Unterrichtung

Landesbeauftragter für den Datenschutz Niedersachsen

Hannover, den 30. Dezember 1998

An den
Herrn Präsidenten des Niedersächsischen Landtages

Hannover

14. Bericht über die Tätigkeit 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 14. Tätigkeitsbericht für die Kalenderjahre 1997 und 1998.

Mit dem Ausdruck meiner vorzüglichen Hochachtung

Dr. Gerhard Dronsch

Inhaltsverzeichnis

Abkürzungen

ABl.	Amtsblatt
Abs.	Absatz
ADV	Automatisierte Datenverarbeitung
AG	Aktiengesellschaft
Aids	Acquired Immune Deficiency Syndrome
AOK	Allgemeine Ortskrankenkasse
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS Innere Sicherheit (PIOS = Personen, Institutionen, Objekte, Sachen)
Art.	Artikel
AsylVfG	Asylverfahrensgesetz
Aufl.	Auflage
AuslG	Ausländergesetz
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
BAKred	Bundesaufsichtsamt für das Kreditwesen
BdB	Bundesverband deutscher Banken
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
BS 2000	Betriebssystem 2000 (Großrechner-Betriebssystem)
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
Btx-StV	Bildschirmtext-Staatsvertrag
Buchst.	Buchstabe
BVerfGE	Bundesverfassungsgericht (Entscheidungssammlung)
BVerwG	Bundesverwaltungsgericht
bzgl.	bezüglich
bzw.	beziehungsweise
ca.	circa
CD-ROM	Compact Disc Read Only Memory
CR	Computer und Recht
DDV	Deutscher Direktmarketing Verband e.V.
DES	Data Encryption Standard
DFG	Deutsche Forschungsgemeinschaft
d. h.	das heißt
DIN	Deutsche Industrie Norm(en)
DNA	Desoxyribonukleinsäure
DÖV	Die Öffentliche Verwaltung
DSB	Datenschutzbeauftragter
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
EC	Eurocheque
ED	Erkennungsdienst
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaften
einschl.	einschließlich
EU	Europäische Union
EUROPOL	Europäisches Polizeiamt
EUV	EU-Vertrag
evtl.	eventuell
FDA	Food and Drug Administration
FeV	Fahrerlaubnis-Verordnung
f(f).	und folgende Seite(n)
ftp	File Transfer Protocol
GBO	Grundbuchordnung
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
GG	Grundgesetz
ggf.	gegebenenfalls
GewAnz-VwV	Gewerbeanzeigenverwaltungsvorschrift
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GMBl.	Gemeinsames Ministerialblatt
GVG	Gerichtsverfassungsgesetz

GwG	Geldwäschegesetz
HIV	Human Immunodeficiency Virus
HTML	Hypertext Markup Language
ICD	International Classification of Disease
IDEA	(Verschlüsselungsalgorithmus)
INPOL	(bundesweites) Informationssystem der Polizei
I/O	Input/Output
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
KDO	Zweckverband Kommunale Datenverarbeitung Oldenburg
Kfz	Kraftfahrzeug
KOMNET	Kommunikationsnetz der Niedersächsischen Landesregierung
LAN	Local Area Network
LfD	Landesbeauftragter für den Datenschutz
LKAN	Landeskriminalamt Niedersachsen
LRG	Landesrundfunkgesetz
LRH	Landesrechnungshof
LT-Drs.	Landtagsdrucksache
MDK	Medizinischer Dienst der Krankenversicherung
MF	Finanzministerium
MFAS	Ministerium für Frauen, Arbeit und Soziales
MI	Innenministerium
MIC	(Verschlüsselungsprogramm des BSI)
MK	Kultusministerium
MO	Magnetic Optical
MS	Microsoft
MVS/VM	Multiple Virtual Storage/Virtual Machine (Großrechner-Betriebssystem)
MVS/RACF	Multiple Virtual Storage/Resource Access Control Facility
NBG	Niedersächsisches Beamtengesetz
NDR	Norddeutscher Rundfunk
Nds.	Niedersächsische(r/s)
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
NMG	Niedersächsisches Meldegesetz
Nr.	Nummer
NSchG	Niedersächsisches Schulgesetz
NWG	Niedersächsisches Wassergesetz
o. g.	oben genannt
OK	Organisierte Kriminalität
OLG	Oberlandesgericht
OP-	Operations-
OWi	Ordnungswidrigkeiten
PersVG	Personalvertretungsgesetz
PC	Personal Computer
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKK	Kurdische Arbeiterpartei
PLZ	Postleitzahl
POLAS	Polizeiliches Auskunftssystem (in Niedersachsen)
P.S.	Postskript(um)

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-rd.	Rivest-Shamir-Adleman-rund
RdErl.	Runderlass
RVO	Reichsversicherungsordnung
S.	Seite
Sächs-VerfGH	Sächsischer Verfassungsgerichtshof
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SchuVVO	Schuldnerverzeichnisverordnung
SGB	Sozialgesetzbuch
SIJUS- Straf	(ADV-System der Staatsanwaltschaften)
s. a.	siehe auch
s. o.	siehe oben
sog.	sogenannt(e/r)
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
TÜ	Telefonüberwachung
u. a.	unter anderem, und andere
u. Ä.	und Ähnliches
UDSV	Teledienstunternehmen-Datenschutzverordnung
UNICEF	United Nations International Children's Emergency Fund
UNIX	(ADV-Betriebssystem für Mehrplatzsysteme)
USA	Vereinigte Staaten von Amerika
usw.	und so weiter
u. U.	unter Umständen
VGH	Verwaltungsgerichtshof
vgl.	vergleiche
VGO	Vollzugsgeschäftsordnung
VV	Verwaltungsvorschrift
VW	Volkswagen
VwVfG	Verwaltungsverfahrensgesetz
VZR	Verkehrszentralregister
Windows NT	(PC-Netzwerk-Betriebssystem)
WORM	Write Once Read Many
WpHG	Wertpapierhandelsgesetz
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
z. T.	zum Teil
z. Z.	zur Zeit

1 Vorbemerkung

Der vorliegende XIV. Tätigkeitsbericht betrifft gemäß § 22 Abs. 3 Satz 1 NDSG zwei Kalenderjahre: 1997 und 1998. Redaktionsschluss war der 27. November 1998. Der Bericht behält die bewährte und vertraute Gliederung bei. Am Ende – Kapitel 29 bis 40 – findet sich wiederum der Bericht über den Datenschutz im nicht-öffentlichen Bereich (§ 22 Abs. 6 Satz 3 NDSG).

Die Seitenzahl ist im Vergleich zum letzten Tätigkeitsbericht erneut etwas reduziert worden. Die Auflagenhöhe des Berichts bleibt auf 9 000 Exemplare gesenkt. Dies ist vor allem deshalb vertretbar, weil ich den Tätigkeitsbericht gemeinsam mit anderen Datenschutzinformationen kostengünstig auch als CD-ROM und im Internet anbiete (vgl. unten 3.4 und 3.5). Angemerkt sei, dass die früheren Tätigkeitsberichte entweder völlig oder fast vergriffen sind.

2 Zur Situation des Datenschutzes

2.1 Informationsgesellschaft und Datenschutz

Wie bereits im letzten Tätigkeitsbericht hervorgehoben (vgl. XIII 2.1), befinden wir uns in einer Zeit des Übergangs von der klassischen Industriegesellschaft zur Informationsgesellschaft. Diese Entwicklung ist unumkehrbar; sie hat sich in den beiden Berichtsjahren beschleunigt, nicht zuletzt im Zusammenhang mit der Globalisierung von Wirtschaft und Wissenschaft. Informationen werden für Staat, Wirtschaft und Private immer wichtiger. Durch den Einsatz der automatisierten Datenverarbeitung hat Information die Qualität eines vierten Produktionsfaktors neben Arbeit, Kapital und Rohstoffen erhalten.

In dem Bericht „Informationsgesellschaft – Chancen, Innovationen und Herausforderungen“, den der Rat für Forschung, Technologie und Innovation im Dezember 1995 dem Bundeskanzler überreichte, wird mit Recht hervorgehoben, dass die Informationsgesellschaft politisch gesehen eine demokratische Gesellschaft bleiben, wirtschaftlich gesehen ihre ökonomische Leistungsfähigkeit erheblich steigern und kulturell gesehen eine Wissensgesellschaft mit einer entsprechenden Informations- und Medienkultur werden muss. Unter dem Aspekt „demokratische Gesellschaft“ kommt dem Datenschutz eine besondere Bedeutung zu. In dem genannten Bericht heißt es zutreffend: „Ein konsequenter Datenschutz zählt ... zu den zentralen Akzeptanzvoraussetzungen der Informationsgesellschaft“ (S. 32).

Was die Wichtigkeit von Informationen anbetrifft, so sei aus meiner Tätigkeit im Berichtszeitraum vor allem ein Fall genannt (vgl. näher unten 27.5.2): In der Mordsache der elfjährigen Christina Nytsch aus Strücklingen (Landkreis Cloppenburg) kam es im April 1998 zum bislang größten Gentest in Deutschland. Ca. 17 900 junge Männer zwischen 18 und 30 Jahren wurden aufgefordert, sich freiwillig einem Speicheltest zu unterziehen. Nur vier Personen weigerten sich. Die in einigen Punkten nicht unproblematische Aktion führte bekanntlich zur Ergreifung des Täters. Der Massen-Gentest wurde begleitet vom Aufbau einer zentralen Gendatei beim Bundeskriminalamt.

Im März/April 1998 führte das Freitzeit-Forschungsinstitut der British American Tobacco (Leiter: Prof. Dr. Horst W. Opaschowski) eine bundesweite Repräsentativbefragung von 3 000 Personen zum Thema Datenschutz durch. Das Ergebnis zeigt eine hohe Unterstützung des Datenschutzes in der Bevölkerung, die manchen Vermutungen widerspricht. Mehr als die Hälfte (55 %) der Bevölkerung ist der Meinung, dass der Datenschutz mehr Bedeutung bekommen sollte.

Wenngleich das Grundrecht auf Datenschutz (besser: auf informationelle Selbstbestimmung) ein tragendes Element der Informationsgesellschaft ist, so ist es doch nicht schrankenlos. Wie im Volkszählungsurteil des Bundesverfassungsgesetzes ausgeführt wird, sind Einschränkungen dieses Grundrechts im überwiegenden Allgemeininteresse zulässig. Die Abwägung zwischen dem Recht auf informationelle Selbstbestimmung und anderen Rechtsgütern - die „Herstellung praktischer Konkordanz“ - ist in erster Linie Aufgabe des Gesetzgebers; es kann aber auch der Rechtsanwender gefordert sein. Bei der Güterabwägung gibt es immer wieder Probleme. Im Berichtszeitraum haben zwei Bereiche eine größere Rolle gespielt: die innere Sicherheit und die Forschung. Es sei je ein Fall genannt:

Im Januar 1997 gab es Meldungen in der Presse, Datenschutz habe die polizeiliche Aufklärung des Mordes an der zehnjährigen Kim Kerkow aus Varel behindert; besonders ausfallend war die Überschrift in der Hamburger Morgenpost vom 18. Januar 1997: „Kim. Datenschutz deckte Mörder.“ Das Schlagwort „Datenschutz ist Täterschutz“ (vgl. bereits XII 2.2) war schnell bei der Hand. Ich legte in einer Presseinformation vom 21. Januar 1997 dar, dass Datenschutzregelungen die Aufklärung des Mordfalles nicht behindert haben; der Niedersächsische Innenminister stimmte dem in der Sitzung des Landtags am 23. Januar 1997 zu. Zum Slogan „Datenschutz ist Täterschutz“ ist zu sagen, dass er verfassungsrechtlich nicht haltbar ist, da er letztendlich die Grundrechtsqualität des Datenschutzes verkennt. Es handelt sich, wie der Bayerische Landesbeauftragte für den Datenschutz in der Süddeutschen Zeitung vom 17. Januar 1997 formuliert hat, um einen Kampfbegriff an der Grenze zur Verleumdung. Auch wenn Politiker und Journalisten etwas zurückhaltender formulieren - wie z. B. „Datenschutz darf nicht zum Täterschutz verkommen“ -, so ist auch diese Wortwahl nicht akzeptabel.

1996 unternahmen auf Bundesebene einige Forschungsinteressenverbände Anstrengungen, das Gleichgewicht zwischen Forschungsfreiheit (Art. 5 Abs. 3 GG) und Datenschutz (Art. 1 und 2 GG) zu Lasten des Letzteren zu verschieben. Die Datenschutzbeauftragten des Bundes und der Länder waren betroffen darüber, dass sich auch die renommierte Deutsche Forschungsgemeinschaft (DFG) hieran beteiligte; vgl. XIII 22. Zwischenzeitlich fanden mit der DFG Gespräche statt, in denen einige Missverständnisse beseitigt und beiden Seiten gerecht werdende Lösungen gefunden wurden (vgl. unten 21.1). Bei gegenseitigem Verständnis ist ein Konflikt zwischen Forschung und Datenschutz grundsätzlich lösbar. Was die Anwendung der Forschungsklausel in § 25 NDSG anbetrifft, darf hervorgehoben werden, dass meine Einwände bislang nur ein Forschungsvorhaben scheitern ließ (XII 24.3).

2.2 Die Situation des Datenschutzes beim Bund

Im Berichtszeitraum sind zahlreiche Bundesgesetze verabschiedet worden, die Eingriffe in das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger vorsehen. Die Tendenz, unter dem Aspekt der Bekämpfung der Kriminalität und des Missbrauchs sozialer Leistungen das Instrumentarium der Kontrolle und Überwachung der Bürgerinnen und Bürger auszuweiten (vgl. XII 2.2), hat angehalten.

Was die Kriminalitätsbekämpfung anbetrifft, ist das herausragende Ereignis sicher die Einführung des sog. Großen Lauschangriffs gewesen (vgl. näher unten 27.4): Gesetz zur Änderung des Grundgesetzes (Artikel 13) vom 26. März 1998 (BGBl. I S. 610) und Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität vom 4. Mai 1998 (BGBl. I S. 845). Ich habe den Großen Lauschangriff zusammen mit fast allen meinen Kollegen abgelehnt, da in das letzte

Refugium von Privatheit eingebrochen wird. Es ist aber anzumerken, dass viele der datenschutzseitig empfohlenen Hürden bei den Bonner Entscheidungen berücksichtigt worden sind.

Es sollte unbestritten sein, dass Sozialleistungsmissbrauch bekämpft werden muss. Der Gesetzgeber muss aber, wenn er neue Regelungen schafft, eine sorgfältige Abwägung mit dem Recht auf informationelle Selbstbestimmung vornehmen (vgl. unten 18.1) Dies war insbesondere bei der Änderung von § 68 Abs. 1 Satz 1 SGB X – Übermittlung von Sozialdaten durch Sozialbehörden – nicht der Fall. Ausgehend insbesondere von einem Münchner Streitfall, wurde diese Norm durch Art. 4 des Ersten Gesetzes zur Änderung des Medizinproduktegesetzes vom 6. August 1998 (BGBl. I S. 2005) – welch ein irreführender Titel! – dahingend geändert, dass auch der „derzeitige oder zukünftige Aufenthalt" übermittelt werden kann. Mit der Mehrheit der Landesbeauftragten für den Datenschutz habe ich dies als eine grundlegende Durchbrechung des Sozialgeheimnisses kritisiert; die Beschäftigten der Leistungsträger würden zu „Hilfsbeamten" von Strafverfolgungs- und Vollstreckungsbehörden.

Seit Jahren beklagt, stehen beim Bund leider immer noch eine umfassende datenschutzrechtliche Überarbeitung der Strafprozessordnung und eine Regelung des Arbeitnehmerdatenschutzes aus.

Am schärfsten ist zu kritisieren, dass es der Bund nicht geschafft hat, in der 13. Legislaturperiode das Bundesdatenschutzgesetz (BDSG) zu novellieren. Die Europäische Datenschutzrichtlinie vom 24. Oktober 1995 war bis zum 24. Oktober 1998 in innerstaatliches Recht umzusetzen. Dies ist dem Bund ohne triftigen Grund nicht gelungen; es ist bei einem Referentenentwurf geblieben. Die Datenschutzbeauftragten des Bundes und der Länder haben von Anfang an die Auffassung vertreten, die durch europäisches Recht begründete Pflicht, das BDSG zu novellieren, solle als Aufforderung und Chance begriffen werden, das deutsche Datenschutzrecht im Hinblick auf die Entwicklung der Informations- und Kommunikationstechnologie zu modernisieren (vgl. z. B. unten Anlage 7). Bis auf eine einzige Regelung hat der Referentenentwurf des Bundesministeriums des Innern (Stand: 7. April 1998) dieses Anliegen bei der Änderung des BDSG nicht aufgegriffen. Die Bonner Koalitionsvereinbarung vom 20. Oktober 1998 spricht nunmehr erfreulicherweise von einer kurzfristigen Umsetzung.

Es soll durchaus anerkannt werden, dass der Bundestag in den letzten Jahren auch datenschutzfreundliche Gesetze beschlossen hat. Dazu gehört insbesondere das zukunftsorientierte Informations- und Kommunkationsdienste-Gesetz vom 22. Juli 1997 (BGBl. I S 1870).

2.3 Die Situation des Datenschutzes in Niedersachsen

Im Berichtszeitraum gab es einige datenschutzgesetzliche Fortschritte, wie z. B. das Niedersächsische Gesetz über Hilfen und Schutzmaßnahmen für psyschisch Kranke vom 16. Juni 1997 (Nds. GVBl. S. 272), das Dritte Gesetz zur Änderung dienstrechtlicher Vorschriften vom 17. Dezember 1997 (Nds. GVBl. S. 528) und das Niedersächsische Sicherheitsüberprüfungsgesetz vom 3. März 1998 (Nds. GVBl. S. 128). Was die gesetzgeberischen Defizite anbetrifft, ist nach wie vor insbesondere das Gesundheitswesen zu nennen.

Das im letzten Tätigkeitsbericht (XIII 2.2) angesprochene datenschutzrechtliche Rollback manifestiert sich in dem Gesetz zur Änderung datenschutz-, gefahrenabwehr- und verwaltungsverfahrensrechtlicher Vorschriften vom 28. November 1997 (Nds. GVBl. S. 489). Allerdings wurden die noch weitergehenden Vorstellungen des Niedersächsischen Innenministeriums – vor allem beim allgemeinen Datenschutzrecht – reduziert.

Niedersachsen ist es nicht gelungen, die bereits unter Nr. 2.2 angesprochene EU-Datenschutzrichtlinie fristgerecht in niedersächsisches Recht umzusetzen, d. h. zum 24. Oktober 1998 insbesondere das NDSG zu ändern (vgl. näher unten 6.2). Kritisch muss angemerkt werden, dass es nicht angebracht war, auf die Umsetzung durch den Bund zu warten. Ich führte in meiner Pressemitteilung vom 9. Januar 1997 aus: „Das Innenministerium wäre gut beraten, statt der Deregulierung des NDSG dessen Anpassung an die EU-Datenschutzrichtlinie zu betreiben. Findet die Anpassung jetzt nicht statt, so läuft das Land Gefahr, nach Ablauf der Übergangsfrist im Oktober 1998 nicht nur ein technisch immer mehr überholtes, sondern auch ein europarechtswidriges Datenschutzrecht zu haben."

Außerordentlich bewährt hat sich, dass die Landesregierung mit Beschluss vom 17. Dezember 1991 (Nds. MBl. 1992, 230) die Datenschutzkontrolle für den nicht-öffentlichen Bereich dem Landesbeauftragten übertrug. Diese Kompetenzerweiterung, die es auch in den Ländern Berlin, Bremen und Hamburg gibt, bewirkt, dass nicht ausreichende Datenschutz-Ressourcen konzentrierter und effektiver eingesetzt werden können. Das Konzept „Datenschutz in einer Hand" macht in der Praxis immer wieder deutlich, dass der Datenschutz im nicht-öffentlichen Bereich unterentwickelt ist und das Übergewicht bei der Verarbeitung personenbezogener Daten nicht mehr beim Staat, sondern bei den nicht-öffentlichen Stellen liegt.

Was die Praxis im öffentlichen und nicht-öffentlichen Bereich in Niedersachsen anbetrifft, sind auch in den Jahren 1997 und 1998 zahlreiche datenschutzrechtliche Verstöße zu verzeichnen, wie die späteren Kapitel belegen. Die Feststellung meines schleswig-holsteinischen Kollegen (Pressemitteilung vom 3. Juli 1998), der Datenschutz habe in den meisten Behörden des Landes eine feste Verankerung und finde nachhaltige Unterstützung, kann ich auf Niedersachsen so prononciert nicht übertragen. Ich muss meine Bitte aus den letzten Tätigkeitsberichten (XII 2.2.1, XIII 2.2) wiederholen, dass die Behörden der Aus- und Fortbildung in Fragen des Datenschutzes erheblich mehr Gewicht beimessen.

2.4 Die Situation des Datenschutzes in Europa

Was die im letzten Tätigkeitsbericht näher behandelte EU-Datenschutzrichtlinie vom 24. Oktober 1995 (XIII 2.2 und 5.1) anbelangt, ist immer noch nicht endgültig geklärt, was Art. 28 Abs. 1 Satz 2 der Richtlinie meint, wenn dort von der „völligen Unabhängigkeit" der Kontrollstellen gesprochen wird. Zahlreiche Stimmen in der Literatur halten es nicht mehr für zulässig, dass die Aufsichtsbehörden im nicht-öffentlichen Bereich weisungsgebunden sind. Was die im Erwägungsgrund Nr. 68 angesprochenen bereichsspezifischen Regelungen anbetrifft, ist hervorzuheben, dass das Europäische Parlament und der Rat am 15. Dezember 1997 eine Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation erlassen haben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 9./10. November 1995 eine Entschließung zur „Weiterentwicklung des Datenschutzes in der Europäischen Union" gefasst. Hiervon hat der Amsterdamer Vertrag vom Juni 1997 erfreulicherweise einiges verwirklicht. Ab 1. Januar 1999 sind auch die Organe und Einrichtungen der Europäischen Union an die EU-Datenschutzrichtlinie gebunden. Ferner hat der Rat eine unabhängige Kontrollinstanz für den Datenschutz einzurichten.

