches Ersuchen im Rahmen der Aufgabenerfüllung liegen kann. Darüber hinaus prüft die übermittelnde Stelle nicht die in der Sphäre des Empfängers liegenden Umstände, es sei denn, es besteht ein besonderer Anlass dafür. Wenn also z. B. als Begründung für das Übermittlungsersuchen angegeben wird, dass Angaben des Betroffenen überprüft werden müssen, darf die ersuchte Stelle im Regelfall davon ausgehen, dass diese Begründung zutrifft. Hingegen verbleibt es für die Übermittlungsvoraussetzungen, die in der Sphäre der ersuchten Stelle liegen, etwa weil nur sie den Sachverhalt kennt, bei ihrer Verantwortung. Sie hat also z. B. zu prüfen, ob eine wirksame Einwilligungserklärung vorliegt oder ob die Angaben aus allgemein zugänglichen Quellen entnommen werden können.

Eine weitergehende Prüfung ist erforderlich, wenn ein besonderer Anlass dafür besteht. Wenn also etwa um die Übersendung einer Liste mit Angaben zu allen Ärzten in Niedersachsen gebeten wird, jedoch Anhaltspunkte dafür bestehen, dass nur Daten von Ärzten mit bestimmten Gebietsbezeichnungen benötigt werden, ist die anfordernde Stelle um eine Begründung zu bitten. Gegebenenfalls muss die Herausgabe der gewünschten Liste verweigert werden.

Die Vorschriften des Niedersächsischen Datenschutzgesetzes verleihen eine Befugnis zur Übermittlung personenbezogener Daten, sie begründen jedoch keine Verpflichtung.

Wenn die Übermittlung im Rahmen einer Amtshilfe erfolgt, genügt allein diese Tatsache nicht, um eine Übermittlung zu rechtfertigen, sondern es muss sich die Befugnis aus einer Rechtsvorschrift, hier dem Niedersächsischen Datenschutzgesetz, ergeben. Es ist jedoch zu beachten, dass jede Behörde anderen Behörden auf Ersuchen Amtshilfe leistet (§ 1 Abs. 1 des Niedersächsischen Verwaltungsverfahrensgesetzes - NVwVfG; § 4 Abs. 1 Verwaltungsverfahrensgesetz - VwVfG). Daher wird, wenn die Voraussetzungen einer Amtshilfe vorliegen (§ 1 Abs. 1 NVwVfG, §§ 4 ff. VwVfG), aus der Befugnis zur Datenübermittlung eine Pflicht. In diesen Fällen muss die Landesärztekammer also, soweit das Niedersächsische Datenschutzgesetz es erlaubt, die gewünschten Angaben machen.

Übermittlung an nichtöffentliche Stellen

Eine Übermittlung von Daten an Stellen oder Personen außerhalb des öffentlichen Bereichs ist mit Einwilligung der Betroffenen zulässig. Wenn sie nicht vorliegt, kann sich die Zulässigkeit aus § 13 NDSG ergeben. Falls die Übermittlung ausnahmsweise zur Erfüllung der Aufgaben der Ärztekammer erforderlich ist, gelten gemäß § 13 Abs. 1 Satz 1 Nr. 1 NDSG die Voraussetzungen des § 10 NDSG, sodass auf die Ausführungen oben verwiesen werden kann.

Die Übermittlung ist ebenfalls zulässig, wenn die Empfänger ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an der Geheimhaltung überwiegt (§ 13 Abs. 1 Satz 1 Nr. 2 NDSG). Ein rechtliches Interesse ist an das Bestehen eines besonderen Rechtsgrundes geknüpft und liegt etwa dann vor, wenn der Auskunftssuchende die Daten zur Durchsetzung von Rechtsansprüchen oder zur Rechtsverteidigung benötigt. Für die glaubhafte Darlegung dieses Interesses genügt eine entsprechende Erklärung des Empfängers, in der er kurz den Sachverhalt darstellt

Hinsichtlich des überwiegenden schutzwürdigen Interesses der Betroffenen ist zu beachten, dass, wie oben ausgeführt, die zu übermittelnden Angaben häufig bereits aus allgemein zugänglichen Quellen entnommen werden können, sodass zumindest in diesen Fällen in der Regel überwiegende schutzwürdige Interessen nicht entgegenstehen werden.

Die übermittelnde Stelle hat die Empfänger zu verpflichten, die Daten nur für die Zwecke zu verarbeiten, zu denen sie übermittelt wurden (§ 13 Abs. 2 NDSG).

Die Übermittlung ist ebenfalls nach § 13 Abs. 1 Satz 1 Nr. 3 NDSG zulässig, wenn der Empfänger ein berechtigtes Interesse geltend macht. Berechtigt ist jedes ideelle und wirtschaftliche Interesse, das auf sachlichen Erwägungen beruht und mit der Rechtsordnung in Einklang steht. Reine Neugierde würde z. B. nicht ausreichen. Die Anforderungen sind also geringer als beim „rechtlichen Interesse". Allerdings ist weiterhin erforderlich, dass die Betroffenen der Übermittlung nicht widersprochen haben. Sie sind, um ihnen diese Widerspruchsmöglichkeit zu geben, über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise und rechtzeitig zu unterrichten (§ 13 Abs. 1 Satz 2 NDSG). Auch hier hat die Verpflichtung nach § 13 Abs. 2 NDSG zu erfolgen.

Auch bei der Übermittlung an nichtöffentliche Stellen hängt die Zulässigkeit also vom jeweiligen Einzelfall ab.

19.3 Übertragung von Aufgaben der Ärztekammer Niedersachsen auf die Kassenärztliche Vereinigung Niedersachsen

Ein Arzt teilte mir mit, die Mutter eines von ihm behandelten Kindes habe sich über ihn bei der Ärztekammer Niedersachsen, Bezirksstelle Oldenburg, beschwert. Der Beschwerdebrief trage den Eingangsstempel „ÄKN/KVN Bez.Stelle Oldb."

Der Arzt zog daraus die nahe liegende Schlussfolgerung, dass für die Bezirksstelle Oldenburg der Ärztekammer Niedersachsen (ÄKN) und der Kassenärztlichen Vereinigung Niedersachsen (KVN) eine gemeinsame Posteingangsstelle besteht. Es sei zu befürchten, dass die Kassenärztliche Vereinigung auf diese Weise über die an die Ärztekammer gerichteten Patientenschreiben informiert werde, obwohl für die Durchführung einer hier möglicherweise in Betracht kommenden berufsrechtlichen Maßnahme nur die Ärztekammer, nicht jedoch die Kassenärztliche Vereinigung zuständig sei.

In der Tat besteht eine enge organisatorische Verflechtung der Bezirksstellen. Die Ärztekammer Niedersachsen errichtet gemäß § 19 Abs. 1 der „Kammersatzung der Ärztekammer Niedersachsen" vom 1. Januar 1998 Bezirksstellen. Nach § 19 Abs. 2 kann die Ärztekammer die Erledigung der Aufgaben dieser Bezirksstellen den Bezirksstellen der Kassenärztlichen Vereinigung Niedersachsen übertragen. Dieser Regelung entspricht § 13 Abs. 2 Satz 2 der Satzung der Kas-

senärztlichen Vereinigung Niedersachsen. Danach kann deren Geschäftsstelle die Führung der Geschäfte der Bezirksstelle der Ärztekammer übernehmen.

Diese organisatorische Verbindung ist aus datenschutzrechtlicher Sicht nicht unproblematisch. Die Ärztekammer und die Kassenärztliche Vereinigung sind unterschiedliche Daten verarbeitende Stellen im Sinne des § 3 Abs. 3 NDSG mit völlig unterschiedlichen gesetzlichen Aufgaben. Gemäß § 9 Abs. 1 NDSG dürfen öffentliche Stellen nur die für ihre Aufgabenerfüllung erforderlichen personenbezogenen Daten erheben. Auch eine Datenübermittlung (§ 11 NDSG) zwischen den beteiligten Stellen darf nur unter den gesetzlichen Voraussetzungen erfolgen. Zudem muss für die Ärzte und sonstige Personen deutlich werden, gegenüber welcher Institution sie ihre Rechte auf Auskunft, Berichtigung, Sperrung oder Löschung geltend machen können.

Gemäß § 2 Abs. 5 NDSG gehen besondere Rechtsvorschriften über die Verarbeitung personenbezogener Daten den Bestimmungen des Niedersächsischen Datenschutzgesetzes vor. Zu diesen Rechtsvorschriften gehören auch Bestimmungen einer Satzung, soweit sie sich auf die „Satzungsunterworfenen", hier also die Ärzte, beziehen. Allerdings enthalten die erwähnten Satzungen der Ärztekammer und der Kassenärztlichen Vereinigung keine das Problem betreffende Regelungen.

Eine ähnliche Zusammenarbeit findet auch zwischen der Zahnärztekammer Niedersachsen und der Kassenzahnärztlichen Vereinigung Niedersachsen statt. Hier allerdings liegt nicht einmal eine die Aufgabenerledigung regelnde Satzung vor.

Die Ärztekammer antwortete mir, es sei ausreichend sichergestellt, dass die organisatorische Verbindung nicht den Datenschutz verletze. Sensible personenbezogene Daten würden ausschließlich durch Sachbearbeiter der Ärztekammer bearbeitet. Eingeräumt wurde allerdings, dass in einigen Bezirksstellen eine Personalunion zwischen den Bezirksstellenvorsitzenden besteht und in anderen der jeweiligen Vorsitzende der einen Organisation der Stellvertreter des anderen ist. Stets haben die Bezirksstellen nur einen Geschäftsführer.

Zugesichert wurde, in Zukunft sicherzustellen, dass nicht mehr ein gemeinsamer Poststempel in einer gemeinsamen Poststelle benutzt wird, sondern dass zumindest eingehende Post, die erkennbar an die eine oder andere Organisation gerichtet ist, auch nur von dem jeweils eigenen Sachbearbeiter geöffnet wird.

Diese datenschutzrechtlichen Verbesserungen habe ich begrüßt. Dennoch genügen sie nicht. Zumindest werden bei den Personen, die Bezirksstellenvorsitzende sowohl der Ärztekammer als auch der Kassenärztlichen Vereinigung sind, weiterhin in Vertretungsfällen und bei den Geschäftsführern personenbezogene Daten aus beiden Bereichen zusammengeführt. Auch im Übrigen wird eine Abschottung nur eingeschränkt realisierbar sein. Für mich ist nicht erkennbar, welche Angaben zu den sensiblen Daten gehören, die ausschließlich vom Sachbearbeiter der Ärztekammer bearbeitet werden. Der Umkehrschluss liegt nahe, dass zumindest in der Vergangenheit bei anderen, nicht als sensibel eingestuften Daten, eine personelle Trennung nicht erfolgte.

Die beste Lösung besteht darin, die Bezirksstellen zu trennen. Wenn diese Trennung kurzfristig nicht zu erreichen ist, muss versucht werden, eine möglichst datenschutzgerechte Organisation zu finden. Ich werde das Gespräch mit der Ärztekammer und der Zahnärztekammer in diesem Sinne fortführen.

19.4 Übermittlung von Patientendaten an Kassenzahnärztliche Vereinigung

Wenig Gespür für die ärztliche Schweigepflicht bewies die Kassenzahnärztliche Vereinigung Niedersachsen (KZVN).

In einem Rundschreiben an die Zahnärzte hieß es, die Krankenkassen nähmen im Zusammenhang mit der Versorgung mit Zahnersatz und Zahnkronen immer häufiger Stellungnahmen des Medizinischen Dienstes der Krankenversicherung Niedersachsen (MDKN) in Anspruch. Wiederholt hätten sich Zahnärzte bei der Kassenzahnärztlichen Vereinigung beschwert, weil die Stellungnahmen des Medizinischen Dienstes fachlich unqualifiziert seien. „Um sich einen Eindruck verschaffen zu können", bat die Kassenzahnärztliche Vereinigung die Ärzte um Übersendung der Stellungnahmen.

Zu Recht sah der Medizinische Dienst in der Herausgabe solcher Gutachten einen Verstoß gegen die ärztliche Schweigepflicht. Abgesehen davon gehören die Kassen- (zahn)ärztlichen Vereinigungen auch nicht zu den in § 277 SGB V genannten Adressaten, die vom Medizinischen Dienst über das Ergebnis der Begutachtung und den Befund unterrichtet werden.

Die Kassenzahnärztliche Vereinigung beteuerte, es sei nicht ihre Absicht gewesen, Patientendaten zu erheben. In der Regel hätten die Zahnärzte nur das Gutachtenblatt zugesandt, aus dem der Patient nicht zu ersehen sei. In den Fällen, in denen mehr Daten übermittelt worden seien, habe man diese gelöscht.

In einem weiteren Rundschreiben wurden die Zahnärzte gebeten, nur das Gutachtenblatt vorzulegen. Ein Patientenbezug müsse vermieden werden.

19.5 Anlaufpraxis für den ärztlichen Notfallbereitschaftsdienst

Ein anspruchsvolles Vorhaben wurde von der Kassenärztlichen Vereinigung Niedersachsen, Bezirksstelle Lüneburg (kurz: KV Lüneburg) verwirklicht, die in einer Stadt ihres Zuständigkeitsbereichs gemeinsam mit einem eingetragenen Verein, in dem sich die meisten der an der Notfallversorgung teilnehmenden Ärzte zusammengeschlossen haben, eine Anlaufpraxis für den ambulanten ärztlichen Notfallbereitschaftsdienst eingerichtet hat.

Der Vorteil einer solchen Anlaufpraxis besteht aus der Sicht des Patienten darin, dass er auch außerhalb der üblichen Sprechstundenzeiten ärztliche Hilfe erhält oder zumindest sicher sein kann, einen Arzt telefonisch zu erreichen.

Der Verein hat ca. 30 Mitglieder. Nicht alle in Betracht kommenden niedergelassenen Ärzte haben sich ihm angeschlossen.

Gemeinsam mit der KV Lüneburg und dem Verein habe ich versucht, Regelungen zu finden, die innerhalb dieser Praxis, deren Größe eher der eines Krankenhauses entspricht, die Wahrung der ärztlichen Schweigepflicht sicherzustellen.

Nach derzeitigem Stand vergibt die Vereinsvorsitzende an jedes Mitglied ein Passwort, das den Zugriff auf die Daten der von ihm behandelten Patienten ermöglicht. Falls ein Patient die Anlaufpraxis aufsucht, der zuvor von einem anderen Vereinsmitglied behandelt wurde, gibt die Arzthelferin mittels eines Überpasswortes den Zugriff auf diese Daten frei. In einer Dienstanweisung wird geregelt, unter welchen Voraussetzungen im Einzelnen die Arzthelferin, die als Angestellte des Vereins der Weisungsbefugnis des Vorstands, nicht des einzelnen Vereinsmitglieds unterliegt, die Freigabe ermöglichen darf.

Zu Beginn der Behandlung wird dem Patienten eine Erklärung vorgelegt, mit der er in die Verwendung der Angaben über seine Behandlung durch den jeweiligen Notdienst habenden Arzt einwilligt.

Eine ähnliche Zugriffsregelung wie für die elektronische Dokumentation besteht für die Papierdokumente.

Kein Zugriff auf die Patientendaten haben die Ärzte, die zwar in der Anlaufpraxis den Notdienst versehen, jedoch nicht Vereinsmitglieder sind. Die Dokumentation besteht hier nur in dem Notfallschein. Der Arzt bewahrt die für ihn bestimmte Durchschrift in seiner Praxis auf und händigt dem Patienten das für den weiterbehandelnden Arzt bestimmte Blatt mit der Bitte aus, es an diesen weiterzuleiten. Damit dürfte ein datenschutzgerechtes Verfahren gefunden worden sein.

19.6 Veranlagung zum Ärztekammerbeitrag

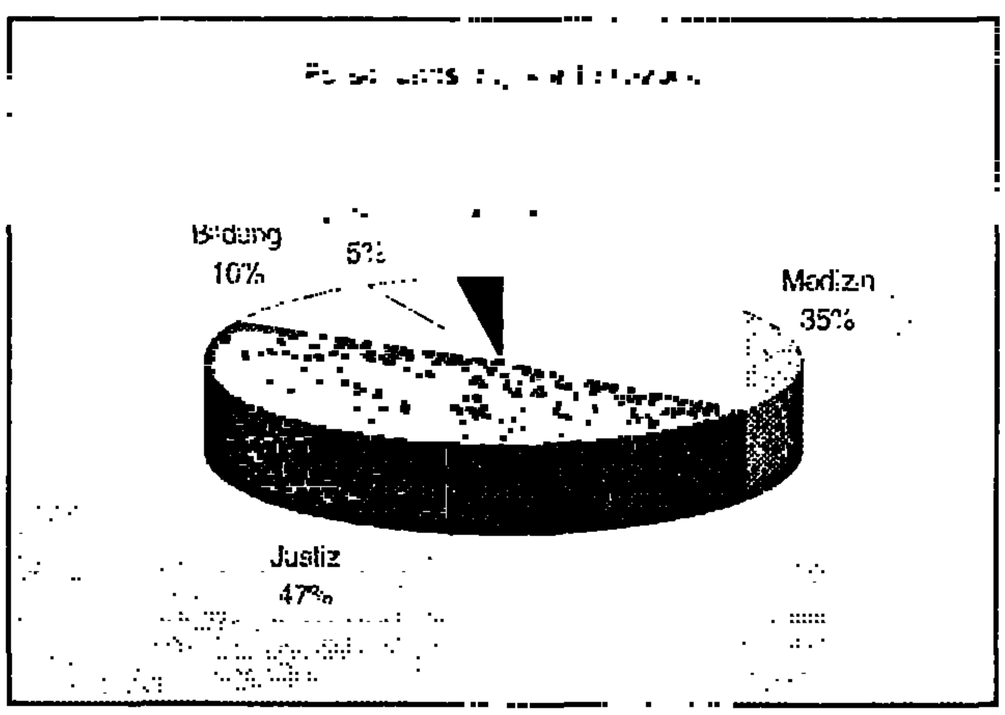
Mit Wirkung vom 1. Januar 1999 ist eine neue Beitragsordnung der Ärztekammer Niedersachsen in Kraft getreten. Als Nachweis der Einkünfte aus ärztlicher Tätigkeit wird ein Auszug des Einkommensteuerbescheides gefordert. Zu dieser Nachweisforderung habe ich mehrere Anfragen erhalten.

Nach Prüfung des Sachverhalts habe ich festgestellt, dass aus meiner Sicht keine datenschutzrechtlichen Bedenken gegen die Vorlage eines Auszugs des Einkommensteuerbescheides bei der Ärztekammer Niedersachsen bestehen. Die Beitragsordnung verlangt lediglich den Nachweis aus ärztlicher Tätigkeit und beschränkt damit die Datenerhebung auf die beitragserheblichen Angaben. Eventuell nicht relevante Angaben wie Kinderzahl, Familienstand, steuerliche Abschreibungen, Schulden, andere Einkünfte (z. B. des Ehegatten) können daher geschwärzt werden. Dies wird auch in dem Schreiben der Ärztekammer zur Veranlagung zum Ärztekammerbeitrag 1999 deutlich, in dem nur ein Auszug des Einkommensteuerbescheides gefordert wird. Ebenso wird in einem Erinnerungsschreiben unter den allgemeinen Hinweisen darauf aufmerksam gemacht, dass die für die Berechnung unbedeutenden Angaben unkenntlich gemacht werden können.

20 Forschung

20.1 Forschung mit personenbezogenen Daten hat Konjunktur

Forschungsvorhaben, bei denen eine Abwägung zwischen öffentlichen Interessen an deren Durchführung und schutzwürdigen Belangen der Betroffenen erfolgt (§ 25 Abs. 2 Nr. 3 NDSG), müssen nach Änderung des NDSG 1997 mir nicht mehr vorgelegt werden. Vielmehr sind jetzt die Datenschutzbeauftragten der forschenden bzw. übermittelnden Stelle zu unterrichten. Drei Jahre nach Einführung lässt sich sagen, dass diese Regelung entgegen den Erwartungen nicht zu einer Reduzierung meiner Beteiligung bei Forschungsvorhaben geführt hat. Es ist sogar ein leichter Anstieg zu verzeichnen. Die Abbildung zeigt die Bereiche, denen die Forschungsvorhaben zugeordnet werden können. Besonders stark sind die Bereiche
Medizin und Justiz
vertreten. Insbesondere im medizinischen Bereich stellt dies sicherlich nur die Spitze des Eisbergs personenbezogener Forschung in Niedersachsen dar. Denn zum einen werden hier viele



Vorhaben über Einwilligungslösungen durchgeführt, bei denen keine Unterrichtungspflicht besteht. Zum anderen werden im medizinischen Bereich oft Daten der eigenen Institution (Hochschule) verwendet; bei diesen rein internen Projekten werden Externe nur selten eingeschaltet. Im Justizbereich sind dagegen Stellen außerhalb des Forschungsinstituts (Gerichte, Strafvollzuganstalten) Objekt der Forschung.

Die von internen Datenschutzbeauftragten berichteten Fallzahlen von Beteiligungen bei Forschungsprojekten lassen vermuten, dass lange nicht in allen Fällen der Unterrichtungspflicht nachgekommen wird. Hier ist noch Aufklärungsarbeit zu leisten. Ich bin auch weiterhin bereit, Forscher bei der datenschutzgerechten Durchführung ihrer Vorhaben zu beraten. Über Durchführung und Ergebnis meiner Beratungstätigkeit geben die folgenden Ausführungen exemplarisch Auskunft.

20.2 PISA soll klären, wie gut unsere Schulen sind

Wie gut können unsere Schüler lesen? Wie sieht es mit der mathematischen Grundbildung aus? Welche naturwissenschaftlichen oder fächerübergreifenden Kenntnisse sind vorhanden? Diese Fakten sollen nun auf den Tisch kommen. In dem OECD-Projekt PISA werden in rund 30 der wichtigsten Industriestaaten Leistungen von ca. 180 000 Schülerinnen und Schüler im Alter von 15 Jahren gemessen. Allein in Niedersachsen werden 3 200 Schülerinnen und Schüler in 83 Schulen befragt. Getestet werden aber eigentlich nicht die Kinder, sondern die Schulen und Bildungskonzepte. Wie gut bereiten unsere Schulen die Jugendlichen auf die Herausforderungen der Zukunft vor? Vermitteln sie das Wissen, die Fertigkeiten und Einstellungen, die Jugendliche und Erwachsene benötigen, um als verantwortliche Bürger aktiv am gesellschaftlichen Leben teilnehmen zu können?

PISA wurde nach einer Planungsphase 1999 in einem Feldtest erprobt. In 2000 hat die Haupterhebung stattgefunden. Dabei fielen nicht nur große Mengen von personenbezogenen Schülerdaten an, auch das private Umfeld der Jugendlichen wurde einbezogen (Eltern, Geschwister usw.). Aus diesem Grund wurde das gesamte Projekt intensiv von den Datenschutzbeauftragten der Länder begleitet. Dabei wurden viele für den Datenschutz relevante Punkte erörtert und umgesetzt. Zu den wichtigsten gehören:

- Die Erhebung ist freiwillig. Einwilligen müssen sowohl die Schüler als auch die Eltern. Die Einwilligung muss den datenschutzrechtlichen Kriterien entsprechen. Als besonderes Problem stellte sich heraus, dass die Eltern die Fragebögen vorab nicht einsehen sollten. Die Projektleiter befürchteten, dass diese sonst Einfluss auf ihre Kinder nehmen könnten und damit die Projektergebnisse verfälschen würden. Das Datenschutzrecht verlangt aber eine "informierte Einwilligung". Die Betroffenen müssen wissen, in was sie einwilligen. Als Kompromiss wurde vereinbart, dass die Fragebögen zwar nicht an alle Eltern verteilt erden, aber in der Schule zur Einsicht bereit gehalten werden.
- Die Weitergabe und Auswertung der Fragebögen erfolgt in anonymer Form. Die Projektverantwortlichen haben selbst den Ablauf des Vorhabens sehr genau beschrieben, um die Objektivität der Ergebnisse zu gewährleisten. Hierbei wurden bereits viele auch für den Datenschutz wichtige Punkte berücksichtigt (z. B. die Verhinderung der Einsicht- und Einflussnahme durch Lehrer). Weitere Punkte wurden auf Anregung der Datenschutzbeauftragten ergänzt.

Die Fragebögen wurden so gestaltet, dass eine Zuordnung zu einzelnen Schülerinnen oder Schülern auch aus dem Zusammenhang der Antworten praktisch nicht möglich ist. Die Projektverantwortlichen hatten anfangs geplant, das genaue Geburtsdatum mit zu erfassen. Zusammen mit anderen Antworten des Fragebogens und mit dem entsprechenden Zusatzwissen hätte die Gefahr der Zuordnung der Fragebögen zu einzelnen Schülerinnen oder Schülern bestanden. Die Projektverantwortlichen ließen sich überzeugen, auf die Erfassung des Geburtstags zu verzichten.

20.3 VW-Unfallforschung

Die Volkswagen AG hat die Niedersächsische Polizei um Unterstützung für die Unfallforschung des Unternehmens gebeten. Die gewonnenen Erkenntnisse sollen dazu dienen, die aktive und passive Sicherheit von Kraftfahrzeugen zu erhöhen. Um eine unter statistischen Gesichtspunkten gesicherte Datenbasis zu erhalten, soll das Unfallgeschehen in einer gesamten Region einbezogen werden. Die Polizei wurde gebeten, alle Verkehrsunfälle mit VW-Modellen - bis auf Bagatell-Unfälle - an die Forschungsgruppe von VW zu melden. Dies soll so schnell wie möglich nach Bekanntwerden des Unfalls geschehen, damit das Forschungsteam möglichst noch am Unfallort erste Daten erheben und eine frühzeitige Untersuchung des Fahrzeugs und eine Befragung der Autoinsassen vornehmen kann.

Es waren einige harte Nüsse zu knacken, um dieses Vorhaben datenschutzrechtlich zulässig zu gestalten. Schließlich werden hier sehr sensitive Daten bei Personen erhoben, die sich oft in kritischen Ausnahmesituationen befinden, und die Datenerhebung erfolgt durch ein privates Unternehmen. Andererseits bestand von Anfang an kein Zweifel daran, dass eine solche Forschung von besonderem öffentlichen Interesse ist. Schließlich geht es um das Leben und die Gesundheit von vielen Menschen.

Auch hier bestand die Lösung in einem Verfahren, dass auf eine Einwilligung der Betroffenen hinausläuft. Eine Befragung der Autoinsassen, eine Übermittlung von Patientendaten an das Forschungsteam oder eine Untersuchung des Unfallfahrzeugs erfolgen erst, wenn die Betroffenen bzw. Verantwortlichen hierin eingewilligt haben.

Das VW-Forschungsteam berücksichtigt die von mir geforderten Maßnahmen, um eine datenschutzrechtlich einwandfreie Durchführung des Vorhabens zu gewährleisten. Hierzu gehören eine Verpflichtung auf das Datengeheimnis aller beteiligten Forscher, eine strenge Zweckbindung der Datenverarbeitung, viele technische und organisatorische Maßnahmen zur Gewährleistung der Vertraulichkeit bis hin zu einer frühestmöglichen Anonymisierung und Löschung der personenbezogenen Daten.

20.4 Auskünfte aus Melderegistern zu Forschungszwecken

Bei zahlreichen Forschungsprojekten werden Name und Anschrift von Personen benötigt, die in besonderer Weise aus der gesamten Bevölkerung eines regionalen Bereiches ausgesucht worden sind. Dies können statistisch ausgesuchte „Testpersonen“ für medizinische Fall-Konstellationen sein oder sämtliche Personen einer bestimmten Altersgruppe. Viele Forscher sehen die Einwohnermelderegister als die geeignete Quelle für ihr Vorhaben an.

Ob derartige Auskünfte erteilt werden dürfen, beurteilt sich nach dem NMG. Soweit es sich bei der Forschungseinrichtung um eine öffentliche Stelle handelt,

muss die Übermittlung der Daten zur Erfüllung der in der Zuständigkeit der Forschungseinrichtung liegenden Aufgaben erforderlich sein (vgl. § 29 NMG). Handelt es sich dagegen um eine nichtöffentliche Einrichtung, muss die Gruppenauskunft insbesondere im öffentlichen Interesse liegen (vgl. § 33 Abs. 3 NMG). Es sind aber auch besondere Fallgestaltungen - insbesondere in tatsächlicher Hinsicht - denkbar, in denen sich die Nutzung der Melderegister unmittelbar nach der speziellen Forschungsregelung in § 25 NDSG beurteilt. Auch für derartige Fragestellungen biete ich weiterhin sowohl den Datenschutzbeauftragten der entsprechenden Forschungseinrichtungen als auch den Forschungseinrichtungen selbst meine Beratung an.

21 Hochschulen

21.1 Evaluation

Schon in der Vergangenheit (vgl. XII. TB 25.1) habe ich mich zu den datenschutzrechtlichen Fragen der Evaluation an Hochschulen geäußert. Inzwischen wird diese sehr häufig eingesetzt. Es wurde eine Zentrale Evaluationsagentur (ZEvA) der Niedersächsischen Hochschulen gegründet, die bei Evaluationen behilflich ist. Auch die wissenschaftliche Kommission Niedersachsen betätigt sich aktiv auf diesem Gebiet.

Die Anwendung der Regelung in der Praxis führt zu der Frage, welche Daten erhoben werden dürfen und wer diese bzw. die hieraus gewonnenen Ergebnisse zu sehen bekommen darf. Bei meiner Bewertung gehe ich von folgenden Grundsätzen aus:

– Für die Evaluation dürfen nur die personenbezogenen Daten erhoben werden, die hierfür tatsächlich erforderlich sind. Eine "vorsorgliche" Erhebung hierüber hinausgehender Daten ist nicht zulässig. Dies erfordert ein entsprechendes Konzept für die Evaluation. Unstrittig ist, dass etwa bei der Evaluation in Forschungsbereichen Daten der Professoren erhoben werden müssen. Die namentliche Nennung der wissenschaftlichen Mitarbeiter sollte aber nur dann erfolgen, wenn diese in nennenswerter Weise eigenständige Forschung betreiben und ihre Arbeit wesentliche Beiträge zur Erreichung der Forschungsziele leistet bzw. leisten soll. Auch der Umfang der Daten zu einer Person muss kritisch geprüft werden. So kann z. B. auf die Angabe konkreter Gründe für "Ausfallzeiten" (z. B. Erziehungsurlaub, Auslandsaufenthalte) im Allgemeinen verzichtet werden.

– Die erhobenen personenbezogenen Daten sind frühestmöglich zu anonymisieren. Die Übermittlung von Ergebnissen darf nur im erforderlichen Umfang geschehen. Dies bedeutete in einem konkreten Fall, dass ein Teil des Evaluationsberichtes nicht veröffentlicht werden durfte, da er zahlreiche konkrete personenbezogene Angaben enthält. Eine Weitergabe dieser Daten an die jeweilige Hochschule, auf die sich die Daten beziehen, sowie eine Weitergabe insgesamt an das Ministerium für Wissenschaft und Kultur halte ich aber für hinnehmbar.

Der von mir geprüfte Evaluationsbericht enthielt auch an anderer Stelle personenbezogene Daten (Namen der Professoren). Sie beziehen sich jedoch lediglich auf die jeweilige Stelle und die Frage ihrer Neubesetzung. Eine Veröffentlichung dieses Teils halte ich daher aus datenschutzrechtlicher Sicht für zulässig.

21.2 Hochschul-Chipkarten

An verschiedenen niedersächsischen Hochschulen gibt es Überlegungen, Hochschul-Chipkarten für Studenten und Bedienstete einzuführen. Für den Einsatz

kommen Funktionen wie die Immatrikulation, die Antragstellung für BAföG, die Nutzung von Mensa und Bibliotheken sowie Standardauskünfte (Termine, Veranstaltungspläne) und persönliche Informationen (Notenspiegel, Studienverlaufsbescheinigungen) in Frage. Auch sonstige universitätsnahe Dienstleistungen (Kopierer, Telefon/Telefax, Uni-Shop, Waschmaschinen, Parkplatz) und sogar eine Kreditkarte oder elektronische Geldbörse könnten mit eingebunden werden.

Wegen der besonderen datenschutzrechtlichen Bedeutung von Chipkartensystemen im Hochschulbereich habe ich mich mit diesem Thema näher befasst. Zentrale Punkte zur rechtlichen Einordnung und zum datenschutzgerechten Umgang gebe ich im Folgenden wieder:

Das Datenschutzrecht enthält bisher nur wenige Regelungen zum Chipkarten-Einsatz. Es muss daher auf das allgemeine Datenschutzrecht zurückgegriffen werden. Verantwortlich für die Datenspeicherung auf einer Chipkarte ist die jeweilige eingebende Stelle, hier also Hochschule, Studentenwerk, Bank oder Dienstleister. Dementsprechend ist das Bundesdatenschutzgesetz bei nichtöffentlichen Stellen bzw. das Niedersächsische Datenschutzgesetz bei öffentlichen Stellen anzuwenden.

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn dies ein Gesetz oder eine Rechtsvorschrift erlaubt oder die Betroffenen eingewilligt haben. Für die Einführung einer obligatorischen Hochschul-Chipkarte für Studierende bedarf es daher einer Rechtsvorschrift; dies kann auch eine Hochschulordnung sein. Solange eine solche nicht besteht, kann eine Hochschul-Chipkarte nur auf freiwilliger Basis eingeführt werden.

Merkmale der datenschutzrechtlichen Einwilligung sind die Informiertheit, Freiwilligkeit und die Widerrufbarkeit mit Wirkung für die Zukunft. Die Widerrufbarkeit ist nur gegeben, wenn die Studierenden ohne unvertretbaren Aufwand von der elektronischen Nutzung der Hochschul-Chipkarte auf eine konventionelle Verfahrensweise umsteigen können.

Den Betroffenen steht ein Auskunftsanspruch über alle zur jeweiligen Person gespeicherten Daten zu. Es muss daher sichergestellt werden, dass die Betroffenen von dem auf der Chipkarte gespeicherten Dateninhalt für alle Kartensegmente unentgeltlich Kenntnis nehmen können.

22 Schulen

22.1 Umfragen und Erhebungen in Schulen

Ein Landkreis hat eine kreisweite Erhebung zu Kinder- und Jugendproblemen durchgeführt. Alle Kinder und Jugendlichen von 11 bis 16 Jahren (ca. 12 000) sollten an einer freiwilligen Fragebogenaktion, die in den Schulen durchgeführt werden sollte, beteiligt werden. Dabei wurden die unterschiedlichsten Themen wie Schule, Familie, Freizeit, Gewalt und Drogen behandelt. Die Umfrage wurde, wie es der Erlass des Niedersächsischen Kultusministeriums vom 25. März 1993 (SVBl. S. 107), geändert durch Erlass vom 21. November 1994 (SVBl. S. 335), vorsieht, bei einer Bezirksregierung beantragt und von dieser auch genehmigt.

Der sehr umfangreiche Fragenkatalog enthielt sehr detaillierte Fragen aus schulfachlicher Sicht zum häuslichen, familiären und zutiefst persönlichen Bereich der Schüler. Die Fragen betrafen auch die persönlichen Angelegenheiten der Erziehungsberechtigten oder ließen Rückschlüsse hierauf zu. Da die Kinder - gemessen an ihrem Alter - die Tragweite der Fragen und der Antworten noch

nicht übersehen und begreifen konnten, war die Kenntnis der Erziehungsberechtigten von den Fragen und ihre ausdrückliche Zustimmung zur Befragung ihrer Kinder zwingend erforderlich. Hier wären nach dem Erlass ausdrückliche Hinweise zur Freiwilligkeit der Teilnahme und die vorherige Zustimmung der Betroffenen, hier also der Erziehungsberechtigten, erforderlich gewesen. Dies gilt auch, wenn die Daten aufgrund der Art der Durchführung der Befragung anonym sind.

Hinsichtlich der zugesicherten Anonymität der Befragung gab es zudem in Einzelfällen die Möglichkeit, einen Personenbezug herzustellen, z. B. für einen Ort, in dem nur ein einziger Schüler für die Befragung in Betracht kam. Weil zu den Fragebogen auch eine Karte gehörte, auf der die Schüler ihren „ungefähren" Wohnort ankreuzen sollten, war hier die Herstellung des Personenbezugs möglich. Ich habe gefordert, in solchen Fällen auf das Ankreuzen des Wohnorts zu verzichten.

Hinsichtlich der Freiwilligkeit der Teilnahme an der Befragung bestanden Zweifel. Der Fragebogen sollte - wie eine Klassenarbeit - unter Aufsicht eines Lehrers möglichst in einer Schulstunde in der Klasse ausgefüllt werden.

Das Verwaltungsgericht Lüneburg musste sich mit dieser Fragebogenaktion befassen. Es hat in einem Einzelfall untersagt, einen bereits ausgefüllten Bogen auszuwerten. Als Begründung hierfür wurde angeführt, zu den Genehmigungsvoraussetzungen für derartige Umfragen zähle, dass die Betroffenen (hier die Erziehungsberechtigten) vorher auf die Freiwilligkeit an der Erhebung hingewiesen worden sind und ihr zugestimmt haben. Das Gericht hat es aber nicht für notwendig gehalten, die gesamte kreisweite Erhebung für unzulässig zu erklären.

22.2 Beihilfen für bedürftige Schüler

Eine niedersächsische Stadt gewährt bedürftigen Schülern unter bestimmten Voraussetzungen Beihilfen für Schulveranstaltungen wie z. B. Studienfahrten/Landheimaufenthalte. Die Anträge wurden bisher mit den entsprechenden Nachweisen (z. B. Bescheid über Hilfe zum Lebensunterhalt nach dem BSHG) in den Schulsekretariaten bearbeitet. Hierdurch erfuhr die Schule viele Einzelheiten über die persönlichen Lebensumstände der Erziehungsberechtigten.

Ich habe eine Änderung dieses Verfahrens veranlasst. Für alle Sozialhilfeempfänger ist nicht mehr die Schule, sondern das Sozialamt Ansprechpartner für die Gewährung dieser Beihilfen. Eine Antragsbearbeitung in den Schulen bzw. im Schulamt findet nicht mehr statt. Bei anderen Bedürftigen reicht anstatt der bislang erforderlichen Einkommensnachweise eine Erklärung über die Einkommenshöhe aus. Darüber hinaus wurden in eine Dienstanweisung für die Schulen datenschutzrechtliche Hinweise aufgenommen.

22.3 Internet-Anschluss für alle niedersächsischen Schulen

Ministerpräsident Gabriel hat in seiner Regierungserklärung vom 15. Dezember 1999 die Landesinitiative „N-21: Schulen in Niedersachsen Online" dargestellt. Es soll eine neue mit 75 Mio. Mark Landesmitteln unterlegte Multimedia-Initiative des Landes gestartet werden, die die Schulen beim Aufbruch in die Wissensgesellschaft unterstützen und fördern soll. Um die dazu notwendigen Impulse zu geben, hat die Landesregierung gemeinsam mit den kommunalen Spitzenverbänden und zahlreichen Wirtschaftsunternehmen den Verein „N-21: Schulen in Niedersachsen Online" gegründet.

Das Aktionsprogramm beinhaltet aufeinander abgestimmte Aktionen zur Ausstattung von Schulen, zur Aus- und Fortbildung von Lehrkräften, zur Entwicklung didaktischer Konzepte und multimedialer Lernumgebungen, zur Intensivierung der Ausbildung im IT- und Medienbereich sowie zur Öffnung des Zugangs zu Internet und Multimedia für breite Bevölkerungsgruppen.

Allen, die von der Initiative betroffen sind, muss die nötige Sensibilität für die Datenschutzprobleme, die die Internetnutzung mit sich bringt, vermittelt werden. Lehrer und Schüler müssen lernen, Gefahrensituationen ebenso sachgerecht einzuschätzen, wie die Möglichkeiten, diesen durch geeignete Schutzmaßnahmen zu begegnen. Daneben sind datenschutzrechtliche Fragen z. B. nach der Zulässigkeit der Veröffentlichung von Lehrer- und Schülerdaten zu klären. Insgesamt muss den Gesichtspunkten des Datenschutzes und der Datensicherheit ein erheblicher Stellenwert in der Landesinitiative zukommen. Schon bei der Multiplikatorenschulung sind diese Aspekte angemessen zu berücksichtigen. Um den Datenschutzbelangen zu nachhaltiger Wirkung zu verhelfen, habe ich dem Kultusministerium meine Mithilfe und Unterstützung angeboten.

23 Natur- und Umweltschutz

Niedersächsisches Bodenschutzgesetz

Am 19. Februar 1999 hat der Niedersächsische Landtag das „Gesetz zur Einführung des Niedersächsischen Bodenschutzgesetzes und zur Änderung des Niedersächsischen Abfallgesetzes“ beschlossen. In § 13 - Datenverarbeitung - ist geregelt, dass die zuständigen Behörden zur Ausführung des Bundes-Bodenschutzgesetzes, des Abfallgesetzes und der aufgrund dieser Gesetze erlassenen Verordnungen die für die Aufgabenerledigung erforderlichen personenbezogenen Daten verarbeiten dürfen. Der für das Liegenschaftskataster zuständigen Behörde dürfen die für die Erfüllung ihrer Aufgaben nach § 11 Abs. 4 Nr. 1 des Niedersächsischen Vermessungs- und Katastergesetzes erforderlichen Daten übermittelt werden. Weiterhin ist die Anwendung des Niedersächsischen Datenschutzgesetzes bei der Verarbeitung personenbezogener Daten im Rahmen dieser Gesetze festgeschrieben

Wenngleich die Zulässigkeit der Datenverarbeitung generalklauselartig formuliert und nur durch das Kriterium der Erforderlichkeit eingegrenzt wird, ist zumindest die Regelung zu begrüßen, dass auf die Verarbeitung personenbezogener Daten das Niedersächsische Datenschutzgesetz Anwendung findet. Es handelt sich um eine anwenderfreundliche Formulierung, die keinen Zweifel darüber lässt, welche datenschutzrechtlichen Vorschriften bei der Ausführung des Gesetzes heranzuziehen sind. Gleiches gilt für die Bestimmung, dass auch für die Verarbeitung personenbezogener Daten bei der Ausführung des Bundes-Bodenschutzgesetzes die Befugnisnormen des § 13 Niedersächsisches Bodenschutzgesetzes gelten. Es handelt sich hier um eine ähnliche Regelung wie in § 171 Niedersächsisches Wassergesetz.

Die Streichung des Sechsten Teils - Altlasten - im Niedersächsischen Abfallgesetz und die Regelung der Materie im Niedersächsischen Bodenschutzgesetz ist aus datenschutzrechtlicher Sicht gutzuheißen.

Soweit eine Einsichtnahme in das Altlastenverzeichnis (§ 6) begehrt wird, richtet sich deren Zulässigkeit nach § 4 Umweltinformationsgesetz (UIG). Nach dieser Vorschrift hat jeder Anspruch auf freien Zugang zu Informationen über die Umwelt, die bei Behörden oder bei natürlichen oder juristischen Personen des privaten Rechts vorhanden sind. Die Behörde kann auf Antrag Auskunft erteilen,

Akteneinsicht gewähren oder Informationsträger in sonstiger Weise zur Verfügung stellen.

24 Wirtschaft

24.1 Aus der Gewerbedatei ins Internet

Als Beitrag zur Wirtschaftsförderung plante eine Stadt, mit Einwilligung der Gewerbetreibenden deren in der Gewerbedatei gespeicherte Grunddaten ins Internet einstellen zu lassen. Die mit den entsprechenden Vorarbeiten beauftragte Privatfirma benötigte hierzu Name, betriebliche Anschrift und angezeigte Tätigkeiten der Gewerbetreibenden (§ 14 Abs. 8 Gewerbeordnung - GewO). Die Daten sollten der Firma im Wege einer Gruppenauskunft aus der Gewerbedatei zur Verfügung gestellt werden, um von den Gewerbetreibenden die Einwilligung zu der Veröffentlichung einholen zu können.

Nach der „Allgemeinen Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c der Gewerbeordnung (GewAnzVwV)“ vom 6. März 1996 - Ziffer 6.3.5 - waren Gruppenauskünfte an Berufsverbände, Adressbuchverlage, Markt- und Meinungsforschungsinstitute, Versicherungen, Handelsauskunfteien usw. nur über Gewerbetreibende zulässig, die der Übermittlung ausdrücklich zugestimmt haben. Dementsprechend hatte ich im XIII. TB (26.2) berichtet, dass mein Anliegen, Gruppenauskünfte nicht zuzulassen, berücksichtigt wurde.

Wenngleich die Gewerbeordnung zwischenzeitlich durch das „Zweite Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften“ vom 16. Juni 1998 erneut geändert wurde, so blieb § 14 GewO insoweit unverändert, als hinsichtlich von Gruppenauskünften erneut keine ausdrücklichen Regelungen im Gesetz geschaffen wurden. Umso mehr bin ich erstaunt, dass das Niedersächsische Ministerium für Wirtschaft, Technologie und Verkehr die GewAnzVwV inzwischen geändert und Gruppenauskünfte trotz fehlender gesetzlicher Bestimmungen nunmehr zugelassen hat, vgl. Rd.Erl. vom 19. Juni 2000, Nds. MBl. S. 431. Meine Argumente, dass beispielsweise in § 33 des Niedersächsischen Meldegesetzes und § 12 des Ausländerzentralregistergesetzes Gruppenauskünfte gesetzlich geregelt worden seien, ließ das Ministerium unberücksichtigt. Der Meinung des Ministeriums, die Zulässigkeit der Gruppenauskunft lasse sich aus § 14 Abs. 8 Satz 1 GewO i. V. m. den Materialien des Gesetzes zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 23. November 1994 und der Kommentarliteratur zur Gewerbeordnung herleiten, vermag ich mich nicht anzuschließen.

24.2 Anti-Korruptions-Register

Die Niedersächsische Landesregierung hat einen Maßnahmekatalog zur Bekämpfung der Korruption beschlossen. Der Katalog enthält ein 12-Punkte-Programm, in dem auch die Einführung eines sog. Korruptionsregisters als präventive Maßnahme vorgesehen ist.

Dabei werden Vergabesperren für Unternehmen, die sich um Aufträge der öffentlichen Hand bewerben, jedoch durch Bestechung von Amtsträgern oder Preisabsprachen den freien Wettbewerb unterlaufen, als geeignetes Mittel zur Korruptionsverhütung angesehen. Rechtliche Grundlage für Auftragssperren sind die Verdingungsordnungen VOB, VOL und VOF. Danach können Unternehmen von Aufgebotsverfahren ausgeschlossen werden, wenn sie nachweislich schwere Verfehlungen begangen haben, die ihre Zuverlässigkeit in Frage stellen. Korruption und Preisabsprachen sind - neben anderen Delikten - solche Aus-

schließungsgründe. Darüber hinaus wird die Einrichtung einer sog. Melde- und Informationsstelle bei der Oberfinanzdirektion Hannover für notwendig gehalten, bei der sich eine Vergabestelle informieren kann, ob ein Bewerber von der Vergabe öffentlicher Aufträge ausgeschlossen wurde.

Das Ministerium für Wirtschaft, Technologie und Verkehr hat den Entwurf eines Erlasses „Öffentliche Auftragsvergabe; Ausschluss von unzuverlässigen Bewerbern von der Teilnahme am Wettbewerb“ vorgelegt, der die Erhebung, Speicherung und Übermittlung von personenbezogenen Daten durch die Melde- und Informationsstelle sowie die Vergabestellen regelt.

Den Zweck des Erlasses, unzuverlässige Unternehmen von der Teilnahme am Wettbewerb auszuschließen und auf diese Weise einen wirkungsvollen Beitrag zur Bekämpfung der Korruption zu leisten, begrüße ich ausdrücklich. Die Einrichtung eines solchen Registers und die Datenverarbeitung bedarf aber einer gesetzlichen Regelung. Wesentliches Merkmal des sog. Korruptionsregisters ist, dass bei der Melde- und Informationsstelle gespeicherte und von den Vergabestellen übermittelte Daten in einer Vielzahl von Fällen weitergegeben werden. Die Einrichtung eines solchen Registers und die Datenverarbeitung sind daher als besonders intensive Eingriffe in das Grundrecht auf informationelle Selbstbestimmung anzusehen, soweit es sich um Einzelkaufleute oder die Firma einer OHG und KG handelt. In Betracht kommt ein solcher Eingriff aber auch bei juristischen Personen, z. B. einer sog. Ein-Mann-GmbH, bei denen ein Durchgriff auf die hinter ihnen stehenden natürlichen Personen möglich ist. Ähnliche Register, wie zum Beispiel das Bundeszentral-, das Gewerbezentral-, das Ausländerzentral- oder das Verkehrszentralregister werden jeweils aufgrund einer gesetzlichen Regelung geführt. Das Gesetz zur Bekämpfung der Schwarzarbeit vom 18. Juni 1997, das eine Zusammenarbeit der Behörden vorsieht, stellt keine geeignete Grundlage für den hier vorgesehenen Austausch von Daten und Informationen dar. Diese folgt vielmehr aus einer Vielzahl von Spezialbestimmungen. Sie umfassen aber nicht die Datenverarbeitung im Rahmen des sog. Korruptionsregisters. Auch die Konferenz der Innenminister und -senatoren hat auf ihrer Sitzung am 4. Mai 2000 beschlossen, dass die Schaffung (bundes-)gesetzlicher Regelungen für die Errichtung eines zentralen Korruptionsregisters für Vergabesperren befürwortet wird.

Im Unterschied zu den genannten öffentlichen Registern soll das vom Ministerium für Wirtschaft, Technologie und Verkehr vorgesehene Korruptionsregister jedoch nur einem beschränkten Kreis zugänglich und eine Datenspeicherung nur für einen relativ kurzen Zeitraum zulässig sein. Da das Recht auf informationelle Selbstbestimmung dem Einzelnen die Befugnis gibt, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, sieht der Erlass des Ministeriums für Wirtschaft, Technologie und Verkehr vor, dass die Datenverarbeitung durch die Melde- und Informationsstelle sowie die Vergabestellen auch dann zulässig sein soll, wenn die Bewerber ihre Einwilligung zu dieser Verfahrensweise erklärt haben.

Eine Einwilligung halte ich nicht für das geeignete Instrument, um diese Datenverarbeitung zu legitimieren. Eine Einwilligung setzt eine freie Willensbestimmung voraus, die hier nach den Umständen - wer seine Einwilligung nicht erteilt, wird bei der Auftragsvergabe nicht berücksichtigt - zweifelhaft ist. Vor allem aber geht es hier um die Festlegung eines generellen Verfahrens. Hierfür sind nicht eine Vielzahl von Einwilligungen, sondern ist eine generelle rechtliche Regelung die angemessene Rechtsgrundlage.

Um eine wirksame Korruptionsbekämpfung bei der Vergabe öffentlicher Aufträge bis zum In-Kraft-Treten einer (bundes-)gesetzlichen Regelung auch in Niedersachsen zu ermöglichen, habe ich zusammen mit dem Ministerium für Wirtschaft, Technologie und Verkehr eine qualifizierte Bietererklärung entwi-

ckelt, die den Belangen des Datenschutzes hinreichend Rechnung trägt. Sie sieht eine umfassende Belehrung der Betroffenen über die Bedeutung der Einwilligung, insbesondere über die Erhebung der Daten, deren Übermittlung und die Empfänger, den Verwendungszweck sowie die Möglichkeit des Widerrufs vor. Das MW hat den Erlass mittlerweile veröffentlicht (Nds. MBl. 2000, S. 611). Er wird am 1. Dezember 2000 in Kraft treten. Ich werde die praktische Umsetzung des Erlasses kritisch begleiten und auf Nachbesserungen hinwirken, soweit diese erforderlich werden.

25 Verkehr

25.1 Behindertenausweis erhalten - Führerschein weg?

In der Vergangenheit ging es häufiger um die Frage, ob Straßenverkehrsbehörden (in ihrer Eigenschaft als Führerscheinstelle) mit Informationen von anderen Behörden versorgt werden dürfen, die diese im Rahmen ihrer eigenen Aufgabenerfüllung erhalten haben. Diese Fragestellung tritt immer dann auf, wenn Informationen bekannt werden, die Zweifel an der Eignung eines Führerscheininhabers zum Führen von Kraftfahrzeugen aufkommen lassen. Während dieses Problem bisher überwiegend bei Sozialbehörden aufgetreten war (vgl. XII. TB 20.12 und XIII. TB 19.2), hatte ich aktuell über den Fall einer Petentin zu entscheiden, der das Versorgungsamt antragsgemäß einen Schwerbehindertenausweis ausgestellt hatte. Zugleich hatte es auf die Möglichkeit einer Parkerleichterung für Schwerbehinderte (Behindertenparkausweis) aufmerksam gemacht. Nachdem die Petentin von der örtlichen Straßenverkehrsbehörde einen entsprechenden Parkausweis erhalten hatte, wurde sie kurze Zeit später von derselben Behörde unter Verweis auf die nun bekannt gewordenen körperlichen Beeinträchtigungen aufgefordert, ein amtsärztliches Gutachten zum Nachweis ihrer Fahreignung vorzulegen. Ihre Fahrerlaubnis war damit akut gefährdet. Die Petentin war von dieser Vorgehensweise unliebsam überrascht, da sie über diese Datenweitergabe weder bei der Antragstellung noch bei der Ausstellung des Behindertenparkausweises informiert worden war. Sie hat mich gebeten, dieses Verfahren in datenschutzrechtlicher Hinsicht zu bewerten.

Im Ergebnis ging es - wie so häufig beim Datenschutz - um die sachgerechte Abwägung zweier widerstreitender Interessen, nämlich dem Persönlichkeitsschutz des Betroffenen auf der einen und dem öffentlichen Interesse an einer weitgehenden Reduzierung des Gefährdungspotentials im Straßenverkehr auf der anderen Seite.