2.5 Neue Datenschutzkonzepte

Das im letzten Tätigkeitsbericht (XIII 2.3) vorgestellte neue Konzept einer „Allianz von Datenschutz und Technologie“ – im Wesentlichen von Spiros Simitis initiiert – hat bei etlichen Autoren Zustimmung gefunden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 23./24. Oktober 1997 eine Entschließung betreffend „Erforderlichkeit datenschutzfreundlicher Technologien“ gefasst (vgl. unten Anlage 9). Erfreulich ist, dass der Grundsatz der Datenvermeidung bereits im Teledienstedatenschutzgesetz vom 22. Juli 1997 (§ 3 Abs. 4) und im Mediendienste-Staatsvertrag (§ 12 Abs. 5) zum Rechtsgebot erhoben wurde.

Auch der 62. Deutsche Juristentag in Bremen hat sich mit einer Neuorientierung des Datenschutzes befasst. Die Abteilung Öffentliches Recht hat am 24. September 1998 u. a. beschlossen: „Bei der gebotenen Neuorientierung muss der Datenschutz als konstitutiver Teil einer umfassenden Informationsordnung begriffen werden, für die das – auf den Gedanken der Informationsgerechtigkeit ausgerichtete – Informationsrecht den rechtlichen Rahmen bildet. ... Das Datenrecht ist als Datenverkehrsordnung auszugestalten. ... Die Reformschritte sind zu einem umfassenden Informationsgesetzbuch zusammenzuführen. Zur Vorbereitung soll unverzüglich eine Kommission eingerichtet werden.“ Die Bremer Beschlüsse führen leider kaum weiter bei der vordringlichen Aufgabe, die technologische Entwicklung zu gestalten. Sie verkennen auch die bisherigen Schwierigkeiten, das Akteneinsichts- und Informationszugangsrecht zu regeln.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mit Entschließung vom 5./6. Oktober 1998 die Bremer Beschlüsse nur grundsätzlich begrüßt (vgl. unten Anlage 17).

3 Der Landesbeauftragte

3.1 Geschäftsstelle

Die Stellenausstattung meiner Geschäftsstelle ist seit Jahren unzureichend. Die Arbeitsbelastung ist im Berichtszeitraum erneut gestiegen, und zwar vor allem hinsichtlich der Bewältigung technischer Problemstellungen und im nichtöffentlichen Bereich. Ich verkenne nicht die Notwendigkeit, dass die Landesregierung spart. Ich bin der Auffassung, dass ich 1997 durch den Abzug meiner Stelle im Kraftfahrdienst meinen Einsparbeitrag erbracht habe; dieser Abzug ist vertretbar gewesen, da ich auf den Fahrdienst des Innenministeriums zurückgreifen kann. Erstaunt war ich, dass der RdErl. d. MF vom 25. November 1997 über Personalkostenbudgetierung im Haushaltsjahr (Nds. MBl. S. 1922) auch mein Kapitel 03 80 erfasste, und zwar ohne vorangegangene korrekte Beteiligung. In einem Gespräch im März 1998 akzeptierte der Staatssekretär des MI die diesseitige Argumentation, dass die Aufwendungen des Landes und der Kommunen auf dem EDV-Sektor dramatisch steigen, dass dem aber keine hinreichende Beratungs- und Kontrolltätigkeit entspricht. MI setzte sich im Rahmen der Haushaltsaufstellung 1999/2000 bei MF für zwei neue Stellen beim LfD ein, stieß aber auf Ablehnung. Ich werde meine Bemühungen um eine Verbesserung der Stellensituation in meiner Geschäftsstelle – zum Nutzen der Bürgerinnen und Bürger des Landes – fortsetzen.

Die technische Modernisierung der Geschäftsstelle setzte sich fort:

Im Jahr 1997 wurde die vorhandene Alis-Installation unter dem Betriebssystem AIX der Firma IBM durch eine neues Bürokommunikationssystem unter dem Netzwerkbetriebssystem Windows NT und dem Softwareprodukt MS Office ersetzt. Alle Mitarbeiter/innen und auch ich wurden in der Anwendung des neuen

Bürokommunikationssystems geschult. Ein zusätzlicher Workshop vor Ort diente der Vertiefung bereits erworbener Anwendungskenntnisse.

In meiner Geschäftsstelle betreibe ich in einem Intranet ein gemeinsames Ablagesystem, das automatisierte Aktenverzeichnis, ein automatisiertes Melderegister für Dateien nach § 32 BDSG und eine gemeinsame Dokumentensammlung. Das Office-System umfasst die Funktionen Textverarbeitung, Bildverarbeitung sowie elektronische Post. Mehrere Testinstallationen sollen meine Erfahrungen im Umgang mit den Firewall-Architekturen erweitern und damit meine Beratungskompetenz stärken. Weiter plane ich die Einrichtung eines IT-Labors, in dem ich technische Prüfungen, Virenscanning, Penetrationsversuche, Softwaretests, Dokumentenmanagement mit Digitalisierung vorhandener Aktenbestände und neu hinzugekommener Papierdokumente prüfen und bewerten will. Mit diesen Maßnahmen bemühe ich mich, meine Geschäftsstelle zu einem „Kompetenzcenter“ in Fragen grundrechtsfreundlicher Techniken auszubauen.

3.2 Außenprüfungen und Beratungen

Was die materiell-rechtlichen Prüfungen im öffentlichen Bereich anbetrifft, sind insbesondere zu nennen: Personaldatenverarbeitung einer Polizeidirektion, Datenverarbeitung im Sozialamt einer Kommune, Einsatz besonderer Mittel nach dem NGefAG (bei einer Polizeidirektion und einer Polizeiinspektion), beim NLfV Mitteilungen an Betroffene nach dem Einsatz bestimmter nachrichtendienstlicher Mittel und Auskunftsablehnungen, Einsatz verdeckter Ermittler bei drei Staatsanwaltschaften, Telefonüberwachung bei einer Generalstaatsanwaltschaft, Mobilfunk beim Landeskriminalamt, DNA-Untersuchungen beim Landeskriminalamt und einer Polizeiinspektion sowie Datenschutzfragen bei einer Ausländerbehörde.

Prüfungs- und Beratungsschwerpunkt im technisch-organisatorischen Bereich waren Anwendungen im Großrechnerbereich unter Einsatz von MVS/RACF der Firma IBM. „Prüflinge“ waren so „dicke Brocken“ wie die Volkswagen AG, das Rechenzentrum der norddeutschen Sparkassen dvg, die PreussenElektra AG, die TUI Infotec GmbH, das Rechenzentrum der Touristik Union, und das Versicherungsrechenzentrum ivv. Meine Erfahrungen hierbei sind unter 30.2 näher beschrieben. Weiter habe ich Prüfungen und Beratungen zu den Sicherungsmaßnahmen bei Einsatz des Betriebssystems Windows NT durchgeführt, das wegen seiner schnell wachsenden Verbreitung ebenfalls von besonderer Bedeutung ist. Aber auch Rechner mit den Betriebssystemen Unix, Novell NetWare und BS 2000 habe ich geprüft. Hierbei gehörten zu den „Prüflingen“ Unternehmen der Wirtschaft und einige Kommunen. Darüber hinaus wurden sehr viele Beratungsgespräche in unterschiedlichsten Themenbereichen geführt.

Durch meine Prüfungen und Beratungen wurden zahlreiche „Sicherheits-Lecks“ beseitigt und viel Überzeugungsarbeit geleistet. Dennoch bin ich mit der Prüftätigkeit insgesamt nicht zufrieden. Prüfungen zur Umsetzung von Datenschutzvorschriften mussten wiederum (siehe meinen letzten Tätigkeitsbericht, XIII 3.3) wegen der unzureichenden Personalausstattung meiner Dienststelle unterbleiben. Der Umfang der technisch-organisatorischen Außenprüfungen musste gegenüber den Vorjahren insgesamt reduziert werden. Die neuen technologischen Entwicklungen, etwa im Bereich Internet, Chipkartensysteme, Telekommunikation oder neue Betriebssysteme, erforderten intensive Einarbeit, datenschutzrechtliche Bewertung und viel Beratungstätigkeit. Dadurch reduzierten sich Zeit und Kapazität für die reine Prüftätigkeit. Mit der gegenwärtigen Stellenausstattung im technisch-organisatorischen Bereich war mehr nicht möglich. Ich habe mich deshalb besonders darauf konzentriert, Behörden und Unternehmen Hilfestellung bei der Selbstkontrolle zu geben. Ergebnis dieser Bemühungen sind zahl-

reiche von mir erstellte Orientierungshilfen und Checklisten zu aktuellen Themenbereichen (vgl. 3.5). Eine Selbstkontrolle kann unabhängige Kontrollen allerdings nicht ersetzen. Eine ausreichende Anzahl an Prüfungen halte ich für eine unabdingbare Voraussetzung, um auf die Einhaltung von Datenschutzvorschriften hinwirken zu können. Die Wiederaufnahme einer angemessenen Anzahl von Prüfungen ist dringend erforderlich; hierfür benötige ich aber eine bessere Stellenausstattung meiner Geschäftsstelle.

3.3 Dateibeschreibung ja – Register nein

Das novellierte NDSG (Gesetz zur Änderung datenschutz-, gefahrenabwehr- und verwaltungsverfahrensrechtlicher Vorschriften vom 28. November 1997, Nds. GVBl. S. 489) verzichtet grundsätzlich auf die zentrale Führung eines Dateienregisters. Nur Dateien, die zur Erfüllung der Aufgaben nach dem Niedersächsischen Verfassungsschutzgesetz oder polizeilicher Aufgaben nach dem Niedersächsischen Gefahrenabwehrgesetz erstellt worden sind, sind mir vorzulegen. Geblieben ist jedoch die Pflicht aller öffentlichen Stellen, Dateibeschreibungen für ihre automatisierten Dateien nach § 8 Abs. 1 NDSG zu fertigen und selbst vorzuhalten, das gilt auch – hier gab es großen Aufklärungsbedarf - für Bezirksschornsteinfeger und Notare. Der Vordruck für die Dateibeschreibung gilt unverändert. Entfallen ist dagegen die Dateibeschreibungspflicht für nichtautomatisierte Dateien.

Meine ersten Erfahrungen mit dieser Änderung sind nicht nur positiv. Während in der Vergangenheit das Register für mich Informationsquelle zur Beobachtung der IuK-Entwicklung öffentlicher Stellen war, bin ich heute darauf angewiesen, notwendige Informationen einzeln einzufordern.

3.4 Service-Angebot Internet

Am 6. Januar 1998 habe ich den Startschuss für mein Internet-Angebot gegeben. Unter der Internet-Adresse

http://www.lfd.niedersachsen.de

können meine Pressemitteilungen, der Tätigkeitsbericht, das Niedersächsische Datenschutzgesetz sowie andere datenschutzrelevante Rechtsvorschriften, meine Empfehlungen, Orientierungshilfen, Checklisten und sonstige Materialien zur eigenen elektronischen Nutzung abgerufen werden. Diese Infobörse ist ein zusätzlicher Service für Bürgerinnen und Bürger sowie für Wirtschaft und Verwaltung.

Die Abrufe datenschutzrelevanter Informationen haben meine Erwartungen weit übertroffen. Überraschenderweise kommen auch viele Abrufe aus dem Ausland.

Ich empfehle, bei persönlichen Schreiben oder Beschwerden über Datenschutzverstöße gesicherte Kommunikationsverfahren zu wählen. Wer im Internet Informationen austauschen will, sollte sich gegen Mithören und Mitlesen durch unbefugte Dritte wirksam durch die Verschlüsselung der zu übermittelnden Daten schützen. Ich empfehle deshalb, bei vertraulichen Informationen an meine Dienststelle meinen öffentlichen PGP-Schlüssel zu verwenden (Verschlüsselung nach dem Programm „Pretty Good Privacy“, das kostenlos aus dem Internet entnommen werden kann). Mein „öffentlicher Schlüssel“ und eine detaillierte Information über Risiken und Empfehlungen beim Umgang mit E-Mail können meinem Internet-Angebot entnommen werden.

3.5 Öffentlichkeitsarbeit

Zur Öffentlichkeitsarbeit eines Landesbeauftragten gehört in erster Linie der Kontakt mit den Medien. Dieser Kontakt ist aus meiner Sicht ausbaufähig.

Auch 1997 und 1998 waren Angehörige meiner Geschäftsstelle und ich an zahlreichen Vortrags- und Diskussionsveranstaltungen beteiligt. Es ging um allgemeine Datenschutzthemen (wie „Aktuelle Fragen des Datenschutzes“) und um datenschutzrechtliche Einzelthemen wie z. B. „Sozialdatenschutz“, „Datenverarbeitung durch Geistliche in Justizvollzugsanstalten“ und „Heimliche Ermittlungsmethoden im Ermittlungsverfahren“. Es ist Tradition geworden, dass ich auf der CeBIT in Hannover – dem weltweit größten Schauplatz, der den aktuellen Entwicklungsstand der Informations- und Kommunikationstechnologie zeigt – ein Datenschutz-Forum veranstalte. 1997 wurde im Rahmen einer Podiumsdiskussion das Thema „Internet – Viel Chancen, wenig Datenschutz?“ behandelt, 1998 das Thema „Wo bleibt der Datenschutz bei der Globalisierung der Informationsmärkte?“ Die Veranstaltungen, deren Durchführung die Deutsche Messe AG großzügig unterstützte, waren sehr gut besucht.

Auch im Berichtszeitraum sind Angehörige meiner Geschäftsstelle und ich mit Aufsätzen in Zeitschriften zu Wort gekommen.

1997 habe ich einen „Leitfaden für die Durchführung von Ordnungswidrigkeitenverfahren im Bereich des Datenschutzes“ herausgegeben.

Neu erstellt habe ich die Orientierungshilfen und Checklisten zu folgenden Themen: Telearbeitsplätze, Grundschutz durch Firewall, externe Wartung und Systembetreuung, Passwort-Gestaltung und –Verwendung, Datenschutz-Prüfkonzept für MVS/VM-Systeme, Orientierungshilfe und Checkliste für Windows NT sowie Auftragsdatenverarbeitung. Meine Orientierungshilfen sollen Geschäfts- und Behördenleitung, Personalleitung und Personalvertretung, Datenschutzbeauftragte sowie Organisations- und DV-Leitung in die Lage versetzen, die Folgen von IuK-Entscheidungen abzuschätzen sowie erforderliche und angemessene Datensicherungskonzepte zu entwickeln.

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 IuK-Verfahren sowie der getroffenen technisch-organisatorischen Maßnahmen zur Verfügung. Die Anfragen hinsichtlich dieser Prüfungsunterlagen zur Selbstkontrolle sind erfreulich häufig. Viele Abrufe kommen inzwischen im Download über das Internet, sodass mir Druckkosten erspart bleiben.

In Kürze wird eine Compact Disc (CD) erscheinen, die eine Zusammenstellung aller datenschutzrelevanten Informationen – diesen Tätigkeitsbericht eingeschlossen – in digitaler Form enthält. Die CD ergänzt mein Serviceangebot und bietet den öffentlichen Stellen sowie den privaten Unternehmen einen modernen Zugang zum Datenschutzrecht und zu Datenschutzfragen in Niedersachsen. Mit HTML- und Hyperlink-Technik soll es einfach und komfortabel möglich sein, zwischen verschiedenen Informationen bzw. Informationsteilbereichen hin und her zu springen. Auch das Herunterladen von benötigten Informationen wird unproblematisch und schnell möglich sein.

Das genannte Informationsmaterial kann – ebenso wie älteres Material, so weit noch vorhanden – bei mir bestellt und kostenlos bezogen werden.

3.6 Zusammenarbeit mit anderen Kontrollorganen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder tagte im Berichtszeitraum viermal. Die Entschließungen der Konferenz sind als Anlagen diesem Bericht beigefügt. Niedersachsen hat weiterhin den Vorsitz im Arbeitskreis Personalwesen.

Gemeinsam mit dem Niedersächsischen Innenministerium nehme ich an den Beratungen des „Düsseldorfer Kreises“, des bundesweiten Zusammenschlusses der obersten Aufsichtsbehörden für den nicht-öffentlichen Bereich, teil. Auch im Berichtszeitraum wurde die Zusammenarbeit mit den Aufsichtsbehörden für den nicht-öffentlichen Bereich verstärkt; die im letzten Tätigkeitsbericht (XIII 3.6) genannten bundesweiten Workshops wurden 1997 in Potsdam und 1998 in Dresden fortgesetzt und fanden großen Zuspruch.

Mit den kirchlichen Datenschutzbeauftragten fand ein häufiger Gedankenaustausch statt.

4 Entwicklung und Probleme der Informations- und Kommunikations-Technik in Verwaltung und Wirtschaft

4.1 Die Informationsgesellschaft

Vor zwei Jahren habe ich vor einer allzu **„**rasanten Fahrt auf der Datenautobahn**“** gewarnt; diese Fahrt ist heute mit überhöhter Geschwindigkeit im Gange. Die Entwicklung des Internets hat tiefgreifende Veränderungen in Wirtschaft, Verwaltung und Gesellschaft bewirkt. Aus der ursprünglichen Entwicklung für Militär und Forschung ist ein weltumspannendes, allgemein zugängliches Netz mit mehr als 100 Millionen Nutzern geworden. Sekundenschnelle Verarbeitung großer Datenmengen, weltweite Kommunikation in digitalen Netzen ohne Grenzen und Zeitverzug, jederzeitige Erreichbarkeit an allen Plätzen der Welt, weltweite Veröffentlichung intimer Informationen (wie der Starr-Bericht über US-Präsident Clinton) sind heute möglich. Die Dezentralisierung des Netzwerkmanagements und die Globalisierung des Informationsaustauschs haben die Grenzen zwischen privaten und staatlichen Akteuren verwischt. Das Internet hat die Integration ganz unterschiedlicher Rechner, Betriebssysteme und Applikationen bewirkt. Arbeitsabläufe und Kommunikationsverfahren in Wirtschaft und Verwaltung sind nicht nur verändert, sie werden revolutioniert.

Die Angebote im Internet werden immer interessanter und bunter. Fast alle Kommunikationswünsche lassen sich unabhängig von Zeit und Ort sowie mit fast jeder eingesetzten Technik lösen. Diese schöne Seite der Medaille hat jedoch auch eine Kehrseite. „Wir müssen mit Digitalvandalismus**,** Softwarepiraterie und Datendiebstahl leben lernen“ so lautet die ernüchternde Prognose des amerikanischen Vordenkers in Fragen menschlicher Kommunikation und digitaler Technik Nicholas Negroponte. Noch nie war die Sammlung personenbezogener Daten so detailliert und perfekt auswertbar wie heute. Im nächsten Jahrzehnt droht geradezu ein Einbruch in unsere Privatsphäre. Das sind Aussagen einer Bestandsaufnahme und aktuellen Analyse zu den Themen Multimedia und Datenschutz des Hamburger Freizeit-Forschungsinstituts von British American Tobacco. Die Mehrheit der hierzu befragten Bürgerinnen und Bürger will einen effektiven, möglichst besseren Datenschutz. Das ausgeprägte Bedürfnis nach Schutz der eigenen Privatsphäre geht leider häufig Hand in Hand mit pauschalem Schimpfen auf „zu viel Datenschutz“. Zu den Kritikern gehört „Electronic Commerce“, die alle Informationen über Kunden und Konkurrenten aus unterschiedlichen und unerschlossenen Datenquellen zusammentragen wollen, um sie in einem „Data-Warehouse“ zu speichern und daraus exakte Aussagen über Kunden- und Konkurrenten-Verhalten mit „Data-Mining“-Werkzeugen zu ge-

winnen. Unternehmen des Direkt-Marketing begründen dies mit „Wir wollen alles über den Kunden wissen, um ihn besser bedienen zu können“. Datenschützer sehen darin eine „Rasterfahndung nach Kunden und Konkurrenten“, die datenschutzrechtlich unzulässig ist.

Dabei sollte heute jede Chance genutzt werden, um durch datenschutzfreundliche Technik das Recht auf informationelle Selbstbestimmung und insbesondere vertrauliche Kommunikation zu schützen. Nur so wird es gelingen, Vertrauen und notwendige Akzeptanz für die Informationsgesellschaft zu gewinnen. Zu solchen datenschutzfreundlichen Techniken gehören intelligente Systeme zur anonymen und pseudonymen Nutzung, wirkungsvolle und praktikable Verschlüsselungsverfahren, die digitale Signatur, E-Cash zum anonymen Bezahlen im Internet, Buchungsverfahren, die ohne personenbezogene Nutzerdaten auskommen, Erreichbarkeitsdienste zur Unterstützung von TK-Wünschen, Watch-Dienste zur Absicherung gegen jugendgefährdende Informationen und weitere Selbstschutz-Intelligenz im Endgerät. Bürgerinnen und Bürger erwarten zu Recht, dass ihre Datenschutzrisiken durch einen angemessenen Systemschutz des Staates abgesichert werden. Systemschutz ist erreichbar, indem z. B. Wahlfreiheit für anonyme Abrechnungsverfahren, permanente Anzeige entstandener Gebühren oder technische Signalisierung von Werbung oder nicht jugendfreier Angebote normiert werden. Das ist im neuen Multimediarecht erfolgt (vgl. unten 8); das Informations- und Kommunikationsdienste-Gesetz schreibt ausdrücklich die Möglichkeit zum „Selbstdatenschutz“ für Bürgerinnen und Bürger vor. Nutzer haben danach die Wahlfreiheit zur anonymen oder pseudonymen Nutzung; das Gesetz führt den Grundsatz der Datenvermeidung ein und schafft einen Rahmen für die Sicherungsinfrastruktur digitaler Signaturen. Der Mediendienstestaatsvertrag hat darüber hinaus die Idee von Wissenschaftlern und Datenschützern verwirklicht, wie im Bereich des Umweltschutzes ein Audit für Datenschutz einzuführen. Anbieter von Mediendiensten können ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen. Über Image-Werbung und Wettbewerbseffekt gegenüber Konkurrenten soll eine kontinuierliche Verbesserung der Datensicherung und des Datenschutzes erreicht werden. Leider sind viele intelligente Ideen und viele gute Ansätze bisher noch Theorie geblieben. Sie müssen noch mit Leben erfüllt werden. Zur Beratung bei der Entwicklung und zur Mithilfe bei der Erprobung bin ich bereit.

4.2 Datenschutz durch Technik

Moderne Informations- und Kommunikationstechnologie dringt in alle Lebensbereiche ein, sie schafft neue Informationsfreiheiten. Diese Entwicklung hat aber auch neue Abhängigkeiten und Gefährdungen hervorgerufen. Mit der Benutzung neuer Informations- und Kommunikationssysteme entstehen vielfältige elektronische Nutzerspuren, Individuen lassen sich elektronisch beobachten, ihr Verhalten kann unbemerkt registriert und gründlich analysiert werden. Über diese Möglichkeiten, die Fülle dieser Daten, über Umfang, Speicherort, Speicherungsdauer sowie Verwendungszweck machen sich viele Benutzer keine Gedanken; häufig fehlt es aber auch an ausreichender Information.

Der Schutz der Privatsphäre des Einzelnen wird bisher mit rechtlichen, technischen und organisatorischen Maßnahmen gesichert. Doch Experten in Wirtschaft und Verwaltung sowie in Wissenschaft und Forschung sind sich einig, dass Individual- und Gemeinwohlinteressen in der unendlichen Welt der Netze nicht mehr allein durch Ge- und Verbote gesichert werden können. Es wächst die simple Erkenntnis, dass der Gefährdung der Privatsphäre wirksam nur durch eine weitgehende Reduzierung der Menge der gespeicherten Daten begegnet werden kann. Der Grundsatz der Datensparsamkeit, wonach nur so wenige per-

sonenbezogene Daten erhoben, gespeichert und genutzt werden dürfen, wie dies unabdingbar ist, muss zu einem klassischen Schutzziel werden. Datenvermeidung ist die stets anzustrebende Form der Datensparsamkeit. Wo dies nicht machbar ist, sollte von frühestmöglicher Anonymisierung oder Pseudonymisierung Gebrauch gemacht werden. Gelungene Beispiele für bereits existierende datenschutzfreundliche Systeme sind das Telefonieren mit vorausbezahlten anonymen Telefonkarten, bargeldloses Parken mit Prepaidkarten, pseudonyme Kur-Chipkarten oder anonyme digitale Fahrkarten.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer gründlichen Untersuchung Kriterien für datenschutzfreundliche Technologien definiert. Anhand konkreter Beispiele aus dem Medienbereich, dem elektronischen Zahlungsverkehr, dem Gesundheitswesen, der Telekommunikation sowie aus den Bereichen Transport und Verkehr werden die gewählten Ansätze und die gefundenen Lösungen datenschutzfreundlicher Technologien aufgezeigt. Es werden Empfehlungen für datenschutzfreundliche Lösungen der jeweiligen Anwendungsfelder gegeben. Diese Ausarbeitung, an der ich aktiv mitgearbeitet habe, kann bei mir unentgeltlich angefordert werden.

4.3 Viel Pioniergeist bei der Verschlüsselung

Im letzten Tätigkeitsbericht (XIII 4.3) habe ich dargelegt, wie wichtig die Einführung von Verschlüsselungsverfahren für die Datensicherheit bei der Übertragung personenbezogener Daten ist. Obwohl bereits seit Jahren allgemein anerkannt wird, dass geeignete Verschlüsselungsverfahren ein hohes Maß an Sicherheit gewährleisten können - bei richtiger Handhabung weit mehr als jede Sicherheitsmaßnahme auf dem Postweg – taten sich manche Verantwortliche von IuK-Projekten äußerst schwer mit der Einführung dieser Verfahren. Verschlüsselungsprodukte seien teuer, ihre Einführung personalintensiv und sie brächten auch sonst nur Scherereien. Diese Vorwürfe sind überzogen; die Verschlüsselung ist günstiger zu haben, als allgemein vermutet wird. Erfreulich sind der erkennbare Umdenkungsprozess und die technische Entwicklung. Die Notwendigkeit, Verschlüsselungsverfahren einzusetzen, wird zunehmend anerkannt, in vielen Bereichen ist ein richtiger Pioniergeist festzustellen:

- Die Palette der Verschlüsselungsprodukte erweitert sich sprunghaft. Es gibt hunderte von Angeboten mit verschiedenen Anwendungsbereichen und Qualitäten. Die Anwenderfreundlichkeit hat sich verbessert. Einige Produkte stecken allerdings noch in den Kinderschuhen und reifen erst beim Kunden.
- Besonders weit entwickelt sind die Verschlüsselungsmethoden im Telebanking-Bereich. Immer mehr Kreditinstitute gehen „online“, sie bieten häufig mehr als die antiquierten Sicherheitsmethoden von PIN- und TAN-Verfahren. Hier hat sich ein schnell wachsender Markt an Sicherheitssoftware gebildet, der national wie international Anerkennung findet und bei den Anbietern dieser Produkte zu einem kräftigen Firmenwachstum geführt hat.
- Im Gesundheitsbereich ist mittlerweile eine Reihe von wichtigen Verfahren eingeführt worden. So versenden inzwischen viele Ärzte, Apotheken, Krankenhäuser usw. (die Leistungserbringer nach SGB V) Abrechnungsdaten an die Krankenkassen und kassenärztlichen Vereinigungen bei elektronischer Übertragung in verschlüsselter Form. Weit entwickelt und mit besonderen Verschlüsselungsverfahren ausgestattet sind auch viele Krebsregister.

- Im bundesweit betriebenen Pilotprojekt SPHINX kommen unterschiedliche Lösungen zum Einsatz, die verschlüsselte und versiegelte Übertragungen von Dokumenten ermöglichen. Das Besondere an diesem Projekt ist, dass diese Produkte einheitlich nach dem Mailtrust-Standard arbeiten und somit untereinander kompatibel sind. An SPHINX nehmen z. Z. eine Reihe von Behörden und Unternehmen teil, auch ich bin mit zwei Arbeitsplätzen beteiligt. Selbst wenn das Projekt z. Z. noch etwas holprig verläuft, bietet es eine hervorragende Ausgangsbasis für eine flächendeckende Einführung einer Ende-zu-Ende-Verschlüsselung für elektronische Post.
- Auch im privaten Bereich gibt es erfreuliche Entwicklungen. So hat z. B. die Zeitschrift c´t ein Trust Center aufgebaut und bietet jeder Privatperson kostenlos einen individuellen zertifizierten Schlüssel für das anerkannte PGP-Verschlüsselungsverfahren an. Die Zahl der verteilten Schlüssel geht mittlerweile in die Tausende. Die Aktion will nachweisen, dass Verschlüsselungsverfahren auch von Bürgern vielfach genutzt werden und dass ein Kryptografieverbot einen empfindlichen Eingriff in das Recht auf informationelle Selbstbestimmung bedeuten würde. Dieser Nachweis ist eindrucksvoll gelungen.
- Beachtenswert sind auch sonst die vielen Aktivitäten beim Aufbau von Trust Centern. Im Internet-Angebot des Deutschen Forschungsnetzes (DFN), das selbst auch ein Trust Center betreibt, findet man eine Liste von ca. 50 weiteren „Certification Authorities“ aus verschiedenen Ländern. Namhafte deutsche Unternehmen stehen in den Startlöchern, um Signaturgesetz konforme Zertifizierungsstellen zu betreiben. Auch das Informatikzentrum Niedersachsen bereitet sich auf diese Aufgabe vor.
- „Last but not least“ sei darauf hingewiesen, dass auch die niedersächsische Landesverwaltung im Rahmen des Projekts zur Automatisierung des Haushaltswirtschaftssystems P 53 flächendeckend Verschlüsselung und digitale Signaturen einführen wird (vgl. 4.7).

Natürlich gibt es auch Negativbeispiele. Bei der Übersendung von sensiblen personenbezogenen Daten von den Staatsanwaltschaften an das zentrale Staatsanwaltschaftliche Verfahrensregister etwa meint man, vorerst ohne Verschlüsselung arbeiten zu können (vgl. 27.2). Insbesondere im Großrechnerbereich bewegt sich auch noch sehr wenig, da hier eingefahrene Verfahren laufen, deren Anpassung aufwendig und teuer sein dürfte. Dies betrifft zum Beispiel die herkömmliche Datenverarbeitung der Kreditwirtschaft, aber auch viele Bereiche der öffentlichen Verwaltung. Insgesamt zeigen aber die oben aufgeführten Beispiele einen eindeutigen Trend: Die Erkenntnis, dass der Weg in die Informationsgesellschaft auch besondere Bemühungen für eine ausreichende Datensicherheit wie die Einführung von Verschlüsselungsverfahren erfordert, setzt sich durch. Solche Anstrengungen können im übrigen auch volkswirtschaftliche Vorteile besitzen. Datensicherheit aus Deutschland ist weltweit gefragt und kann zum Exportschlager avancieren. An diesem Trend haben die Landesdatenschutzbeauftragten durch Forderungen, Begleitung von Projekten und Beratungen maßgeblich mitgewirkt. Ich werde diesen Weg weiter beschreiten und den Einsatz von Verschlüsselungsverfahren auch dort einfordern, wo sich solche Verfahren noch nicht durchgesetzt haben.

4.4 Weltspitze: Das deutsche Signaturgesetz

Am 1. August 1997 ist das Gesetz zur digitalen Signatur als Artikel 3 des Informations- und Kommunikationsdienste-Gesetzes in Kraft getreten. Die ergänzende Signaturverordnung ist seit dem 1. November 1997 in Kraft. Mit diesen Regelungen hinkt der Gesetzgeber in Deutschland einmal nicht der technischen

Entwicklung weit hinterher, sondern hat in ungewohnter Weise Maßstäbe gesetzt, die weltweit Beachtung finden.

Das Signaturgesetz soll Rahmenbedingungen schaffen, unter denen digitale Signaturen als sicher gelten. Fälschungen von digitalen Signaturen oder Verfälschungen von signierten Daten sollen zuverlässig festgestellt werden können: Mit Hilfe von digitalen Schlüsseln werden elektronische Dokumente signiert. Vertrauenswürdige Zertifizierungsstellen („Trust Center“) stellen diese Schlüssel zur Verfügung und erlauben es jedermann, Signaturen auf ihre Echtheit hin zu überprüfen (vgl. XIII 4.3.3). Technische und organisatorische Festlegungen sollen die Sicherheit und Zuverlässigkeit des Verfahrens garantieren. Das Signaturgesetz birgt gewaltige Chancen: Wirtschaft und Verwaltung haben die Möglichkeit, nicht nur ihre bisherige elektronische Datenverarbeitung und Kommunikation sicherer zu gestalten, sondern in vielen Bereichen den Umstieg vom Papierdokument zum elektronischen Dokument zu vollziehen. Das Signaturgesetz kann daher ein ganz wichtiger, bisher noch fehlender Baustein sein, um die Informations- und Kommunikationstechnik von einem Hilfsmittel der Datenverarbeitung zu einem verlässlichen und selbstverständlichen Basiskommunikationsmittel zu machen. Auch für den Datenschutz ist die digitale Signatur ein wichtiger Bestandteil notwendiger technischer und organisatorischer Maßnahmen. Noch verbinden sich aber viele Fragezeichen mit dem Signaturgesetz. Das Gesetz beschreibt bewusst nur ein Verfahren, ohne einen konkreten Zwang zu dessen Einführung in irgend einem Bereich auszuüben. Ob dieses in der Gesellschaft angenommen wird, hängt von vielen Faktoren ab. Ist das Signaturverfahren ausreichend sicher und kann dem Anwender dieses Gefühl der Sicherheit auch vermittelt werden? Oder sind die geforderten Sicherheitsmaßnahmen unnötig aufwendig und viel zu teuer? Hat die Regelung die nötige Reife oder sind zu viele Ungereimtheiten vorhanden? Ganz wichtig ist auch, wohin sich die europäische und die internationale Entwicklung bewegt.

Fest steht auf jeden Fall, dass z. Z. auf diesem Gebiet eine tiefgreifende Aufbruchstimmung vorherrscht (vgl. 4.3). Vielerorts entstehen Trust Center, die sich um eine Zertifizierung nach dem Signaturgesetz bemühen. Es gibt viele Projekte, bei denen die Einführung der digitalen Signatur erwogen oder in Pilotfeldern untersucht wird. Auf Seiten der Anwender ist allerdings noch ein Zögern zu erkennen, einerseits weil die Trust Center noch im Aufbau oder noch nicht endgültig zertifiziert und die nach der Signaturverordnung erforderlichen Maßnahmen noch nicht im Detail festgelegt sind, andererseits weil die Einführung von Signaturverfahren mit Kosten verbunden ist, die insbesondere dann erheblich sind, wenn das Verfahren gesetzeskonform betrieben werden soll.

Die Datenschutzbeauftragten haben sich schon früh mit Signaturverfahren auseinandergesetzt und z. B. in Entschließungen von 1995 (XIII, Anlage 3) und 1996 (XIII, Anlage 21) ihren Einsatz bei der Übertragung elektronisch gespeicherter personenbezogener Daten gefordert. Die oben geschilderte Situation führt nun zu einer Fortentwicklung und Konkretisierung dieser eher allgemein gehaltenen Forderungen. Nach Aufbau und endgültiger Zertifizierung von Trust Centern und Signaturkomponenten werden verlässliche Signaturverfahren zum Stand der Technik. Es lassen sich Bereiche formulieren, in denen der Einsatz geboten oder zwingend erforderlich ist. Dies gilt z. B. für

– elektronische Dokumente mit rechtsverbindlichen Vorgängen (z. B. per E-Mail zugestellte Verwaltungsakte, elektronische Archivierung von Beweismaterial, elektronisches Grundbuch, Telebanking),

– Daten in vernetzten Systemen, wenn der Verlust der Integrität oder Authentizität dieser Daten die gesellschaftliche Stellung, die wirtschaftlichen Verhältnisse, Gesundheit, Leben oder Freiheit des Betroffenen erheblich beeinträchtigen würde (z. B. ärztliche Verschreibungen auf Chipkarten).

In diesen Verfahren sind Signaturgesetz konforme Signaturen einzuführen. Auch bei weniger sensiblen Daten sollten geeignete Signaturverfahren gewählt werden, z. B. bei der Vorgangsbearbeitung, beim allgemeinen E-Mail-Verkehr oder beim Datenträgeraustausch. Ich habe mich auch für die Aufnahme entsprechender Festlegungen in den „Normen, Standards und Empfehlungen für den Einsatz der IuK-Technik in der Landesverwaltung“ eingesetzt. Bei meiner Kontrolltätigkeit werde ich auf die Einführung angemessener Verfahren drängen. Auch wenn das „Pflänzlein“ noch zart ist, halte ich die Vision für realistisch, dass in absehbarer Zukunft bei sehr vielen elektronischen Datenverarbeitungsvorgängen, insbesondere bei Kommunikationsvorgängen zwischen verschiedenen Rechnern, Signaturverfahren zum Einsatz kommen werden.

4.5 Bietet das Landesnetz IZN-net ausreichende Sicherheit für offene Kommunikation?

Im Dezember 1992 hat die Landesregierung der damals beim Innenministerium angesiedelten Zentralen Stelle für IuK-Technik den Auftrag erteilt, ein landesweites Telekommunikationsnetz aufzubauen, das die unterschiedlichen Anforderungen der Netzbenutzer berücksichtigt und eine gleichberechtigte Nutzung der Kommunikationsmittel Sprache, Texte, Daten und Bilder ermöglicht. Das damals unter der Bezeichnung TELENET betriebene Projekt sollte die vorhandenen Teilnetze verschiedener Fachverwaltungen vereinen, Parallelführungen vermeiden sowie den Betrieb optimieren und ausbauen. Mit dem Projekt sollten die bestehenden Rechenzentren der Landesverwaltung, die lokalen Netze und Einzelplatz-PC in den einzelnen Behörden sowie die telefonische Kommunikation in einer Netzstruktur miteinander verbunden werden.

Auch wenn der Name des Projekts inzwischen „werbewirksam“ gemacht wurde - es heißt jetzt IZN-net nach dem betreibenden Landesbetrieb Informatikzentrum Niedersachsen - ist der Projektauftrag noch immer nicht erfüllt. Ich werde nicht müde darauf hinzuweisen, dass sich mit dem Konzept IZN-net besondere Risiken für Sicherheit und Vertraulichkeit der Kommunikation ergeben, die in einer Technikfolgenabschätzung analysiert werden müssen und denen durch ein angemessenes Maßnahmebündel begegnet werden muss. Gerade bei diesem umfassenden Infrastrukturprojekt der Landesverwaltung ist es wichtig, dass für die einzelnen Umsetzungsschritte des Projektes Technikfolgenabschätzungen durchgeführt werden (vgl. 4.11 u. 4.12). Für das erste Teilprojekt, landesweiter E-Mail-Verkehr nach dem X.400-Standard, wurde dies auch in vorbildlicher Weise beachtet (XIII. Tätigkeitsbericht 4.6.2). Die in der Technikfolgenabschätzung erarbeiteten Sicherungsmaßnahmen sind weitestgehend umgesetzt worden. Bedauerlich bleibt, dass die vorgeschlagene Verbindungsverschlüsselung nur in einer Pilotphase zum Einsatz kam und danach still und heimlich wieder abgestellt wurde. Auch für das zweite Teilprojekt, die Ersetzung der analogen Telefonanlage der Ministerien durch eine ISDN-Anlage, wurde ebenfalls eine Technikfolgenabschätzung begonnen. Die ISDN-Leistungsmerkmale wurden auf Gefahren hin untersucht und deren Einsatz unter Berücksichtigung datenschutzrechtlicher Belange konzipiert. Anfang 1996 wurde dieser positive Ansatz abrupt und ohne Begründung beendet. Seitdem sind Fortschritte bei der datenschutzgerechten Gestaltung des Projektes Mangelware. Meinen wiederholten Forderungen nach Fortführung der Technikfolgenabschätzungen und Umsetzung von Maßnahmen wurde nur sehr zögerlich und spärlich gefolgt. Die Einführung von virtuellen LAN und die Beschaffungen für die Realisierung von Internet-Anschlüssen an das Landesnetz sind dann aus meiner Sicht unkoordiniert und konfus verlaufen.

Erst nach massiver Forderung wird für mich erkennbar an einem Sicherheitskonzept gearbeitet. Das für IuK-Koordinierung zuständige Finanzministerium hat mir zugesagt, dass Gefahren- und Risikoanalysen sowie Sicherheitskonzepte für folgende Bereiche erstellt werden:

- IZN-net (technische Netzgrundstruktur bis Schicht 3 des ISO/OSI-Modells),
- IZN-Network-Management-System,
- IZN-Internet/Intranet (Anschluss des Landesnetzes an das Internet),
- IZN-Office (Bürobasissoftware für Arbeitsplatzrechner der Landesverwaltung).

Fest steht heute, dass das IZN-net selbst nur geringe Schutzmaßnahmen bieten kann. Nutzer des Netzes müssen daher für ihre Anwendungen selbst ausreichende Schutzmaßnahmen treffen. Von besonderer Bedeutung wird die Technikfolgenabschätzung zum Internet-Anschluss sein. Hierfür ist die Einrichtung einer zentralen Firewall vorgesehen, die bereits im Test eingesetzt wird. Weiter ist vordringlich zu untersuchen, inwieweit durch diese Öffnung des Landesnetzes die angeschlossenen lokalen Netzwerke gefährdet werden und welche zusätzlichen Sicherungsmaßnahmen zu treffen sind (vgl. 4.6).

Die versprochenen Abschätzungen müssen zügig durchgeführt und die notwendigen Schutzmaßnahmen rechtzeitig und vollständig umgesetzt werden. Nur so kann davon ausgegangen werden, dass das Landesnetz und alle angeschlossenen LAN ausreichende Sicherheit bieten, um einen datenschutzgerechten Betrieb zu gewährleisten.

4.6 Wie schütze ich mein Bürokommunikationsnetz?

4.6.1 Gefahren aus fremden Netzen

Viele Stellen in Wirtschaft und Verwaltung haben einen Internet-Anschluss oder sind auf andere Weise mit fremden Netzen verbunden. Dies erscheint notwendig, um aktuelle Informationen schnell und weiterverarbeitungsfähig zu gewinnen. Informationsanbieter sehen Chancen zum modernen Kunden- bzw. Bürgerservice durch eigene Veröffentlichungen. In der Wirtschaft wird das Internet darüber hinaus als kostengünstiges Übertragungsmedium der internen Kommunikation benutzt; das lokale Netz wird so zu einem weltweiten Firmennetz erweitert. Nicht immer ausreichend bedacht wird dabei allerdings, dass mit dem Zugang zum Internet für jeden Benutzer zahlreiche Gefahren und signifikante Risiken verbunden sind. Schwächen finden sich z. B. in den Datenübertragungsprotokollen sowie in den Installationen der Programme. Sobald ein Computer an ein offenes Datennetz angeschlossen wird, ist er von einer unbekannten Zahl anderer Rechner aus erreichbar. Die Vertraulichkeit der gespeicherten Daten und der Kommunikationsinhalte ist gefährdet.