Das Recht auf informationelle Selbstbestimmung der Petentin war hier insbesondere deswegen berührt, weil von dem Grundsatz der Zweckbindung abgewichen worden war. Das Zweckbindungsgebot als eine der tragenden Säulen des Datenschutzrechts verlangt, dass personenbezogene Daten nur zu dem Zweck verarbeitet werden dürfen, zu dem sie auch erhoben worden sind. Dieser Grundsatz war hier durchbrochen worden, weil die ausschließlich für den beantragten Behindertenparkausweis erhobenen Informationen anschließend zur Überprüfung der Fahreignung genutzt worden waren. Derartige Zweckdurchbrechungen sind nicht grundsätzlich ausgeschlossen. Sie bedürfen aber nach dem sog. Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahre 1983 einer normenklaren Rechtsgrundlage, die Voraussetzung, Umfang und Zweck des in der Verarbeitung liegenden Eingriffs in das Recht auf informationelle Selbstbestimmung hinreichend klar umschreibt und dem Verhältnismäßigkeitsgrundsatz Rechnung trägt. Im Straßenverkehrsrecht findet sich eine solche Grundlage nicht. An dieser Stelle will ich aber nicht verschweigen, dass in der Praxis gelegentlich auch die Ansicht vertreten wird, eine solche erlaubende Rechtsnorm sei

hier überhaupt nicht erforderlich, weil es „nur" um die Weitergabe von Daten innerhalb derselben Fachbehörde und in demselben Rechtsgebiet (hier dem Straßenverkehrsrecht) geht. Dieser Ansicht konnte und kann ich mich nicht anschließen, weil dem Grundsatz der Zweckbindung eine wesentliche Rolle bei der Verarbeitung personenbezogener Daten zukommt und es in der Sache letztlich doch um zwei völlig unabhängige Sachverhalte ging.

Auf der anderen Seite verkenne ich aber nicht, dass die Führerscheinstellen nach geltendem Recht verpflichtet sind, allen ihnen bekannt werdenden Tatsachen nachzugehen, die Bedenken an der Eignung von Fahrerlaubnisinhabern begründen könnten. Dies gilt insbesondere dann, wenn Erkrankungen oder Mängel (z. B. auch Bewegungsbehinderungen) vorliegen. In diesen Fällen kommt neben dem schärfsten Mittel, dem Entzug der Fahrerlaubnis, auch die Erteilung von Auflagen in Betracht, u. a. durch eine Beschränkung der Fahrerlaubnis auf bestimmte Fahrzeugarten oder den Einbau besonderer technischer Hilfsmittel und Vorrichtungen. Diese weitgehende Befugnis der Führerscheinstellen ist vor dem Hintergrund des hohen Gefährdungspotentials im öffentlichen Straßenverkehr zu sehen; dieses so gering wie möglich zu halten, liegt unbestritten im öffentlichen Interesse.

Im Rahmen dieser Interessenabwägung habe ich die Auffassung vertreten, dass solche zweckändernden Datenübermittlungen dann - noch - zulässig sind, wenn sie zur Abwehr einer drohenden Gefährdung von Verkehrsteilnehmern unerlässlich sind und habe dies auch der Petentin mitgeteilt. Dies setzt aber auch voraus, dass die Antragsteller für einen Behindertenparkausweis deutlich darauf hingewiesen werden, dass körperliche Beeinträchtigungen zu einer Überprüfung ihrer Fahreignung führen können, damit sie von den Konsequenzen der freiwilligen Offenbarung ihrer gesundheitlichen Situation (zu einem anderen Zweck) nicht unliebsam überrascht werden.

Da ich die Aufklärung der Betroffenen über die zweckwidrige Nutzung ihrer Daten für dringend erforderlich halte, habe ich mich an das Niedersächsische Ministerium für Wirtschaft, Technologie und Verkehr mit dem Vorschlag gewandt, zumindest den für die Ausstellung von Behindertenparkausweisen verwendeten Antragsvordruck um einen deutlichen Hinweis zu ergänzen und dies durch einen entsprechenden Erlass des Ministeriums umzusetzen.

Inzwischen hat mir das Wirtschaftsministerium mitgeteilt, dass die Beratungen auf Bund-Länder-Ebene mehrheitlich zum Ergebnis gekommen seien, eine Ergänzung des Straßenverkehrsrechts um eine erlaubende Befugnis zur zweckändernden Nutzung solcher Informationen sei nicht erforderlich. Hingewiesen wurde auch auf eine Erlassregelung in Nordrhein-Westfalen, in der den Straßenverkehrsbehörden empfohlen wird, bei der Antragsbearbeitung von Parksonderrechten die Führerscheinstelle nur dann zu informieren, wenn bisher nicht bekannte offensichtliche Eignungsmängel vorliegen. In allen anderen Fällen sollen die Betroffenen auf die allgemein geltende Verpflichtung hingewiesen werden, nur dann am Straßenverkehr teilzunehmen, wenn sie in geeigneter Weise Vorsorge getroffen haben, dass andere Verkehrsteilnehmer nicht gefährdet werden.

Ich halte diese nordrhein-westfälische Regelung für einen gangbaren Weg. Ob dies in vergleichbarer Weise auch für Niedersachsen übernommen wird, soll - so das Wirtschaftsministerium - im nächsten Jahr entschieden werden.

25.2 Parksünderdatei; ein Erfolg in der unendlichen Geschichte

Seit vielen Jahren habe ich die in Niedersachsen ohne Rechtsgrundlage bestehenden Parksünderdateien in datenschutzrechtlicher Hinsicht kritisiert - zunächst ohne Erfolg (XII. TB 30.3 und XIII. TB 27.3). Nun sind sie Geschichte: Das

Niedersächsische Innenministerium hat die nachgeordneten Behörden gebeten, die bisherigen Verfahren zur Speicherung von Verwarnungen bei Parkverstößen zum 1. Januar 2000 einzustellen.

Was war passiert? Seit Anfang der neunziger Jahre wurden die Daten von Falschparkern, die wegen dieses Verkehrsverstosses mit einem Verwarnungsgeld belegt worden waren, von einigen niedersächsischen Ordnungswidrigkeitenbehörden in einer Datei gespeichert, um auf diese Weise wiederholte Parkverstöße zu erkennen und diesen Umstand im Ordnungswidrigkeitenverfahren berücksichtigen zu können. Man mag es für sinnvoll halten, gegen hartnäckige Parksünder auf diese Weise vorzugehen. Eine die Speicherung solcher Verwarnungsgeldverfahren erlaubende gesetzliche Grundlage existierte und existiert aber nicht, zumal angenommen werden muss, dass der Gesetzgeber bewusst keine über die Eintragungspflichten im Verkehrszentralregister (bei Bußgeldern von mehr als 80 DM) hinausgehenden Speicherungen von Ordnungswidrigkeitenverfahren zulassen wollte. Folgerichtig dürfen Bagatelldelikte im Bereich des Verkehrsordnungswidrigkeitenrechts, wie typischerweise das Falschparken, nach Verfahrenserledigung nicht weiterhin gespeichert und gegen die Betroffenen verwendet werden.

Das Niedersächsische Innenministerium hielt die Fortführung dieser „Mehrfachtäterdateien“ einerseits für sinnvoll, teilte andererseits aber auch meine Auffassung, dass dies nur im Falle einer Ergänzung des Straßenverkehrsrechts zulässig wäre. In der Vergangenheit wurden daher seitens des Innenministeriums zahlreiche Gesetzgebungsinitiativen ergriffen.

Die letzte Erörterung auf Bund-/Länderebene hatte ergeben, dass diese Initiative schon auf Fachebene nicht mehrheitsfähig ist. So ist der niedersächsische Vorstoß u. a. auch deswegen mehrheitlich abgelehnt worden, weil Parkverstöße nicht zum sicherheitsrelevanten Bereich gehören und deshalb die heutige Differenzierung bei der Speicherung im Verkehrszentralregister sachgerecht ist. Außerdem stellt es eine Ungleichbehandlung dar, zwar Verwarnungen wegen Parkverstößen, nicht aber Verwarnungen aus anderem Anlass (z. B. wegen wiederholter geringfügiger Geschwindigkeitsverstöße) zu speichern. Hauptargument war jedoch, dass bei der Erteilung eines Verwarnungsgeldes dem Täter das Fehlverhalten nur vorgehalten wird, ohne darüber zu entscheiden, ob es sich tatsächlich um ein zu verwarnendes Verhalten gehandelt hat. Ein Verwarnungsgeld stellt immer nur ein Angebot an den Beschuldigten dar, das Verfahren auf diese Weise kostengünstig zu beenden. Eine Feststellung, dass der Beschuldigte die Ordnungswidrigkeit tatsächlich begangen hat, ist damit nicht verbunden, auch dann nicht, wenn der Betroffene mit der Verwarnung einverstanden ist. Daher - so die Mehrheit der Länder und der Bund - wäre es mit der grundsätzlichen Konzeption des Verwarnungsgeldverfahrens nicht zu vereinen, eine solche örtliche Speicherung zuzulassen.

Aufgrund dieses Meinungsbildes auf Bund-/Länderebene wird das Niedersächsische Innenministerium daher keine weiteren Initiativen mehr in dieser Sache ergreifen und hat die Einstellung der „Mehrfachtäterdateien“ zum Jahresbeginn 2000 veranlasst.

26 Rechtspflege

26.1 Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

Nachdem bereits 1994 ein Entwurf des Bundesrates zur Änderung des Strafverfahrensrechts (StVÄG 1994) gescheitert war, legte die Bundesregierung in der 13. Legislaturperiode einen Gesetzesentwurf zur Änderung und Ergänzung des Strafverfahrensrechts - Strafverfahrensänderungsgesetz 1996 (StVÄG 1996) -

vor. Damit sollten bereichsspezifische Regelungen zur Datenverarbeitung im Strafverfahren geschaffen werden, um das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützte Recht auf informationelle Selbstbestimmung zu gewährleisten. Der Entwurf unterfiel jedoch der Diskontinuität.

Die Bundesregierung hat in der 14. Legislaturperiode erneut den Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrens - Strafverfahrensänderungsgesetz 1999 (StVÄG 1999) - vorgelegt, der nach Abschluss der parlamentarischen Beratungen am 2. August 2000 vom Bundestag beschlossen worden ist (BGBl. I S. 1253). Das Gesetz, welches eine überarbeitete Fassung des Entwurfs aus dem Jahre 1996 darstellt, schafft Rechtsgrundlagen für die strafprozessuale Ermittlungstätigkeit, insbesondere die Fahndung und die längerfristige Observation, die Verwendung von Informationen, die in einem Strafverfahren erhoben worden sind, und die Verarbeitung personenbezogener Daten in Dateien und ihre Nutzung. Ich begrüße ausdrücklich, dass mit diesem Gesetz endlich die durch das sog. Volkszählungsurteil des Bundesverfassungsgerichts erforderlichen und seit langem überfälligen datenschutzrechtlichen Regelungen in die Strafprozessordnung eingefügt worden sind. Die Übergangsfrist zur Umsetzung des Urteils des Bundesverfassungsgerichts war seit langem abgelaufen.

Die zu diesem Zweck vorgenommenen Änderungen der Strafprozessordnung enthalten jedoch gegenüber dem Entwurf des StVÄG 1996 deutliche Verschlechterungen für den Schutz des Rechts auf informationelle Selbstbestimmung (siehe schon Anlage 1 XIV. TB). Darüber hinaus hatten mehrere Bundesländer im Bundesrat den Vermittlungsausschuss mit dem Ziel angerufen, den Strafverfolgungsbehörden zusätzliche Informationen aus der Ermittlungstätigkeit der Polizei im Bereich der Gefahrenabwehr zur Verfügung zu stellen. Trotz der Kritik der Datenschutzbeauftragten des Bundes und der Länder, die sie in einer Entschließung auf der 59. Datenschutzkonferenz vom 14. und 15. März 2000 in Hannover (Anlage 18) artikuliert haben, hat der Vermittlungsausschuss den ursprünglichen Gesetzesentwurf im Wesentlichen gebilligt, jedoch in einigen Punkten korrigiert. Bundestag und Bundesrat haben dem dabei erzielten Kompromiss zugestimmt.

Danach dürfen z. B. Informationen, die die Polizeibehörden im Bereich der Gefahrenabwehr erworben haben, uneingeschränkt für die Strafverfolgung genutzt werden. Werden diese von einem verdeckten Ermittler im Rahmen der Eigensicherung in einer Wohnung gewonnen, so ist die Verwertung dieser Informationen unter Beachtung des Art. 13 GG (Unverletzlichkeit der Wohnung) und des Grundsatzes der Verhältnismäßigkeit zulässig. Bei der Öffentlichkeitsfahndung zur Aufenthaltsermittlung oder Identitätsfeststellung unter anderem eines unbekannten Zeugen, die grundsätzlich vom Richter anzuordnen ist, bedarf die in einem Eilfall durch die Staatsanwaltschaft oder die Polizei erfolgte Anordnung bei wiederholter Ausstrahlung im Fernsehen oder im Internet nach spätestens einer Woche der richterlichen Bestätigung. Die Verwendung von personenbezogenen Daten aus Strafverfahren durch die Polizei soll insbesondere auch zur Vorbeugung und Bekämpfung von Straftaten möglich sein. Ausgeschlossen ist hingegen die Verwendung in Fällen, in denen die Polizei ausschließlich zum Schutz privater Rechte tätig wird.

Durch diese Regelungen wird die strikte Trennung der Zweckbindung von Daten aus dem Bereich der Gefahrenabwehr und der Strafverfolgung weitgehend aufgehoben und dem Schutz des allgemeinen Persönlichkeitsrechts insbesondere von unbeteiligten Zeugen nicht ausreichend Rechnung getragen. Der Gesetzgeber hat die Chance, den verfassungsrechtlich gebotenen Ausgleich zwischen dem Persönlichkeitsschutz einerseits und einer effektiven Strafverfolgung andererseits herzustellen („praktische Konkordanz"), leider nicht genutzt. Ich werde die praktische Umsetzung der Regelungen des StVÄG kritisch begleiten.

26.2 Aufbewahrungsbestimmungen im Justizbereich

Obwohl die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber mehrfach, zuletzt auf ihrer Konferenz am 7. und 8. Oktober 1999 in Rostock, aufgefordert haben, für die Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung eine formelle gesetzliche Grundlage zu schaffen, die den Anforderungen des sog. Volkszählungsgesetzes genügt (Anlage 7), ist der Gesetzgeber bislang untätig geblieben. Diese Fragen werden nach wie vor durch die Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden geregelt (Aufbewahrungsbestimmungen), bei denen es sich lediglich um Verwaltungsvorschriften handelt.

Nachdem nunmehr auch zwei Oberlandesgerichte die Notwendigkeit einer gesetzlichen Regelung über die Aufbewahrung, Aussonderung und Vernichtung der Akten anerkannt und gemahnt haben, dass die Schaffung der erforderlichen gesetzlichen Grundlage nicht länger als mittelfristige Aufgabe zu sehen, sondern alsbald in Angriff zu nehmen sei, haben die Ressortminister reagiert. Die 71. Konferenz der Justizministerinnen und -minister hat am 24. und 25. Mai 2000 in Potsdam beschlossen, eine länderoffene Arbeitsgruppe einzusetzen, die bis zum Frühjahr 2001 geeignete Vorschläge erarbeiten soll. Im Vergleich zu der früheren Untätigkeit ist dies als ein erster wichtiger Schritt zu begrüßen. Die weitere Entwicklung bleibt abzuwarten.

26.3 Genomanalyse im Strafverfahren

26.3.1 DNA-Analyse („Genetischer Fingerabdruck")

Mit dem Strafverfahrensänderungsgesetz - DNA-Analyse („Genetischer Fingerabdruck" - StVÄG) vom 17. März 1997 (BGBl. I S. 534) hat der Gesetzgeber Vorschriften über die Durchführung von molekulargenetischen Untersuchungen zur Abstammungsfeststellung und zur Ermittlung des Beschuldigten (sog. genetischer Fingerabdruck) in die Strafprozessordnung (StPO) eingefügt.

§ 81 e Abs. 1 StPO erlaubt die Untersuchung von Körpermaterial, das durch einen körperlichen Eingriff nach §§ 81 a, 81 c StPO bei dem Beschuldigten, dem Opfer bzw. Verletzten oder unbeteiligten Dritten gewonnen worden ist. Dieses Material soll molekulargenetisch ausgewertet und mit den Ergebnissen der Spurenanalyse verglichen werden. § 81 e Abs. 2 StPO gestattet die Vornahme entsprechender Untersuchungen an Spurenmaterial, das die Strafverfolgungsbehörden ohne körperlichen Eingriff aufgefunden, sichergestellt oder beschlagnahmt haben (sog. offene Spuren). Von den getroffenen Maßnahmen sind die Beteiligten gemäß § 101 Abs. 1 StPO zu benachrichtigen.

Molekulargenetische Untersuchungen dürfen gemäß § 81 a Abs. 3 StPO in dem Anlassverfahren oder einem anderen anhängigen Strafverfahren nur zur Feststellung der Abstammung oder zur Klärung der Frage vorgenommen werden, ob Spurenmaterial von dem Beschuldigten oder dem Verletzten stammt. Andere Zwecke, etwa eine Untersuchung auf äußere Körpermerkmale des Spurenlegers (z. B. Größe, Haar- und Augenfarbe) dürfen damit nicht verbunden werden. § 81 e Abs. 1 Satz 3 StPO stellt klar, dass weitergehende Gen-Analysen insbesondere mit dem Ziel der Ermittlung schutzbedürftiger Erbanlagen oder von Persönlichkeitsmerkmalen nicht zulässig sind. Soweit bei der Untersuchung solche Merkmale als Überschussinformationen anfallen, weil auch nicht codierende Abschnitte des Genoms Rückschlüsse auf Persönlichkeitsmerkmale zulassen, ist es verboten, den zur Verfügung stehenden Informationsgehalt zu erschließen. Gleichwohl festgestellte Tatsachen dürfen nicht an Dritte weitergegeben und auch nicht in das Strafverfahren eingeführt werden.

Die entnommenen Körperzellen des Beschuldigten, des Opfers oder des Verletzten sind unverzüglich zu vernichten, sobald sie nicht mehr erforderlich sind. Das ist nach dem rechtskräftigen Abschluss der anhängigen Strafverfahren der Fall. Die Vernichtungsregelung des § 81 a Abs. 3 Halbsatz 2 StPO gilt jedoch nicht für das Spurenmaterial, sodass jedenfalls eine Asservierung des offenen Materials zu Zwecken der Strafverfolgung zulässig ist.

Nach § 81 f Abs. 1 Satz 1 StPO ist nur der Richter zur Anordnung einer molekulargenetischen Untersuchung befugt. Eine Anordnung durch die Staatsanwaltschaft oder ihre Hilfsbeamten ist auch bei Gefahr im Verzuge ausgeschlossen. Der Richtervorbehalt umfasst sowohl die Untersuchung von Körper- als auch von Spurenmaterial.

Die richterliche Anordnung der molekulargenetischen Untersuchung kann nicht durch eine Einwilligung der Betroffenen ersetzt werden. Wegen der besonderen Tragweite des Eingriffs in das Persönlichkeitsrecht, die mit der Genom-Analyse verbunden ist, kommt dem Richtervorbehalt eine absolute Bedeutung zu. Bei der Bemessung der Tiefe des Eingriffs kann nicht allein auf die Art der Angaben abgestellt werden, die den Betroffenen abverlangt werden. Entscheidend sind auch ihre Nutzbarkeit und deren Verwendungsmöglichkeiten. Da auch die nicht codierenden Bereiche der DNA nicht völlig persönlichkeitsneutral sind, können Wahrscheinlichkeitsrückschlüsse auf psychische, charakter- und krankheitsbezogene Merkmale gezogen werden. Mit der DNA-Analyse wird den Behörden gleichsam der Schlüssel zum Kern der Persönlichkeit der Betroffenen an die Hand gegeben. Die damit einhergehenden Gefahren, die angesichts der mit hoher Geschwindigkeit voranschreitenden weltweiten Forschung zur Entschlüsselung des menschlichen Erbguts immer deutlicher werden, werden durch die Verknüpfung mit den - ebenfalls ungewissen - Möglichkeiten der modernen Datenverarbeitung noch verstärkt.

Im Gegensatz zu anderen Bundesländern wird in der Praxis der niedersächsischen Strafverfolgungsbehörden aus Gründen der Rechtssicherheit in allen Fällen jedenfalls für die molekulargenetische Untersuchung eine richterliche Anordnung eingeholt. Die Entnahme von Körperzellen wird dagegen auf der Grundlage einer Einwilligung der Betroffenen durchgeführt. Das ist nicht zu beanstanden, da bereits die Abnahme einer Blutprobe gemäß § 81 a StPO mit deren Einverständnis möglich ist. Dies muss dann erst recht für die Entnahme von Körperzellen gelten, bei der in die körperliche Integrität der Betroffenen nicht eingegriffen wird.

Eine wirksame Einwilligung in die Entnahme von Körperzellen setzt jedoch eine frühzeitige und umfassende Belehrung über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck und über die Empfänger der Daten voraus. Die Betroffenen sind unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie nicht verpflichtet sind, die Einwilligung zu erteilen, und sie mit Wirkung für die Zukunft widerrufen können. Die bislang verwendeten polizeilichen Vordrucke zur Abnahme von Speichelproben genügen diesen Anforderungen nicht. Trotzdem finden sie - wie zuletzt in Hannover im Rahmen eines strafrechtlichen Ermittlungsverfahrens gegen einen Serienvergewaltiger (EG-Fessel) - auch bei sog. Massenreihenuntersuchungen Verwendung, bei denen Unverdächtige freiwillig Speichelproben zum Zwecke der Abnahme eines „genetischen Fingerabdrucks“ abgeben, obwohl die Voraussetzungen des §§ 81 c Abs. 2, 81 e Abs. 1 StPO nicht vorliegen. Eine ordnungsgemäße Belehrung der Betroffenen findet nicht statt. Weder in der Ladung noch in dem Erfassungsbogen, den die Probanden unterzeichnen, werden sie darüber aufgeklärt, dass sie keine Speichelprobe abgeben müssen. Sie werden als Zeugen vorgeladen, obwohl sie keine Aussage bekunden, sondern die Abnahme von Körperzellen dulden sollen. Ihnen wird nicht eröffnet, dass ihre DNA-Identifizierungsmuster mit dem Bestand der DNA-Analyse-Datei abgeglichen werden. An der Freiwillig-

keit ihrer gleichwohl erklärten Einwilligung bestehen erhebliche Zweifel, da im Falle der Weigerung in Aussicht gestellt wird, die Entnahme einer Speichelprobe gerichtlich anordnen zu lassen. Auf diese Weise werden die engen Voraussetzungen des § 81 c StPO, der Untersuchungen und körperliche Eingriffe bei Nichtverdächtigen einschränken soll, umgangen und „freiwillige Massentests" in rechtsstaatlich bedenklicher Weise zu einem Standardverfahren kriminalistischer Ermittlungen gemacht.

Ich habe dem Niedersächsischen Innenministerium schon vor längerer Zeit Vorschläge zur Neugestaltung der Vordrucke und umfassender schriftlicher Belehrungen unterbreitet, die den Belangen des Datenschutzes ausreichend Rechnung tragen.

Der Richter hat in der Anordnung der molekulargenetischen Untersuchung den zu beauftragenden Sachverständigen zu bestimmen. Er kann gemäß § 81 f Abs. 2 Satz 1 StPO nur aus einem begrenzten Personenkreis ausgewählt werden. Dazu zählen öffentlich bestellte oder nach dem Verpflichtungsgesetz verpflichtete Sachverständige. In Betracht kommen auch Amtsträger, die jedoch der ermittelnden Behörde nicht angehören oder organisatorisch und sachlich von der jeweiligen Dienststelle getrennt sind. § 81 f Abs. 2 Satz 2 und 3 StPO schreiben weitere datenschutzrechtliche Vorkehrungen vor. Der Sachverständige ist verpflichtet, technische und organisatorische Maßnahmen zu ergreifen, um auszuschließen, dass unzulässige molekulargenetische Untersuchungen stattfinden. Zu empfehlen ist die Schaffung eines ständig zu aktualisierenden Verzeichnisses anerkannter Methoden der DNA-Analyse und dessen Einbindung in die Richtlinien für das Straf- und Bußgeldverfahren (RiStBV. Dritte dürfen nicht unbefugt Kenntnis von den Untersuchungs- und Zwischenergebnissen erlangen. Darüber hinaus kommt eine Verschlüsselung des Untersuchungsmaterials und der gewonnenen Daten in Betracht, sobald der Stand der Untersuchung dies erlaubt. Dem Sachverständigen ist das Untersuchungsmaterial ohne Mitteilung des Namens, der Anschrift und des Geburtstages und -monats des Betroffenen zu übergeben (Anonymisierung). Ist der Sachverständige eine nichtöffentliche Stelle, eröffnet § 81 f Abs. 2 Satz 4 StPO die Möglichkeit der Kontrolle durch den Landesbeauftragten für den Datenschutz Niedersachsen ohne Anlass und selbst dann, wenn eine Verarbeitung in Dateien nicht erfolgt.

26.3.2 DNA-Identitätsfeststellungsgesetz (DNA-Analyse-Datei)

Durch das Gesetz zur Änderung der Strafprozessordnung (DNA-Identitätsfeststellungsgesetz - DNA-IFG) vom 7. September 1998 (BGBl. I S. 2646) und das Gesetz zur Änderung des DNA-Identitätsfeststellungsgesetzes vom 2. Juni 1999 (BGBl. I S. 1242) hat der Gesetzgeber Vorschriften über die Entnahme von Körperzellen, deren molekulargenetische Untersuchung und die Speicherung der DNA-Identifizierungsmuster geschaffen, die der Vorsorge für die künftige Strafverfolgung dienen. Von § 81 g StPO werden Personen erfasst, die gegenwärtig als Beschuldigte einer Straftat von erheblicher Bedeutung verfolgt werden, und bei denen aufgrund bestimmter Umstände anzunehmen ist, dass zu einem späteren Zeitpunkt weitere vergleichbare Strafverfahren gegen sie zu führen sein werden. § 2 DNA-IFG erstreckt die nach § 81 g StPO zulässigen Maßnahmen auf rechtskräftig Verurteilte und ihnen gleichgestellte Personen, sofern die Eintragung im Bundeszentral- oder Erziehungsregister noch nicht getilgt ist.

Diese Vorschriften haben die Aufgabe, eine schnellere Täteridentifizierung und damit eine bessere Aufklärung von schweren Straftaten, insbesondere im Bereich der Sexual- und Tötungsdelikte zu bewirken. Durch die Aufnahme der DNA-Identifizierungsmuster in die beim Bundeskriminalamt (BKA am

17. April 1998 errichtete Verbundanwendung „DNA-Analyse-Datei“ soll darüber hinaus der noch effizientere Betrieb dieser Datei sichergestellt werden.

§ 81 g Abs. 1 StPO gestattet körperliche Eingriffe zur DNA-Identitätsfeststellung nur in der Form einer Entnahme von Körperzellen. Diese Maßnahme ist aber nur zulässig, wenn sie zur Erreichung ihres Zwecks auch erforderlich ist. Das ist z. B. nicht der Fall, wenn den Strafverfolgungsbehörden ein für spätere Identifizierungszwecke geeignetes DNA-Muster aufgrund von früheren Maßnahmen nach §§ 81 e und 81 f StPO bereits zur Verfügung steht. Auf welche Art die Entnahme zu erfolgen hat, schreibt das Gesetz nicht vor. In der polizeilichen Praxis wird im Regelfall ein Abstrich von Schleimhautzellen in der Mundhöhle vorgenommen. In Betracht kommt aber auch eine Blutprobe, die von einem Arzt abzunehmen ist. Die Vorschrift gestattet darüber hinaus die molekulargenetische Untersuchung des gewonnenen Körpermaterials. Diese Regelung entspricht den in § 81 e StPO getroffenen Bestimmungen. Sie war erforderlich, weil sich der Anwendungsbereich des § 81 e StPO nicht auf den in § 81 g StPO genannten Fall erstreckt. Der Zweck dieser Maßnahmen besteht in der Identitätsfeststellung in künftigen Strafverfahren. Die Entnahme von Körperzellen darf daher nur mit dem Ziel erfolgen, Material für die nachfolgende molekulargenetische Untersuchung zu gewinnen. Diese ist wiederum auf das Ziel der Feststellung des DNA-Identifizierungsmusters gerichtet (§ 81 g Abs. 2 Satz 1 StPO).

Die Maßnahmen dürfen sich nur gegen einen Beschuldigten bzw. Verurteilten richten, der verdächtig ist, eine Straftat von erheblicher Bedeutung begangen zu haben. Als Beispiele nennt das Gesetz Verbrechen, Vergehen gegen die sexuelle Selbstbestimmung, gefährliche Körperverletzung, Diebstahl in einem besonders schweren Fall oder Erpressung. Als Anhaltspunkt dafür, wann eine solche Straftat in Betracht kommt, ist der als Anlage zu § 2 c DNA-IFG genannte - nicht abschließende - Straftatenkatalog anzusehen. Die Entnahme von Körperzellen und deren Untersuchung sind nur zulässig, wenn eine Wiederholungsgefahr besteht. Aufgrund der Art und Ausführung der Anlasstat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse muss eine sog. Negativprognose gestellt werden, d.h. es ist eine weitere „kriminelle Karriere“ wegen vergleichbarer Taten zu erwarten.

§ 81 g Abs. 3 StPO verweist für die Zuständigkeit zur Anordnung der Maßnahmen und die datenschutzrechtlichen Vorkehrungen auf §§ 81 a Abs. 2, 81 f StPO. Für die Entnahme von Körperzellen bedarf es gemäß § 81 a Abs. 2 StPO grundsätzlich einer richterlichen Anordnung. Dadurch soll gewährleistet werden, dass auch die Gefahrenprognose durch den Richter getroffen wird. Im Eilfall sind auch die Staatsanwaltschaft oder ihre Hilfsbeamten zur Anordnung befugt. Die Entnahme von Körperzellen ist ebenso wie bei Maßnahmen nach § 81 e StPO zulässig, wenn der Beschuldigte bzw. Verurteilte wirksam eingewilligt hat. Bei inhaftierten Verurteilten ist jedoch zu gewährleisten, dass ihre Entscheidung, die Einwilligung zu erteilen oder sie zu verweigern, keine Auswirkungen auf Maßnahmen im Vollzug hat. Wird die Gewährung von Vollzugslockerungen davon abhängig gemacht, dass der Verurteilte einwilligt, kann von einer freiwilligen Entscheidung keine Rede sein.

Die Anordnung der molekulargenetischen Untersuchung ist gemäß §§ 81 g Abs. 3, 81 f Abs. 1 StPO allein dem Richter vorbehalten. Sie kann nicht durch die Einwilligung der Betroffenen ersetzt werden, denn dadurch wären sie gezwungen, sich selbst eine negative Prognose zur Begehung künftiger Straftaten zu stellen. Es ist jedoch niemand gezwungen, durch aktives Tun an seiner eigenen Strafverfolgung mitzuwirken. Gerade das würde ein Beschuldigter bzw. Verurteilter aber tun, wenn er in die molekulargenetische Untersuchung einwilligt, auch wenn er sie lediglich dulden muss. Die Untersuchung erfolgt allein zu dem Zweck, das DNA-Identifizierungsmuster in der DNA-Analyse-Datei zu

speichern. Ein Vergleich des DNA-Profils mit dem Spurenmaterial eines Strafverfahrens soll die schnelle Identifizierung des Täters ermöglichen. Der Einwilligung kommt damit faktisch eine selbstbezichtigende Wirkung zu, da der Betroffene allein durch den Abgleich der DNA-Profile überführt werden kann. Dieser mit der Einwilligung verbundene Zwang zur Selbstbelastung entfällt bei einem ausschließlichen Richtervorbehalt. Die 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher am 7. und 8. Oktober 1999 in Rostock eine Entschließung gefasst, dass DNA-Analysen zur vorbeugenden Verbrechensbekämpfung nur aufgrund einer richterlichen Anordnung zulässig sein sollten (Anlage 9). Die niedersächsischen Strafverfolgungsbehörden führen in der Praxis aus Gründen der Rechtssicherheit auch hier in allen Fällen eine richterliche Anordnung herbei. Bestrebungen, die Untersuchung der Körperzellen auf der Grundlage von Einwilligungen zu ermöglichen, werde ich mit Nachdruck entgegen treten.

Über die Schutzvorkehrungen des § 81 f Abs. 2 StPO hinaus, auf die § 81 g Abs. 3 StPO verweist, enthält § 81 g Abs. 2 StPO eine Vielzahl von Bestimmungen, die den Belangen des Datenschutzes Rechnung tragen sollen. § 81 g Abs. 2 Satz 1 Halbsatz 1 StPO stellt eine strenge Zweckbindung auf. Entnommene Körperzellen dürfen nur zur Feststellung des DNA-Identifizierungsmusters zur Vorsorge für die künftige Strafverfolgung genutzt werden. Andere Untersuchungen, etwa zu Zwecken der Forschung oder der Gefahrenabwehr, sind unzulässig. Das Vernichtungsgebot des § 81 g Abs. 2 Satz 1 Halbsatz 2 StPO erstreckt sich auf das gesamte dem Beschuldigten entnommene Körpermaterial, ungeachtet der Frage, ob es für die molekulargenetische Untersuchung verwendet worden ist oder nicht. Es umfasst auch Zwischenprodukte und aufbereitetes Material, um zu einem späteren Zeitpunkt auftretende Missbräuche zu verhindern. § 81 g Abs. 2 Satz 2 StPO begründet ein Feststellungs- und Untersuchungsverbot, das sich an die in § 81 e Abs. 1 Satz 3 StPO getroffene Regelung anlehnt. Es soll gewährleisten, dass Untersuchungen, die auf die Erstellung eines „Persönlichkeitsprofils" gerichtet wären, unterbleiben.

Die DNA-Identifizierungsmuster dürfen dagegen nach den Vorschriften des Bundeskriminalamtgesetzes (BKAG verarbeitet und genutzt werden (§ 3 DNA-IFG). Während der Gesetzgeber für die Gewinnung von Körperzellen und deren Untersuchung detaillierte Vorschriften in die Strafprozessordnung eingefügt hat, bleiben die Regelungen zur Speicherung unausgewogen und lückenhaft (§§ 32, 34 BKAG). So ergibt sich aus diesen Vorschriften nur in Verbindung mit der jeweils gültigen Errichtungsanordnung die im Einzelfall zulässige Dauer der Speicherung. Die Errichtungsanordnung sieht zudem vor, dass eine Speicherung solcher DNA-Identifizierungsmuster zulässig sein soll, die auf der Grundlage einer Einwilligung des Betroffenen in die molekulargenetische Untersuchung erlangt worden sind. Damit wird der gesetzlich vorgesehene Richtervorbehalt unterlaufen. Bei Verurteilten oder ihnen gleichgestellten Personen im Sinne von § 2 DNA-IFG ist bislang nicht geklärt, welche Folgen die Tilgung der Eintragung im Bundeszentral- oder Erziehungsregister für die Speicherung hat.

DNA-Identifizierungsmuster eines Beschuldigten, die nach § 81 e StPO gewonnen worden sind, dürfen gemäß § 3 Satz 3 DNA-IFG unter den Voraussetzungen des § 81 g Abs. 1 StPO in der DNA-Analyse-Datei gespeichert werden. Der Gesetzgeber hat von einer Verweisung auf § 81 g Abs. 3 StPO, der eine richterliche Anordnung statuiert, abgesehen, weil er der Ansicht war, die molekulargenetische Untersuchung der Körperzellen gemäß § 81 e StPO ordne in jedem Fall ein Richter an. Er hat dabei jedoch übersehen, dass der Richter bei seiner Entscheidung gemäß § 81 e StPO nicht zugleich über die Voraussetzungen des § 81 g Abs. 1 StPO entscheidet. Das hat zur Folge, dass die DNA-Identifizierungsmuster eines Beschuldigten ohne richterliche Entscheidung allein auf der Grundlage einer polizeilichen Prognose in die DNA-Analyse-Datei

eingestellt werden. Auf diese Weise wird der Richtervorbehalt umgangen, dem - wie dargelegt - eine besondere Bedeutung zukommt. Ich habe gegenüber dem Niedersächsischen Innenministerium deutlich gemacht, dass zukünftig in allen Fällen ein sog. Doppelbeschluss herbeigeführt werden muss, in denen die materiellen Voraussetzungen der §§ 81 e und 81 g StPO vorliegen. Auf diese Weise wird gewährleistet, dass ein Richter die Negativprognose stellt. Eine Antwort des Ministeriums steht auch hier noch aus.

Ich habe eine datenschutzrechtliche Kontrolle von DNA-Maßnahmen einzelner Polizeibehörden und Staatsanwaltschaften eingeleitet und in die Kontrolle auch die in Hannover durchgeführte Massenreihenuntersuchung (EG-Fessel) einbezogen. Im Rahmen der Kontrolle sollen neben den organisatorischen und technischen Vorkehrungen zum Datenschutz die Erhebung der DNA-Identifizierungsmuster durch die Entnahme und molekulargenetische Untersuchung von Körperzellen, deren Speicherung in der DNA-Analyse-Datei und schließlich der Abruf, die Übermittlung und die sonstige Verarbeitung bzw. Nutzung der personenbezogenen Daten untersucht werden. Die Kontrolle erstreckt sich auf entsprechende Daten in der Spuren- und der Personendatei der DNA-Analyse-Datei. Es werden sowohl Verfahren untersucht, bei denen Körperzellen aufgrund einer Einverständniserklärung der Betroffenen entnommen worden sind, als auch Verfahren, bei denen die DNA-Analyse aufgrund einer richterlichen Anordnung erfolgt ist. Die Kontrolle ist bislang noch nicht abgeschlossen.

26.4 Parlamentarische Kontrolle des sog. „Großen Lauschangriffs“

Mit dem Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität vom 4.5.1998 (BGBl. I S. 845) wurde in § 100 c Abs. 1 Nr. 3 Strafprozessordnung (StPO) der politisch umstrittene Einsatz technischer Mittel zur akustischen Überwachung von Wohnungen zu repressiven Zwecken eingeführt - sog. „Großer Lauschangriff“ (vgl. XIV.TB 27.4). Dazu wurde Art. 13 Grundgesetz (GG) durch das Gesetz zur Änderung des Grundgesetzes (Artikel 13) vom 26.3.1998 (BGBl. I S. 610) neu gefasst.

Durch den Einsatz technischer Mittel zur akustischen Wohnraumüberwachung, der gemäß Art. 13 Abs. 4 und 5 GG auch zu präventiven Zwecken zulässig ist, kann in das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG), das allgemeine Persönlichkeitsrecht und den dadurch gewährleisteten Schutz der Privatsphäre, das Recht am gesprochenen Wort und das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) eingegriffen werden. Um eine effektive Kontrolle der Exekutive durch das Parlament auf diesem Gebiet der besonders intensiven Grundrechtseingriffe zu schaffen, verpflichtet Art. 13 Abs. 6 Satz 1 GG die Bundesregierung zur jährlichen Unterrichtung des Bundestages über die Maßnahmen nach Art. 13 Abs. 3 bis 5 GG. Ein vom Bundestag gewähltes Gremium übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus. § 100 e Strafprozessordnung (StPO) konkretisiert die Berichtspflicht in der Weise, dass die Bundesregierung den Bundestag auf der Grundlage der Mitteilungen der Staatsanwaltschaften an die obersten Landesjustizbehörden über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahme zu unterrichten hat.

Es handelt sich dabei nicht um eine parlamentarische Kontrolle, die den gerichtlichen Rechtsschutz ersetzen könnte. Der Bundestag überprüft also nicht die Rechtmäßigkeit jeder einzelnen Überwachungsmaßnahme, sondern die „Normeffizienz“ von Art. 13 Abs. 3 bis 5 GG und der zu seiner Ausführung ergangenen einfachgesetzlichen Regelungen (§§ 100 c bis 101 StPO). Die Normeffizienz ist sowohl an der Frage zu messen, ob die Überwachungsmaßnahmen die

Strafverfolgung und die Gefahrenabwehr verbessern, als auch daran, ob die gesetzgeberischen Maßnahmen zur Sicherung der Grundrechte ihre Wirkung entfalten.

Die Bundesregierung hat am 27. Dezember 1999 den ersten Bericht (BT-Drs. 14/2452) vorgelegt, der über Maßnahmen nach Art. 13 Abs. 3 GG i. V. m. § 100 c Abs. 1 Nr. 3 StPO im Jahr 1998 informiert. In Niedersachsen sind lediglich zwei (!) Maßnahmen durchgeführt worden, von denen nur eine Relevanz für das Verfahren gehabt hat.

Der Bericht ermöglicht nur eine eingeschränkte parlamentarische Kontrolle. Wesentliche Informationen, die bewertende Aussagen zur Effizienz der Maßnahmen und zur Intensität der damit verbundenen Grundrechtseingriffe ermöglichen, fehlen. Die Datenschutzbeauftragten des Bundes und der Länder haben daher am 26. Juni 2000 eine Entschließung gefasst, in der die Bundesregierung aufgefordert wird, die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der gerichtlichen Anordnung genannten, anzugeben, und die Berichte in Anlehnung an die sog. „Wire-tap-Reports" der Vereinigten Staaten von Amerika zu ergänzen, um eine wirksame parlamentarische Kontrolle zu gewährleisten (Anlage 21).

Der Bundestag hat die Berichtspflicht durch eine Entschließung vom 16. Januar 1998 ergänzt, derzufolge die Bundesregierung unabhängig von der Pflicht gemäß Art. 13 Abs. 6 Satz 1 GG spätestens zum 31. Januar 2002 einen detaillierten Erfahrungsbericht vorzulegen hat, um eine parlamentarische Gesetzesfolgenabschätzung vornehmen zu können (BT-Drs. 13/9644, 13/9661 S. 8). Der Bundestag ist offensichtlich der Meinung, die jährlichen Berichte der Bundesregierung würden eine solche Einschätzung nicht erlauben. Spätestens zu diesem Zeitpunkt wird der Bundestag entscheiden müssen, ob der „Große Lauschangriff" als besonders intensiver Grundrechtseingriff trotz der geringen praktischen Bedeutung (1998: insgesamt nur neun Maßnahmen) weiterhin erforderlich ist.

Nach Art. 13 Abs. 6 Satz 3 GG gewährleisten die Länder eine gleichwertige parlamentarische Kontrolle, was Ausdruck des sich aus Art. 28 Abs. 1 Satz 1 GG ergebenden Homogenitätsprinzips ist. Die parlamentarische Kontrolle der Länder bezieht sich zunächst auf präventive polizeiliche Maßnahmen zur akustischen Wohraumüberwachung, die im Zuständigkeitsbereich der Länder stattgefunden haben (Art. 13 Abs. 4 und 5 GG). In Niedersachsen unterrichtet das Innenministerium gemäß § 37 Niedersächsisches Gefahrenabwehrgesetz (NGefAG) in Abständen von sechs Monaten ein Kontrollgremium des Niedersächsischen Landtages über die akustischen Maßnahmen zur Überwachung von Wohnungen nach § 35 NGefAG. Die Forderungen der Datenschutzbeauftragten des Bundes und der Länder gelten gleichermaßen für diese Berichte, soweit sie hinter den Anforderungen für eine wirksame parlamentarische Kontrolle zurück bleiben.

Der Niedersächsische Landtag muss auch über die nach Art. 13 Abs. 3 GG i. V. m. § 100 c Abs. 1 Nr. 3 StPO von den Strafverfolgungsbehörden vorgenommenen repressiven Überwachungsmaßnahmen unterrichtet werden. Die Datenschutzbeauftragen des Bundes und der Länder haben in einer weiteren Entschließung vom 17. Juni 1999 (Anlage 5) deutlich gemacht, dass das Grundgesetz eine effektive parlamentarische Kontrolle der „Großen Lauschangriffe" auch auf Landesebene vorschreibt. Bei Maßnahmen zur Strafverfolgung durch Landesbehörden besteht die parlamentarische Verantwortlichkeit gegenüber den Landesparlamenten.

Das Niedersächsische Justizministerium, das zunächst der Meinung war, im Bereich der Strafverfolgung bestehe keine Pflicht der Landesregierung zur Bericht-

erstattung gegenüber dem Landtag, ist nunmehr in Übereinstimmung mit dem Präsidenten des Niedersächsischen Landtages der Auffassung, dass es auch in diesem Bereich einer umfassenden parlamentarischen Kontrolle und einer gesetzlichen Regelung bedarf. Diese sollte gewährleisten, dass die vom Niedersächsischen Justizministerium vorzulegenden Berichte über die nach § 100 c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen im Plenum des Niedersächsischen Landtages öffentlich beraten und erörtert werden können. Ich habe dem Niedersächsischen Justizministerium vorgeschlagen, sich dafür einzusetzen, den Rechts- und Verfassungsausschuss des Niedersächsischen Landtages mit der Vorbereitung der Erörterung im Plenum zu betrauen. Eine Antwort steht noch aus.

26.5 Evaluation der Überwachung der Telekommunikation

Die Überwachung der Telekommunikation gemäß §§ 100 a, 100 b StPO stellt einen erheblichen Eingriff in das durch Art. 10 Grundgesetz (GG) geschützte Fernmeldegeheimnis dar. Indem das Grundrecht die einzelnen Kommunikationsvorgänge dem staatlichen Zugriff entzieht, will es zugleich die Bedingungen einer freien Telekommunikation überhaupt aufrechterhalten. Mit der Verbürgung der Unverletzlichkeit des Fernmeldegeheimnisses soll vermieden werden, dass der Meinungs- und Informationsaustausch mittels Fernmeldeanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen.

Die Telekommunikation kann aber auch dafür missbraucht werden, Straftaten zu planen und zu verabreden. Um diese verhindern oder verfolgen zu können, bedarf es der Beschränkung des Fernmeldegeheimnisses. Sie ist gemäß Art. 10 Abs. 2 GG möglich, soweit ein legitimer Gemeinwohlzweck vorliegt und der Eingriff in das Fernmeldegeheimnis geeignet und erforderlich ist, um den Zweck zu erreichen. Die Verfolgung von schweren Straftaten, dem die Überwachung der Telekommunikation gemäß §§ 100 a, 100 b Strafprozessordnung (StPO) dienen soll, stellt einen solchen Zweck dar. Dabei erfasst die Überwachung alle Formen der Nachrichtenübermittlung mittels technischer Einrichtungen insbesondere durch Mobilfunk, Satellitenübertragung, Bildtelefon, Telex, Teletex, Telebox, Fernschreiben, die Kommunikation mit Online-Diensten und Videodienste. Auch die Übertragung von Daten im Netzbereich (Mailbox, Internet) fällt darunter.

Auf diese Weise können sich die Strafverfolgungsbehörden nicht nur von den Inhalten und Umständen einer Telekommunikation Kenntnis verschaffen, sondern über die Verbindungsdaten auch konkrete Bewegungsprofile erstellen. Dabei greifen sie in die Grundrechte Beschuldigter und auch in diejenigen unbeteiligter Dritter ein. Wegen der besonderen Bedeutung dieses Eingriffsinstrumentes habe ich in der Vergangenheit (vgl. XIV. TB 27.6.1) bereits mehrfach eine effektive Erfolgskontrolle angemahnt. Nur auf diese Weise lässt sich überprüfen, ob die Befugnisse der Strafverfolgungsbehörden zur Überwachung und Aufzeichnung des Fernmeldeverkehrs geeignet und erforderlich sind, schwere Straftaten wirksam zu bekämpfen. Die von den Landesjustizverwaltungen eingeführten statistischen Erhebungen sind insoweit nicht aussagekräftig. Ihnen fehlen wesentliche Angaben, die eine bewertende Aussage zur Effizienz der Maßnahmen und der Intensität der damit verbundenen Grundrechtseingriffe ermöglichen.

Die Notwendigkeit einer effektiven Erfolgskontrolle hat auch das Bundesministerium der Justiz erkannt. Es hat im August 1999 ein Forschungsvorhaben zur

Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO öffentlich ausgeschrieben und an das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg vergeben. Das Institut konnte mit den Arbeiten jedoch noch nicht sofort beginnen, da die Strafprozessordnung bislang keine Forschungsklausel enthielt, die eine Informationsübermittlung für wissenschaftliche Zwecke regelt. Um die Durchführung des Vorhabens zu beschleunigen, hatte die 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber in einer Entschließung aufgefordert, das Gesetzgebungsverfahren zum StVÄG 1999 zügig abzuschließen, damit die entsprechende Befugnisnorm für die Datenübermittlung zu Forschungszwecken als sichere gesetzliche Grundlage endlich zur Verfügung steht (Anlage 18).

Der Bundesgesetzgeber hat mittlerweile das Gesetzgebungsverfahren abgeschlossen (vgl. 26.3) und das Strafverfahrensänderungsgesetz 1999 - StVÄG 1999 - am 2. August 2000 beschlossen (BGBl. I, S. 1253). Eine Forschungsklausel ist nunmehr in §§ 476 i. V. m. 477 Abs. 2 Satz 3 StPO enthalten. Sie erlaubt Einrichtungen, die wissenschaftliche Forschung betreiben, die Verarbeitung und Nutzung personenbezogener Daten, soweit es für die Durchführung bestimmter Forschungsvorhaben erforderlich ist.

26.6 Täter-Opfer-Ausgleich

Der durch das Verbrechensbekämpfungsgesetz vom 28. Oktober 1994 (BGBl. I S. 3186) in das Strafgesetzbuch (StGB) eingefügte § 46 a über den Täter-Opfer-Ausgleich (TOA und die Schadenswiedergutmachung erlaubt den Gerichten, eine Entschädigung des Opfers durch den Täter oder auch nur sein ernsthaftes Bemühen um einen Täter-Opfer-Ausgleich strafmildernd zu berücksichtigen oder sogar ganz von Strafe abzusehen. In bestimmten Fällen kann gemäß § 153 b Strafprozessordnung (StPO) auch bereits die Staatsanwaltschaft mit Zustimmung des Gerichts von der Erhebung einer öffentlichen Klage Abstand nehmen. Zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs sind durch das Gesetz vom 20. Dezember 1999 die §§ 155 a und 155 b in die StPO eingefügt und § 153 a Abs. 1 StPO ergänzt worden.

Die Vorschriften der §§ 155 a und 155 b StPO enthalten keine detaillierten verfahrenstechnischen Vorgaben, damit Raum für landesrechtliche Regelungen bleibt, die den jeweils landesspezifischen Gegebenheiten und entwickelten Konzepten zur Durchführung des TOA Rechnung tragen. Die einheitliche Anwendung des TOA, der in Niedersachsen im Rahmen von Modellversuchen seit längerer Zeit auch bei Strafsachen gegen Erwachsene praktiziert wird (vgl. LT-Drs. 14/750), regelt die am 1. Mai 2000 in Kraft getretene Richtlinie für den Täter-Opfer-Ausgleich im allgemeinen Strafrecht (TOA-Richtlinie).

Die zentrale datenschutzrechtliche Frage ist, unter welchen Voraussetzungen öffentliche und private Ausgleichsstellen zur Durchführung des TOA umfassende Informationen, insbesondere über Opfer von Straftaten, erhalten. Gemäß § 155 b Abs. 1 Satz 1 StPO können die Staatsanwaltschaft und das Gericht zum Zweck des TOA einer von ihnen mit der Durchführung beauftragten Stelle von Amts wegen oder auf deren Antrag die hierfür erforderlichen personenbezogenen Daten übermitteln. Eine Einwilligung der Betroffenen ist nicht vorgesehen. Die Übermittlung unterbleibt nur bei einem dem TOA ausdrücklich entgegenstehenden Willen des Verletzten (§ 155 a Satz 3 StPO). Die Achtung und die wirksame Unterstützung der Opfer von Straftaten ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können aber nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an die Ausgleichsstellen den Willen und die Eigenverantwortung der Opfer uneingeschränkt res-

pektieren. Deshalb sollten personenbezogene Daten nur mit Einwilligung des Opfers an die Ausgleichsstellen übermittelt werden, wie die Datenschutzbeauftragten des Bundes und der Länder bereits in ihrer Entschließung vom 7. und 8. Oktober 1999 (Anlage 13) betont haben.

Die TOA-Richtlinie sieht keine entsprechende Regelung vor, sondern statuiert, dass die Staatsanwaltschaft der beauftragten Stelle die zur Durchführung des TOA erforderlichen Daten übermittelt. Dabei hat die Staatsanwaltschaft die datenschutzrechtliche Regelung des § 155 b Abs. 1 StPO zu beachten. Diese Vorschrift schreibt eine strikte Zweckbindung vor. Personenbezogene Informationen der Betroffenen dürfen nur für Zwecke des TOA oder der Schadenswiedergutmachung und nur, soweit sie erforderlich sind, übermittelt werden. Dazu dürfen der beauftragten Stelle nach § 155 Abs. 1 Satz 1 StPO Akten zur Einsichtnahme übersandt werden, soweit dies erforderlich ist. Gemäß § 155 Abs. 1 Satz 2 StPO dürfen Akten „auch" übersandt werden, soweit die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordern würde. Durch den Verweis auf die Regelung des § 155 b Abs. 1 StPO ist eine Übersendung der Akten an die beauftragte Stelle nach Landesrecht ohne weiteres mit der Begründung möglich, die Erteilung von Auskünften erfordere einen Aufwand, der außer Verhältnis zu dem beabsichtigten Zweck - der Information der Ausgleichsstellen - stehe. Es ist durch geeignete Maßnahmen sicherzustellen, dass die Aktenübersendung der Ausnahme- und nicht der Regelfall ist, um dem Grundsatz der Erforderlichkeit der Datenübermittlung Geltung zu verschaffen.

Die Konfliktschlichtungsstellen haben aufgrund der TOA-Richtlinie bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten § 155 b Abs. 2 bis 4 StPO zu beachten. Absatz 2 schreibt zwar vor, dass die Erhebung und Verarbeitung von Daten durch die beauftragte Stelle nur zulässig ist, soweit dies für die Durchführung des TOA und der Schadenswiedergutmachung erforderlich ist und der Betroffene eingewilligt hat. Die Regelung berücksichtigt aber nicht hinreichend die Anforderungen, die das NDSG an die Einwilligung stellt. Ich habe daher das Justizministerium gebeten, bei einer zukünftigen Überarbeitung der TOA-Richtlinie in diese eine Vorschrift aufzunehmen, die eine umfassende Belehrung und eine schriftliche Einwilligung der Betroffenen vorschreibt.