Der Anschluss an Internet bzw. Intranet erfolgt dabei häufig auf folgende Weise:

- Direktanschluss eines einzelnen Rechners an das Internet

  Ein einzelner Rechner wird per Modem und Telefonleitung über einen Internet-Provider an das „Netz der Netze“ angeschlossen. Die „Insel“-Lösung spielt besonders bei kleinen Behörden und im privaten Bereich eine große Rolle. Bei Angriffsversuchen ist nur der einzelne Rechner gefährdet.

– LAN-Anbindung an ein Intranet

  Hier verfügt das LAN über eine Verbindung zu anderen Netzen des Unternehmens bzw. zu anderen Verwaltungsrechnern in einem Intranet. Bei eventuellen Angriffen besteht sowohl ein Sicherheitsrisiko für den an das Intranet angeschlossenen Rechner als auch für das gesamte LAN.

– Internet-Anschluss über eine zentrale Firewall

  Hier hat der Rechner einen Zugang zum Intranet (z. B. LAN, VLAN) seines Unternehmens oder seiner Verwaltung, und von dort aus besteht ein einziger zentraler Zugang zum Internet. Eventuelle Angriffe aus dem Internet können an der zentralen Übergangsstelle vom Internet zum Intranet abgefangen werden. Der einzelne Rechner bzw. das ungeschützte LAN bleiben trotz zentraler Firewall aus dem Intranet heraus angreifbar.

4.6.2 Grundschutz durch Firewall

Grundsätzlich sollte der Anschluss an fremde Netze nur über einen zentralen, kontrollierten und abgesicherten Zugang (Firewall) erfolgen. Andere Zugänge, z. B. separate Modemverbindungen am Arbeitsplatz, sind zu verbieten und, soweit möglich, technisch zu unterbinden. Wird ein Internetzugang benötigt, so kann die Inernetnutzung über separate Rechner erfolgen, die vom lokalen Netz physikalisch getrennt sind und auf denen keine datenschutzrelevanten Daten verarbeitet werden. Auch sollten immer nur die Dienste bereitgestellt werden, die zur Aufgabenerfüllung erforderlich sind.

Ein solch kontrollierter Zugang könnte eine Firewall sein. Darunter wird eine technische Schwelle zwischen zwei Netzen verstanden, die erst überwunden werden muss, um Rechner im jeweils anderen Netz zu erreichen. Die Firewall hat die Aufgabe, nur zugelassene netzübergreifende Aktivitäten zu ermöglichen und Missbrauchsversuche frühzeitig zu erkennen. Firewall-Lösungen sind auch geeignet, „grenzüberschreitende“ Aktivitäten interner Nutzer zu überprüfen. Firewall-Systeme weisen folgende Charakteristika auf:

– Die Firewall ist definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nicht vertrauenswürdigen Netz.

– Zu dem durch Firewall geschützten Netz wird ein einheitliches Sicherheitsniveau gewährleistet.

– Die Anforderungen aller vernetzten Stellen werden in einer „Security Policy“ (Sicherheitspolitik) definiert.

– Die Benutzerprofile der internen Teilnehmer, die mit Rechnern in externen Netzen kommunizieren dürfen, werden auf der Firewall abgebildet und jeweils kontrolliert.

Die Stärke der Firewall hängt wesentlich von der eingesetzten Technik und ihrer korrekten Administration ab.

4.6.3 Auswahl, Konfiguration und Wartung von Firewall-Systemen

Bei der Beurteilung der Frage, ob man sein LAN an ein fremdes Netz anschliessen muss, sollte ein strenger Massstab angelegt werden. Auch wenn die Erforderlichkeit bejaht wird, ist zu prüfen, ob der Verwendungszweck nicht schon durch den Anschluss eines isolierten Rechners erreicht werden kann. Die Art des Zugangs hängt wesentlich davon ab, welche Dienste im Netzverbund genutzt werden sollen. Die Kommunikationsanforderungen müssen auf Grund der unterschiedlichen Aufgaben sowohl für den zentralen Zugang zu fremden Nezten als auch für jeden einzelnen Rechner analysiert werden.

Diese Fragen sind in einer Technikfolgenabschätzung zu untersuchen. Dabei sind der Schutzbedarf der zu verarbeitenden Daten zu klären sowie die Sicherungsziele der datenverarbeitenden Stelle und die Risiken der unterschiedlichen Dienste zu bedenken. Wichtig für die Auswahl eines Firewall-Systems ist es, für den zu schützenden Bereich das erforderliche Schutzniveau zu definieren. Drei Lösungsvarianten sind anzutreffen:

1. hohes Schutzniveau im internen Netz orientiert am höchsten vorhandenen Schutzbedarf;
2. niedriges Schutzniveau orientiert an Verfahren mit geringem oder mittlerem Schutzbedarf und
3. mittleres Schutzniveau mit zusätzlichen Massnahmen für einzelne Netzkomponenten mit höherem Schutzbedarf.

Die Varianten 1 und 2 entsprechen am ehesten zentralen Firewall-Lösungen. Die Variante 2 ist jedoch indiskutabel und mit dem Datenschutzrecht unvereinbar. Variante 3 entspricht einem System gestaffelter Firewalls. Neben einer zentralen Firewall, die das Netzwerk nach außen sichert, werden Netze mit höherem Schutzbedarf durch weitere Firewalls abgesichert. Gestaffelte Firewall-Systeme können selbst bei einheitlich hohem Schutzniveau im Gesamtnetz sinnvoll sein, um mögliche Schäden auf einzelne Netzsegmente zu begrenzen.

Firewall-Systeme müssen transparent und einfach aufgebaut sein. Mit zunehmender Komplexität steigt die Wahrscheinlichkeit von Fehlern. Daher sollten alle nicht für den Betrieb der Firewall benötigten Anwendungen und Systemprogramme gelöscht werden. Bedienung und Konfiguration der Firewall müssen benutzerfreundlich sein. Ausserdem sollten „black boxes“ vermieden werden. Vertrauenswürdige Systeme müssen ihre Funktionsweise offenlegen; nur dann ist es Experten möglich, Hintertüren zu verschliessen und die Gefahr von Sicherheitslücken fundiert zu bewerten.

Bei der Anschaffung von Firewall-Systemen sollte man nicht die allerneuesten Produkte auswählen, da diese noch „Kinderkrankheiten“ und unerkannte Sicherheitsschwächen haben können. Stattdessen ist ein gut untersuchtes und zertifiziertes Produkt zu bevorzugen, bei dem zum einen die Stabilität gewährleistet ist und zum anderen etwaige Mängel ausgeräumt werden können. Durch den Einsatz verschiedener Produkte, die unabhängig voneinander entwickelt wurden und arbeiten, lässt sich das Sicherheitsniveau steigern. „Monokulturen“ sollten vermieden werden, denn wenn ein Angreifer einen bisher unentdeckten Fehler ausnutzt, kann leicht der gesamte Schutzwall zusammenbrechen.

Bei der Konfiguration einer Firewall folgt man am besten der Regel „Alles, was nicht ausdrücklich erlaubt ist, ist verboten.“ Dies trägt zur Übersichtlichkeit und Sicherheit bei. Wenn man bei der Definition der Regeln etwas übersehen hat, wird nur die Funktionalität und nicht die Sicherheit eingeschränkt. Während man eine Einschränkung der Funktionalität im Bedarfsfall schnell merkt, bleiben Einbußen in der Sicherheit oft unerkannt. Allerdings gibt es keine 100%ige Sicherheit. Meist erhöht sich im Laufe der Zeit das Missbrauchsrisiko, z. B. durch Bekanntwerden von Schwachstellen, Herausbilden neuer Angriffsformen oder auch durch Verbessern der Systemausstattung von Angreifern. Daher sollten Administratoren ständig die Diskussion um Sicherheitslücken verfolgen und das Sicherheitsniveau regelmäßig neu bewerten, damit die Sicherung dem Stand der Technik entspricht.

4.6.4 Pflichten eines Firewall-Betreibers

Eine Firewall hat üblicherweise die Aufgabe, ordnungsgemäßen und zugelassenen Netzverkehr zu sichern, unzulässige bzw. rechtswidrige Nutzung abzuwehren sowie unerlaubte, private Nutzung von innen zu verhindern. Die reine Transportsteuerung in einer Firewall, die als Dienstleistung für Dritte angeboten wird, ist rechtlich gesehen „geschäftsmäßiges Erbringen von Telekommunikationsdiensten“ im Sinne des Telekommunikationsgesetzes (TKG). Anbieter von TK-Diensten haben das Fernmeldegeheimnis zu wahren (§ 85 TKG). Diensteanbieter dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur zum Erbringen der TK-Dienste verwenden. Selbstverständlich haben auch Betreiber von „Corporate Networks“ das Fernmeldegeheimnis zu wahren. Dies gilt in Niedersachsen z. B. für das Informatikzentrum Niedersachsen als TK-Netzbetreiber der Landesverwaltung sowie für Vereine und Verbände, die TK-Netze für ihre Mitglieder betreiben.

Auch Unternehmen und Behörden, die ihren Mitarbeitern Telekommunikationseinrichtungen zur privaten Nutzung gegen Entgelt zur Verfügung stellen, gelten als geschäftsmäßige TK-Diensteanbieter. Dies gilt nicht für rein dienstliche Tätigkeit. Der Arbeitgeber/Dienstherr kann und sollte den dienstlichen Umgang mit TK-Einrichtungen durch Betriebs- oder Dienstvereinbarung regeln. Bei Mischformen dienstlicher und privater Nutzung muss er für eine Differenzierung im Umgang mit Protokolldaten sorgen, um das Fernmeldegeheimnis zu wahren. Ist dies technisch nicht möglich, muss der Dienstherr auf ein Monitoring verzichten.

Üblicherweise werden mit der Firewall jedoch neben der reinen Transportsteuerung auch andere Dienste angeboten, z. B. ein Domain Name Service, ein Proxy Server und eine zentrale Virenkontrolle. Diese Dienstleistungen sind Teledienste im Sinne des neuen Teledienstesrechts. Für die individuelle Nutzung solcher Dienste gelten das Teledienstegesetz (TDG), das einheitliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste schafft, und das Teledienstedatenschutzgesetz (TDDSG), das die Datenschutzvorschriften für den Betrieb von Telediensten enthält.

4.6.5 Selbstkontrolle mit der Checkliste „Grundschutz durch Firewall“

Für Verantwortliche in Wirtschaft und Verwaltung habe ich eine Orientierungshilfe „Grundschutz durch Firewall“ erstellt, mit der ich auf Gefahren beim Anschluss von LAN an fremde Netze aufmerksam machen will. Die Orientierungshilfe zeigt Sicherheitsrisiken im Internet auf und beschreibt, wie man die Netzübergänge zwischen geschütztem LAN und unkontrollierbaren Außenbereichen durch Firewall sichern kann. Die Orientierungshilfe behandelt unterschiedliche Firewall-Architekturen und gibt Empfehlungen zur Auswahl, Konfiguration und Wartung. Eine Checkliste für den datenschutzgerechten Einsatz von Firewall-Systemen weist Betreiber auf rechtliche, technische und organisatorische Probleme und Fragen hin.

4.7 P 53: Das bedeutendste Infrastrukturvorhaben des Landes

Das Land Niedersachsen führt zum 1. Januar 2000 die erste Stufe eines integrierten, automatisierten Haushaltswirtschaftssystems mit den Bereichen Mittelverteilung, Mittelbewirtschaftung und Kasse ein (als 53. Projekt der Verwaltungsreform P 53 genannt). Über die hierfür beschaffte Standardsoftware "Public Performance Management" (PPM) des niederländischen-amerikanischen Softwareherstellers BaaN werden alle haushaltsmittelbewirtschaftenden Stellen direkt im Dialog über PC-Arbeitsplätze angebunden sein.

Derzeit sind Aus- und Einzahlungen trotz eines automatisierten Kassensystems sehr arbeitsintensiv. Künftig übernimmt der „Computer" fast alle Aufgaben: Das Ablegen von Belegen entfällt, Daten müssen nur einmal erfasst werden, Daten der Kassenanordnungen werden am Bildschirm direkt eingegeben, die Kassen- und Buchführungsfunktionen werden automationsunterstützt abgewickelt. Die Daten gelangen über das IZN-net (Landesnetz) an das zentrale Datenhaltungssystem im Informatikzentrum Niedersachsen (IZN). Von dort werden die Auszahlungsdaten an den zentralen Bankrechner weitergegeben. Bei den Einnahmen vollzieht sich der umgekehrte Weg. Die Software ermöglicht die Kosten- und Leistungsrechnung und unterstützt ein notwendiges Controlling.

Für die flächendeckende Einführung dieses Verfahrens werden in den nächsten drei Jahren ca. 200 Mio. DM in den Ausbau des Landesnetzes, die Errichtung und Erweiterung lokaler Netze sowie in Hardware (Server, PC, Drucker) und Software investiert. Zukünftig wird an rd. 12.000 Arbeitsplätzen in der niedersächsischen Landesverwaltung das elektronische Kassenwesen eingesetzt. An 55.000 Arbeitsplätzen wird das IZN-net vielfältig genutzt werden. Die im Rahmen des Projektes P 53 neu auszustattenden IuK-Arbeitsplätze werden mit vorkonfigurierten PC mit dem Betriebssystem Windows NT ausgestattet. Die PC können an das lokale Netz ihrer Dienststelle angeschlossen oder als stand-alone-Lösung betrieben werden. Sie sind aber von Beginn an so einzurichten, dass sie über die bloße Bereitstellung von Office-Software wie Textverarbeitung, Tabellenkalkulation usw. hinaus Zugang zu typischen Diensten der Bürokommunikation haben. Hierzu zählen E-Mail, Verzeichnisdienste, Ablagesysteme und Informationsdienste, aber auch Verschlüsselungstechnik und digitale Signatur. Die Verschlüsselung gehört nicht zum Grundschutz des IZN-net, sondern ist Aufgabe der Anwendung.

Dem IZN als zentraler IuK-Dienstleistungsinstanz ist die Betriebsverantwortung (zentrale Administration) für das Gesamtsystem übertragen worden. Alternativ kann die jeweilige Ortsdienststelle diese Administrationsaufgabe übernehmen, wobei die Option für eine zentrale Administration gesichert sein muss. Aufgaben der Administration sind Feineinstellung der Systeme, Systembetrieb, Problemmanagement, Softwareverteilung und Benutzerbetreuung über Hotline.

P 53 ist das anspruchsvollste und bedeutendste Reformvorhaben der Landesverwaltung. Das Projekt erfordert eine strategische Sicht über den „Tellerrand" hinweg, wie die IuK-Technik und die Infrastruktur im Land Niedersachsen auf längere Sicht aussehen soll. Diese notwendige Sicht wurde leider erst sehr spät in einer eingeforderten Technikfolgenabschätzung entwickelt. Zentrale Punkte der neuen IuK-Infrastruktur sind die digitale Signatur für kassenwirksame Vorgänge, eine Ende-zu-Ende-Verschlüsselung und die konsequente Nutzung von Sicherungsfunktionen des Betriebssystems Windows NT.

Ich begrüße die Entscheidung des Finanzministeriums zum Einsatz von Verschlüsselungstechnik für das Projekt; die Verschlüsselung ist auch für mich zentrale Voraussetzung für eine gesicherte Datenübertragung aller kassenrelevanten Daten. Zudem ist eine angemessene Verschlüsselungstechnik unabdingbare Infrastrukturvoraussetzung für eine vertrauliche Kommunikation im aufzubauen-

den Landesnetz. Sie sollte jedoch nicht nur proprietärer Bestandteil der zu beschaffenden Software des Systems Haushaltswirtschaft sein, sondern Infrastrukturmaßnahme des IZN-net werden. Zur Beweissicherung einer erfolgten Kommunikation sollten Zustellungs- und Empfangsnachweise bzw. Sende- und Empfangsübergabenachweise geführt werden. Diese Daten müssen dem Anwender zur Verfügung stehen.

Das Verfahrenskonzept P 53 bedarf in einigen Punkten noch der Klärung und Konkretisierung. So ist der Punkt „Versiegelung“ (Digitale Signatur) noch nicht konkret genug beschrieben. Es muß deutlich werden, welche innerbehördlichen Organisationskontrollen im Verfahrensablauf geplant sind. Datenschutzrechtlich problematisch ist die externe Wartung und Systembetreuung. Bei der Wartung von Netzen und Arbeitsplatzcomputern durch das IZN müssen eine Reihe von Sicherheitsvorkehrungen getroffen werden, um den Datenschutz zu gewährleisten. Art und Umfang der Datensicherungsmaßnahmen richten sich danach, wie die Wartung durchgeführt wird. Dies ist detailliert zu beschreiben. Die Integration vorhandener Netzwerkbetriebssysteme (UNIX, NOVELL etc.) muss festgelegt werden. Die Sicherungsfunktionen dieser Systeme sind aufzuzeigen. Ich stehe auch weiterhin zur Beratung bei der Erarbeitung der erforderlichen Technikfolgenabschätzungen (vgl. 4.5) und der erforderlichen Datensicherungskonzepte zur Verfügung.

4.8 Telearbeit: Arbeitsplatz außer Haus

Unter Telearbeit versteht man im allgemeinen eine berufliche Tätigkeit, die außerhalb konventioneller Betriebsstätten unter Nutzung von Telekommunikation durchgeführt wird. In Wirtschaft und Verwaltung wird sie zunehmend als Mittel zur Kostenreduzierung und zur Flexibilisierung der Arbeitszeit eingesetzt. Viele Organisationsformen sind heute erkennbar, so z. B.

- Teleheimarbeit, bei der die Beschäftigten zu Hause arbeiten,
- Alternierende Telearbeit als Kombination aus Büroarbeit und Arbeit zu Hause,
- Telearbeit in Satellitenbüros, die Unternehmen bzw. Behörden für mehrere Mitarbeiter in Wohnortnähe einrichten,
- Virtuelle Büros, die von rechtlich unabhängigen und räumlich getrennten Selbständigen auf Dauer oder für die Abwicklung von Projekten eingerichtet werden,
- Telecenter, die mit multifunktionaler Informations- und Kommunikationstechnologie ausgestattet sind, und
- Mobile Telearbeit, bei der, unterstützt durch entsprechende Informations- und Kommunikationstechnik (z. B. Notebooks mit Mobilanschluß), unabhängig von einer festen Arbeitsstätte gearbeitet werden kann.

Die Telearbeiter stehen dabei in unterschiedlichen Beschäftigungsverhältnissen zu ihren Auftraggebern, z. B. auf der Basis eines Arbeitnehmerverhältnisses, Tätigkeit nach dem Heimarbeitsgesetz, Mitarbeit von freien Mitarbeiter/innen im arbeitnehmerähnlichem Status und als Selbständige, die Zeit und Ort des Arbeitsausübung selbst festlegen, sowie den Arbeitsablauf frei gestalten. Für die technische Realisierung des Datenaustausches zwischen Telearbeitsplatz und Arbeitsstätte stehen vielfältige technische Kommunikationsmöglichkeiten (Konferenzsystem, Remote-Access zu einer Workstation, E-Mail als öffentliche Lösung über das Internet) zur Verfügung. Häufig wird dabei außer Acht gelassen, dass für die Telearbeit im Rahmen eines Arbeits- oder Dienstverhältnisses der Arbeitgeber/Dienstherr die datenschutzrechtliche Verantwortung trägt. Dabei ist

für Stellen der Wirtschaft (nicht-öffentliche Stellen) das Bundesdatenschutzgesetz (BDSG) und für öffentliche Stellen in Niedersachsen das Niedersächsische Datenschutzgesetz (NDSG) anzuwenden.

Erfolgt eine Verarbeitung personenbezogener Daten durch Telearbeiter auf der Basis von Werkverträgen in der Privatwohnung oder in Nachbarschafts- oder Satellitenbüros, unterliegt die Telearbeit in der Regel den Vorschriften der Datenverarbeitung im Auftrag (§ 11 BDSG bzw. § 6 NDSG). Ein solcher Telearbeiter darf die Daten nur nach den Weisungen des Auftraggebers verarbeiten und nutzen. Auch hier bleibt der Auftraggeber für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich. Dies gilt nicht, sobald dem Telearbeiter eine rechtliche Zuständigkeit für die Aufgabe zugewiesen worden ist (sog. Funktionsübertragung).

Für die Telearbeit sind Kontrollmöglichkeiten nicht nur durch den Arbeitgeber, sondern auch durch den internen Datenschutzbeauftragten (§§ 36, 37 BDSG bzw. § 8 NDSG), den Landesbeauftragten für den Datenschutz (§ 22 NDSG) bzw. die Aufsichtsbehörde für die Datenverabeitung im nicht-öffentlichen Bereich (§ 38 BDSG) zu gewährleisten. Hierfür muss ein Zugang zum häuslichen Arbeitsplatz gesichert sein. Dazu bedarf es wegen des Grundrechts auf Unverletzlichkeit der Wohnung jedoch der ausdrücklichen Einwilligung der betroffenen Beschäftigten. Diese muss als Voraussetzung für die Ausübung der Telearbeit erklärt werden. Erfolgt der Widerruf einer solchen Einwilligung, ist die Telearbeitsmöglichkeit sofort aufzuheben.

4.9 Behindert der Datenschutz die „Neuen Steuerungsinstrumente“?

Die Neuorientierung der öffentlichen Verwaltung ist in vollem Gange. Sicherstellung der Finanzkraft, bürgernahe und transparente Leistungserbringung, wirtschaftliche Gestaltung der internen Verwaltungsprozesse und Verbesserung der Mitarbeiterqualifikation/-motivation sind propagierte Ziele. Durch Einsatz moderner Informations- und Kommunikationstechniken sollen die notwendigen Funktionalitäten der Kameralistik gewahrt und gleichzeitig die Anforderungen wie doppelte Buchführung, Budgetierung, Kosten- und Leistungsrechnung, Führungssystem, zentrale Speicherung der Personaldaten sowie Controlling eingeführt werden.