26.7 Mitteilungen zum Wählerverzeichnung nach Nr. 12 MiStra

Wird jemand wegen eines Verbrechens zu einer Freiheitsstrafe von mindestens einem Jahr verurteilt, verliert er gemäß § 45 Abs. 1 StGB für die Dauer von fünf Jahren automatisch das passive Wahlrecht, d.h. die Fähigkeit, Rechte aus öffentlichen Wahlen zu erlangen. Soweit das Gesetz es besonders vorsieht, kann das Gericht einem Verurteilten, der zu einer Freiheitsstrafe von weniger als einem Jahr verurteilt worden ist, gemäß § 45 Abs. 2 und 5 StGB für die Dauer von zwei bis fünf Jahren sowohl das passive als auch das aktive Wahlrecht aberkennen. Im letzteren Fall verliert er dann das Recht, in öffentlichen Angelegenheiten zu wählen oder abzustimmen.

Die Staatsanwaltschaft unterrichtet nach Nr. 12 der Anordnung über Mitteilungen in Strafsachen (MiStra, die auf § 13 Abs. 1 Nr. 5 Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG) beruht, die für das Wählerverzeichnis zuständigen Gemeinden. Der Verlust des Wahlrechts wird nach § 45 a Abs. 1 StGB mit der Rechtskraft des Urteils wirksam. Mitzuteilen ist nur die Tatsache der rechtskräftigen Verurteilung. In den Fällen des § 45 Abs. 2 und 5 StGB ist ergänzend der Zeitraum mitzuteilen, für den das erkennende Gericht das aktive bzw. passive Wahlrecht aberkannt hat. Die Mitteilung enthält keine Informationen zu Beginn und Ende der Nebenfolge, da sie gemäß § 45 a Abs. 2 Satz 1

StGB erst von dem Tage an gerechnet werden kann, an dem die Freiheitsstrafe verbüßt, verjährt oder erlassen worden ist.

Über den Endzeitpunkt des Verlustes des Wahlrechts, den die Staatsanwaltschaft nach Erledigung der Vollstreckung der Freiheitsstrafe errechnet, wird das Bundeszentralregister informiert. Eine Unterrichtung der Gemeinden erfolgte bislang nicht, weil Nr. 12 MiStra bzw. § 13 Abs. 1 Nr. 5 EGGVG sog. Folgemitteilungen nur für den Fall der vorzeitigen Wiederverleihung des aktiven bzw. passiven Wahlrechts vorsah. Dadurch bestand die Gefahr, dass jemand zu Wahlen und Abstimmungen, z. B. zum Deutschen Bundestag oder zum Niedersächsischen Landtag, nicht zugelassen wurde, obwohl sich die Nebenfolge durch Zeitablauf erledigt, die für das Wählerverzeichnis zuständige Gemeinde davon aber keine Kenntnis erlangt hatte.

Mittlerweile ist beabsichtigt, Nr. 12 MiStra dahin gehend zu ändern, dass bei Mitteilungen zum Wählerverzeichnis auch der später errechnete Zeitpunkt des Ablauf der Nebenfolge oder die Wiederverleihung der Fähigkeiten und Rechte mitzuteilen sind. Diese Mitteilung soll an den Empfänger der Erstmitteilung und an die zuständige Gemeinde gerichtet werden. Auf diese Weise wird erreicht, dass Verurteilte ihr Wahlrecht nur für den gesetzlich vorgesehenen oder vom Gericht angeordneten Zeitraum verlieren, und vermieden, dass die Gemeinden, die an Stelle der Folgemitteilungen einen Auszug aus dem Bundeszentralregister anfordern können, mehr Informationen erhalten, als sie benötigen. Der Registerauszug gibt nämlich im Regelfall die gesamte „kriminelle Karriere" eines Verurteilten wieder. Das stünde aber in Widerspruch zu dem begrenzten Inhalt der Erstmitteilung, die lediglich die Tatsache der rechtskräftigen Verurteilung und bei § 45 Abs. 2 und 5 StGB den Zeitraum der Verlustes des Wahlrechtes enthält.

26.8 Weitergabe von Daten an gemeinnützige Einrichtungen

In Strafverfahren gestattet § 153 a Strafprozessordnung bei Vergehen ein vorläufiges Absehen von der Erhebung der öffentlichen Klage z. B. mit der Auflage, einen Geldbetrag zugunsten einer gemeinnützigen Einrichtung zu zahlen, wenn der Beschuldigte zustimmt, die Auflage geeignet ist, das öffentliche Interesse an der Strafverfolgung zu beseitigen, und die Schwere der Schuld nicht entgegensteht. Zu diesem Zweck werden von den Gerichten und Staatsanwaltschaften Überweisungsvordrucke ausgehändigt, aus denen nach dem Ausfüllen Namen und Kontonummer der Betroffenen sowie das Aktenzeichen des Strafverfahrens ersichtlich sind. Gehen die Zahlungsanweisungen bei den Organisationen ein, können diese - wie darüber hinaus auch die Kreditinstitute - erkennen, dass es sich bei der Überweisung nicht um eine freiwillige Spende, sondern um die Erfüllung einer gerichtlichen Auflage handelt.

Ich habe das Justizministerium mehrfach darum gebeten, ein anderes Verfahren zu ermöglichen, das die Weitergabe personenbezogener Daten an gemeinnützige Einrichtungen auf die zwingend notwendigen Informationen beschränkt. Ich habe vorgeschlagen, den Einrichtungen lediglich die Initialen der Betroffenen, die Postleitzahl, den Wohnort sowie das Aktenzeichen der Staatsanwaltschaft mitzuteilen oder Geldauflagen nur noch der Staatskasse zuzuweisen. Eine weitere Möglichkeit besteht darin, von einer Mitteilung an die gemeinnützigen Einrichtungen abzusehen und den durch Rückfragen ausgelösten Mehraufwand in Kauf zu nehmen. Durch diese Änderungen wird den datenschutzrechtlichen Interessen hinreichend Rechnung getragen. Eine Antwort des Ministeriums steht noch aus.

26.9 Niedersächsisches Ausführungsgesetz zur Insolvenzordnung

Am 1. Januar 1999 ist die Insolvenzordnung (InsO in Kraft getreten. Sie sieht ein besonderes Verbraucherinsolvenzverfahren mit der Möglichkeit der Restschuldbefreiung für Privatpersonen vor, die keine oder nur eine geringfügige wirtschaftliche Tätigkeit ausüben. Dieses Verfahren ist nur zulässig, wenn zuvor außergerichtlich der Versuch unternommen worden ist, auf der Grundlage eines Plans eine Einigung mit den Gläubigern zu erzielen. Hierüber ist dem Insolvenzgericht eine Bescheinigung vorzulegen, die von einer „geeigneten Person oder Stelle" ausgestellt worden ist. Die Insolvenzordnung ermächtigt die Länder zu bestimmen, welche Personen oder Stellen als geeignet anzusehen sind. Von dieser Ermächtigung hat Niedersachsen durch das ebenfalls am 1. Januar 1999 in Kraft getretene niedersächsische „Gesetz zur Ausführung der Insolvenzordnung und zur Änderung anderer Gesetze" vom 17. Dezember 1998 (Nds. AGInsO - GVBI. S. 710 ff.) Gebrauch gemacht. Geeignete Stellen sind danach die Schuldnerberatungsstellen in der Trägerschaft von Gemeinden, Landkreisen, Kirchen, Religionsgesellschaften des öffentlichen Rechts (öffentliche Stellen) und Verbänden der freien Wohlfahrtspflege, ferner Schuldnerberatungsstellen in der Trägerschaft von gemeinnützigen juristischen Personen des privaten Rechts (nichtöffentliche Stellen), sofern sie in einem verwaltungsbehördlichen Verfahren als geeignet anerkannt worden sind.

Im Rahmen der Tätigkeit der Schuldnerberatungsstellen fallen eine Vielzahl sensibler Daten an, die eines besonderen Schutzes bedürfen. Da die Verarbeitung von personenbezogenen Daten durch nichtöffentliche Stellen grundsätzlich nur dann von den Vorschriften des Bundesdatenschutzgesetzes (BDSG) erfasst wird, wenn sie in oder aus Dateien verarbeitet werden, regelt § 5 Abs. 6 des Nds. AGInsO, dass die Vorschriften des Dritten Abschnitts des BDSG auch dann Anwendung finden, wenn die Daten lediglich in Akten verarbeitet werden. Um zu verhindern, dass für die öffentlichen Stellen mit dem NDSG und für die nichtöffentlichen Stellen mit dem BDSG unterschiedliche Datenschutzgesetze gelten, habe ich im Rahmen des Gesetzgebungsverfahrens den Vorschlag unterbreitet, geeignete Stellen, die in privater Trägerschaft stehen, zu öffentlichen Stellen im Sinne NDSG zu erklären. Auf diese Weise unterlägen die Schuldnerberatungsstellen unabhängig von der jeweiligen Trägerschaft den weitergehenden Regelungen des NDSG. Der Niedersächsische Landtag hat diesen Vorschlag jedoch nicht aufgegriffen, was bedauerlicherweise zur Folge hat, dass sich der Datenschutz bei den Schuldnerberatungsstellen nach verschiedenen Datenschutzgesetzen richtet.

26.10 Dienstordnung für Notare (DONot)

Abgesehen von der Pflicht zur Verschwiegenheit des Notars, mit der ein Übermittlungsverbot besteht, das über das allgemeine Datenschutzrecht hinausgeht (§ 18 der Bundesnotarordnung [BNotO in der Fassung vom 19. Dezember 1998 [BGBl. I, S. 3836]), enthalten die BNotO, das Beurkundungsgesetz (BeurkG) vom 31. August 1998 (BGBl. I S. 2585) und die Dienstordnung für Notare (DONot) nur vereinzelte Regelungen über die Speicherung, Übermittlung und Löschung von Informationen in Urkunden und Akten. Für die Datenverarbeitung in Dateien sehen diese Regelungen bislang keine Vorschriften vor.

Das Justizministerium hat - federführend für die Justizverwaltungen der Länder - den Entwurf einer Neufassung der Dienstordnung für Notare vorgelegt, der an zahlreichen Stellen den Datenschutz im Notariat verbessern soll. Auch wenn die DONot als Verwaltungsvorschrift ein bereichsspezifisches Gesetz nicht zu ersetzen vermag, dürfte sie als eine Regelung anzusehen sein, die den Belangen des Datenschutzes im Notariat besser als bisher Rechnung tragen wird. Zwar haben

meine Vorschläge nicht in allen Punkten Berücksichtigung gefunden, etwa durch eine eigene Vorschrift klarzustellen, dass Notarinnen und Notare als öffentliche Stellen hinsichtlich ihrer Datenverarbeitung der Kontrolle der Landesdatenschutzbeauftragten unterliegen. Angesichts der Vielgestaltigkeit der Interessen war dies aber auch nicht zu erwarten. Es ist jedoch positiv hervorzuheben, dass mich das Justizministerium im Vorfeld der Entwurfsvorlage in vorbildlicher Weise frühzeitig und umfassend beteiligt hat und es für meine Vorschläge zur Verbesserung des Datenschutzes stets offen war. So hat es in Aussicht gestellt, die Kontrollkompetenzen der Datenschutzbeauftragten und die Anforderungen an den Datenschutz zumindest in den Ausführungsvorschriften für die Angelegenheiten der Notare (AVNot zu regeln, und mich bei einer noch einzusetzenden Arbeitsgruppe „EDV im Notariat" in bewährter Weise zu beteiligen.

27 Strafvollzug

Umsetzung der datenschutzrechtlichen Regelungen des 4. Strafvollzugsänderungsgesetzes

Nach einem über mehr als zwanzigjährigen Gesetzgebungsverfahren trat zum 1. Dezember 1998 das 4. Strafvollzugsänderungsgesetz vom 26. August 1998 BGBl. I S. 2461) in Kraft, mit dem erstmals bereichsspezifische Datenschutzregelungen für den Justizvollzug geschaffen wurden. Eine allgemeine Bewertung dieser Normen habe ich bereits im XIV. Tätigkeitsbericht vorgenommen (XIV. TB 28.1).

Dabei hatte ich auch die zu langen Aufbewahrungsfristen für die Gefangenenpersonalakten und andere sensible Unterlagen kritisiert. Die Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizbehörden sind 1999 von den Landesjustizverwaltungen aktualisiert worden. Es ist bedauerlicherweise festzustellen, dass die im Strafvollzugsgesetz als Maximalfristen genannten Zeiträume, die nicht über -, wohl aber unterschritten werden dürfen, dort undifferenziert für die Vollzugsbehörden als verbindlich festgelegt wurden. Diese verwaltungsseitige Einschränkung des gesetzlichen Spielraums wird weiter Gegenstand der Erörterungen der Landesbeauftragten für den Datenschutz mit den Länderjustizverwaltungen sein.

In Gesprächen mit dem Justizministerium und verschiedenen Justizvollzugsanstalten konnte ich nicht feststellen, dass die Vorgaben des neuen Gesetzes zu spürbaren Initiativen zur Vermeidung datenschutzrechtlicher Defizite geführt haben. Ich werde daher eine Orientierungshilfe mit rechtlichen Rahmenbedingungen und Checklisten erarbeiten, die den Justizvollzugsanstalten eine strukturierte Überprüfung und Verbesserung des Umgangs mit den personenbezogenen Daten der Gefangenen und Dritten ermöglichen sollen. Ich werde anschließend berichten, wie dieses Angebot von den Justizvollzugsbehörden angenommen wird.

Datenschutz im nichtöffentlichen Bereich

28 Grundsätzliches zum Datenschutz in der Wirtschaft

28.1 Erläuterung des neuen Datenschutzverständnisses

Der „Datenhunger" der gewerblichen Wirtschaft ist in den letzten Jahren immer stärker spürbar geworden. Dies ist einhergegangen mit einer Ausbreitung des kommerziellen Adressenhandels und des Direktmarketing, einem Wirtschaftsbe-

reich, der zweistellige Zuwachsraten pro Jahr verzeichnet und 1998 einen Jahresumsatz von 36 Milliarden DM erzielt hat . Der Deutsche Direktmarketing Verband hat seine Mitgliederzahl in den letzten zehn Jahren von gut 300 auf über 800 gesteigert. Insbesondere das Internet mit seinen vielen bewusst oder unbewusst gelegten personenbezogenen Datenspuren erweist sich als sprudelnde Quelle für Datenjäger jeder Provenienz. Manche sehen in diesem Zusammenhang die Gefahr einer „Verramschung des Persönlichkeitsrechts im Internet" (Weichert, in: E-Privacy, S. 158, 166). Data-warehousing und data-mining sind aber auch außerhalb von Internetnutzungen übliche und empfohlene Marketingstrategien zur verstärkten Kundenbindung. Auf die Entschließung der Konferenz der Datenschutzbeauftragten von Bund und Ländern zu diesem Thema vom 14./15. März 2000 (Anlage 16) weise ich hin.

Auch gegenüber diesen Entwicklungen und Erscheinungsformen erweisen sich die Instrumente des „neuen" Datenschutzes (vgl. oben 3.1 und 4.2) als richtig und wichtig, nämlich im Vorfeld durch Beratung und aktives Einschalten Einfluss auf die Technik- und Systemgestaltung zu nehmen, damit datenschutzgerechte und datenschutzfreundliche Lösungen erreicht werden.

Generell gilt, dass gerade bei der Datenschutzaufsicht im nichtöffentlichen Bereich das neue Aufgabenverständnis gefordert ist und sich bewähren muss. Aktivitäten, die außerhalb der Bearbeitung von Einzelfällen im Sinne des neuen Ansatzes durch Beratung im Vorfeld oder gemeinsame Projekte zu datenschutzgerechten und datenschutzfreundlichen Lösungen beizutragen versuchen, werden nach der zum 1. September 2000 erfolgten Verstärkung im Arbeitsgebiet Datenschutz im nichtöffentlichen Bereich in der nächsten Zeit verstärkt von der Geschäftsstelle in Angriff genommen werden können.

28.2 Kontrolltätigkeit: Zahlen, Fakten und Erfahrungen

28.2.1 Meldepflicht nach § 32 BDSG

Unternehmen, die personenbezogene Daten geschäftsmäßig

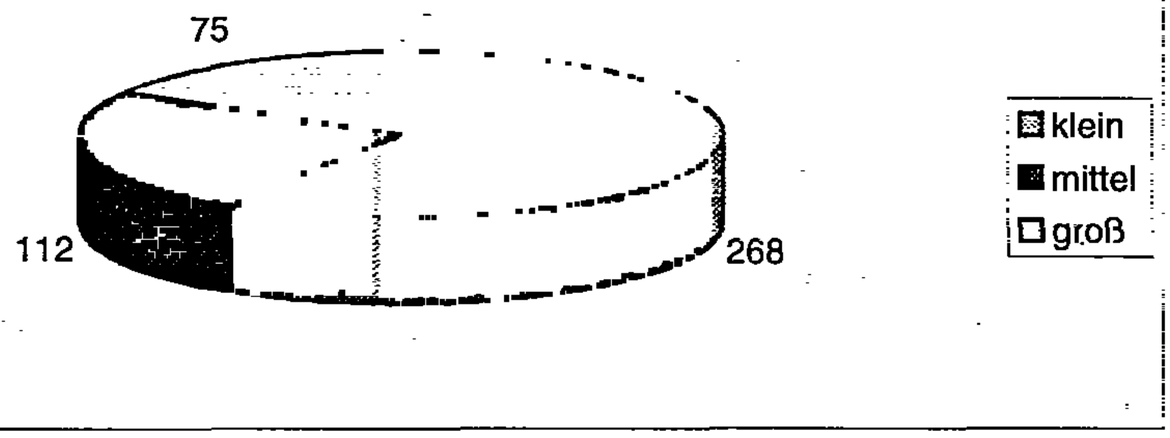
- zum Zwecke der Übermittlung speichern,
- zum Zwecke der anonymisierten Übermittlung speichern oder
- im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen,

sowie ihre Zweigniederlassungen und unselbständigen Zweigstellen haben mir die Aufnahme und Beendigung ihrer Tätigkeit innerhalb eines Monats mitzuteilen.

Im September 2000 waren 455 Unternehmen im Melderegister eingetragen. Das bedeutet eine Zunahme von 51 Firmen seit dem Jahre 1998. Im gleichen Zeitraum wurden 11 Firmen aus dem Register gelöscht. Grund für die Löschung war der Wegfall der meldepflichtigen Tätigkeit oder die Geschäftsaufgabe.

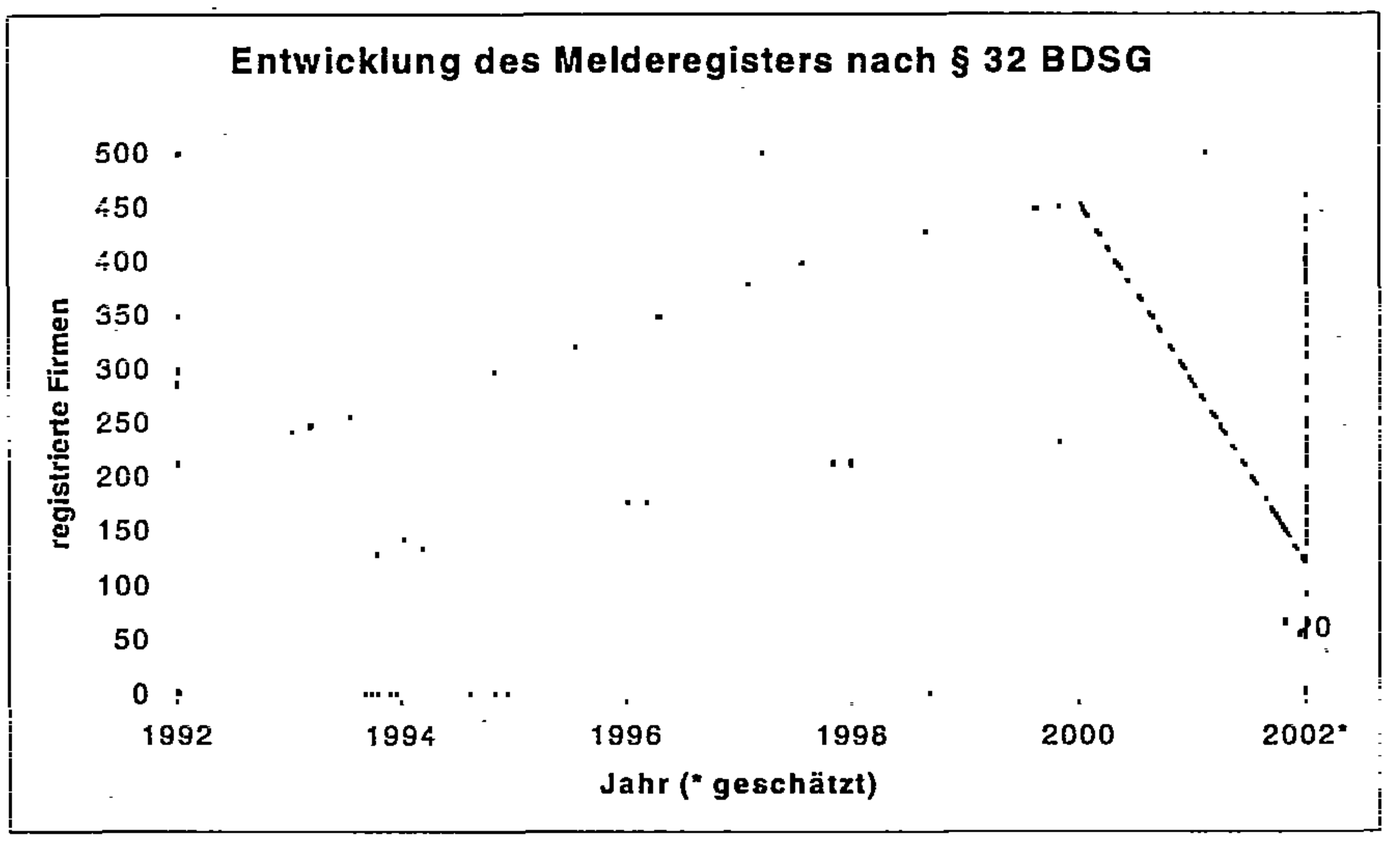
Folgende Grafik zeigt die Verteilung der registrierten Unternehmen nach ihrer Größe:

Aufteilung der registrierten Unternehmen nach Betriebsgröße im Melderegister nach § 32 BDSG



Die 455 Firmen werden von mir nach den in der folgenden Tabelle aufgeführten Betriebsarten unterschieden. Die Aufstellung zeigt zudem die Veränderungen gegenüber den in meinen Tätigkeitsberichten der vergangenen Jahre veröffentlichten Zahlen.

Betriebsarten	Anzahl der Meldungen in den Jahren				
	1992	**1994**	**1996**	**1998**	**2000**
Service-Rechenzentren	65	85	114	128	161
Rechenzentren	66	70	72	90	88
Aktenvernichtungsunternehmen	9	26	45	59	73
Datenerfassungsunternehmen	28	37	40	40	47
Auskunfteien	27	29	31	33	37
Datenarchivierung	14	17	21	22	4
Adressverlage	3	3	5	16	17
Mailboxen	0	0	5	16	6
Markt- und Meinungsforschung	2	2	4	4	5
Telefon-Marketing	0	0	0	4	15
Lettershop	0	0	0	2	1
Internetprovider	0	0	0	1	1
Gesamt	214	269	337	415	455



Die Statistik zeigt, dass die Zahl der gemeldeten Betriebe weiterhin ansteigt. Ein wesentlicher Grund dafür ist neben der gestiegenen Sensibilität für datenschutzrechtliche Belange in den Betrieben die Präsenz des LfD im Internet.

Während der vergangenen Monate nahm die Zahl der aus dem Internet abgerufenen Meldeformulare deutlich zu. Auch die von mir vorbereiteten Merkblätter zur Meldepflicht fanden großen Zuspruch.

Um diesen Trend zu verstärken und den Unternehmen weitere Hilfen anzubieten, werde ich mein Internetangebot diesen Interessen anpassen und dieses Medium verstärkt für die Verbreitung von Informationen zum Meldeverfahren nutzen.

28.2.2 Änderung der Meldepflicht durch das novellierte BDSG

Der Entwurf des BDSG sieht in den §§ 4 d, 4 e einige Änderungen hinsichtlich der Meldepflicht vor.

In Zukunft wird die Meldepflicht entfallen, wenn die verantwortliche Stelle einen Datenschutzbeauftragten bestellt hat. Nach § 4 f Abs. 1 des Entwurfs hat diese Bestellung zu erfolgen, wenn mehr als vier Arbeitnehmer mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind oder mindestens 20 Personen auf andere Weise personenbezogene Daten erheben, verarbeiten oder nutzen. Keine Meldepflicht besteht selbstverständlich auch, wenn ein Datenschutzbeauftragter freiwillig berufen wird.

Auch wenn die Datenverarbeitung nicht von einem betrieblichen Datenschutzbeauftragten überwacht wird, hat dies nicht zwingend eine Meldepflicht zur Folge. Sie besteht nämlich nicht, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, damit höchstens vier Arbeitnehmer beschäftigt sind und entweder eine Einwilligung der Betroffenen vorliegt oder die Datenverarbeitung der Zweckerreichung eines Vertragsverhältnisses dient. Wenn also beispielsweise in einem Handwerksbetrieb eine Angestellte Kundendaten verarbeitet, ist weder die Bestellung eines Datenschutzbeauftragten noch eine Meldung erforderlich.

Eine Erleichterung soll auch für Unternehmen geschaffen werden, die personenbezogene Daten im Auftrag verarbeiten. Anders als nach § 32 BDSG in der noch

geltenden Fassung müssen sie nicht generell, sondern nur unter den oben genannten Voraussetzungen die Datenverarbeitung melden.

Hingegen sind Stellen, die personenbezogene Daten zum Zwecke der Übermittlung oder zum Zwecke einer anonymisierten Übermittlung speichern, also insbesondere Adressenhändler, Auskunfteien, Markt- und Meinungsforschungsinstitute, verpflichtet, die automatisierte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten selbst dann zu melden, wenn sie einen Datenschutzbeauftragten bestellt haben oder weniger als fünf Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind.

Der Inhalt der Meldungen (§ 4 d BDSG n. F.) wird sich nicht wesentlich ändern.

Nach In-Kraft-Treten des novellierten BDSG werde ich die Änderungen zusammenfassen und einen überarbeiteten Meldevordruck zur Verfügung stellen.

28.3 Kontrolle vor Ort

Die Zahl meiner durchgeführten Routine-Prüfungen fiel niedriger aus als in den Vorjahren. Gewichtige Gründe dafür, dass mein Vorsatz, zu größerer Prüffrequenz zu kommen, nicht eingehalten wurde, waren neben fehlender Personalkapazität der wachsende Ruf nach Beratungen vor Ort und die Entscheidung zu verstärkter Beteiligung an neuen Projekten aus dem Bereich der Wirtschaft.

Meine Prüfungen und Beratungen zeigen eine deutlich gestiegene Zahl verschiedener Betriebssystem-Versionen und Derivate, insbesondere im Unix-Bereich. Die vorgefundenen Rechnerarchitekturen waren klassische Mehrplatzsysteme, Client/Server-Systeme sowie heterogene Systeme in Netzen kombiniert mit Großrechnern. Das im XIV. TB unter 30.2.2 vorgestellte Prüfverfahren hat sich im praktischen Einsatz bewährt. Das Konzept setzt auf Selbstkontrolle durch Orientierungshilfen und Checklisten, die der Prüfling vor dem eigentlichen Prüfungstermin erhält und selbst abarbeitet und ausfüllt. Dieses Verfahren hat sehr zu einem effizienten und erfolgreichen Ablauf der Prüfungstätigkeit beigetragen.

Typische Mängel waren beispielsweise schwache Passwortverfahren, unzureichende Protokollierungen und Protokollauswertungen, fehlende Arbeitsanweisungen, nicht datenschutzgerechter Umgang mit Systemverwalter-Kennungen, unzureichende Sicherung der Netzinfrastruktur und fehlende gesicherte Pausenfunktionen. Hinzu kamen systemspezifische Punkte wie besondere Probleme bei der Protokollierung und fehlendes Fachwissen der Administration bei Novell, der Umgang mit der etc./password bei Unix, die Verwendung des Auditor-Attributs bei RACF oder die Beibehaltung von Standardeinstellungen bei Windows NT. Nur gelegentlich war zusätzliche Sicherungs-Software im Einsatz. Die geprüften Stellen haben meine Empfehlungen und Forderungen stets zügig umgesetzt. Meine Bereitschaft zur zeitnahen Beratung vor Ort wird gern angenommen.

29 Adresshandel

Wie auch in der Vergangenheit habe ich im Berichtszeitraum immer wieder Beschwerden von Bürgern über unverlangt zugesandte Werbung erhalten. Stets ist ihr Erstaunen groß, wenn ich sie darüber informiere, dass der Handel mit ihren Adressen und anderen Angaben zu ihrer Person vom Bundesdatenschutzgesetz in den Grenzen des § 29 erlaubt wird, auch wenn keine Einwilligung vorliegt.

Akzeptiert werden in aller Regel meine Ausführungen, dass der Gesetzgeber einen Ausgleich zwischen unterschiedlichen Interessen schaffen musste. Das Di-

rektmarketing hat sich zu einem wichtigen Wirtschaftszweig entwickelt, der 1998 einen Jahresumsatz von 36 Milliarden DM erwirtschaft hat. Demgegenüber steht der Anspruch der Betroffenen darauf, dass ihre persönlichen Daten nicht unbeschränkt zu einem Handelsgut werden. Der Gesetzgeber hat diesen Interessenkonflikt dadurch zu lösen versucht, dass nur die vom sog. „Listenprivileg" (§§ 29 Abs. 2 Satz 1 Nr. 1 b, 28 Abs. 2 Nr. 1 b BDSG) bezeichneten Daten relativ unproblematisch weitergegeben werden dürfen, im Übrigen aber eine genaue Prüfung des berechtigten Interesses des Empfängers der Daten an ihrer Kenntnis zu erfolgen hat.

Diese Information über die Rechtslage verbinde ich mit dem Hinweis auf Möglichkeiten, unverlangte Werbung zu verhindern. Dabei leistet mir nach wie vor das von mir in Zusammenarbeit mit anderen Landesbeauftragten herausgegebene Merkblatt „Tips zum Adressenhandel und gegen die Werbepapierflut im Briefkasten" gute Dienste, das zu meinem Internetangebot gehört und kostenlos bei mir bezogen werden kann.

Im nächsten Jahr werde ich, um einen besseren Einblick in die Geschäftspraktiken zu erhalten, einen Kontroll- und Beratungsbesuch bei einem Adressenhändler durchführen.

30 Kundendaten und Werbung

Kundenumfrage durch ein Automobilunternehmen

Ein Kunde eines Autohauses aus Leverkusen wurde von einem Berliner Unternehmen im Auftrag eines Kraftfahrzeugherstellers angeschrieben und gebeten, Kundendienstleistungen und Kundenbetreuung zu beurteilen und Erfahrungen mit der Werkstatt mitzuteilen. Dabei war dem Berliner Unternehmen nicht nur die Adresse des Kunden, sondern auch sein Kraftfahrzeugtyp, die Werkstatt und die Tatsache, dass er vor einiger Zeit mit diesem Kraftfahrzeug in der Werkstatt war, bekannt. Noch mehr verunsichert war der Kunde, als man ihm von Seiten des Autohauses mitteilte, dass die Adressen der Kunden vom Hersteller online aus dem Computer der Werkstätten abgerufen werden, ohne dass diese davon etwas wissen oder erfahren. Der Chef der Werkstatt gab zu erkennen, dass er dieses Verfahren mitmachen müsse, um die Vertretung der Automarke zu behalten.

Meine Nachfrage beim Datenschutzbeauftragten des Kraftfahrzeugherstellers ergab, dass dieses Unternehmen bereits seit über 10 Jahren eine Händler-Image-Analyse durchführt, um die Kundenzufriedenheit und damit auch die Qualität der Kundenbetreuung festzustellen.

Die Kundenbefragung erfolgt im Rahmen einer Auftragsdatenverarbeitung sowohl für den Hersteller als auch für die Vertragshändler. Der Hersteller hat mit dem Berliner Unternehmen eine Rahmenvereinbarung zur Einhaltung der Datenschutzbestimmungen geschlossen und nimmt auch für die einzelnen Vertragshändler die Verantwortung und Kontrolle in datenschutzrechtlicher Hinsicht wahr. Die Händler schließen Einzelverträge mit dem Unternehmen, auf dessen Grundlage sie in einem Online-Verfahren bestimmte Stammdaten aller Kunden ausschließlich zum Zweck der Kundenbefragung zur Verfügung stellen. Die Daten werden also nicht in einem automatisierten Verfahren von dem Berliner Unternehmen beim Händler abgerufen. Das Unternehmen übersendet den Kunden Bögen mit Fragen zur Bewertung der Betreuung durch die Werkstatt und wertet die Antworten aus. Die Bögen werden getrennt von den Adressen aufbewahrt und mit Code-Nummern versehen. Namen und Anschrift werden mit den Befragungsdaten nicht wieder zusammengeführt. Die Ergebnisse werden dem

Händler und auch dem Hersteller nur als anonymes statistisches Material zur Verfügung gestellt.

Dieses Verfahren zur Nutzung der Daten ist gemäß § 28 Abs. 1 Satz 1 Nr. 1 i. V. m. § 11 BDSG rechtmäßig. Der Kaufvertrag über ein Kraftfahrzeug beinhaltet auch die Gewährleistung, den Kundendienst und die Betreuung des Kunden. Die Kundenbefragung dient diesen Vertragszwecken. Das Automobilunternehmen ist für die Einhaltung der Vorschriften des BDSG und anderer Vorschriften über den Datenschutz verantwortlich (§ 11 Abs.1 Satz 1 BDSG). Entsprechende Vereinbarungen sind geschlossen worden und die Kontrolle in datenschutzrechtlicher Hinsicht ist gewährleistet.

31 Auskunfteien

31.1 Speicherung unrichtiger Daten

Ein Petent machte mir gegenüber geltend, dass die über ihn bei einer Auskunftei gespeicherten Daten über den Familienstand unzutreffend seien und dass Daten über den gesetzlich vorgesehenen Zeitraum von fünf Jahren hinaus gespeichert würden.

Auf meine Nachfrage teilte mir das Unternehmen mit: Die Angaben zum Familienstand des Betroffenen konnten nicht genauer überprüft werden und sind daher gelöscht worden. Weiterhin bat ich das Unternehmen zu prüfen, ob die seit über fünf Jahren gespeicherten Daten über die Voranschriften sowie Angaben über die Eröffnung eines Konkursverfahrens für die Auskunftserteilung noch erforderlich seien oder ob diese Daten gem. § 35 Abs. 2 Nr. 4 BDSG zu löschen seien. Die Auskunftei teilte mir daraufhin mit, dass diese Daten gelöscht würden.

Durch diese Eingabe ist erneut deutlich geworden, dass insbesondere Bürger mit negativen Wirtschaftsdaten sich über die zu ihrer Person gespeicherten Daten Eigenauskünfte einholen sollten, um sie ggf. korrigieren oder löschen zu lassen.

31.2 Speicherung von Bonitätsmerkmalen

Ein Petent beschwerte sich bei mir darüber, dass bei dem von einer Auskunftei gespeicherten Datensatz nicht nur seine Anschrift und Amtsbezeichnung, sondern auch seine dienstliche Funktion und seine Tätigkeit in einer gemeinnützigen Organisation vermerkt worden seien. Er machte geltend, dass seine schutzwürdigen Interessen der Verwendung der Daten entgegenstünden, weil die Angaben nicht zur Beurteilung der Kreditwürdigkeit und Zahlungsfähigkeit notwendig seien.

Mit der Geschäftsführung der Auskunftei habe ich in einem ausführlichen Gedankenaustausch über den Umfang objektiver und aussagekräftiger Informationen zur Bonität und zu sonstigen wirtschaftlichen Verhältnissen Einvernehmen erzielt, dass die dienstliche Funktion und die Erwähnung des Ehrenamtes aus dem Datensatz des Petenten zu löschen sind.

32 Kreditwirtschaft

32.1 Speicherung von Daten eines ehemaligen Kunden einer Bank

Ein Petent wandte sich an mich, weil er Werbung einer Bank erhalten hatte, die auf eine Verwendung seiner Geburtsdaten schließen ließ. Er hatte vor Jahren bereits seine Konten bei dieser Bank aufgelöst und sich den Genossenschaftsanteil auszahlen lassen.

Die Recherchen des dortigen Datenschutzbeauftragten ergaben, dass die Konten zwar 1995 aufgelöst, durch eine Umstellung des EDV-Systems im gleichen Jahr jedoch diese Daten des alten Systems in das neue übernommen worden waren. Dabei ging das neue System in diesem Fall davon aus, dass es sich hier um Daten eines Kunden „im Aufbau" handelte und nicht um einen ehemaligen Kunden. Die Datensätze ehemaliger Kunden werden in regelmäßigen Abständen von der Rechenzentrale gelöscht.

Aufgrund der Anfrage wurde das alte Datenmaterial durchgesehen und - sofern keine Geschäftsverbindung mehr bestand - gelöscht.

32.2 Kombinierter Vordruck zur Kontoeröffnung und Geldanlage

Ein Finanzdienstleister verwendet zur Datenerhebung bei Kontoeröffnung und zur Geldanlage einen kombinierten Vordruck. Ein Petent monierte, dass auf dem von dem Kreditinstitut herausgegebenen Formular zur Kontoeröffnung/Geldanlage auch die Angaben Familienstand, Beruf, Branche, Arbeitgeber, Selbstständigkeit, Staatsangehörigkeit, Steuerausländer und gebietsfremd verlangt werden. Dabei wird nicht zwischen notwendigen und freiwilligen Angaben unterschieden, sodass der Eindruck entsteht, als seien alle Angaben für eine Kontoeröffnung notwendig. Der Petent kritisierte weiterhin, dass selbst in den Fällen, in denen Außendienstmitarbeiter den Kunden betreuen, eine vollständige Kopie des Personalausweises gefordert wird, obwohl die Legitimationsprüfung durch diesen erfolgen könnte.

In dem von dem Petenten beanstandeten Vordruck werden im Kopfteil die Stammdaten erfasst. Danach sind verschiedene Rubriken anzukreuzen - je nachdem welche Kontoart oder Anlageform gewählt wird. In gesonderten Spalten sind Angaben über die gesetzlichen Vertreter (bei Kontoeröffnung für einen Minderjährigen), Zahlungswege und Korrespondenzkonto zu machen. Ferner besteht die Möglichkeit zur Vereinbarung eines Geheimwortes.

Abschließend folgt eine umfangreiche Erklärung zu den Geschäftsbedingungen, die datenschutzrechtliche Einwilligungserklärung zur Übermittlung personenbezogener Daten an Firmen der Unternehmensgruppe, über das Einverständnis zur schriftlichen oder fernmündlichen Kontaktaufnahme und ein Hinweis nach § 8 Geldwäschegesetz (GWG).

Auf meine Anfrage zeigte sich der Datenschutzbeauftragte des Unternehmens sehr kooperativ. Meine Anregung, getrennte Antragsformulare für eine Kontoeröffnung oder Geldanlage einzuführen, wurde zwar mit dem Argument der Kundenfreundlichkeit nicht aufgenommen, allerdings sollen bei der Überarbeitung der Vordrucke künftig die für den jeweiligen Zweck zwingend benötigten Felder gekennzeichnet und somit von den freiwillig zu machenden Angaben unterschieden werden. Damit soll nach dem Grundsatz der Datensparsamkeit verhindert werden, dass es bei den unterschiedlichen Verwendungszwecken des Vordrucks zur Erhebung überflüssiger Informationen kommt. Die Frage nach dem Steuerausland wird herausgenommen. Die Angaben über „Staatsangehörigkeit" und „gebietsfremd" sind Daten, die für Meldungen an die Deutsche Bundesbank benötigt werden. Angaben zu Beruf, Branche, Arbeitgeber und Selbstständigkeit

dienen der qualifizierten Beratung und Betreuung des Kunden bei seiner Geldanlage. Zudem wird in Zukunft bei der Legitimationsprüfung auf die Kopie des Personalausweises oder eines Passes verzichtet. Die Überarbeitung des Vordruckes ist noch nicht abgeschlossen und wird mit mir abgestimmt.

Des Weiteren ging der Datenschutzbeauftragte des Unternehmens darauf ein, wie die Bearbeitung dieses Vordrucks künftig erfolgen soll, wenn Kunden in den Einwilligungserklärungen Positionen zur Datenübermittlung an die Unternehmensgruppe oder zur Werbung per Telefon, Telefax und E-Mail streichen. Er ist der Auffassung, dass der übrige Antrag dennoch weiter gelten solle. Zurzeit bestehe in der Bank-Software jedoch noch nicht die Möglichkeit, die (teilweisen) Streichungen zu berücksichtigen. Übergangsweise werde daher vom Datenschutzbeauftragten in diesen Fällen ein sog. Werbeverbotskennzeichen gesetzt, welches zumindest eine nicht gewünschte Kontaktaufnahme ausschließt. Eine Verhinderung der Datenübermittlung ist zurzeit nur durch Arbeitsanweisung geregelt. Für eine umfassende EDV-technische Lösung liegt der Entwicklungsabteilung der EDV bereits ein Auftrag des Datenschutzbeauftragten vor.

32.3 Abruf von Kontoauszügen bei mehreren Kontoinhabern

Ein Petent unterhielt bei einer Bank ein privates Girokonto. Gleichzeitig führte er das Schullandheimkonto seiner Schule. Als ein Kollege mit der Karte für das Schullandheimkonto (die auf den Namen des Petenten lautete) aus dem Automaten Kontoauszüge zog, erhielt er einen Auszug, auf dem die private Kontonummer des Petenten ausgedruckt war und dazu einen zweiten Auszug mit dem Stand des Schulkontos, aber ohne Kontonummer. Der Kontoinhaber war der berechtigten Auffassung, dass bereits die Existenz eines weiteren Kontos eine individuelle datengeschützte Angelegenheit sei.

Die Bank machte geltend, auch bei Kunden, die mehrere Konten unterhalten, solle sichergestellt werden, dass der Kunde allgemeine Informationen (z. B. Zinsänderungen) über den Kontoauszugsdrucker unverzüglich erhält. Deshalb werde diese Information auf dem Kontoauszug gedruckt, welchen der Kunde zufällig gerade als ersten zieht. Grundsätzlich soll die Nutzung der Kundenkarte nur durch den Kontoinhaber erfolgen.

Das Kreditinstitut bot deshalb die Möglichkeit, für Kontobevollmächtigte eine eigene Kundenkarte zu beantragen. Als Kontobevollmächtigtem werden ihm dann selbstverständlich nur die vorliegenden Informationen für das Konto zur Verfügung gestellt, für das die Bevollmächtigung gilt. Außerdem ist es möglich, als Kontoinhaber die Schule, das Schullandheim oder einen Treuhänder zu benennen.

Gegen diese Regelungen habe ich keine datenschutzrechtlichen Bedenken.

32.4 Gestaltung von Freistellungsaufträgen

Ein Petent machte geltend, die Gestaltung der Freistellungsaufträge eines Finanzdienstleisters erlaubten, dass an das Bundesamt für Finanzen auch nicht meldepflichtige Daten wie die Konto- bzw. Vertragsnummer übermittelt würden.

In der Stellungnahme führte das Unternehmen aus: Grundsätzlich komme es bei Erhebung der Daten im Freistellungsauftrag darauf an, Daten der Vertragsinhaber (und deren Partner) sowie den entsprechenden Freibetrag zu erfassen. Nach den ergänzenden Hinweisen zu § 44 a EStG sei eine maschinell lesbare Gestaltung des Freistellungsauftrages zugelassen, was wiederum eine eindeutige Zu-

ordnung zu den übrigen Kundendaten ermöglichen müsse. Dies geschehe bei dem Finanzdienstleister über die Bausparnummer, die deshalb als Such-/Ordnungsbegriff in den Freistellungsauftrag aufgenommen werde.

Für jede Bausparnummer sei ein eigener Freistellungsauftrag zu stellen. Bei Zusammenveranlagung unterschrieben beide Ehepartner den Freistellungsauftrag. In den Freistellungsaufträgen bestätigten die Kunden, dass sie mit allen Freistellungsaufträgen zusammen die steuerlichen Höchstbeträge nicht überschreiten würden. Das Unternehmen fasse die Beträge aus den Freistellungsaufträgen zusammen und teile sie gemeinsam mit anderen Daten (§ 45 d EStG) auf Verlangen dem Bundesamt für Finanzen mit. Diese Übermittlung erfolge ohne die Bausparnummer. Im Übrigen sei in § 45 d Abs. 2 EStG eindeutig geregelt, dass die Mitteilungen über die Freistellungsaufträge ausschließlich zur Prüfung der rechtmäßigen Inanspruchnahme des Sparerfreibetrages und des Pauschbetrages für Werbungskosten verwendet werden dürfen. Dies gelte insbesondere für das Bundesamt für Finanzen.

Aufgrund dieser Stellungnahme sah ich keine Veranlassung, den Finanzdienstleister zu rügen.

33 Versicherungen

33.1 Verantwortung eines Versicherungsvertreter für Kundendaten

Ein Mitarbeiter im Außendienst einer Versicherungsgruppe war in den Ruhestand getreten und hatte die von ihm erhobenen Angaben über seine Kunden seinem Arbeitgeber zur Verfügung gestellt. Nun musste er feststellen, dass über einen längeren Zeitraum in seinem früheren Tätigkeitsfeld ein häufiger Wechsel der Außendienstmitarbeiter stattfand. Dies beunruhigte auch seine früheren Kunden, da sie vermuteten, dass hochsensible Daten allen diesen Mitarbeitern zur Verfügung stehen würden. Die Gefahr der missbräuchlichen Nutzung dieser Daten war für den Mitarbeiter Anlass, sich seiner eigenen Verantwortung für die Weitergabe von Kundendaten an seinen Arbeitgeber beim Ausscheiden zu vergewissern.

Ich habe dem Petenten mitgeteilt, dass die von einem Mitarbeiter gespeicherten Kundendaten als Geschäftsdaten der Versicherung anzusehen sind. Damit ist die Weitergabe an den von der Versicherung bestimmten Nachfolger eine arbeitsrechtliche Vertragspflicht. Aufgabe der Versicherung ist es, durch Verträge mit den Außendienstmitarbeitern einen ausreichenden Datenschutz zu vereinbaren und auch zu kontrollieren. Die Versicherung hat dafür eigens einen Datenschutzbeauftragten zu bestellen.

33.2 Fragebogen für Berufsunfähigkeits-/Invaliditätsversicherung

Eine Petentin übersandte mir einen Antrag auf Leistungen aus einer Berufsunfähigkeits-/Invaliditätsversicherung. Dabei erschienen ihr einige Fragen als zu weitgehend und damit unzulässig.

Das Bundesdatenschutzgesetz regelt die Verarbeitung und Nutzung von personenbezogenen Daten durch nichtöffentliche Stellen, soweit die Daten in oder aus Dateien verarbeitet oder genutzt werden (§ 1 Abs. 2 Nr. 3, § 27 Abs. 1 Satz 1 Nr. 1 i. V. m. § 3 Abs. 2 BDSG).

Meine Prüfung ergab, dass die Versicherung die personenbezogenen Daten, die im Zusammenhang mit einer Prüfung der Leistungspflicht aus einer Berufsunfähigkeitsversicherung erhoben werden müssen, nicht elektronisch speichert, son-

dern die Fragebögen in einer Akte aufbewahrt. Sie begründete dies damit, dass einerseits Anträge auf Leistungen aus der Berufsunfähigkeits-/Invaliditätsversicherung relativ selten gestellt würden, andererseits die erhobenen Informationen sehr umfangreich seien und sich daher der Aufwand für eine elektronische Bearbeitung der Fälle nicht lohne. Es handelte sich also nicht um eine Datei. Das BDSG wäre allerdings auch anwendbar, wenn Akten und Aktensammlungen durch automatisierte Verfahren umgeordnet und ausgewertet werden können. Das Unternehmen bestätigte mir, dass dies hier nicht zutrifft. Das Bundesdatenschutzgesetz findet daher in diesem Fall keine Anwendung.

Dennoch habe ich mir erlaubt, das Unternehmen darauf hinzuweisen, dass nur die früheren Erkrankungen anzugeben sind, die im Zusammenhang mit der beantragten Leistung stehen. Ich habe empfohlen, die Fragen entsprechend präziser zu formulieren.

34 Arbeitnehmerdatenschutz

34.1 Mithören von Telefongesprächen in Call-Centern

Ein Call-Center hat mich um rechtliche Beratung zur Frage der Zulässigkeit des Mithörens von geschäftlichen Telefongesprächen mit Kunden gebeten. Das Unternehmen wollte zur Erhöhung seiner Service-Qualität ein Telefon-Coaching einführen. Zweimal im Jahr sollte die Gesprächsqualität aller Mitarbeiterinnen und Mitarbeiter überprüft werden, um festzustellen, ob diese den von der Firma angestrebten Eindruck eines kompetenten Unternehmensservice vermitteln.

Zu diesem Zweck sollte ein zweiter Telefonhörer in den Callmaster (Telefonapparat) eingestöpselt und mehrere Telefonate des zu beurteilenden Mitarbeiters von einem Telefon-Coach mitgehört werden. Anschließend sollte die Gesprächsführung bei diesen Telefonaten analysiert und mit dem betreffenden Mitarbeiter erörtert werden. Eine Aufzeichnung der Telefongespräche war nicht beabsichtigt. Zwischen Unternehmen und Betriebsrat bestanden Meinungsverschiedenheiten darüber, ob der Kunde, der mit dem Call-Center telefoniert, vom Mithören seines Gesprächs unterrichtet werden muss.

Nach der Rechtsprechung des Bundesverfassungsgerichts umfasst das verfassungsrechtlich geschützte allgemeine Persönlichkeitsrecht auch das Recht am eigenen Wort. Dieses besteht in der Befugnis des Menschen, selbst zu bestimmen, ob seine Worte nur seinem Gesprächspartner, einem weiteren Personenkreis oder der Öffentlichkeit zugänglich sein sollen. Der Schutz erstreckt sich auch auf dienstliche/geschäftliche Telefongespräche. Ein heimliches Mithören oder Mithören lassen des dienstlichen Telefonats eines Arbeitnehmers durch den Arbeitgeber verletzt das Recht des Ersteren am eigenen Wort (BverfGE 34, 239, 246 ff.; BVerfG, NJW 1992, 815). Ein solches Mithören setzt grundsätzlich die Einwilligung des Arbeitnehmers voraus. Diese kann - wie das Bundesverfassungsgericht festgestellt hat - weder aus der Benutzung des Diensttelefons allein noch aus der bloßen Kenntnis einer Abhörmöglichkeit gefolgert werden. Soll ein Gespräch des Arbeitnehmers mitgehört werden, so muss dieser grundsätzlich auf die beabsichtigte Maßnahme hingewiesen werden. Ihm muss die Möglichkeit eingeräumt werden, sich dem Mithören zu entziehen. Der gleiche rechtliche Schutz kommt dem gesprochenen Wort des Kunden zu.

Das Bundesverfassungsgericht hat allerdings im Zusammenhang mit einer heimlichen Tonbandaufnahme betont, das Recht auf freie Entfaltung der Persönlichkeit des Sprechers sei in aller Regel noch nicht betroffen, soweit der objektive Gehalt des Gesagten, wie z. B. bei fernmündlichen Durchsagen, Bestellungen oder Börsennachrichten, so sehr im Vordergrund stehe, dass die Persönlichkeit des Sprechenden nahezu vollends dahinter zurücktrete und das gespro-

chene Wort seinen privaten Charakter einbüße (BVerfGE 34, 247). In die gleiche Richtung gehen auch die Ausführungen des Bundesarbeitsgerichts in seinem Beschluss vom 30. August 1995 (RDV 1996, 30, 32). In dieser Entscheidung hat das Gericht eine Betriebsvereinbarung, die es dem Arbeitgeber erlaubt, externe Telefongespräche des Arbeitnehmers in dessen Gegenwart zu Ausbildungszwecken mitzuhören, für zulässig gehalten. Bezüglich der durch das Mithören betroffenen Arbeitnehmerinteressen hebt das Gericht hervor, sie seien in dem zu entscheidenden Fall nur von geringem Gewicht, denn die Gespräche seien ausschließlich geschäftlicher Natur, bezögen sich nur auf Reservierungen und damit im Zusammenhang stehende Informationen, die die geschützte Eigensphäre des Arbeitnehmers kaum berührten. Zudem erfolgten die Eingriffe in der schonendsten Art, da sie auf die Probezeit beschränkt seien und nur am Arbeitsplatz des Arbeitnehmers stattfänden.

Ein standardisierter Gesprächsinhalt im Sinne dieser Rechtsprechung kann nur im Ausnahmefall angenommen werden. In der Regel ist bei Telefonaten mit Call-Centern, die zur Geschäftsanbahnung und -abwicklung geführt werden, davon auszugehen, dass sie durchaus von der Individualität des Gesprächspartners in Gedankenführung und Ausdruck sowie seinem Temperament - man denke etwa nur an Reklamationen - geprägt sein werden. Überdies kann es im Hinblick auf das Persönlichkeitsrecht der Betroffenen keine unterschiedliche Bewertung des Gesprächsanteils des Arbeitnehmers und des Gesprächsanteils des Kunden/Zwischenhändlers in einem gemeinsamen dienstlichen Telefonat im Call-Center geben. Sie wäre angesichts der rechtlichen Gleichwertigkeit der jeweiligen Gesprächsbeiträge offensichtlich willkürlich.

Dem Kunden muss deshalb wie dem Arbeitnehmer die Möglichkeit gegeben werden, sich dem Mithören zu entziehen. Er muss deshalb im Falle eines beabsichtigten Mithörens vorher informiert werden. Setzt er trotz dieses Hinweises das Telefonat fort, kann darin eine konkludente Einwilligung in die Maßnahme gesehen werden.