Bei der Übernahme betriebswirtschaftlicher Managementmethoden kann es zu Konflikten mit rechtlichen Regelungen kommen, die nicht immer mit den neuen Steuerungsinstrumenten in Einklang stehen. In der Diskussion um angemessene Mittel wird vielfach der Datenschutz als Verhinderungsinstrument „verteufelt“; eine bedauerliche Fehleinschätzung, denn der Datenschutz kann sogar als Gestaltungselement für eine effektive und effiziente Verwaltung dienen.

Meine Erkenntnisse aus Beratungsgesprächen mit den Projektgruppen zeigen deutlich auf, dass der Erfolg der neuen Steuerungsmodelle ganz wesentlich vom Verständnis und der Akzeptanz der Mitarbeiterinnen und Mitarbeiter abhängen wird. Dies könnte durch die von mir empfohlene Zielsetzung der Datenvermeidung (Datensparsamkeit) gefördert werden. Dem Datenschutz würde dadurch hinreichend Rechnung getragen, dass nur die für die genannten Aufgaben unabdingbar erforderlichen Daten verarbeitet und im Übrigen anonyme Verarbeitungsformen verwirklicht werden. Als erforderlich sind nur solche Daten anzusehen, ohne die eine Aufgabe überhaupt nicht, nicht vollständig, nicht rechtzeitig oder nur mit unverhältnismässigen Schwierigkeiten erfüllt werden kann. In den meisten Fällen sollte es ausreichen, z. B. eine Kosten- und Leistungsrechnung auf Dienststellenebene durchzuführen und auf eine Detailuntersuchung von kleineren Einheiten zu verzichten. Soweit eine produktbezogene, bedarfsgerechte Budgetierung sowie Produktkostenvergleiche offengelegt werden sollen,

kann dies grundsätzlich mit anonymisierten Daten der Beschäftigten bezogen auf eine Besoldungs- und Vergütungsgruppe bzw. Organisationseinheit erreicht werden. Dies gilt um so mehr, als Marktpreise für Verwaltungsdienstleister nicht entstehen können; ein Vergleich der Produktkosten ist innerhalb des Verwaltungsbereichs auch ohne Personal-Istkosten durchführbar. Da z. B. die Anzahl der Kinder oder besondere Kosten für eine Krankheit eines Bediensteten nicht zu den vom Dienstherrn beeinflussbaren Größen zählen, ist die Verarbeitung der Daten auch aus dieser Sicht nicht erforderlich.

Die wichtigsten Forderungen an die neuen Steuerungsmodelle sind im folgenden aufgeführt:

- Für die Berechnung der Personalkosten der einzelnen Leistungen dürfen nicht die tatsächlichen Personalkosten verwendet werden. Dies betrifft die Löhne und Gehälter, Beihilfen usw. und gilt sowohl für die Kosten- und Leistungsrechnung als auch für die Budgetierung. Evtl. sind die von der KGST ermittelten Personalkosten oder die aus der Gesamtheit der Personalkosten einer Besoldungs- oder Vergütungsgruppe der jeweiligen Dienststelle errechneten Mittelwerte zu verwenden.
- Bei Verwendung von Sachkosten in der Kosten- und Leistungsrechnung sollten nur aggregierte Daten verwendet werden. Dabei ist die größte Einheit zu wählen, mit der die Ziele erreicht werden.
- Auch die Leistungsdaten sollten nur anonymisiert in die Kosten- und Leistungsrechnung einfließen. Dabei ist auf eine ausreichende Anonymisierung zu achten. 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 Kennziffern nicht personenbezogen konkretisiert werden.
- Bei der Erstellung von Controllingberichten ist darauf zu achten, dass Rückschlüsse auf Leistungen einzelner Beschäftigter nicht möglich sind. Behördliche Datenschutzbeauftragte sollten Einblick in das Gesamtsystem erhalten, um überprüfen zu können, ob ggf. durch Datenverknüpfungen oder andere technische Möglichkeiten datenschutzrelevante Informationen missbräuchlich genutzt werden können.
- Im Rahmen der Kosten- und Leistungskontrolle dürfen keine Maßnahmen eingeleitet werden, die zu einer Bewertung der Arbeitsweise einzelner Mitarbeiter führen. Die Mitarbeiterführung verbleibt im bisherigen Rahmen bei den jeweiligen Vorgesetzten.
- Bei der Einführung eines zentralen Personaldatenbanksystems sind besondere technische und organisatorische Maßnahmen zu treffen, um eine datenschutzgerechte Verarbeitung der Daten sicherzustellen.

4.10 Outsourcing: nicht immer, aber immer öfter

Zunehmende Spezialisierung in Hardware, Software und Personal sowie mögliche Kosteneinsparungen und hohe Flexibilität sind heute Gründe, bestehende Verfahrensabläufe zu überdenken. Immer häufiger wird in Wirtschaft und Verwaltung das Modell „Outsourcing“ gewählt. Der Begriff stammt aus dem amerikanischen Wirtschaftsleben und setzt sich aus den Worten „Outside Resource Using“ zusammen. Die verbreitete Grundeinstellung zu „Outsourcing“ scheint negativ, zumindest skeptisch zu sein. Es sprechen jedoch auch gute Gründe für dieses Modell:

- hohe Qualität der Verarbeitung durch Spezialisierung,

– Interessenferne der Auftragnehmer gegenüber den Daten der Betroffenen,

– Geschäftsinteresse an untadeligem Image und

– effektive Sicherheitssysteme durch optimale Betriebsgröße.

Datenschutzrechtlich zu unterscheiden sind die Auftragsdatenverarbeitung und die Funktionsübertragung. Bei der Auftragsdatenverarbeitung bleibt die datenschutzrechtliche Verantwortung für die Verarbeitung der personenbezogenen Daten beim Auftraggeber. Er schreibt die technischen und organisatorischen Maßnahmen zur Datensicherung und zur Gewährleistung der Vertraulichkeit beim Auftragnehmer vor. Dem Serviceunternehmen wird nur die tatsächliche Verarbeitung nach Weisung und unter Verantwortung des Auftraggebers übertragen. Bei der Datenverarbeitung im Auftrag wird damit lediglich eine „Hilfsfunktion“ der eigentlichen Aufgabe ausgelagert.

Werden dagegen die der Verarbeitung zugrunde liegenden Aufgaben oder Geschäftszwecke ganz oder teilweise abgegeben, erbringt der Auftragnehmer über die technische Durchführung hinaus materielle Leistungen mit Hilfe der überlassenen Daten, dann spricht die Fachliteratur von einer „Funktionsübertragung“. In diesem Fall wird also dem Dienstleister eine Aufgabe übertragen, die er eigenverantwortlich wahrnimmt.

Deutliche Erkennungsmerkmale sind bei

Auftragsdatenverarbeitung

– fehlende Entscheidungsbefugnis des Auftragnehmers,

– weisungsgebundene Unterstützung,

– fehlende (vertragliche) Beziehung des Auftragnehmers zum Betroffenen,

– Umgang nur mit Daten, die der Auftraggeber zur Verfügung stellt,

Funktionsübertragung

– Überlassung von Nutzungsrechten an den Daten,

– eigenverantwortliche Sicherstellung von Zulässigkeit und Richtigkeit der Daten durch den Dienstleister,

– Sicherstellen der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch).

Bei einer Auftragsdatenverarbeitung sind die datenschutzrechtlichen Anforderungen für Stellen der Wirtschaft in § 11 BDSG und für öffentliche Stellen des Landes Niedersachsen in § 6 NDSG geregelt. Bereichsspezifische Vorschriften gehen dem allgemeinen Datenschutzrecht vor, so z. B.

– § 80 SGB X bei der Verarbeitung von Sozialdaten im Auftrage,

– § 5 NStatG, der bei Vergabe statistischer Auswertungen die Kenntnisnahme von Hilfsmerkmalen untersagt,

– besondere Berufsgeheimnisse wie z. B. § 203 StGB für Ärzte, Apotheker, Angehörige der privaten Kranken-, Unfall- oder Lebensversicherungen, Rechtsanwälte, Steuerberater u. a.,

– § 30 Abgabenordnung (Steuergeheimnis).

Die Auftraggeber in Wirtschaft und Verwaltung sind in gleicher Weise verpflichtet, die zu übertragende Datenverarbeitung oder –nutzung, die vom Auftragnehmer einzuhaltenden technischen und organisatorischen Datensicherungsmaßnahmen sowie etwaige Unterauftragsverhältnisse schriftlich festzule-

gen. Neben diesen Mindestfestlegungen sollten auch die folgenden Pflichten bestimmt werden:

– Externe Personen oder Stellen, die mit der Auftragsdatenverarbeitung betraut sind, haben nach den Weisungen des Auftraggebers zu arbeiten.

– Der Auftraggeber hat vor Beginn der Arbeiten sicherzustellen, dass der Auftragnehmer personenbezogene Daten nur zur Kenntnis nehmen kann, soweit dies unvermeidbar ist.

Meine Orientierungshilfe und Checkliste „Datenschutz bei Auftragsdatenverarbeitung“ weist auf Gefahren und Risiken bei der Datenverarbeitung im Auftrag hin und gibt konkrete Empfehlungen für vertragliche Vereinbarungen sowie technische und organisatorische Sicherungsmaßnahmen. Im Hinblick auf die Vielschichtigkeit der Auftragsdatenverarbeitung, von der schlichten Datenerfassung, über das Bereitstellen von Rechnerleistung, die Verarbeitung im Rahmen eines umfassenden Hardware- und Softwarekonzeptes, bis hin zur individuellen Entwicklung und Implementierung komplexer automatisierter Verfahren, ergeben sich im Einzelfall Fragestellungen und Forderungen. Es ist daher sinnvoll, anhand der Checkliste zu prüfen, ob die im Einzelfall bestehenden oder beabsichtigten vertraglichen Vereinbarungen den datenschutzrechtlichen Anforderungen entsprechen. Der regelungsfreie Raum sollte möglichst klein gehalten werden.

4.11 Wartung und Systembetreuung „outgesourct“

Die Abhängigkeit von einer funktionierenden Datenverarbeitung ist in vielen Branchen der Wirtschaft und in der Verwaltung bereits so groß, daß der kurzfristige Ausfall der Datenverarbeitung existenzbedrohend sein kann. Dieses Risiko sowie zunehmende Systemkomplexität und verteilte Systemarchitekturen führen dazu, daß immer mehr Anwender ihre Systeme nicht mehr selbst warten. Als Folge davon werden Verträge für Wartungsarbeiten und Systembetreuung durch externe Personen oder Stellen abgeschlossen – häufig mit dem Unternehmen, das das eingesetzte Verfahren entwickelt und vertrieben hat.

Durch externe Wartung und Systembetreuung verliert die datenverarbeitende Stelle sehr schnell das notwendige Wissen über das eingesetzte technische System und ist häufig nicht in der Lage, die Tätigkeit des externen Wartungspersonals nachzuvollziehen. Viele Unternehmen und Behörden machen sich über diese Risiken der externen Wartung keine Gedanken. Dabei tragen die datenverarbeitenden Stellen für externe Wartungs- und Systembetreuungsarbeiten die datenschutzrechtliche Verantwortung. Wartung und Systembetreuung unterliegen den Regelungen der Datenverarbeitung im Auftrag (§ 11 BDSG bzw. § 6 NDSG).

Wartung und Systembetreuung durch externe Personen oder Stellen schaffen Gefahren und Risiken, z. B.:

– Für die Wartung wird ein weiterer Zugang zum Rechner geschaffen, über den sich Personen mit umfassenden Rechten anmelden können oder der als Zugang für „Hacker“ mißbraucht wird.

– Die datenverarbeitende Stelle kann bei der Fernwartung nur begrenzt kontrollieren, welche Person tatsächlich die Wartung vornimmt, welche Daten übertragen werden und welche Sicherungsmaßnahmen beim Auftragnehmer getroffen worden sind.

– Das Wartungspersonal kann künftig auf den gesamten Datenbestand zugreifen.

– Der Datenverkehr zwischen Rechner und Wartungsfirma kann abgehört werden.

Eine Wartung der Datenverarbeitungsanlagen durch externe Personen oder Stellen sollte nur dann gewählt werden, wenn eine eigene Wartung nur eingeschränkt oder gar nicht möglich ist. Die Kenntnisnahme personenbezogener Daten durch den Auftragnehmer sollte grundsätzlich ausgeschlossen sein. Wird die Fernwartung aus dem Ausland durchgeführt, ist sicherzustellen, daß die jeweiligen Regelungen über die Übermittlung von personenbezogenen Daten an Stellen außerhalb der Bundesrepublik Deutschland (§ 14 NDSG, §§ 28 ff BDSG) angewendet werden. Als Ergebnis bleibt festzuhalten, dass auf eine Wartung und Systembetreuung durch externe Personen oder Stellen verzichtet werden muß, wenn diese nicht durch ausreichende technische und organisatorische Maßnahmen gesichert werden kann.

Meine Orientierungshilfe, die ich im Rahmen der Beratung des Projektes P 53 „Automatisierte Haushaltsbewirtschaftung“ erarbeitet habe, setzt sich detailliert mit den oben beschriebenen Gefahren auseinander. Die Checkliste erfragt die getroffenen Festlegungen und Maßnahmen, gegliedert nach „Allgemeine Anforderungen“, „Wartung und Systembetreuung vor Ort“, „Wartung und Systembetreuung außer Haus“ sowie „Fernwartung“.

4.12 Technikfolgenabschätzung

4.12.1 Manch einer tut sich schwer

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 1993 erlassenen, inzwischen geänderten Regelung zur Technikfolgenabschätzung hat Niedersachsen früher als andere Länder im allgemeinen Datenschutzrecht ein wichtiges Verfahren eingeführt, um den Gefahren der rasanten Entwicklung neuer Technologien im Informations- und Kommunikationsbereich zu begegnen. Die inzwischen fünfjährigen Erfahrungen in Niedersachsen zeigen, dass dieses Verfahren bei richtigem Einsatz sehr erfolgreich sein kann (siehe 4.12.3).

Die Technikfolgenabschätzungen insgesamt zeigen jedoch auch, dass sich viele betroffenen Stellen schwer mit der Umsetzung dieser Regelung tun. Es gibt große Unsicherheiten, wann die Erstellung einer Technikfolgenabschätzung erforderlich ist. Was ist eigentlich ein automatisiertes Verfahren? Was sind neue Technologien? Was sind wesentliche Änderungen von Verfahren?

Deutlich unterschiedliche Auffassungen bestehen über den Umfang, den eine Technikfolgenabschätzung haben sollte. Ich habe Technikfolgenabschätzungen erhalten, die weniger als eine Seite ausmachten und andere, die sich über mehr als 50 Seiten erstreckten. Das eine ist so falsch wie das andere. Die zu kurz geratenen Versuche haben nur eine Feigenblattfunktion, ohne wirklich auf die vorhandenen Gefahren einzugehen. Die zu lang geratenen verlieren sich in unnötigen Detailbetrachtungen, versuchen für jedermann allgemeinverständlich zu formulieren und sind dann möglicherweise an den Stellen zu kurz geraten, auf die es tatsächlich ankommt.

Probleme gibt es auch bei der zeitlichen Umsetzung der Technikfolgenabschätzung. In der Prioritätenliste des Projektablaufplans befindet sie sich weit hinten. Auf diese Weise besteht die Gefahr, dass die Einführung des neuen Verfahrens bereits zu weit fortgeschritten ist und die in der Technikfolgenabschätzung getroffenen Empfehlungen nicht mehr oder nur mit sehr hohem finanziellen und

zeitlichen Aufwand durchgeführt werden können. Dies kann im Extremfall teure Schadensersatzforderungen zur Folge haben.

Schließlich tun sich manche bei der Durchführung und inhaltlichen Gestaltung der Technikfolgenabschätzung schwer. Wovon soll man ausgehen? Ist von der Aufstellung der Technik auf der grünen Wiese auszugehen, um die erst ein absicherndes Gebäude erstellt werden muss oder setzt man ein Datensicherungskonzept voraus und untersucht lediglich etwaige Sicherheitslücken? Können andere Verfahren oder Systeme, mit denen das geplante in Verbindung stehen soll, in der Abschätzung unberücksichtigt bleiben?

4.12.2 Der Weg zum Erfolg

Die aufgeführten Unsicherheiten und Probleme lassen sich aus den Weg räumen. Um hierbei Hilfestellung zu leisten, habe ich im Folgenden Hinweise aufgeführt, die an die Ersteller von Technikfolgenabschätzungen gerichtet sind.

Technikfolgenabschätzung ist eine Chance: Man sollte keine zeitraubenden Prüfungen anstellen, ob man einer Technikfolgenabschätzung entgehen kann. Die Methode bietet die Möglichkeit, auf effiziente Weise notwendige Sicherungsmaßnahmen im Verfahren zu berücksichtigen. Sie sollte ein Standardinstrument für alle neu einzuführenden automatisierten Verfahren werden, seien es spezielle Anwendungen, Standard-Software oder IuK-Infrastuktur. Wenn allerdings von einer anderen Stelle die Ausarbeitung einer gelungenen Technikfolgenabschätzung für ein vergleichbares Verfahren zur Verfügung steht, kann eine erneute Technikfolgenabschätzung überflüssig sein.

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. Zum Abschätzungsprozess gehört deshalb, dass nach Auswahl der erforderlichen Sicherungsmaßnahmen überprüft wird, ob gegen alle anfangs aufgelisteten Gefahren ausreichende Maßnahmen ausgewählt wurden.

Technikfolgenabschätzungen müssen vollständig und in sich abgeschlossen sein: Sicherungsmaßnahmen generell vorauszusetzen oder in Teilen auf andere Abschätzungen oder Konzepte zu verweisen, führt zu großer Unübersichtlichkeit und gefährdet den Erfolg der Technikfolgenabschätzung. Soweit Schnittstellen zu anderen Systemen vorhanden sind oder das Verfahren auf anderen aufsetzt, muss klar werden, wie die hierdurch entstehenden Gefahren beherrscht werden sollen.

Fakten statt Romane: In allen Bereichen der Abschätzung reichen stichwortartige Beschreibungen aus, die für informierte Entscheider, nicht aber allgemein verständlich sein müssen. Es brauchen nicht alle Details aufgeführt werden. Die Sicherungsmaßnahmen sollen die Eckpfeiler darstellen, die für die weiteren Entscheidungen wichtig sind. Die Details der Systemkonfiguration und der dienstlichen Organisation sollten nicht in der Technikfolgenabschätzung, sondern in einem separaten Datensicherungskonzept dargestellt werden. Wenn dies beherzigt wird, ist die Technikfolgenabschätzung kurzfristig und mit geringem personellen Aufwand durchführbar.

Wer zu spät abschätzt, den bestraft das Leben: Bereits wenn das Verfahren erst in Umrissen Gestalt annimmt, ist mit der Technikfolgenabschätzung zu beginnen. Sie muss vor der Entscheidung über die Einführung des Verfahrens und vor

den ersten Ausschreibungen fertig gestellt sein. Auf diese Weise greift sie steuernd und gestaltend in die Verfahrensplanung ein und erreicht ihren Zweck.

4.12.3 Erfolge und Misserfolge

Im folgenden sind die wichtigsten mir bekannten Technikfolgenabschätzungen aufgeführt, die aufgrund der Regelungen des NDSG erstellt wurden. Die Pfeile und Kommentare deuten an, inwieweit ich die Ausgestaltung der Abschätzungen für gelungen halte.

X.400/MININET

Erste Technikfolgenabschätzung mit wichtigen Aussagen zum E-Mail-Projekt der Landesverwaltung. Für ein Vorbild aber zu lang geraten.

KOMNET

Engagiert begonnen mit wichtigen Aussagen zu ISDN-Leistungsmerkmalen, dann aber leider abrupt abbrechend.

DIBS

Recht gut gelungene Abschätzung über die Automatisierung der Bezüge-Vorgangsbearbeitung, vielleicht noch einen Tick zu lang.

KDO-Internet

Kurzgefasste Abschätzung der Risiken bei Internet-Anschluss mit ausführlichem Anhang. Wermutstropfen: Die KDO verlangt eine Gebühr für Kopien der Technikfolgenabschätzung.

Landkreis Friesland

Mustergültige Technikfolgenabschätzung über die Einführung moderner PC-gestützter Bürokommunikation. In enger Zusammenarbeit mit dem LfD erstellt.

AIDA

Kurze Abschätzung über die elektronische Archivierung von Patientendaten in der Medizinische Hochschule Hannover. Ausreichend, aber an einigen Stellen sehr knapp.

SAMBA

Mehr Sollkonzept als wirkliche Abschätzung der Gefahren und Risiken der automatisierten Beihilfeabrechnung in der Landesverwaltung.

Ich hoffe, dass bei zukünftigen Verfahrensentwicklungen meine oben genannten Empfehlungen beherzigt werden. Dann werden sicherlich die Pfeile wesentlich häufiger nach oben zeigen.