Der Hinweis auf eine beabsichtigte konkrete Mithörmaßnahme muss zeitnah erfolgen, damit der Gesprächspartner von seinem Recht am gesprochenen Wort in der ihm angemessen erscheinenden Weise Gebrauch machen kann. Es reicht deshalb nicht aus, wenn etwa ohne zeitlichen Bezug zu einer solchen Maßnahme in einem vorangehenden Schriftwechsel nur allgemein auf die Mithörmöglichkeit hingewiesen würde.

Für die Arbeitnehmer stellt das Mithören dienstlicher Gespräche eine Verhaltens- und Leistungskontrolle dar, gegen die unter den genannten Voraussetzungen keine Bedenken bestehen. Als Maßnahme der Arbeitnehmerüberwachung durch technische Einrichtungen unterliegt sie nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz der Mitbestimmung des Betriebsrats.

Von strafrechtlicher Relevanz ist das Mithören von Telefonaten der Mitarbeiter nur unter besonderen Umständen. Nach § 201 Abs. 2 Satz 1 StGB wird zwar bestraft, wer unbefugt das nicht zu seiner Kenntnis bestimmte nichtöffentliche Wort eines anderen mit einem Abhörgerät aufzeichnet. Der Bundesgerichtshof geht allerdings davon aus, dass übliche und von der Post zugelassene Mithöreinrichtungen nicht zu den Abhörgeräten im Sinne dieser Vorschrift zählen

34.2 Videoüberwachung am Arbeitsplatz

Aus Anlass von Eingaben betroffener Arbeitnehmer war ich in jüngster Zeit mehrfach mit der Frage befasst, ob und unter welchen Voraussetzungen ein Arbeitgeber berechtigt ist, Videokameras zur Arbeitsplatzbeobachtung zu installieren. Die betroffenen Arbeitnehmer fühlten sich durch offen oder versteckt ange-

brachte Videokameras einem permanenten und unzumutbaren Überwachungsdruck ausgesetzt.

Nach Schätzungen der Industrie waren in Deutschland bereits 1998 bei einer hohen Dunkelziffer und rasant zunehmenden Absatzzahlen mehr als 500 000 Videokameras installiert. Videokameras werden nicht nur zu privaten Zwecken, sondern im öffentlichen Dienst und in der Privatwirtschaft zunehmend auch zur Personalüberwachung und Arbeitsplatzbeobachtung eingesetzt. Über den Fachhandel und Versandhäuser werden mittlerweile preisgünstig „Videowanzen“ angeboten, die eine für den Arbeitnehmer und Kunden unauffällige Überwachung und Beobachtung der Arbeits- und Verkaufsräume ermöglichen.

Die Motive und Begründungen der Arbeitgeber sind vielfältig. Vielfach soll der offene Videoeinsatz der Verhütung von Straftaten und somit als Akt der Fürsorge auch der Sicherheit der Arbeitnehmer und Kunden dienen. Verdeckte Videoanlagen werden bei Verdacht auf kriminelle Handlungen häufig zu Ermittlungszwecken und anschließend zur Beweissicherung in Arbeitsgerichts- oder Strafverfahren eingesetzt. Nach dem altbekannten Motto „Vertrauen ist gut, Kontrolle ist besser“ werden von Arbeitgeberseite oftmals auch Aspekte der reinen Leistungskontrolle zur Rechtfertigung des Videoeinsatzes angeführt. Vereinzelt werden auch Pausenräume, Kantinen oder andere Gemeinschaftsräume in die Überwachung einbezogen.

Gesetzliche Regelungen über den Einsatz von Videoüberwachungsanlagen am Arbeitsplatz gibt es bislang nicht. Auch die im Rahmen der Novellierung des Bundesdatenschutzgesetzes vorgesehene Regelung zur Videoüberwachung (§ 6 b des Entwurfs) erfasst in ihrem Geltungsbereich nur öffentlich zugängliche Räume. Ausführliche Regelungen zur Videoüberwachung in den Betrieben und Unternehmen sollen vielmehr erst im Rahmen eines Arbeitnehmerdatenschutzgesetzes getroffen werden. Grundsätzlich gilt daher bis auf weiteres zur Zulässigkeit der Videoüberwachung am Arbeitsplatz folgendes:

- Eine verdeckt und ohne Wissen des Arbeitnehmers durchgeführte Videoüberwachung stellt nach der gefestigten Rechtssprechung des Bundesarbeitsgerichts einen unzulässigen Eingriff in das Persönlichkeitsrecht des Arbeitnehmers dar, wenn keine überwiegenden schutzwürdigen Interessen des Arbeitgebers ersichtlich sind (vgl. Urt. v. 7. Oktober 1987 - 5 AZR 116/86).

- Das einen Eingriff in das Persönlichkeitsrecht rechtfertigende schutzwürdige Interesse des Arbeitgebers, etwa zum Schutz vor Verlust von Firmeneigentum durch Diebstahl, Unterschlagung oder Verrates von Betriebsgeheimnissen, muss vor Beginn der Videoüberwachung durch konkrete Anhaltspunkte und Verdachtsmomente belegt sein. Eine vage Vermutung oder ein pauschaler Verdacht gegen die gesamte Belegschaft genügt den Anforderungen nicht.

- Eine unter diesen Voraussetzungen statthafte Videoüberwachung ist grundsätzlich offen mittels einer sichtbaren Anlage und nach vorheriger Information der Belegschaft durchzuführen.

- Eine Überwachung durch verdeckte Kameras ist als „ultima ratio“ nur dann zulässig, wenn dieses Mittel die einzige Möglichkeit darstellt, berechtigte und schützenswerte Interessen des Arbeitgebers zu wahren.

- Die Videoüberwachung unterliegt der Mitbestimmung des Betriebsrates oder der Personalvertretung. Eine unzulässige Videoüberwachung wird durch eine Zustimmung des Betriebs- oder Personalrates nicht legitimiert (vgl. BAG, Urt. v. 15. Mai 1991 - 5 AZR 115/90).

– Die durch eine rechtswidrige Überwachung gewonnen Erkenntnisse unterliegen einem Verwertungsgebot und können somit in arbeitsgerichtlichen Verfahren nicht verwertet werden.

Es bleibt nur zu hoffen, dass durch das nun schon seit längerem angekündigte und von den Datenschutzbeauftragten wiederholt eingeforderte Arbeitnehmerdatenschutzgesetz auch für den Bereich der Videoüberwachung alsbald ausreichende Regelungen zum Schutz der Persönlichkeitsrechte der Arbeitnehmer getroffen werden.

34.3 Surfen am Arbeitsplatz

In vielen Betrieben der Wirtschaft und Dienststellen des öffentlichen Dienstes gehört die Kommunikation über Internet und E-Mail längst zum unverzichtbaren Standard der Bürokommunikation. Die modernen Kommunikations- und Informationsdienste werden nicht nur betrieblich, sondern häufig mit oder ohne ausdrückliche Zustimmung des Arbeitgebers auch zu privaten Zwecken genutzt.

Anfragen von Arbeitnehmern und Betriebsräten lassen vermuten, dass sich Arbeitgeber immer häufiger veranlasst sehen, die Surfgewohnheiten ihrer Arbeitnehmer und den Umfang der E-Mail-Nutzung zu kontrollieren, die private Nutzung der betrieblichen Kommunikations- und Informationsdienste einzuschränken oder gar gänzlich zu untersagen. Bei den betroffenen Beschäftigten bestehen z. B. Unsicherheiten darüber, ob und unter welchen Voraussetzungen der Arbeitgeber berechtigt ist, Einsicht in Internetprotokolle oder private E-Mails zu nehmen.

Die Rechtslage ist je nach den betrieblichen oder behördlichen Gegebenheiten differenziert zu beurteilen. Sofern der Arbeitgeber die private Nutzung der betrieblichen Kommunikations- und Informationsdienste ausschließt, sind die Regelungen des BDSG, des Betriebsverfassungsgesetzes und einer ggf. abgeschlossenen Betriebsvereinbarung maßgeblich. Problematisch wird es, wenn der Arbeitgeber es den Arbeitnehmern gestattet, Internet und E-Mail auch zu privaten Zwecken zu nutzen. In diesem Fall ist er, ohne dass es auf die Absicht der Gewinnerzielung ankäme, „geschäftsmäßiger Anbieter von Telekommunikations- und Telediensten“ im Sinne des TKG bzw. TDG. Er unterliegt dann den bereichsspezifischen Regelungen zum Schutz des Fernmeldegeheimnisses und den Datenschutzregelungen des TKG und des TDG.

Nach jüngst veröffentlichten Pressemitteilungen gibt es im Bundesarbeitsministerium Überlegungen, den Arbeitnehmern im Rahmen des noch für diese Legislaturperiode angekündigten Arbeitnehmerdatenschutzgesetzes das Recht einzuräumen, privat am Arbeitsplatz im Internet zu surfen oder auch private E-Mails zu verschicken. Der im Mai 2000 ergangene sog. "Telefonkosten- und Surferlass", der die Versteuerung der privaten Nutzung der Telekommunikationseinrichtungen unter erheblichem Verwaltungsaufwand vorsah, ist demgegenüber kontraproduktiv und wurde deswegen im Oktober 2000 wieder aufgehoben.

Die Modalitäten der privaten Nutzung, so der zeitliche Umfang der Internetnutzung und die Modalitäten der Auswertung der Protokollierung, können gesondert durch Betriebsvereinbarung oder Tarifvertrag vereinbart werden. Die weitere Entwicklung bleibt abzuwarten.

35 Privates Gesundheitswesen

Einwilligungserklärung der Patienten zur Datenweitergabe an Privatverrechnungsstellen (PVS) und an die Rechtsschutzstelle der Ärzte

Ein größeres Klinikum bat mich, die von den Ärzten im Rahmen der privaten Liquidation selbst erstellten Schweigepflichtentbindungserklärungen zu prüfen. Eine der mir vorgelegten Entbindungserklärungen sollte die korrekte Rechnungserstellung durch die PVS ermöglichen. Weiterhin war vorgesehen, dass Honorarforderungen, die nicht auf erstes Anfordern ausgeglichen wurden, zum Zwecke der weiteren Geltendmachung und eventuellen Beitreibung von den Ärzten an die Rechtsschutzstelle der Ärzteschaft (rechtsfähiger Verein) abgetreten und alle in diesem Zusammenhang erforderlichen persönlichen Behandlungsdaten übermittelt werden. Der Patient sollte sein Einverständnis zu der Abtretung erklären.

Das Klinikum hatte die Ärzte bereits darauf hingewiesen, dass es keiner Einwilligung des Patienten zur Abtretung bedarf und es sicherlich gewollt sei, dass der Patient zur Übermittlung der für eine Abtretung erforderlichen Angaben sein Einverständnis gebe, dies aber nicht formuliert worden sei. Datenschutzrechtlich fehle daher die Zweckbindung für die Datenübermittlung.

In der Vergangenheit habe ich mich wiederholt mit den Einwilligungserklärungen der Patienten bezüglich der Datenübermittlung an die PVS beschäftigt. Auf meine Anregung hat sich der Düsseldorfer Kreis (Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich) mit der Datenverarbeitung durch die Privatverrechnungsstellen befasst. Einigkeit besteht, dass der Arzt eine schriftliche Einwilligung des Patienten einholen muss. Die vom Düsseldorfer Kreis gestellten Anforderungen an den Inhalt der Einwilligungserklärung werden im Wesentlichen durch die Vordrucke der PVS erfüllt. In der mir vom Klinikum vorgelegten Einwilligungserklärung für die Datenübermittlung an die PVS war kein Hinweis auf die Folgen der Verweigerung der Einwilligung aufgenommen worden. Da die Einwilligung des Betroffenen eine umfassende Information voraussetzt, ist der Patient auch auf die Folgen der Nichtzustimmung hinzuweisen. Ich habe daher empfohlen, den Musterentwurf der PVS zu verwenden.

Bezüglich der Einwilligungserklärung zur Datenübermittlung an die Rechtsschutzstelle der Ärzteschaft wurde von mir zunächst der Datenumfang der Übermittlung geprüft. Bei Nichtzahlung werden auf Anweisung des Arztes von der PVS nur die Schuldnerdaten (Name, Adresse, Geburtsdatum), der Betrag, der Gläubiger, die Rechnungsnummer und das Rechnungsdatum an die Rechtsschutzstelle übermittelt. Diesen Datenumfang halte ich für angemessen und erforderlich. In der mir zugesandten Einwilligungserklärung des Klinikums war für den Patienten jedoch nicht ersichtlich, ob er mit der Abtretung auch in die Datenübermittlung eingewilligt hat. Die Kritik der Mitarbeiterin des Klinikums an der Einwilligungserklärung war daher zutreffend.

Die Rechtsschutzstelle der Ärzteschaft legte mir den von ihr erarbeiteten Musterentwurf einer Einwilligungserklärung vor. Diese Erklärung konnte ich - mit einer geringfügigen Korrektur - den privat liquidierenden Ärzten als Grundlage für eigene Formulare empfehlen.

36 Andere Bereiche

36.1 Elektronische Häuser- und Gebäudekarte des Tele-Info Verlags

Zu erheblichem Aufsehen bei Hauseigentümern und in der Fachöffentlichkeit hat die Elektronische Häuser- und Gebäudekarte „CityServer“ des Tele-Info Verlags geführt.

In dieser Häuser- und Gebäudekarte sind Aufnahmen von Häusern gespeichert, die von einem mit mehreren Kameras und einem Satellitennavigationssystem ausgestatteten Fahrzeug aufgenommen werden. Weiterhin enthält sie die dreidimensionalen Geokoordinaten (DGPS) des jeweiligen Kamerastandpunkts und einen Stadtplan ebenfalls im DGPS-System. Der Betrachter sieht fortlaufende Bilder, die von der Fahrbahn aus die Häuser rechts und links der Fahrbahn zeigen, und den Stadtplan, auf dem durch ein Symbol markiert wird, in welchem Teil der Straße sich der Betrachter befindet. An einigen Häusern ist die Hausnummer zu erkennen. Es besteht die Möglichkeit, die fortlaufenden Bilder anzuhalten und ein bestimmtes Bild zu vergrößern, sodass die Häuserfront und die Hausnummer, soweit sie aufgenommen wurde, deutlicher erkennbar sind. Auf diese Weise sollen alle Städte bis zu einer Größe von 20 000 Einwohnern aufgenommen werden. Als Verwendungsmöglichkeit werden u. a. der Einsatz durch Polizei, Feuerwehr, Rettungsdienste, in der Stadt- und Verkehrsplanung, durch Zustelldienste und Speditionen, Banken und Versicherungen und Versorgungsunternehmen genannt.

Neben dem je nach Größe der aufgenommenen Stadt bis zu mehreren hunderttausend DM teuren „CityServer“ bietet der Tele-Info Verlag für einige Städte Aufnahmen auf CD-ROM für weniger als 40 DM an.

Nach Zusicherung des Verlags ist es nicht möglich, Straße und Hausnummer einzugeben und auf diese Weise die Ansicht eines bestimmten Hauses aufzurufen. Meine Prüfung einer CD-ROM bestätigte dies.

Ich bin zu dem Ergebnis gelangt, dass die Elektronische Häuser- und Gebäudekarte derzeit nicht gegen das Bundesdatenschutzgesetz verstößt. Fraglich ist bereits, ob es sich um personenbezogene Daten handelt (zweifelnd LG Waldshut-Tiengen, Urteil vom 29. Oktober 1999, DuD 2000, 106, 109). Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG). Zwar werden sich häufig z. B. mit Hilfe einer Telefon-CD-ROM die Bewohner des abgebildeten Hauses feststellen lassen, sodass es sich um „bestimmbare“ Personen handelt. Zu berücksichtigen ist jedoch, dass es sich zunächst einmal um Abbildungen einer Sache handelt. Diese Abbildungen ermöglichen (in den Fällen, in denen die Qualität der Häuseraufnahmen ausreicht) Angaben über diese Sache. Problematisch ist jedoch, wann eine Angabe über eine Sache zu einer Angabe über eine Person wird. Nicht jede Beziehung einer Person zu einer Sache kann ausreichen, weil der Personenbezug sonst keine begrenzende Funktion mehr hätte. Wenn man hier Angaben über eine Person annimmt, ist der Aussagewert der Aufnahmen insbesondere auf der CD-ROM allerdings so gering, dass kaum Rückschlüsse auf tatsächliche oder sachliche Verhältnisse der Personen gezogen werden können.

Zumindest jedoch ist das Bundesdatenschutzgesetz deshalb nicht anwendbar, weil die Voraussetzungen des Dateibegriffs nicht erfüllt sind (im Einzelnen dazu mein Aufsatz in DuD 1999, 533). Eine automatisierte Datei liegt nicht vor, weil nicht die Möglichkeit besteht, die Häuser- und Gebäudekarte automatisiert nach zwei personenbezogenen Merkmalen auszuwerten. Anknüpfungspunkt für eine Auswertung ist lediglich das nicht personenbezogene Merkmal „Geokoordinate“, das sowohl auf die Referenzinformationen „Straße“ und „Stadtplan“ als

auch auf die in der Straße befindliche Gebäudeaufnahme führt. Dasselbe gilt für eine möglicherweise in Betracht kommende Auswertung über die Katasterkoordinaten.

Es ist auch nicht entscheidend, ob eine Auswertung in der Weise erfolgen kann, dass bei Eingabe der Straße und Hausnummer ein bestimmtes Haus ausgewählt wird. Auch wenn dies möglich ist, liegt nur ein zur Auswertung geeignetes Merkmal vor.

Aber selbst wenn man unterstellt, dass zwei personenbezogene Merkmale vorhanden sind, wäre der Dateibegriff nicht erfüllt, weil diese Merkmale keine „automatisierte Auswertung" ermöglichen würden. Im nichtöffentlichen Bereich werden Dateien in den Schutzbereich des Gesetzes einbezogen, weil und soweit sie leichter erschließ- und auswertbar sind. Demgemäß nimmt ein Teil der Literatur nur dann eine automatisierte Auswertbarkeit an, wenn die Suchkriterien logisch miteinander verknüpft werden können. Nur dann bestehe eine Gefahr durch eine erhöhte Auswertbarkeit. Dagegen reiche es nicht aus, wenn nur nach einem einzigen Suchbegriff und nur nacheinander nach weiteren Suchbegriffen ausgewertet werden könne. Diese Kombinationsmöglichkeit besteht bei der Häuser- und Gebäudekarte nicht, weil sie entweder über die Geokoordinaten oder, wenn diese Möglichkeit in Zukunft geschaffen werden sollte, über die Katasterkoordinaten, ausgewertet werden kann. Wenn man nicht so weit gehen will, eine Kombinationsmöglichkeit zu fordern, ist zumindest Voraussetzung, dass eine Auswertung nach dem einen oder dem anderen Merkmal zu verschiedenen Ergebnissen führt, etwa wenn aus einer Datei mit den Angaben „Name, Geburtsdatum, Geschlecht, Beruf", Personen mit bestimmten Berufen, bestimmte Altersgruppen oder nach Anschriften geordnete Gruppen herausgefiltert werden können. Bei der Häuser- und Gebäudekarte ist das Ergebnis immer nur, dass ein bestimmtes Haus ausgewählt werden kann, gleichgültig, ob man die Katasterkoordinaten, die Geokoordinaten oder (unterstellt, dies wäre möglich) die Anschrift des Hauses eingibt. Weitere Erkenntnisse werden nicht gewonnen. Eine für die Annahme des Dateibegriffs erhöhte Auswertbarkeit liegt nicht vor. Hinzu kommt, dass die Geokoordinate nur auf die Referenzinformation „Straße" und auf die in dem fraglichen Straßenabschnitt befindlichen Gebäudeaufnahmen führt. Der Anwender muss sich also regelrecht an ein Haus herantasten. Von einer „automatisierten" Auswertung wird man daher kaum sprechen können.

Im novellierten Bundesdatenschutzgesetz wird der Dateibegriff voraussichtlich ersetzt werden durch die Voraussetzung einer Verarbeitung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen, sodass es für die Anwendbarkeit des Gesetzes nicht mehr auf das Vorliegen einer Datei ankommen wird. Auch nach dem neuen Bundesdatenschutzgesetz muss es sich jedoch um personenbezogene Daten handeln (dazu oben).

Unabhängig von der Frage des fehlenden Dateibezugs bin ich der Auffassung, dass der Speicherung der Daten gemäß § 29 Abs. 1 Satz 1 Nr. 2 BDSG keine offensichtlich überwiegenden schutzwürdigen Interessen entgegenstehen würden, wenn die Vorschrift anwendbar wäre. Bei dieser Interessenabwägung ist nicht nur das Recht auf informationelle Selbstbestimmung der Betroffenen, sondern es sind auf Seiten des Tele-Info Verlags die von Art. 12 geschützte berufliche Tätigkeit und die von Art. 14 GG geschützte wirtschaftliche Betätigungsfreiheit zu berücksichtigen (LG Waldshut-Tiengen, a.a.O., 109; VG Karlsruhe, Beschluss vom 1. Dezember 1999, DuD 2000, 294, 297). Wenn man aufgrund des geringen Aussagewerts der Aufnahmen nicht schon dazu gelangt, keine „Einzelangaben über persönliche und sachliche Verhältnisse" (s. o.) anzunehmen, muss diese Tatsache zumindest im Rahmen der Interessenabwägung berücksichtigt werden. Die Aufnahme eines Hauses etwa in einer gemischten Innenstadtbebauung hat einen so geringen Informationsgehalt, dass auch in Verbindung mit anderen Daten kaum Rückschlüsse auf die Verhältnisse der Bewohner möglich sind.

Eher wird man eine Aussage bei einem exklusiven Villenvorort annehmen können. Aber auch hier kommen allenfalls vage Schlussfolgerungen in Betracht. Es handelt sich bei der veröffentlichten Gebäudeansicht, wie es das LG Waldshut-Tiengen und das VG Karlsruhe formulieren, um einen sehr marginalen Ausschnitt aus dem Persönlichkeitsbild, dessen Aussagekraft andere öffentlich zugängliche personenbezogene Daten nicht übersteigt (LG Waldshut-Tiengen, a.a.O., 108; VG Karlsruhe, a.a.O., 297).

Viele Eigentümer sehen allerdings ihre schutzwürdigen Interessen verletzt, weil sie fürchten, Diebesbanden könnten die Häuseraufnahmen nutzen, um Einbrüche zu planen. Ich habe Verständnis für diese Befürchtungen, teile sie aber nicht. Einbrecher werden das Objekt stets in Augenschein nehmen und sich nicht mit Aufnahmen begnügen, die nicht die für Einbrüche interessante Rückseite des Gebäudes erkennen lassen. Auch kann nur durch eine Prüfung vor Ort z. B. erkannt werden, ob das Haus von einem Hund bewacht wird oder ob eine Alarmanlage installiert und wie diese beschaffen ist.

Auch eine Eigentumsverletzung liegt nicht vor. Nach der Rechtsprechung des Bundesgerichtshofs kommt sie nicht in Betracht, wenn von einer öffentlichen Straße aus Häuser fotografiert werden. Ebenso wenig wird in das allgemeine Persönlichkeitsrecht in seiner Ausprägung des Schutzes der Privat- und Intimsphäre eingegriffen. Durch die Aufnahme und gewerbliche Weiterverarbeitung von Abbildungen der Außenansicht des Wohngebäudes wird nur der Teilbereich des Persönlichkeitsrechts berührt, der ohnehin der Öffentlichkeit zugewandt ist, und deshalb von vornherein allenfalls einen sehr begrenzten Schutz genießen kann. Einblicke in die Privat- oder gar Intimsphäre ermöglichen die Abbildungen nicht (LG Waldshut-Tiengen, a.a.O., 108; VG Karlsruhe, a.a.O., 296).

Einer Speicherung der Häuseraufnahmen stehen also keine überwiegenden schutzwürdigen Interessen entgegen. Bei einer Übermittlung wäre jeweils zu prüfen, ob sie mit § 29 Abs. 2 Satz 1 Nr. 1 a, Nr. 2 BDSG zu vereinbaren wäre. Der Verwendung der Häuser- und Gebäudekarte durch öffentliche Stellen zur Erfüllung ihrer Aufgaben werden schutzwürdige Interessen der Betroffenen regelmäßig nicht entgegenstehen. Bei einer Nutzung beispielsweise durch eine Bank im Zusammenhang mit der Entscheidung über einen Kreditantrag (falls diese in der Werbung des Tele-Info Verlags behauptete Möglichkeit überhaupt in Betracht kommt) wird die Aufnahme eines Hauses neben dem Grundbuchauszug und einem eventuellen Wertgutachten allenfalls ergänzend herangezogen werden. Es ist nicht erkennbar, wie die Häuseraufnahmen neben diesen aussagekräftigeren Unterlagen schutzwürdige Interessen des Kreditnehmers verletzen können.

Meine Auffassung ist unter Datenschutzbeauftragten nicht unumstritten. Sie wurde jedoch durch die genannten Entscheidungen bestätigt. Das OLG Karlsruhe (Urt. vom 16. März 2000) musste sich im Zusammenhang mit der Berufung gegen das Urteil des LG Landshut-Tiengen inhaltlich nicht im Einzelnen mit dessen Entscheidung auseinander setzen, weil die Berufung bereits aus anderen Gründen zurückgewiesen wurde, hat jedoch mit der Formulierung, die Entscheidung des Landgerichts beruhe auf „durchaus beachtlichen Gründen", zu erkennen gegeben, dass es dessen Auffassung teilt.

Der Tele-Info Verlag hat ohne Anerkennung einer Rechtspflicht angeboten, bei einem Widerspruch die Aufnahme eines Hauses zu löschen.

Wie auch bei digitalisierten Abbildungen von Personen (vgl. 5.1) wird der Gesetzgeber bei der Novellierung des Bundesdatenschutzgesetzes zu entscheiden haben, inwieweit für die kommerzielle Nutzung eines solchen Bildmaterials rechtliche Schranken geschaffen werden sollen. Unabhängig von gesetzgeberischen Aktivitäten kann bereits jetzt die Anwendbarkeit der Häuser- und Gebäu-

dekarte entscheidend beschränkt werden. Die wirkungsvollste Möglichkeit, eine Verknüpfung der Häuseraufnahmen mit Namen und Anschrift und die damit befürchteten Erkenntnis- und Missbrauchsmöglichkeiten zu verhindern, besteht darin, gegenüber den Anbietern von Telekommunikationsdienstleistungen Widerspruch gegen die Veröffentlichung der Wohnanschrift in gedruckten und elektronischen Telefonverzeichnisse einzulegen. Ich habe Interessenten auf diese Möglichkeit hingewiesen und entsprechende Musterschreiben zur Verfügung gestellt.

36.2 Weiterleitung eines Lebenslaufes durch eine Fortbildungseinrichtung

Bei einem insbesondere in der Qualifizierung von Arbeitslosen engagierten Fortbildungsträger habe ich einen datenschutzrechtlichen Verstoß feststellen müssen. Eine Teilnehmerin speicherte in dem Institut ihren Lebenslauf auf der Festplatte. Später wurde dieser Text durch das Institut an mehrere andere Zweigstellen per E-Mail weitergeleitet, da er als Musterlebenslauf weiterverwendet werden sollte. Dabei wurden die vollständigen Angaben aus dem „echten" Lebenslauf übernommen.