5 Datenschutz beim Landtag

Nennung personenbezogener Daten eines Petenten bei einer Plenardebatte über Eingaben

Im folgenden Fall hat mich der Landtag um eine Stellungnahme gebeten:

Der Förderverein Niedersächsischer Flüchtlingsrat e.V. setzte sich für eine ausländische Familie ein, deren Asylantrag rechtskräftig abgelehnt worden war. Er erbat eine Aufenthaltserlaubnis nach der damals geltenden Härtefallregelung. Die Petition wurde im zuständigen Landtagsausschuss unterschiedlich bewertet. Es kam deshalb zu einer Diskussion im Plenum des Landtags. In der zum Teil lebhaften Aussprache wies der Innenminister darauf hin, dass zwei männliche Familienmitglieder wegen gemeinschaftlicher gefährlicher Körperverletzung rechtskräftig verurteilt worden seien. Auf Befragen nannte er das Strafmaß. Zudem machte der Minister Angaben über die Höhe der von der Familie monatlich bezogenen Sozialhilfe. Die Ausländerkommission des Landtages warf daraufhin die Frage auf, ob die Nennung dieser personenbezogenen Daten mit dem Grundrecht auf Datenschutz vereinbar sei.

Dies habe ich im Ergebnis bejaht. Aus datenschutzrechtlicher Sicht ist die Bekanntgabe von personenbezogenen Daten über die Familie in der Landtagssitzung als Datenübermittlung an einen unbestimmten Personenkreis anzusehen. Zwar richtet sich die Datenverarbeitung im parlamentarischen Bereich nach dem NDSG. Als vorrangige Rechtsgrundlage ist hier jedoch Art. 22 Abs. 1 i. V. m. Art. 26 der Niedersächsischen Verfassung zu beachten, wonach die Verhandlungen des Landtages öffentlich stattfinden. Dies gilt auch für die abschließende Behandlung von Eingaben (§ 54 der Geschäftsordnung des Landtages). Das Öffentlichkeitsprinzip soll den Bürgerinnen und Bürgern die Kontrolle der von ihnen gewählten Abgeordneten ermöglichen, dem Willen der Volksvertretung Publizität verschaffen und insgesamt eine Identifikation der Wähler mit den Volksvertretern fördern.

Hinter den geäußerten Bedenken gegen die Angaben des Innenministers stand die Einschätzung, die Preisgabe der Daten über die Familie sei zur Beurteilung des Petitionsbegehrens nicht erforderlich gewesen. An die Erforderlichkeit sind strikte Anforderungen zu stellen. Erforderlich ist eine Datenverarbeitung, wenn ohne sie eine Aufgabe nicht oder nur unzureichend oder verspätet erfüllt werden könnte. Es reicht dagegen nicht aus, wenn eine personenbezogene Angabe zur Aufgabenerfüllung nur dienlich oder etwa als Hintergrundinformation zur Abrundung eines Gesamtbildes nützlich ist. Bei der Anwendung des Erforderlichkeitsprinzips im Parlamentsbereich müssen jedoch die Funktionsvoraussetzungen parlamentarischer Arbeit berücksichtigt werden. Hier geht es nicht um administrative, sondern um politische Entscheidungen, bei denen den Abgeordneten ein weiter „Beurteilungsspielraum“ zusteht. Als erforderlich für die Erörterung einer Petition müssen deshalb alle personenbezogenen Daten angesehen werden, die für die rechtliche und politische Bewertung des Vorgangs von Bedeutung sein können.

Im vorliegenden Falle handelt es sich bei den Angaben des Innenministers nicht um Informationen aus dem unantastbaren Bereich privater Lebensgestaltung. Die Unterrichtung über die bezogene Sozialhilfe hat vielmehr einen unmittelbaren Bezug zur Frage nach der wirtschaftlichen Integration, die für die Beurteilung des Bleiberechts nach der früheren Härtefallregelung von Belang war.

Ebenso durfte der Gesichtspunkt berücksichtigt werden, ob von einem Ausländer Gewalttätigkeiten ausgehen. Würden solche Umstände aus dem Meinungsbildungsprozess ausgeschieden, so würde die Grundlage für die politische Bewertung durch die Abgeordneten unzulässig verkürzt.

Problematisch ist aus meiner Sicht nicht das Verhalten des Innenministers, sondern die Ausgestaltung des Petitionsverfahrens, die – wie dieser Fall eindrücklich zeigt – notwendigerweise dazu führen muss, dass auch sehr sensible Informationen über Bürgerinnen und Bürger im Rahmen einer parlamentarischen Beratung ungeschützt der Öffentlichkeit preisgegeben werden. Nach den Beratungen der Petitionen in den zuständigen Landtagsausschüssen werden deren Beschlussempfehlungen in Eingabenübersichten zusammengefasst, aus denen sich Namen und Anschriften der Petenten ergeben. Die Eingabenübersichten werden als Landtagsdrucksachen veröffentlicht. Erst diese Angaben führen dazu, dass die Petitionen im Landtag personenbezogen erörtert werden.

Ich habe dies bereits im XI. Tätigkeitsbericht unter 5.1 kritisiert, eine Änderung jedoch bislang nicht erreichen können. Der Gesetzgebungs- und Beratungsdienst des Landtages vertritt die Auffassung, das Öffentlichkeitsprinzip der Verfassung erzwinge diese Verfahrensweise. Ebenso wie das Öffentlichkeitsprinzip hat jedoch auch das Grundrecht auf Datenschutz Verfassungsrang. Widerstreitende verfassungsrechtliche Belange müssen nach dem Grundsatz der praktischen Konkordanz im Einzelfall zum Ausgleich gebracht werden, damit die jeweils verfassungsrechtlich geschützten Güter so weit wie möglich ihre Wirkung entfalten können. Dies geschieht bei der derzeitigen Verfahrensweise nicht. Das Persönlichkeitsrecht der Petenten bleibt vielmehr auf der Strecke.

Der Bundestag und andere Landesparlamente sehen dagegen – zum Teil schon seit Jahren – von Angaben zur Person der Petenten in den Eingabenübersichten ab oder stellen auf andere Weise sicher, dass deren Namen der Öffentlichkeit nicht zur Kenntnis gelangen. Auch die Konferenz der Präsidentinnen und Präsidenten der deutschen Landesparlamente hat sich in einer Entschließung zum parlamentsspezifischen Datenschutzrecht vom 8./11. Mai 1995 dafür ausgesprochen, Vorkehrungen gegen das Bekanntwerden geheimhaltungsbedürftiger personenbezogener Daten zu treffen, und in diesem Zusammenhang die Anonymisierung der Eingabenübersichten genannt. Ich appelliere hiermit erneut an den Landtag, diese Forderung auch in Niedersachsen umzusetzen.

Darüber hinaus halte ich es für erforderlich, dass der Landtag spezifische datenschutzrechtliche Regelungen über die Datenverarbeitung im Parlament schafft, wie sie auch von der genannten Konferenz vorgeschlagen werden. Die bisher geltenden Vorschriften des NDSG berücksichtigen die Besonderheiten der Datenverarbeitung in diesem Bereich nicht.

6 Datenschutzrecht - allgemein

6.1 Novellierung des NDSG

Das NDSG ist 1997 zusammen mit dem NGefAG überarbeitet worden (vgl. XIII 6.1). Die wichtigste angestrebte Änderung hatte das Innenministerium allerdings schon im Zuge der Vorbereitung der Gesetzesnovelle auf meinen Widerspruch hin fallen gelassen: Die geplante Einschränkung der Verpflichtung öffentlicher Stellen zur Bestellung von behördlichen Datenschutzbeauftragten. Das Datenschutzressort ging zunächst von der Einschätzung aus, im öffentlichen Bereich könne die Zahl der mit automatisierter Datenverarbeitung betrauten Bediensteten, die die Bestellung eines behördlichen Datenschutzbeauftragten erforderlich macht, erheblich erhöht werden. Zur Diskussion stand eine Anhebung der derzeitigen Mindestzahl von 5 auf 40 Personen. Anders als im nicht-öffentlichen

Bereich, der durch die Selbstkontrolle durch den betrieblichen Datenschutzbeauftragten und eine ergänzende Anlassaufsicht durch die Aufsichtbehörde geprägt werde – so wurde argumentiert –, bestünden im öffentlichen Bereich weitgehende Kontrollmöglichkeiten durch den LfD. Insbesondere die Gemeinden sollten deshalb durch die Möglichkeit einer Verringerung der Zahl der behördlichen Datenschutzbeauftragten finanziell entlastet werden.

Unvermeidbar hätte dies zu einem Abbau des Datenschutzstandards im kommunalen Bereich geführt. Ein Wegfall von vor Ort wirkenden behördlichen Datenschutzbeauftragten kann selbstverständlich nicht durch meine ohnehin personell unzureichend ausgestattete Dienststelle aufgefangen werden. Nicht wenige Kommunen haben sich mit der seit 1993 bestehenden Verpflichtung zur Bestellung eines Datenschutzbeauftragten Zeit gelassen. Es wäre kaum verständlich gewesen, wenn ihnen – nachdem sie nun ihrer gesetzlichen Verpflichtung nachgekommen sind – signalisiert würde, sie könnten die Maßnahme wieder rückgängig machen. Mit der Rechtsänderung wäre der ursprüngliche Ansatz des NDSG aufgegeben worden, die Verpflichtung zur Bestellung behördlicher Datenschutzbeauftragter im Wesentlichen an den gleichen Kriterien zu orientieren wie die Bestellung von betrieblichen Datenschutzbeauftragten im nichtöffentlichen Bereich. Firmen und Unternehmen wäre sicher kaum verständlich zu machen, dass der Gesetzgeber sie einer Verpflichtung unterwirft, die der Landesgesetzgeber für die öffentliche Verwaltung nicht gelten lassen will. Vor allem aber sprach gegen diese Regelungsabsicht, dass sie nicht in Einklang mit der EU-Datenschutzrichtlinie zu bringen war. Die Richtlinie, die bereits bis zum 24. Oktober 1998 auch in niedersächsisches Recht hätte umgesetzt werden müssen, schreibt eine Bestellung von behördlichen Datenschutzbeauftragten vor, sofern keine Meldung automatisierter Datenverarbeitungsvorgänge an eine Kontrollstelle erfolgt.

Im Wesentlichen hat der Gesetzgeber folgende Änderungen des NDSG vorgenommen:

1. Beschränkung des Gesetzeszwecks

   Das Gesetz ist auf die Sicherstellung des Rechts auf informationelle Selbstbestimmung beschränkt worden. Die weitere Aufgabe, „einer Beeinträchtigung der Wirkungsmöglichkeiten der Verfassungsorgane des Landes oder der Organe der kommunalen Gebietskörperschaften infolge der automatisierten Datenverarbeitung entgegenzuwirken“, wurde gestrichen. Sie steht mit dem Persönlichkeitsrecht in keinem Zusammenhang, sondern sollte einen Informationsvorsprung der Exekutive gegenüber der Legislative durch die automatisierte Datenverarbeitung verhindern. Praktische Bedeutung hat die Vorschrift nicht erlangt.

2. Technische und organisatorische Maßnahmen

   Bei der Regelung der technisch-organisatorischen Maßnahmen (§ 7 NDSG) ist – so die Gesetzesbegründung – klargestellt worden, dass eine derartige Maßnahme in angemessenem Verhältnis zum angestrebten Schutzzweck stehen muss. Dieser Klarstellung bedurfte es aus meiner Sicht nicht. Die entsprechende Forderung ergab sich bisher schon aus der Gesetzesbegründung zum Entwurf des NDSG vom 4. Juni 1992 – LT-Drs. 12/3290.

   Wichtiger ist die Konkretisierung des Gesetzgebers zur Frage, wann vor dem Einsatz automatisierter Datenverarbeitungsverfahren eine Technikfolgenabschätzung durchgeführt werden muss, um festzustellen, ob die für die Betroffenen mit der Datenverarbeitung verbundenen Risiken wirksam beherrscht werden können. Die Technikfolgenabschätzung ist nach den Verwaltungsvorschriften zum NDSG erforderlich, wenn Daten verarbeitet werden sollen, deren Missbrauch Gesundheit, Leben oder Freiheit der Betroffenen gefähr-

den (Daten der Schutzstufe E) oder deren gesellschaftliche Stellung oder wirtschaftliche Verhältnisse erheblich beeinträchtigen könnte (Daten der Schutzstufe D); zum anderen dann, wenn durch die Verwendung neuer Technologien Gefahren für die Betroffenen entstehen können. Die bisher in den VV zum NDSG (Nr. 5.2) vorgesehene Einschränkung, wonach eine Technikfolgenabschätzung bei Daten der Schutzstufe D nur notwendig war, wenn diese in einem vernetzten Rechnersystem mit mindestens 20 Rechnereinheiten oder Bildschirmarbeitsplätzen verarbeitet werden sollten, ist entfallen. Andererseits hat der Gesetzgeber bestimmt, dass bei Daten der Schutzstufen A bis C nur dann eine Technikfolgenabschätzung durchgeführt werden muss, wenn es sich um Technologien handelt, die erstmals im Geltungsbereich des NDSG eingesetzt werden sollen.

3. Dateibeschreibung / Dateienregister

   Die Pflicht, für nicht-automatisierte Dateien eine Dateibeschreibung zu erstellen und ein Verzeichnis über die bei der automatisierten Datenverarbeitung eingesetzten Geräte und die verwendeten Programme zu führen, ist entfallen.

   Eine Dateibeschreibung ist nur noch für automatisierte Dateien vorgesehen. Das bisher beim LfD zu führende Dateienregister ist im Wesentlichen abgeschafft worden. Dateibeschreibungen sind mir grundsätzlich nicht mehr zu übersenden. Eine Ausnahme gilt wegen der besonderen Sensibilität der Daten für Dateien, die zur Aufgabenerfüllung durch den Verfassungsschutz nach dem Niedersächsischen Verfassungsschutzgesetz oder durch die Polizei nach dem NGefAG erstellt worden sind. Für den Bereich des Verfassungsschutzes und der Polizei verfügt der LfD für Kontrollzwecke weiterhin über ein Dateienregister, das Bürgerinnen und Bürgern allerdings nicht zur Einsicht zur Verfügung steht.

4. Datenerhebung bei Dritten

   Ausgeweitet worden sind die Möglicheiten zur Datenerhebung bei Dritten. Eine solche Erhebung kommt jetzt auch in Betracht (§ 9 Abs. 1 Satz 3 Nr. 6 NDSG), wenn es die zu erfüllende Aufgabe ihrer Art nach erforderlich macht, sich zur Beschaffung von personenbezogenen Informationen an Dritte zu wenden oder wenn die Erhebung bei den Betroffenen einen unverhältnismäßigen Aufwand erfordern würde. Diese Datenerhebungen sind jedoch ausgeschlossen, wenn Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Die Regelung ist aus dem BDSG (§ 13 Abs. 2 Satz 2 Nr. 2) übernommen worden. Während der Gesetzgeber 1993 bei der Verabschiedung des NDSG eine derartige Datenerhebung ausdrücklich nicht für notwendig hielt, ist dies 1997 anders beurteilt worden. Klagen über eine etwaige Unzulänglichkeit der bisher geltenden Regelung sind mir allerdings nicht bekannt geworden.

   Geändert wurde auch § 9 Abs. 1 Satz 3 Nr. 3 NDSG. Nach dem bisherigen Gesetzeswortlaut durfte eine Datenerhebung bei Dritten erfolgen, wenn Angaben der Betroffenen überprüft werden mussten, „weil Anhaltspunkte für deren Unrichtigkeit bestehen“. Der zitierte letzte Halbsatz ist jetzt gestrichen worden. Dem unbefangenen Leser drängt sich damit der Schluss auf, dass die Befugnisse zur Datenerhebung bei Dritten in diesem Punkt ausgeweitet werden sollten. Dies ist jedoch nicht der Fall. Der Gesetzgeber ist vielmehr der Auffassung, dass die frühere Hervorhebung von entsprechenden Anhaltspunkten „lediglich erläuternder Natur“ gewesen sei (vgl. Schriftlicher Bericht zum Entwurf eines Dritten Gesetzes zur Änderung datenschutz- und verwaltungsverfahrensrechtlicher Vorschriften – LT-Drs. 13/3754 Seite 2). Demnach müssen auch weiterhin im Einzelfall konkret belegbare Zweifel an

der Richtigkeit der vom Betroffenen gemachten Angaben eine Überprüfung bei Dritten rechtfertigen. Mir ist schleierhaft, warum eine Rechtsvorschrift überarbeitet wird, wenn deren Regelungsgehalt eindeutig ist und inhaltlich nicht geändert werden soll. Den Mitarbeiterinnen und Mitarbeitern in den Behörden, die das NDSG anzuwenden haben, dürfte sich das Geheimnis dieser Regelung kaum erschließen.

5. Regelmäßige Datenübermittlungen

   Die Bestimmung, dass regelmäßige Datenübermittlungen durch Rechtsvorschrift zugelassen werden müssen (§ 12 Abs. 6 NDSG a.F.), ist mit meiner Zustimmung gestrichen worden. Die Regelung hat in der Verwaltungspraxis zu vielfältigen Problemen geführt. Insbesondere gab es Abgrenzungsschwierigkeiten bei der Frage, wann eine regelmäßige Datenverarbeitung vorlag. Für automatisierte Abrufverfahren ist das Erfordernis einer Rechtsvorschrift erhalten geblieben.

6. Forschung

   Auch die bisherige Verpflichtung, den LfD über die Verarbeitung personenbezogener Daten für Forschungsvorhaben dann zu unterrichten, wenn eine Abwägung zwischen dem öffentlichen Interesse an dem Vorhaben und dem schutzwürdigen Interesse der Betroffenen vorzunehmen ist (§ 25 Abs. 2 Nr. 3 NDSG), wurde auf meine Anregung hin gestrichen. Anstelle des LfD ist der behördliche Datenschutzbeauftragte der forschenden Stelle zu unterrichten. Damit wird deren datenschutzrechtliche Verantwortung hervorgehoben.

6.2 Anpassung des NDSG an die EU-Datenschutzrichtlinie

Die Arbeiten zur Novellierung des NDSG waren gerade abgeschlossen, als schon die nächste Änderung vorbereitet werden musste. Bis zum 24. Oktober 1998 war die 1995 vom Rat der Europäischen Union verabschiedete EU-Datenschutzrichtlinie in den Mitgliedstaaten der EU umzusetzen. Um die Verwaltungspraxis nicht mit kurzfristig aufeinander folgenden Rechtsänderungen zu belasten, hatte ich – leider erfolglos – vorgeschlagen, das Gesetz in einem Zuge zu überarbeiten.

Die Änderungen aufgrund der Richtlinie betreffen in erster Linie die Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen, für deren Regelung der Bund zuständig ist. Daneben sind aber auch einige wichtige Änderungen bei der Datenverarbeitung öffentlicher Stellen vorzunehmen. Dem Bund ist es trotz vielfacher Aufforderungen durch den Bundes- sowie die Landesbeauftragten für den Datenschutz nicht gelungen, das BDSG zeitgerecht zu novellieren. Auch Niedersachsen hat die Umsetzungsfrist nicht einhalten können. Die Landesregierung hat jedoch einen Gesetzentwurf erarbeitet, der im Frühjahr nächsten Jahres in den Landtag eingebracht werden soll.

Bis zum Inkrafttreten dieser Rechtsvorschriften sind nach der Rechtsprechung des Europäischen Gerichtshofs zur nicht fristgerechten Umsetzung von EU-Richtlinien die Vorschriften der Datenschutzrichtlinie, die den Bürgerinnen und Bürgern hinreichend bestimmte und unbedingte Rechte gegenüber dem Staat einräumen, unmittelbar anzuwenden.

Der Gesetzentwurf, der neben der Anpassung an die Richtlinie einige weitere Vorschriften enthält, sieht im Wesentlichen folgende Änderungen vor:

1. Wegfall des Dateibegriffs

   Der Sprachgebrauch des NDSG wird an die EU-Richtlinie angepasst. Der bisherige Dateibegriff entfällt. Er wird durch den Begriff der automatisierten Verarbeitung ersetzt. Materielle Bedeutung hat der Dateibegriff nicht mehr, als Anknüpfungspunkt für die Dateibeschreibung ist er entbehrlich. Auch die EU-Richtlinie verlangt seine Beibehaltung nicht. Zwar erfasst deren Anwendungsbereich neben automatisiert verarbeiteten Daten auch herkömmlich verarbeitete Informationen, die in einer Datei gespeichert werden. Der Dateibegriff dient in diesem Zusammenhang aber nur als Abgrenzung zur Akte, für die die Richtlinie nicht gilt. Diese Abgrenzungsnotwendigkeit ist für das NDSG, das seit 1993 Akten voll in seinen Geltungsbereich einbezogen hat, nicht gegeben. Der Dateibegriff wird lediglich für eine Übergangszeit noch eine Rolle spielen, soweit er in bereichsspezifischen Regelungen verwendet wird. Diese Vorschriften müssen an das NDSG angepasst werden.

   Mit dem Wegfall des Dateibegriffs tritt an die Stelle der bisherigen Dateibeschreibung eine Beschreibung der automatisierten Datenverarbeitung.

2. Wartungs- und Systembetreuungsarbeiten

   Die rechtliche Einordnung von Wartungs- und Systembetreuungsarbeiten durch externe Personen oder Stellen bei automatisierter Datenverarbeitung ist umstritten. Zwar werden diese Arbeiten vom Innenministerium und mir übereinstimmend als Auftragsdatenverarbeitung angesehen, zur Beseitigung der bestehenden Unklarheiten habe ich mich jedoch für eine gesetzliche Regelung ausgesprochen. Das Innenministerium möchte sich dagegen mit einer Klarstellung in der Gesetzesbegründung begnügen. Gesetzlich festgelegt werden sollte auch, dass der Auftraggeber vor Beginn der Arbeiten sicherzustellen hat, dass sein Auftragnehmer personenbezogene Daten nur zur Kenntnis nehmen kann, soweit dies unvermeidbar ist.

3. Chipkarten

   Für Chipkarten und andere miniaturisierte Datenverarbeitungssysteme, die Bürgerinnen und Bürgern mit sich führen und die mit anderen Datenverarbeitungssystemen direkt kommunizieren, sieht der Entwurf eine Regelung zur Auskunftspflicht vor. Da die Betroffenen den Inhalt der Chipkarte regelmäßig nicht einsehen können, soll jede Stelle, die Daten auf der Chipkarte verarbeitet, verpflichtet werden, den Betroffenen – z. B. durch ein Bereitstellen von Lesegeräten – Auskunft über die gespeicherten Daten zu erteilen. Die Stelle, die für die Herausgabe der Chipkarte verantwortlich ist, hat zudem Auskunft nach § 16 NDSG zu geben.

   Das Transparenzgebot erfordert es, den elektronischen Kommunikationsvorgang zwischen Kartenterminal und Karte erkennbar zu machen. Das Innenministerium stimmt dieser Bewertung zu, lehnt jedoch die von mir vorgeschlagene entsprechende gesetzliche Regelung ab. Es verweist darauf, dass sich die angestrebte Rechtsfolge schon aus § 9 Abs. 1 NDSG ergebe, wonach personenbezogene Daten grundsätzlich nur mit Kenntnis des Betroffenen erhoben werden dürfen.

   Aus meiner Sicht zeigt sich an dieser wie an vielen anderen Stellen (vgl. 6.1) ein problematisches Grundverständnis bei der Schaffung datenschutzrechtlicher Vorschriften. Gerade wenn es um die Ausübung von Grundrechten geht, darf im Vordergrund einer gesetzlichen Regelung nicht die äußerste Verknappung einer Vorschrift stehen, deren Verständnis sich erst dem Fachmann nach eingehender Analyse erschließt. Will man die Ausübung des Per-

sönlichkeitsrechts fördern, muss man vielmehr auch den Bürgerinnen und Bürgern ein sachgerechtes Verständnis der sie betreffenden Regelungen ermöglichen.

Eine Verpflichtung zur Benutzung einer Chipkarte oder anderer mobiler Kleinrechner kann nur durch Rechtsvorschrift begründet werden. Auch dies sollte gesetzlich festgelegt werden.

4. Behördliche Datenschutzbeauftragte

Zur Kontrolle der Verarbeitung personenbezogener Daten sieht die EU-Datenschutzrichtlinie eine zentrale Meldepflicht über die automatisierte Datenverarbeitung gegenüber der jeweiligen Kontrollbehörde vor. Auf dieses bürokratische Verfahren kann verzichtet werden, wenn statt dessen behördeninterne Datenschutzbeauftragte bestellt werden, wie dies in Niedersachsen seit 1993 gesetzlich vorgeschrieben ist. Die bisherige Einschränkung, dass ein Datenschutzbeauftragter nur bestellt werden muss, wenn mindestens fünf Bedienstete bei der öffentlichen Stelle ständig mit Aufgaben der automatisierten Datenverarbeitung beschäftigt sind, ist jedoch – will man die Meldepflicht vermeiden – mit der Richtlinie nicht vereinbar. Sie wird deshalb gestrichen.

Der niedersächsische Gesetzgeber war seinerzeit bestrebt, die Stellung und die Aufgaben des Datenschutzbeauftragten nicht im Einzelnen festzulegen, um den öffentlichen Stellen, insbesondere den Kommunen, ein möglichst großes Maß an Gestaltungsfreiheit zu lassen. Mehr, als dass der Datenschutzbeauftragte die öffentliche Stelle zu unterstützen habe und dies vor allem bei der Prüfung technischer und organisatorischer Maßnahmen sowie der Erstellung von Dateibeschreibungen, sagt das Gesetz nicht. Dieses Minimalprogramm machte es möglich, die Aufgaben des Datenschutzbeauftragten von vornherein stark einzuengen. In der Regel haben die öffentlichen Stellen von dieser Möglichkeit allerdings keinen Gebrauch gemacht. Sie sind statt dessen meinen weitergehenden Vorschlägen gefolgt, die im Interesse des Datenschutzes auf eine angemessene Aufgabenbeschreibung abzielen. Der bisherige einschränkende gesetzgeberische Ansatz ist mit der EU-Datenschutzrichtlinie nicht vereinbar. Sie verlangt eine wirksame, effektive Aufgabenwahrnehmung durch den behördeninternen Datenschutzbeauftragten.

Das Innenministerium geht auch hier wieder zaghaft vor. Der Gesetzentwurf bestimmt, dass der Datenschutzbeauftragte auf die Einhaltung der Datenschutzvorschriften hinwirken, Technikfolgenabschätzungen (Vorabprüfungen) durchführen und die Bediensteten über die Datenschutzerfordernisse zu unterrichten habe. Zur Stärkung des behördeninternen Beauftragten reicht dies allerdings nicht aus. Nach meiner Auffassung muss ihm zusätzlich die Aufgabe übertragen werden, die Anwendung der Datenverarbeitungsprogramme zu überwachen. Über Vorhaben der automatisierten Datenverarbeitung ist er zu unterrichten und zu ihnen anzuhören. Er sollte das Recht zur Akteneinsicht erhalten. Vor allem aber halte ich es für erforderlich, der öffentlichen Stelle die Verpflichtung aufzuerlegen, ihren Datenschutzbeauftragten zu unterstützen. Nur wenn dieser den nötigen Rückhalt seiner Behörde erhält, kann er seine Aufgaben auch gegen Widerstände wirkungsvoll wahrnehmen. In der Vergangenheit hat es vereinzelt Klagen von Datenschutzbeauftragten gegeben, die diese Unterstützung vermissten.

Zum Ausbau der Stellung des Datenschutzbeauftragten gehört auch, dass er mit den notwendigen räumlichen, personellen und sächlichen Mitteln ausgestattet wird und dass er – sofern er nicht ausschließlich in dieser Funktion tätig wird – im erforderlichen Umfang von seinen anderen Aufgaben freizu-

stellen ist. Die Richtlinie hebt hervor, dass der behördeninterne Beauftragte die Einhaltung der einschlägigen Rechtsvorschriften unabhängig zu überwachen hat. Dies bedeutet, dass er bei seiner Tätigkeit weisungsfrei sein muss. Es darf keine organisatorische Zuordnung erfolgen, die ihn an seiner Überwachungstätigkeit hindern könnte. Auch diese Weisungsfreiheit muss als zentraler Regelungspunkt der Richtlinie noch gesetzlich verankert werden.

5. Automatisierte Einzelentscheidungen

   Der Gesetzentwurf will der automatisierten Datenverarbeitung dort eine Grenze ziehen, wo Entscheidungen anstehen, die rechtliche Folgen für die betroffenen Bürgerinnen und Bürger haben oder diese erheblich beeinträchtigen. In einem solchen Fall darf die Entscheidung grundsätzlich nicht ausschließlich auf die automatisierte Datenverarbeitung gestützt, sie muss vielmehr von den handelnden Personen verantwortet werden. Eine vergleichbare Regelung besteht bisher schon für dienst- und arbeitsrechtliche Entscheidungen sowie Beurteilungen.

6. Datenübermittlungen ins Ausland

   Mit der Umsetzung der Richtlinie erfolgt eine Angleichung der Rechtsvorschriften der Mitgliedsstaaten der EU, die Grundlage für einen freien und ungehinderten Datenverkehr innerhalb der Gemeinschaft ist. Datenübermittlungen in EU-Staaten sind damit nach denselben Rechtsvorschriften zu beurteilen wie Übermittlungen innerhalb der Bundesrepublik Deutschland. Für die Übermittlung in Drittstaaten sollen die bisherigen Regelungen im Kern erhalten bleiben, die gleichwertige Datenschutzbestimmungen im jeweiligen Empfängerland fordern. Für den Fall, dass diese Voraussetzung nicht erfüllt ist, sind bestimmte Ausnahmen vorgesehen.

7. Widerspruchsrecht

   Die EU-Datenschutzrichtlinie räumt den Betroffenen ein Widerspruchsrecht gegen die Verarbeitung ihrer Daten ein, wenn dieser schutzwürdige Gründe, die sich aus einer besonderen Situation ergeben, entgegenstehen. Diese besonderen persönlichen Umstände sollen die verantwortliche Stelle unabhängig von der Rechtmäßigkeitsprüfung der beabsichtigten Datenverarbeitung veranlassen, eine zusätzliche Abwägung zwischen dem öffentlichen Interesse an der Datenverarbeitung und den vom Betroffenen vorgetragenen schutzwürdigen Belangen vorzunehmen. Ergibt die Abwägung, dass die schutzwürdigen Belange überwiegen, ist die Datenverarbeitung unzulässig. Das Widerspruchsrecht, das mit dem Rechtsbehelf der Verwaltungsgerichtsordnung nichts zu tun hat, entfällt allerdings dann, wenn ein Gesetz die Datenverarbeitung ausdrücklich vorsieht. In diesem Fall wird davon ausgegangen, dass der Gesetzgeber bei Schaffung der jeweiligen Rechtsvorschrift die notwendige Güterabwägung bereits vorgenommen hat.

8. Haftung

   Bisher kennt das NDSG eine verschuldensunabhängige Haftung nur bei automatisierter Datenverarbeitung. Diese Beschränkung wird entfallen. Künftig hat die verantwortliche öffentliche Stelle auch einen Schaden zu ersetzen, der durch eine rechtswidrige nichtautomatisierte Datenverarbeitung entsteht, bei der ein Verschulden aber nicht nachgewiesen werden kann. Von dieser Haftung kann sie sich entlasten, wenn sie nachweist, dass sie den Schaden stiftenden Umstand nicht zu vertreten hat.

7 Statistik

Volkszählung 2001

Es ist wieder so weit. Nach 1987 ist für das Jahr 2001 geplant, eine erneute Volkszählung durchzuführen. Dieses Vorhaben wird im Grundsatz von allen EU-Staaten getragen und soll europaweit durchgeführt werden. Ursprünglich war geplant, hierfür eine verbindliche EU-Verordnung zu erlassen. Unter anderem aufgrund deutscher Kritik ist man aber hiervon abgerückt; Grundlage ist nun eine von der europäischen Statistikbehörde EUROSTAT vorgelegte unverbindliche „Leitlinie für das gemeinschaftliche Programm der Volks- und Wohnungszählungen im Jahre 2001“.

Der Bund strebt einen Methodenwechsel weg von den bisher durchgeführten Primärerhebungen bei allen Einwohnern an. Favorisiert wird ein Verfahren, das vor allem vorhandene Datenbestände auswertet. Hierfür werden vor allem finanzielle Gründe angeführt; die Kosten einer traditionellen Erhebung würden wahrscheinlich mehr als zwei Milliarden DM betragen. Auch die großen Akzeptanzprobleme der letzten Volkszählung spielen bei diesen Überlegungen eine wichtige Rolle.

Da eine Volkszählung, gleichgültig wie sie durchgeführt wird, einen hohen rechtlichen, finanziellen und organisatorischen Aufwand bedeutet, müssen bereits heute die Weichen hierfür gestellt werden. Die statistischen Ämter des Bundes und der Länder haben sich daher im Jahre 1998 intensiv über der Volkszählung 2001 beraten. Sie haben sich auf zwei mögliche Modelle festgelegt, das „Bundesmodell“ und das „Ländermodell“. Die folgenden Schaubilder veranschaulichen diese Versionen.

Das vom Bund vorgeschlagene Bundesmodell stützt sich im wesentlichen auf drei Quellen, auf die Einwohner-Melderegister, die Erwerbstätigkeitsstatistiken (z. B. Beschäftigtendatei und Arbeitslosendatei der Bundesanstalt für Arbeit, Personalstandsstatistik) und detaillierte Angaben des Mikrozensus, der regelmäßig bei 1 % der Bevölkerung durchgeführt wird und ausführliche Informationen über Haushalte, Wohnungen und Gebäude sowie den Bildungsstand abfragt. Das Bundesmodell liefert, wenn auch mit gewissen Fehlerquoten, alle wichtigen Daten und befriedigt zum Beispiel die Wünsche der Europäischen Union. Abgesehen von den Statistikdaten aus den Melderegistern sind mit diesem Modell allerdings nur bedingt Angaben auf Kreis- oder Gemeindeebene möglich.

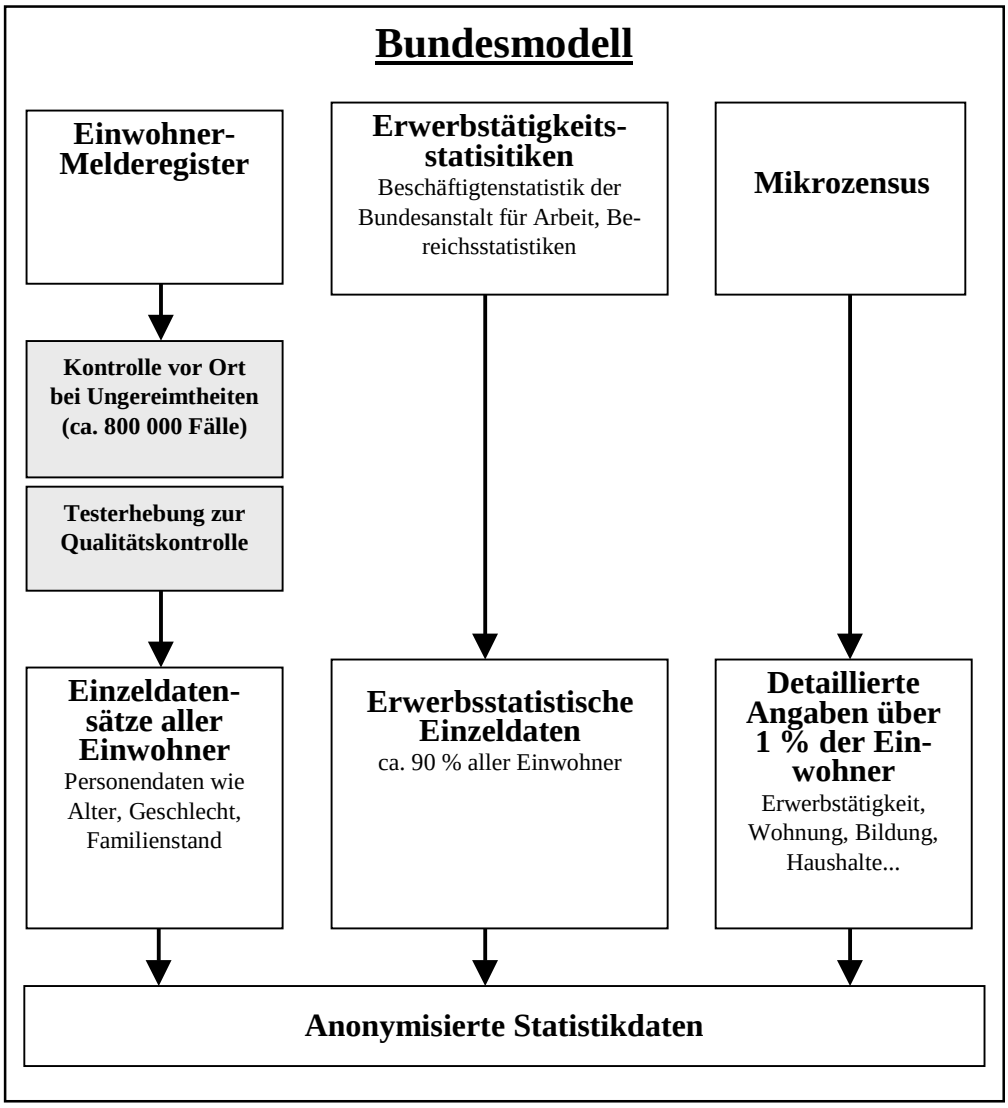


Abb. 1 Grobdarstellung des Volkszählungsablaufs beim Bundesmodell. Die dunklen Flächen deuten Direktbefragungen beim Betroffenen an.

Aus den Reihen der statistischen Landesämter kommt Kritik am Bundesmodell, da es nicht eine ausreichende, insbesondere regionale Tiefe ermöglicht. Die Arbeitsgruppe „Gemeinschaftsweiter Zensus 2001“, die sich aus den Amtsleitern der statistischen Ämter gebildet hat, favorisiert das Ländermodell, das im Ergebnis die gleichen Daten liefert wie eine herkömmliche Volkszählung. Wichtigster zusätzlicher Bestandteil des Ländermodells gegenüber dem Bundesmodell ist eine Gebäude- und Wohnungszählung, die als primärstatistische Erhebung postalisch oder bei Zweifelsfällen auch vor Ort geplant ist. Zusätzlich ist in diesem Modell eine Ergänzungsstichprobe im Erwerbsbereich geplant, da die vorhandenen Statistiken Lücken bei Selbständigen und geringfügig Beschäftigten aufweisen. Die Kosten des Ländermodells liegen nach ersten Schätzungen zwar deutlich unter denen einer herkömmlichen Volkszählung, sie wären aber ungefähr zehnmal so hoch wie bei einer Erhebung nach dem Bundesmodell.

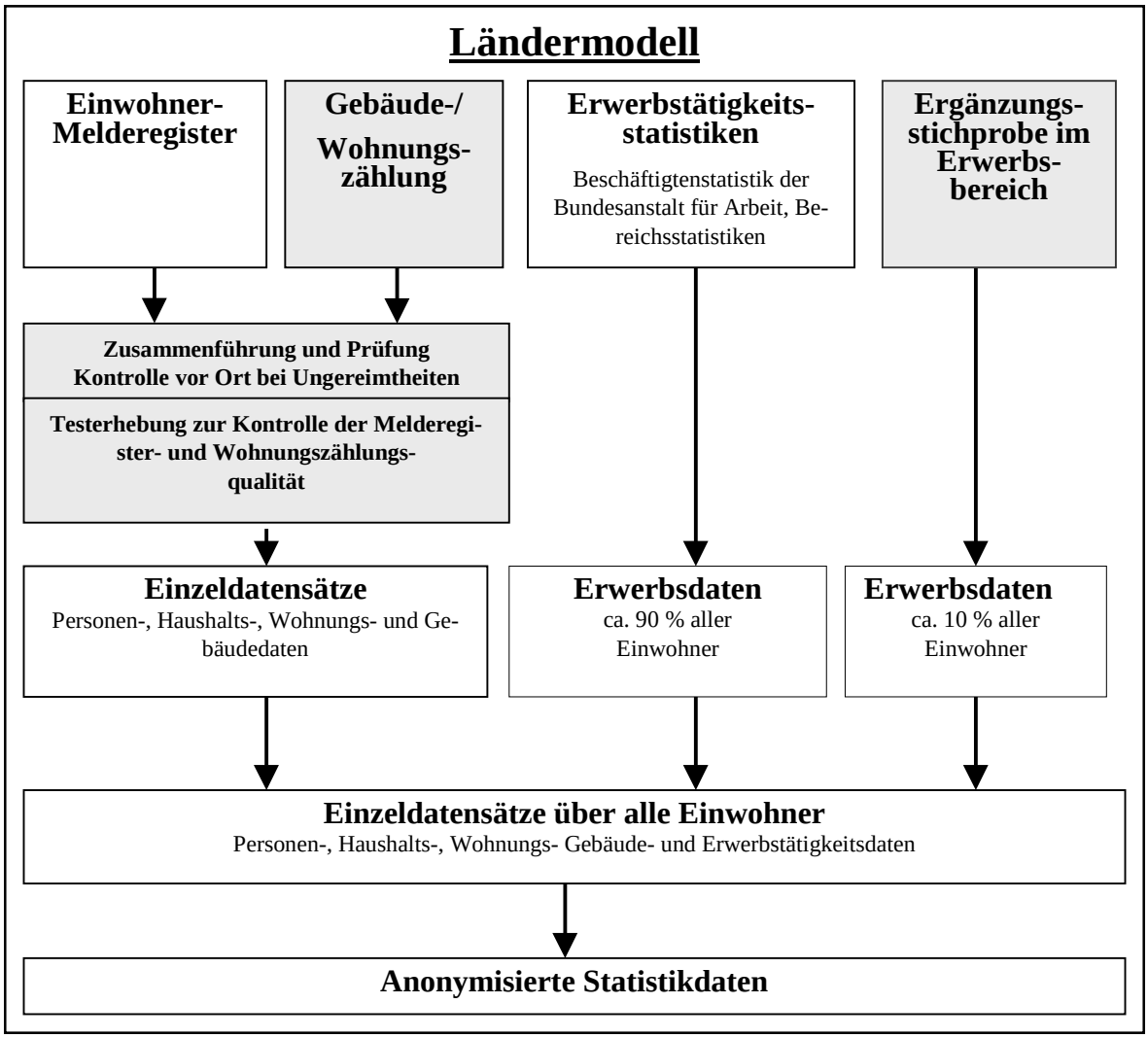


Abb. 2 Grobdarstellung des Volkszählungsablaufs beim Ländermodell. Die dunklen Flächen deuten Direkterhebungen beim Betroffenen an.

Ich habe mich frühzeitig mit den im Rahmen dieser Volkszählung auftretenden datenschutzrechtlichen Problemen auseinandergesetzt. Volkszählungen stellen nach wie vor einen bedeutenden Einschnitt in das Recht auf informationelle Selbstbestimmung dar. Dass dies auch heute noch von vielen Bürgerinnen und Bürgern so empfunden wird, zeigen die regelmäßig auftretenden Proteste, die im Rahmen der Mikrozensuserhebungen an mich herangetragen werden. Auch heute, mehr als fünfzehn Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts, sehen viele Menschen in dieser intimen Befragung, zu der sie gesetzlich verpflichtet werden, eine Drangsalierung durch den Staat. Bei der Planung der Volkszählung 2001 halte ich es daher für ganz besonders wichtig, die Erforderlichkeit dieser Erhebung genauestens zu prüfen und zu begründen. Wenn diese nicht eindeutig gegeben ist, sollte auf die Zählung vollständig verzichtet werden. Wenn sie unvermeidbar sein sollte, ist der geringstmögliche Eingriff in das Recht auf informationelle Selbstbestimmung zu wählen. Das Ländermodell stellt einen sehr weiten Eingriff dar, der einer herkömmlichen Volkszählung gleichkommt. Abgesehen davon, dass für jede Form von Volks-

zählung 2001 erst eine gesetzliche Grundlage geschaffen werden muss, hierüber sind sich alle Beteiligten einig, stehe ich insbesondere dem Ländermodell grundsätzlich skeptisch gegenüber. Eine genaue Bewertung bedarf allerdings noch weiterer Informationen und eingehender Untersuchungen.