Bei der Aufklärung des Sachverhalts stellte sich heraus, dass den Arbeitssuchenden im Rahmen einer PC-Schulung angeboten wird, Bewerbungsschreiben, Lebensläufe u.Ä. zu verfassen. Dabei wird ihnen geraten, die geschriebenen Texte auf Diskette zu speichern. Diese wird gegen Unkostenerstattung zur Verfügung gestellt. Da die Betroffene ihre Daten nicht auf Diskette gespeichert hatte, erfolgte die Speicherung auf der Festplatte.

Nachdem dieser Sachverhalt bekannt geworden war, wurde seitens des Fortbildungsträgers mit der Betroffenen ein Gespräch geführt und die Löschung der Daten in den Zweigstellen veranlasst. Es ist davon auszugehen, dass künftig das Angebot der Speicherung auf eigenen Disketten von allen Schulungsteilnehmern genutzt wird und der Fortbildungsträger die entsprechenden Hinweise im eigenen Interesse verstärkt.

36.3 Selbstauskunft von Mietinteressenten bei Vermietungen

Im Berichtszeitraum hatte ich mehrere Anfragen zu Fragebögen, die Mietinteressenten von Wohnungseigentümern, Hausverwaltungen oder Maklern vorgelegt werden. Die Mietinteressenten fühlten sich gezwungen, solche Fragebögen auszufüllen, um eine Chance auf den Abschluss eines Mietvertrages zu erhalten. Gerade deshalb ging es ihnen darum, die bezweifelte Zulässigkeit einzelner Fragen von mir prüfen zu lassen.

Voraussetzung für die Anwendung des Dritten Abschnitts des BDSG ist, dass personenbezogene Daten „in oder aus Dateien" verarbeitet werden (§ 1 Abs. 2 Nr. 3, § 27 Abs. 1 Satz 1 Nr. 1 i. V. m. § 3 Abs. 2 BDSG). Bei den von mir in diesem Zusammenhang befragten Vermietern wird das ausgefüllte Formular in der Mietakte aufbewahrt. Eine Verarbeitung der Angaben in einer Datei erfolgt nicht. Die Selbstauskünfte von nicht berücksichtigten Bewerbern werden nach Abschluss der Mietverhandlungen vernichtet. Somit ist das BDSG nicht anwendbar. Ich habe dennoch die Petenten auf die Rechtsprechung der Zivilgerichte hingewiesen:

Die herrschende Rechtsprechung geht dahin, dass solche Fragebögen nicht generell unzulässig sind. Zulässig sind danach Fragen, an deren Beantwortung für den Vermieter ein „berechtigtes, billigenswertes und schützenswertes Interesse" besteht. Unzulässig sind Fragen, die diskriminierend sind und für die kein sachlicher Grund besteht. Dabei ist das Informationsinteresse des Vermieters gegen

das Interesse der Mietinteressenten, ihre Privatsphäre zu schützen, abzuwägen. Soweit die Rechtsprechung eine Verpflichtung zur Auskunft annimmt, hat dies bei Falschangaben zur Folge, dass der Mietvertrag durch den Vermieter wegen arglistiger Täuschung nach § 123 BGB angefochten werden kann. Fragen, die einen Einbruch in die zu schützende Individualsphäre des Mietinteressenten darstellen, berechtigen bei wahrheitswidriger Beantwortung den Vermieter dagegen nicht zur Anfechtung des Mietvertrages.

Die Rechtsprechung ist in der Ausfüllung der unbestimmten Rechtsbegriffe uneinheitlich und einzelfallbezogen. Von einem Teil der Gerichte wird eine Reihe der in den Fragebögen vorgesehenen Angaben als unzulässig angesehen. Dies sind z. B. Angaben über

- Familienstand des Mieters,
- Detailangaben zu Familienangehörigen (z. B. Geburtsname, -datum, Verwandtschaftsgrad, Einkommen), die über Namen und Alter hinausgehen,
- die derzeitige Wohnung, soweit Auskünfte über den monatlichen Mietzins, Name und Anschrift des derzeitigen Vermieters verlangt werden,
- den Arbeitgeber des Vertragsschließenden und seines Ehegatten.
- Genauere Angaben zum Ehegatten bzw. Mitmieter sind für den Vermieter nur dann von Interesse, wenn der Ehegatte auch Mietvertragspartner sein soll. In diesem Fall ist die Selbstauskunft bei dem Ehegatten selbst einzuholen. Im Übrigen habe ich auf die Interessenvertretung durch Mietervereine hingewiesen.

Anlagen Entschließungen der Datenschutzbeauftragten des Bundes und der Länder

Anlage 1

25./26. März 1999: Modernisierung des Datenschutzrechts jetzt - **umfassende Novellierung des BDSG nicht aufschieben**

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

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

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

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

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

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

Anlage 2

25./26. März 1999: **Geplante erweiterte Speicherung von Verbindungsdaten in der Telekommunikation**

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

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

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

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

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

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

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

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

Anlage 3

25./26. März 1999: **Transparente Hard- und Software**

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

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

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

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

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

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

Anlage 4

25./26. März 1999: **Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL '98)**

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

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

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

Anlage 5

17. Juni 1999: **Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern**

Bei der Einführung der Befugnis zum „Großen Lauschangriff" hat der Gesetzgeber im Grundgesetz ein Verfahren zur parlamentarischen Kontrolle weit reichender Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung verankert (Artikel 13 Abs. 6 GG). Dieses Verfahren dient nach dem Willen des Gesetzgebers der parlamentarischen Kontrolle der Normeffizienz und hebt zugleich die politische Kontrollfunktion der Parlamente gegenüber der Exekutive hervor. Auch wenn es die Überprüfung von Lauschangriffen durch die Gerichte und Datenschutzbeauftragten nicht ersetzt, hat es gleichwohl eine grundrechtssichernde Bedeutung. Jetzt ist jedoch bekannt geworden, dass einige Landesjustizverwaltungen der Ansicht sind, Art. 13 Abs. 6 GG sehe eine Berichtspflicht über Lauschangriffe zu Strafverfolgungszwecken gegenüber den Landesparlamenten nicht vor.

Im Gegensatz dazu vertritt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Auffassung, dass die Verfassung eine effektive parlamentarische Kontrolle von Lauschangriffen auf Landesebene vorschreibt, die der Kontrolle auf Bundesebene gleichwertig sein muss. Bei Maßnahmen zur Strafverfolgung durch Landesbehörden besteht die parlamentarische Verantwortlichkeit gegenüber den Landesparlamenten. Die Landtage müssen die Möglichkeit haben, die ihnen in anonymisierter Form übermittelten Berichte der Landesregierungen öffentlich zu erörtern. Die Landesparlamente sollten deshalb durch Gesetz eine regelmäßige Berichtspflicht der Landesregierung für präventiv-polizeiliche und repressive Lauschangriffe vorsehen. Nur auf diese Weise ist eine wirksame parlamentarische Kontrolle der Ausübung dieser einschneidenden Überwachungsbefugnis gewährleistet.

Wird durch eine solche Kontrolle deutlich, dass die akustische Wohnraumüberwachung für Zwecke der Strafverfolgung in der Praxis nicht die vom Gesetzgeber angestrebte Effizienz im Verhältnis zur Häufigkeit und Intensität der Grundrechtseingriffe zeigt, können Landesregierungen, die das Bundesrecht in eigener Verantwortung auszuführen haben, über den Bundesrat darauf hinwirken, die Befugnis für eine derartige Überwachung wieder aufzuheben oder zumindest zu modifizieren.

Anlage 6

25. August 1999: **Gesundheitsreform**

Die Datenschutzbeauftragten von Bund und Ländern erklären zu dem Entwurf eines Gesetzes "Gesundheitsreform 2000":

Die Datenschutzbeauftragten haben großes Verständnis für die Bemühungen, die Kosten im Gesundheitswesen zu begrenzen und eine gute Versorgung der Patientinnen und Patienten sicherzustellen. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, beim Eingriff in das Recht auf informationelle Selbstbestimmung das Prinzip der Erforderlichkeit und der Verhältnismäßigkeit zu wahren.

Der Entwurf lässt jede Begründung vermissen, warum die bisherigen Kontrollmechanismen, die das Entstehen umfangreicher medizinischer Patientendatenbestände bei den Krankenkassen vermeiden, ungeeignet sein sollen, die Wirtschaftlichkeit und Qualität ärztlicher Leistungserbringung sicherzustellen.

Der Entwurf gibt das bisherige Konzept der Datenverarbeitung in der gesetzlichen Krankenversicherung auf. Insbesondere standen bisher aus dem ambulanten Bereich personenbezogene Abrechnungsdaten mit medizinischen Inhalten und Diagnosedaten den Krankenkassen nur ausnahmsweise zu Prüfzwecken zur Verfügung, künftig sollen diese Informationen den Krankenkassen dagegen generell versichertenbezogen übermittelt werden. Damit entstehen bei den gesetzlichen Krankenkassen vollständige personenbezogene medizinische Datenbestände der gesetzlich Versicherten mit der Möglichkeit, für jede einzelne Person umfassende Darstellungen ihres Gesundheitszustandes zu bilden. Bei den Kassen entstehen gläserne Patientinnen und Patienten. Das Patientengeheimnis wird ausgehöhlt.

Die Datenschutzbeauftragten richten an den Gesetzgeber die dringende Bitte, die bisher versäumte eingehende Prüfung von Erforderlichkeit und Verhältnismäßigkeit der weiterreichenden Datenverarbeitungsbestimmungen nachzuholen. Der Bundesbeauftragte für den Datenschutz, mit dem der Entwurf entgegen anders lautenden Äußerungen von Regierungsvertretern in der Sache bisher in keiner Weise abgestimmt wurde, sowie die Datenschutzbeauftragten der Länder stehen hierfür zur Diskussion zur Verfügung.

Insbesondere klärungsbedürftig sind folgende Punkte:

Der Entwurf erweitert die Aufgaben der Krankenkassen auch auf eine steuernde und durch die Patientinnen und Patienten nicht geforderte Beratung über Gesundheitserhaltungsmaßnahmen und auf eine Prüfung der u. a. durch die Ärztinnen und Ärzte erbrachten Leistungen. Er sieht dafür umfangreiche Datenerhebungs- und -verarbeitungsbefugnisse vor.

Der Wortlaut des Entwurfes beschreibt diese Aufgabe allerdings nur vage. Er lässt nicht erkennen, was auf die Patientinnen und Patienten zukommt. Weder ist klar geregelt, wie weit die Beratung reichen darf, noch mit welchen Rechtsfolgen die oder der Einzelne rechnen muss. Es ist zu befürchten, dass diese Beratung dazu dienen wird, die Patientinnen und Patienten, Ärztinnen und Ärzte und die sonstigen Leistungserbringer zu kontrollieren und zu beeinflussen und dass hierdurch das Arzt-Patienten-Vertrauensverhältnis belastet wird.

Wegen der vagen Aufgabenbeschreibung sind auch die damit verbundenen Datenverarbeitungs- und -zusammenführungsbefugnisse in gleicher Weise unklar und verschwommen. Eine Präzisierung und Eingrenzung ist dringend erforderlich.

Der Entwurf sieht im Gegensatz zum bisherigen System vor, dass Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die

Diagnosen nach dem international gültigen ICD-10-Schlüssel zu codieren, sind diese medizinischen Informationen z. B. im Bereich der Psychotherapie auch hochdifferenziert.

Die zur Begründung besonders angeführten Punkte "Unterrichtung der Versicherten über die in Anspruch genommenen Leistungen, Kontrolle der Einhaltung der zweijährigen Gewährleistungspflicht bei den Zahnärzten, Unterstützung der Versicherten bei Behandlungsfehlern" vermögen insoweit nicht zu überzeugen. Bereits jetzt können die Versicherten über die beanspruchten Leistungen und deren Kosten informiert werden und von ihrer Krankenkasse auch im Übrigen Unterstützung erbitten, sodass keine Notwendigkeit für die Anlegung derart sensibler, umfangreicher und zentraler Datenbestände ersichtlich ist.

Der Eingriff in die Rechte der Patientinnen und Patienten steht damit in keinem Verhältnis zu den angegebenen Zwecken.

Die beabsichtigte Einführung von zentralen Datenannahme- und -verteilstellen, bei denen nicht einmal klar ist, in welcher Rechtsform (öffentlich oder privat) sie betrieben werden sollen, hat eine weitere, diesmal Krankenkassen übergreifende zentrale Sammlung medizinischer personenbezogener Patientendaten zur Folge. Wegen des hohen weiteren Gefährdungspotentials von derart umfassenden Datenbeständen müsste der Entwurf im Einzelnen begründen, warum eine konsequente Umsetzung der schon bisher möglichen Kontrollmechanismen nicht ausreicht.

Die angesprochenen Punkte stellen besonders gewichtige, aber keineswegs die einzigen Probleme dar. Zu nennen sind hier nur beispielsweise die Verlängerung der Speicherdauer von Patientendaten beim Medizinischen Dienst der Krankenversicherung (MDK) von 5 auf 10 Jahre, unzureichende Regelungen bei den Speicherfristen, bei Umfang, Zweckbindung und Freiwilligkeit der Datenerhebung beim Hausarztmodell, der integrierten Versorgung und den Bonus-Modellen sowie unzureichende Pseudonymisierung bei den Arbeitsgemeinschaften. Abzulehnen ist auch die völlig mangelhafte Zweckbindung der Daten bei den Krankenkassen.

Anlage 7

7./8. Oktober 1999: **Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften**

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

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

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

Anlage 8

7./8. Oktober 1999: **Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation**

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weitreichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten lässt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31.12.1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern statt dessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100 a StPO neu geregelt werden.

Anlage 9

7./8. Oktober 1999: DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

In der Strafprozessordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u. a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis - also ohne richterliche Anordnung - erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z. B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflusst, ist dennoch davon auszugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen - abweichend von den gesetzlich vorgesehenen Verfahren - systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Reglung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

Anlage10

7./8. Oktober 1999: **Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union**

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: "Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern".

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs. 1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m: Art. 1 Abs. 1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

Anlage 11

7./8. Oktober 1999: **Patientenschutz durch Pseudonymisierung**

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des "gläsernen Patienten" verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

Anlage 12

7./8. Oktober 1999: Eckpunkte der deutschen Kryptopolitik - **ein Schritt in die richtige Richtung**

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

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

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

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

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,
- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern, Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen), Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,
- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,
- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offengelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

Anlage 13

7./8. Oktober 1999: **„Täter-Opfer-Ausgleich und Datenschutz“**

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

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

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

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

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

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

Anlage 14

14./15. März 2000: **Risiken und Grenzen der Videoüberwachung**

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht darin die Gefahr, dass diese Entwicklung zur einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen

- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen
- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten
- sowie die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozessrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch video-technisch gewonnener - insbesondere biometrischer - Daten und deren Abgleiche.

Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch öffentliche Stellen dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.
   - Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. Dafür kommen - soweit nicht überwiegende

schutzwürdige Belange von Betroffenen entgegenstehen - unter Anderem in Betracht

- die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden.
- für die Verkehrslenkung nur Übersichtsaufnahmen,
- der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.
- Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.
- Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.
- Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.
- Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.
- Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.

Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung durch Private Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

Anlage 15

14./15. März 2000: **Für eine freie Telekommunikation in der freien Gesellschaft**

Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

– Erhebliche Zunahme der Telekommunikationsvorgänge

  Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, e-mail und mail-boxen sowie das Internet genutzt.

– Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten

– Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.

– Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch e-mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.

– Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.

– Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.

– Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.

– Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten

  Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.

– Entwicklung des Internets zum Massenkommunikationsmittel

  Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.

– Schwer durchschaubare Rechtslage

– Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar..

– Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

– Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: 1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802

– Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen - der Katalog wurde

seit Einführung 11 mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.

– Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.

– Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen "ENFOPOL", befasst sich u. a. mit der Frage, welchen Anforderungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weitergehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

– Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.

– Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.

– Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.

– Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.

– Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Ein-

griffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.

- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.

- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstelenanlagen in Hotels, Krankenhäuser oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.

- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselung von elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.

- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.

- Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

Anlage 16

14./15. März 2000: **Data Warehouse**

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an. Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im „Data Warehouse" werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. „Data Mining" bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem „Daten-Lagerhaus" gesammelt werden.
- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden ist. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.
- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.
- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.
- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern" rechtswidrig.
- Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). „Data Mining" ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von „Data Warehouse"- und „Data Mining"-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

Anlage 17

14./15. März 2000: **Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zu den Abhörmaßnahmen des BND**

Das Bundesverfassungsgericht hat für die Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen wurden, deutliche Schranken gezogen, die weit über den Gegenstand des Verfahrens hinaus bedeutsam sind.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses zur Aufrechterhaltung einer freien Telekommunikation, die eine Grundvoraussetzung der Informationsgesellschaft darstellt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichtes zu den verdachtslosen Abhörmaßnahmen des BND auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird (Telefon, E-Mail, Telefax, Internet-Abrufe o. Ä.).

Die Anforderungen des Urteils müssen auch Konsequenzen für Fallgestaltungen, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem Einsatz technischer Mittel.

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

- Zur Sicherung der Zweckbindung der erlangten Daten und für die Kontrolle ihrer Verwendung muss ihre Herkunft aus Eingriffen in das Fernmeldegeheimnis oder vergleichbaren Eingriffen durch eine entsprechende Kennzeichnung nach der Erfassung auch bei den Übermittlungsempfängern erkennbar bleiben.
- Die erlangten Daten müssen bei allen speichernden Stellen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind - es sei denn, der Rechtsschutz der Betroffenen würde dadurch verkürzt. Die Praxis von Verfassungsschutzämtern, nicht (mehr) erforderliche Daten, wenn sie sich in Unterlagen befinden, nicht zu schwärzen, kann - zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden - nicht mehr aufrechterhalten werden. Um die Notwendigkeit einer späteren Schwärzung zu vermeiden, sollten bereichsspezifischen Vernichtungsregelungen bereits bei der Aktenführung Rechnung getragen werden.
- Die Vernichtungspflicht ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln. Eine Löschung oder Vernichtung ist nach einem Auskunftsantrag bei allen personenbezogenen Daten unzulässig. Zudem sind personenbezogene Daten, die durch die o.g. Maßnahmen erlangt wurden, nach einer Unterrichtung der Betroffenen für einen angemessenen Zeitraum - ausschließlich zum Zweck der Sicherung des Rechtsschutzes - aufzubewahren.
- Überwachte Personen müssen von Eingriffen unterrichtet werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet wird; dies gilt auch für weitere Betroffene, es sei denn, überwiegende schutzwürdige Belange der überwachten Person stehen dem entgegen (Schutz vor unnötiger Bloßstellung).
- Wie bei Eingriffen in das Fernmeldegeheimnis ist dies auch bei anderen verdeckten Maßnahmen Voraussetzung dafür, dass die Betroffenen von den ihnen zustehenden Rechten Gebrauch machen können, und daher von Art. 19 Abs. 4 GG geboten. Speicherfristen können die Unterrichtungspflicht nicht beseitigen, irrelevante Daten sind umgehend zu löschen.
- Damit sind Regelungen z. B. in Landesverfassungsschutz- und Polizeigesetzen nicht zu vereinbaren, wonach eine Unterrichtung der Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmeldegeheimnis gleichkom-

men, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Eingriffes ausgeschlossen werden kann.

- Zusätzlich zur unbefristeten Benachrichtigungspflicht ist eine Mitteilung an die Datenschutzkontrollstelle für den Fall vorzusehen, dass die Unterrichtung der Betroffenen länger als fünf Jahre zurückgestellt wird.

- Der Umgang des Verfassungsschutzes mit personenbezogenen Daten, die in Durchbrechung des Fernmeldegeheimnisses erhoben worden sind, ist durch eine unabhängige Datenschutzkontrollstelle lückenlos zu überprüfen.

- Eine Kontrolllücke bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden, wäre verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet.

- Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten einschließlich der Benachrichtigung - bei Datenübermittlungen auch bei den Datenempfängern - erstrecken.

- Der Gesetzgeber sollte festlegen, dass die Übermittlung der Daten, die Prüfung der Erforderlichkeit weiterer Speicherung sowie die Durchführung der Vernichtung und Löschung der Daten aus G 10-Maßnahmen zu protokollieren sind.

- Für eine effektive Kontrolle sind die zuständigen Stellen personell und sachlich angemessen auszustatten.

- Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weitergehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist.

Anlage 18

14./15. März 2000: **Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)**

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluss des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,
- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z. B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, sodass sie uneingeschränkt zur Strafverfolgung genutzt werden können,
- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,
- nicht am Verfahren beteiligte Dritte schon bei „berechtigtem Interesse" Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

Anlage 19

14./15. März 2000: **Unzulässiger Speicherungsumfang in „INPOL-neu“ geplant**

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung „INPOL-neu“ eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur soweit eingegriffen wird, wie dies im Rahmen der Erforderllichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes-Kriminalaktennachweis (KAN) die „gesamte kriminelle Karriere“ jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereit gehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventiven als auch im repressiven Bereich auf „Straftaten mit länderübergreifender, internationaler oder erheblichen Bedeutung“. Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die „Straftaten“, nicht die einzelne Person und auch nicht das „Gesamtbild einer Person“. Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten einzelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

Anlage 20

10. Oktober 2000: **Auftragsdatenverarbeitung durch das Bundeskriminalamt**

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollen aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden.

§ 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen, zu. Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises und der Innenministerkonferenz gefasst worden.

Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.

Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im Wesentlichen mit Kosten- und Zeitargumenten begründet. Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen.

Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz stautuierte Schwelle, dass nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.

Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren an die Innenminister/-senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

Die Datenschutzbeauftragten warnen vor einer solchen Entwicklung und fordern dazu auf, die für die Datenverarbeitung beim BKA gesetzlich gezogenen Grenzen strikt zu beachten.

Anlage 21

12./13. Oktober 2000: **Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung**

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 3 GG zur Strafverfolgung eingesetzten „Großen Lauschangriffe" zu unterrichten. § 100e StPO konkretisiert die Berichtspflicht dahingehend, dass die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.

Diese Berichte sollen eine laufenden parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen. Der Bundestag soll aufgrund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahme zu überprüfen.

Diesen Anforderungen wird der erste von der Bundesregierung vorgelegte Bericht nicht in vollem Umfang gerecht. So wurde nur die Gesamtzahl der von der Anordnung Betroffenen erfasst, wobei zwischen Beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird.

Nach § 100e Abs. 1 StPO muss über den Umfang der Maßnahme berichtet werden. Hierzu zählt die Angabe über die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der gerichtlichen Anordnung genannten. Von dem „Großen Lauschangriff" ist jeder betroffen, dessen gesprochenes Wort in der Wohnung abgehört wird. Er greift auch in die grundrechtlich geschützten Rechte der am Verfahren Unbeteiligten, wie z. B. unverdächtige Familienangehörige, Bekannte, Besucherinnen und Besucher sowie sonstige Personen, die nicht selbst Wohnungsinhaber sind, ein. Dem wollte der Gesetzgeber mit der Einführung der Berichtspflicht Rechnung tragen.

Die Beschränkung der Berichtspflicht auf Wohnungsinhaber und Beschuldigte gibt nicht den wirklichen Umfang der von der Maßnahme betroffenen Personen wieder. Somit erfüllt sie den Zweck der im Grundgesetz vorgesehenen Berichtspflicht nicht.

Darüber hinaus wäre es wünschenswert, wenn - wie in den „Wire-tap-Reports" der USA - die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Die oben genannten Forderungen gelten deshalb gleichermaßen bzw. in entsprechender Weise für die den Landesparlamenten vorzulegenden jährlichen Berichte über die nach § 100 c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen bzw. über die von der Polizei zur Gefahrenabwehr veranlassten „Großen Lauschangriffe".

Anlage 22

12./13. Oktober 2000: Vom Bürgerbüro zum Internet - **Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung**

Bei der Modernisierung der öffentlichen Verwaltung soll insbesondere die Dienstleistungs- und Serviceorientierung verbessert werden. Dazu sollen unter anderem Dienstleistungen in multifunktionalen Servicecentern (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) gebündelt und die Möglichkeiten der modernen Informations- und Kommunikations-Technik intensiver genutzt werden (Information, Kommunikation und Transaktion über das Internet, Einrichtung von Call-Centern).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauftragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personenbezogener Daten gewährleistet wird. Nur Serviceangebote, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen letztlich sowohl Bürgerinnen und Bürgern als auch der Verwaltung selbst.

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

Anlage 23

12./13. Oktober 2000: **Novellierung des BDSG**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz - § 3a E-BDSG) und die Einführung des Datenschutzaudit (§ 9a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in die bewährten Strukturen des betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltensweisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.

Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudit in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

Anlage 24

12./13. Oktober 2000: **Datensparsamkeit bei der Rundfunkfinanzierung**

Die Finanzierung des öffentlich-rechtlichen Rundfunks ist derzeit Gegenstand öffentlicher Diskussion in der Politik und unter den Rundfunkanstalten selbst. Erörtert wird hierbei auch, ob die Erhebung von Rundfunkgebühren, die an das „Bereithalten eines Rundfunkempfangsgerätes“ anknüpfen, im Hinblick auf veränderte Gerätetechniken und bestehende Mängel im Verfahren modifiziert oder durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte.

Künftig wird kaum noch überschaubar sein, welche Geräte zum Rundfunkempfang geeignet sind. Über die eigentlichen Fernseh- und Rundfunkgeräte hinaus ist dies bereits heute beispielsweise mit Personalcomputern, die über einen Internetzugang verfügen, oder mit bestimmten Mobiltelefonen möglich. In naher Zukunft werden neue Technologien wie UMTS weitere Empfangsmöglichkeiten eröffnen. Sofern der Besitz derartiger multifunktionaler Geräte zum Kriterium für die Rundfunkgebührenpflicht gemacht wird, würde das zu einer erheblichen Ausweitung von Datenabgleichen führen. Schon das gegenwärtig praktizierte Gebühreneinzugsverfahren erfordert in großem Umfang die Verarbeitung personenbezogener Daten. Nach den Angaben der Rundfunkanstalten meldet ein signifikanter Teil der Rundfunkteilnehmerinnen und -teilnehmer trotz der Verpflichtung hierzu seine Geräte nicht an. Um möglichst alle Gebührenpflichtigen zu erfassen, nutzen die Rundfunkanstalten Daten aus dem Melderegister, vom privaten Adresshandel und setzen vor Ort Rundfunkgebührenbeauftragte ein, die einzelne Haushalte aufsuchen. Damit wird in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung vieler gesetzestreuer Bürgerinnen und Bürger eingegriffen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesländer auf, einer Neuordnung ein Modell zu Grunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Nach ihrer Überzeugung lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen, das Recht auf informationelle Selbstbestimmung weniger stark einschränkenden Finanzierungsmodellen als dem derzeit praktizierten gewährleisten

Anlage 25

12./13. Oktober 2000: **Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms**

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.

Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine „genetische Diskriminierung" bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen zu verhindern. Auf der Grundlage dieser und in der „Entschließung über Genomanalyse und informationelle Selbstbestimmung" vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.

2. Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnnen Informationen zu löschen oder an den Betroffenen herauszugeben.

3. Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten.

4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.

5. Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u. a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.

6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen

Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe.

   Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

   Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden.

   Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden. Demnächst werden nicht nur - wie bisher - Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

214 (Ausgegeben am 22. Dezember 2000)