Wichtigster Baustein der Modelle, insbesondere des Bundesmodells, ist das Einwohnermelderegister. Der Erfolg der Modelle ist mit der Qualität der Melderegister eng verknüpft. Es gibt daher bereits jetzt besondere Bemühungen, deren Qualität zu verbessern. Ursprünglich war beabsichtigt, die Melderegister um zusätzliche Angaben für statistische Zwecke zu erweitern. Hierbei ging es u. a. um Daten zur Schulbildung und zum Pendlerverhalten. Dieser Plan wurde aufgrund datenschutzrechtlicher Bedenken fallengelassen. Nach dem Volkszählungsurteil muss nämlich die Datenverarbeitung für statistische Zwecke von der Verarbeitung zu Verwaltungszwecken getrennt sein. Eine Übertragung statistischer Aufgaben auf die Meldeämter wäre im übrigen auch systemfremd. Aufgegeben nach datenschutzrechtlichen Einwänden wurde die weitere Absicht, nicht wahlberechtigten Inhabern von Nebenwohnungen bei der Bundestagswahl 1998 „negative Wahlbenachrichtigungen“ zuzusenden. Aus der Reaktion der Empfänger wollte man Anhaltspunkte für die Unrichtigkeit des Melderegisters gewinnen. Aus Sicht des Datenschutzes halte ich es für unvertretbar, Verdachtsschöpfungen „ins Blaue hinein“ unter dem Vorwand der Wahl ablaufen zu lassen. Der eigentliche Zweck der Aktion, die Registerbereinigung, sollte offenkundig gegenüber den Einwohnern verschleiert werden. Der Runderlass zur allgemeinen Verbesserung der Qualität der Melderegister wurde mittlerweile überarbeitet. Gegen die neue Fassung habe ich keine Einwände mehr.

Ich werde die Überlegungen und Planungen zur Durchführung einer Volkszählung 2001 auch weiter intensiv begleiten, datenschutzrechtlich bewerten und ggf. auf Missstände hinweisen. Ich bin zuversichtlich, dass aufgrund dieser Begleitung und aufgrund der vorhandenen Sensibilität bei der Durchführung von Volkszählungen ein Verfahren gefunden wird, dass das Recht auf informationelle Selbstbestimmung angemessen berücksichtigt.

8 Neue Medien

8.1 Neues Recht für Tele- und Mediendienste

Am 1. August 1997 ist das neue Tele- und Mediendiensterecht in Kraft getreten. Auch wenn die Datenschutzbeauftragten des Bundes und der Länder intensiv mitgearbeitet haben und um Klarheit bemüht waren, ist die richtige rechtliche Einordnung von Technik und Diensten für Nichtfachleute schwierig geblieben. Am anschaulichsten lässt sich die juristische Bewertung von Telekommunikationsvorgängen an einem Modell übereinander lagernder Regelungsschichten erklären.

Das rechtliche Fundament für Tele- und Mediendienste bildet das Telekommunikationsgesetz (TKG). Es regelt die technischen Vorgänge des Aussendens, Übermittelns und Empfangens von Nachrichten. Es beschäftigt sich nicht mit dem Inhalt der Information, sondern regelt den technischen Betrieb der Telekommunikation. Die technische Ebene der Netze wird überlagert von der Diensteebene, die die unterschiedlichen Kommunikationsformen ermöglicht. Auf dieser Ebene werden mit Hilfe bestimmter Festlegungen (Protokolle) die einzelnen Kommunikationsarten definiert, Verantwortlichkeiten und Pflichten der Diensteanbieter sowie Rechte der Nutzer bestimmt.

Für die individuelle Nutzung solcher Dienste, die der Bundeskompetenz unterliegen, wurden mit dem Informations- und Kommunikationsdienste-Gesetz (IuKDG) drei Gesetze neu geschaffen:

– das Teledienstegesetz (TDG), das einheitliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste schafft,

– das Teledienstedatenschutzgesetz (TDDSG), das die Datenschutzvorschriften für den Betrieb von Telediensten enthält, und

– das Signaturgesetz (SiG), das Rahmenbedingungen für die digitale Signatur vorgibt.

Unter das IuKDG fallen Individual-Dienste wie z. B. der Internet-Zugang, die elektronische Post, unmoderierte Chatrooms, das Telebanking, elektronische Buchungssysteme, Telespiele, Abrufdienste und auch elektronische Verwaltungsdienstleistungen. Elektronische Dienste, die sich an die Allgemeinheit richten, fallen unter das Medienrecht. Dazu gehören Dienste wie video on demand, Verteildienste mit redaktioneller Gestaltung, Fernsehtext/Radiotext, Push-Dienste, aber auch eigene, gestaltete Homepages mit Informationen von Behörden und Unternehmen. Diese Dienste fallen unter den Mediendienste-Staatsvertrag (MDStV). Dienste, die darüber hinaus den Rundfunkbegriff erfüllen, werden von den Bestimmungen des Rundfunkstaatsvertrags erfasst, z. B. pay per channel, pay per view, near video on demand.

Für den Inhalt der Kommunikation „in Multimedia“ gelten die Datenschutzregelungen, die auch außerhalb der Telekommunikation anzuwenden sind und die vielfach als das sogenannte „Offline-Recht“ bezeichnet werden. In Frage kommen das Bundesdatenschutzgesetz, die Landesdatenschutzgesetze und spezielles Datenschutzrecht sowie das Vertragsrecht, das Presserecht oder das Urheberrecht. Die Zuordnung zu den drei Schichten ist nicht immer logisch und eindeutig. Vielmehr gibt es eine Reihe von Unschärfen und Überlappungen. So stellt z. B. die Sprachtelefonie eigentlich einen Teledienst dar, gleichwohl wird sie im TKG geregelt, das darüber hinaus sogar noch Bestimmungen zur Inhaltsebene enthält (§§ 85, 86, 89 Abs. 4 TKG). Die Datenschutzbeauftragten haben in ihrem Kooperationskreis „IuK-Datenschutz“ einen Katalog aller denkbaren Dienste erstellt, der das jeweils materiell geltende Datenschutzrecht und die Datenschutz-Kontrollzuständigkeit zuordnet. Bis auf wenige Ausnahmen konnte Übereinstimmung aller Kontrollinstanzen erzielt werden. Der langwierige und schwierige Abstimmungsprozess hat jedoch noch einmal verdeutlicht, wie mühsam es für Diensteanbieter und Benutzer sein muss, selbständig die richtige Einordnung zu finden. Es ist deshalb lobend hervorzuheben, dass Bund und Länder in einem pragmatischen Kompromiß versucht haben, die Datenschutzvorschriften der unterschiedlichen Regelungswerke weitgehend anzupassen. Der Vorteil der weitestgehend gleichlautenden Datenschutzregelungen besteht darin, daß die Anbieter der Dienste in der Praxis nicht entscheiden müssen, welcher Art ihr Dienst ist und welches Regelungswerk zur Anwendung kommt.

Das neue Tele- und Medienrecht sieht folgende Pflichten für Diensteanbieter vor:

– Werden Daten über Multimedia-Nutzer erhoben, so sind sie zuvor zu unterrichten.

– Es muß sichergestellt werden, dass sich der Nutzer zu jeder Zeit aus dem Tele- und Mediendienst ausklinken und die Verbindung abbrechen kann.

– Der Nutzer hat das Recht, jederzeit seine personenbezogenen Daten unentgeltlich beim Diensteanbieter einzusehen, auf Verlangen auch elektronisch.

– Daten der Nutzer dürfen ausschließlich zweckgebunden verwendet werden. Es ist verboten, Tele- und Mediendienste von einer Einwilligung des Nutzers in die Verarbeitung seiner Daten für andere Zwecke abhängig zu machen.

- Die Dienste sind von vorherein so zu gestalten, dass keine oder so wenig wie möglich personenbezogene Daten erhoben und verarbeitet werden (Datenvermeidung).
- „Soweit dies technisch möglich und zumutbar ist“, müssen Tele- und Mediendienste so abgerechnet werden, dass der Nutzer anonym oder unter Pseudonym auftreten kann.
- Informationen über die Inanspruchnahme verschiedener Dienste dürfen nicht zusammengeführt und zu einem Persönlichkeitsprofil verdichtet werden.
- Es muß ausgeschlossen werden, dass Dritte personenbezogene Daten über die Inanspruchnahme von Diensten zur Kenntnis nehmen.

Es wird jetzt darauf ankommen, die neuen Bestimmungen des Tele- und Mediendiensterechts allgemein bekannt zu machen und mit Leben zu füllen. Die Datenschutzbeauftragten haben sich mehrfach in Beschlüssen und Ausarbeitungen an Diensteanbieter, Netzbetreiber und Endgerätehersteller gewandt, um datenschutzfreundliche Technologien einzufordern (vgl. 8.3). Vor allem muss es Nutzern ermöglicht werden, Angebote anonym oder unter Pseudonym in Anspruch zu nehmen und zu bezahlen. Damit könnte technisch verhindert werden, dass persönliche Nutzerprofile über Kommunikations-, Seh- und Abrufgewohnheiten entstehen und missbraucht werden. Weitere Informationen über den Datenschutz bei Multimedia, Empfehlungen zum gesicherten Einsatz von E-Mail sowie Hinweise zum gesicherten Internet-Anschluss sind in meinem Internet-Angebot nachzulesen.

8.2 Telekommunikationsrecht muss verbessert werden

Der Rat der Europäischen Union hat am 1. Dezember 1997 die „Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation“ (früher: ISDN-Richtlinie) angenommen. Die Richtlinie ergänzt die allgemeine Datenschutzrichtlinie und schreibt einen europaweiten Mindeststandard beim Datenschutz in der Telekommunikation vor. Die Anpassungsfrist endete zeitgleich mit der Frist für die allgemeine Datenschutzrichtlinie am 24. Oktober 1998. Doch bisher sind Anpassungen des Telekommunikationsgesetzes und der Telekommunikationsdiensteunternehmen-Datenschutzverordnung (TDSV) nicht erkennbar. Vielmehr gelten die alten Datenschutzvorschriften unverändert fort. Hinzu gekommen ist seit Anfang 1998 nur die Telekommunikations-Kundenschutzverordnung, die auch einige datenschutzrechtliche Regelungen enthält.

Die derzeit geltende TDSV basiert noch auf einer Ermächtigungsgrundlage aus dem Post- und Telekommunikationsregulierungsgesetz (PTRegG), das im Rahmen der Postreform II 1994 erlassen worden war. Die TDSV ist damit dringend novellierungsbedürftig. Es ist zu hoffen, dass der Gesetzgeber seine „Schularbeiten“ bald macht und dabei gleich eine Anpassung an die datenschutzfreundlichen Regelungen des TDDSG und des MDStV vornimmt. So sollten der Grundsatz der Datensparsamkeit normiert, anonyme oder zumindest pseudonyme Nutzungsmöglichkeiten geschaffen und die Wahlmöglichkeiten der Telefonkunden beim Einzelverbindungsnachweis des Diensteanbieters nach holländischem Vorbild verbessert werden.

8.3 Datenschutzfreundliche Technologien in der Telekommunikation

Telekommunikationsdienste werden bisher fast ausschliesslich unter Verfügbarkeits-, Performance- und Sicherheitsaspekten der Betreiber konzipiert. Das Recht der Bürgerinnen und Bürger auf vertrauliche Kommunikation wird allenfalls in Randbereichen berücksichtigt, meist jedoch als Restriktion diskreditiert. Die Aspekte der Datenvermeidung, der Pseudonymisierung und der Anonymisierung haben bis heute keine besondere Bedeutung bei der Konzeption und der Ausprägung der TK-Netze erlangt. Dabei sind die Techniken und Verfahren zur Datenverminderung und Datenvermeidung bereits seit längerer Zeit bekannt und erforscht.

Die zunehmende Bedeutung der Telekommunikation im täglichen Leben und der gesetzlich normierte Grundsatz der Datenvermeidung zwingen dazu, das Recht der Nutzenden auf unbeobachtbare, gesicherte Telekommunikation heute stärker in den Mittelpunkt der Entwicklung und Gestaltung von Telekommunikationsnetzen und -diensten zu stellen. Im Endgerätebereich sind die Voraussetzungen für eine breite Einführung von Prepaid Chipkarten sicherlich am leichtesten umzusetzen. Diese Technik ist geeignet, Verbindungs-, Bestands- und Entgeltdaten weitgehend zu vermeiden bzw. zumindest zu reduzieren. Allen Nutzerinnen und Nutzern von TK-Netzen sollte die Möglichkeit der anonymen Entgeltzahlung wahlweise angeboten werden. Über bestehende Möglichkeiten zur Datenvermeidung und Datenreduzierung sollte die Öffentlichkeit stets aktuell informiert werden.

Will man die gesamte Kommunikation zwischen Sender und Empfänger schützen, so wären die derzeitigen Netzstrukturen mehr oder weniger stark zu modifizieren. Im Dialog mit den Herstellern und Betreibern von TK-Netzen sowie den wissenschaftlichen Forschungsgemeinschaften und -instituten sollte die Einbringung datenvermeidender und anonymisierender Technologien in zukünftige Netze weiter erörtert werden. Unter Berücksichtigung des Ziels, die unbeobachtbare, gesicherte Kommunikation zu erreichen, erscheinen auch der technische Aufwand und die teilweise noch notwendige Entwicklungsarbeit hierzu gerechtfertigt.

Eine konsequente Umsetzung der Forderungen zur Datenvermeidung und -reduktion scheint im Widerspruch zu bestehenden gesetzlichen Regelungen zu stehen. So werden z. B. nach § 90 Abs. 1 TKG Telekommunikationsdiensteunternehmen, die geschäftsmässig Telekommunikationsdienste anbieten, verpflichtet, Kundendateien zu führen, in denen Namen und Anschrift enthalten sind, um diese den Sicherheitsbehörden, Gerichten, Staatsanwaltschaft und Regulierungsbehörden auf Abruf zur Verfügung zu stellen. Könnte auf Bestandsdaten verzichtet werden, liefe diese Regelung ins Leere. Ebenso wären bei vollständig unbeobachtbarer TK-Nutzung keinerlei Überwachungsmaßnahmen mehr möglich (§ 100 a StPO/§ 88 TKG). Betreiber von Mobilkommunikationsnetzen sind zwar wegen der Verschlüsselung des Funkverkehrs in der Mobilkommunikation verpflichtet, eine Entschlüsselungsschnittstelle zu schaffen, um Polizei und Geheimdiensten eine Überwachung zu ermöglichen. Doch sind sich Experten einig, dass dies wirkungslos ist, da es Umgehungsmöglichkeiten der Überwachung durch mehrfache Verschlüsselung gibt. Diese Beispiele verdeutlichen, dass es Interessenskonflikte zwischen den Sicherheits- und Überwachungsbedürfnissen des Staates und dem Schutz der persönlichen Daten der Einzelnen und damit dem Schutz des Rechts auf informationelle Selbstbestimmung gibt.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Kriterien für datenschutzfreundliche Technik in der Telekommunikation definiert. In einem 50-seitigen Arbeitspapier "Datenschutz in der Telekommunikation" werden die bei verschiedenen TK-Diensten anfallenden personenbezogenen Daten beschrie-

ben und Hilfen bei der Bewertung von neuen Telekommunikationslösungen gegeben. Die Untersuchung belegt, dass datenschutzfreundliche Technologien auf dem Gebiet der Telekommunikation heute bereits zur Verfügung stehen, und fordert zur Anwendung auf.

Die Untersuchung, an der ich intensiv mitgearbeitet habe, ist primär als Orientierungshilfe für Entscheidungsträger, für Datenschutzbeauftragte in Wirtschaft und Verwaltung sowie als Information für eine interessierte Öffentlichkeit gedacht. Die Datenschutzbeauftragten des Bundes und der Länder wenden sich mit dieser Untersuchung auch an Hersteller von Telekommunikationsanlagen, an Netzbetreiber sowie an TK-Diensteanbieter und fordern sie auf, möglichst anonyme oder zumindest datensparsame Lösungen zu entwicklen und bereitzustellen.

Auf Einladung der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen haben die Autoren mit Herstellern von Telekommunikationsanlagen und mit Telekommunikationsanbietern über deren Vorstellungen und Absichten diskutiert. Dabei hat sich gezeigt, dass alle aufgezeigten Lösungsvorschläge realisierbar sind. Der Weg für eine datenschutzfreundliche TK-Technologie scheint damit geebnet.

8.4 Datenschutzaufsicht bei Tele- und Mediendiensteanbietern

Die Datenschutzaufsicht nach IuKDG und MDStV ist mir als Aufsichtsbehörde für die Wirtschaft übertragen worden. Sie ist als Regelaufsicht gestaltet und erfolgt somit routinemässig. Die Aufsicht kann daher auch durchgeführt werden, wenn keine Anhaltspunkte für eine Verletzung von Datenschutzvorschriften bestehen. Ich verstehe meine Rolle jedoch nicht so sehr als die eines Kontrolleurs, sondern mehr als die eines „Dienstleisters“ der öffentlichen Verwaltung und der Wirtschaft. Mein Interesse ist nicht darauf gerichtet, mit Berichten über Datenschutzskandale in Presse, Funk und Fernsehen zu erscheinen. Vielmehr ist mir daran gelegen, durch frühzeitige Beratung Datenschutzverstöße zu vermeiden.

Mit der Verabschiedung der Gesetze wollte der Gesetzgeber gerade in dieser Wachstumsbranche geeignete rechtliche Rahmenbedingungen für die marktwirtschaftliche Entwicklung schaffen. Zugleich sollte den mit dem Verbreiten der Technologien wachsenden Gefahren für das mit Verfassungsrang ausgestattete Recht auf informationelle Selbstbestimmung Rechnung getragen werden.

Um mir einen Überblick über die meiner Aufsicht unterstehenden Unternehmen im Tele- und Mediendienstebereich zu verschaffen, habe ich die meiner Kontrolle unterliegenden Internet-Provider angeschrieben und über die neuen datenschutzrechtlichen Bestimmungen im Tele- und Mediendiensterecht unterrichtet. Mit der Bitte um Zusammenarbeit habe ich einen Fragenkatalog aller Datenschutzaspekte beigefügt, den ich zusammen mit den Allgemeinen Geschäftsbedingungen zurückerbeten habe. Ich beabsichtige, nach Auswertung aller Fragen eine Orientierungshilfe zu erstellen, die Diensteanbieter in die Lage versetzt, angemessene Datensicherungskonzepte zu entwickeln und zu betreiben.

9 Ausweis- und Melderecht

9.1 Einsichtnahme von Polizei und Ordnungswidrigkeitenbehörden in das Personalausweis- bzw. Passregister

Mit der Einsichtnahme der Polizei bzw. der Ordnungswidrigkeitenbehörde in das Personalausweis- oder Passregister wird in das Recht auf informationelle Selbstbestimmung der Betroffenen eingegriffen (vgl. XII 11.2). Ich erhalte nach

wie vor zahlreiche Eingaben von Betroffenen zur Nutzung der Register für Zwecke der Verfolgung von Verkehrsordnungswidrigkeiten (Abgleich des Lichtbildes mit Frontfotos). Dies und auch viele Anfragen von Ausweisbehörden veranlassten mich, dem Niedersächsischen Innenministerium klarstellende Hinweise in den Verwaltungsvorschriften zu empfehlen. Leider ist das Niedersächsische Innenministerium meiner Anregung nicht gefolgt. Aus Sicht des Datenschutzes ebenfalls bedauerlich ist, dass das Innenministerium seine bisherige Auffassung zur Beschränkung der Einsichtnahme auf nicht geringfügige Verkehrsordnungswidrigkeiten aufgegeben hat.

Anfragende Ausweisbehörden äußern oft Zweifel, ob die Ordnungswidrigkeitenbehörden das im Personalausweisgesetz und im Paßgesetz vorgesehene datenschutzrechtliche Prinzip beachten, die Daten grundsätzlich beim Betroffenen zu erheben. Ausnahmen von dem Grundsatz sind nur zugelassen, wenn die Datenerhebung bei dem Betroffenen nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Unverhältnismäßig ist der Aufwand dann, wenn er in keinem vernünftigen Verhältnis zum angestrebten Erfolg steht. Wenn sich Anforderungen von Lichtbildern durch einzelne Ordnungswidrigkeitenbehörden außergewöhnlich häufen, könnte der Eindruck einer gesetzlich nicht vorgesehenen Nutzung der Register als Auskunftei entstehen.

In letzter Zeit hat sich eine neue Variante ergeben. Mehrere Ausweisbehörden legten mir Einsichtsverlangen von Ordnungswidrigkeitenbehörden vor, die sich nicht nur auf den Halter des Fahrzeuges, sondern z. B. auch auf die namentlich nicht benannten weiblichen nahen Verwandten und andere weibliche Personen, die mit in einem Haushalt leben, bzw. auf den Ehemann oder Lebensgefährten beziehen. Eine derartige Kombination von Auskünften aus dem Melderegister und dem Personalausweisregister ist auch nach Auffassung des Niedersächsischen Innenministeriums nicht zulässig. Ob die Daten bei den Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können, kann nur geprüft werden, wenn die Person der ersuchenden Stelle namentlich bekannt ist. Es muss daher zunächst der Betroffene ermittelt und die Datenerhebung bei ihm versucht werden, bevor eine Kopie des Lichtbildes angefordert werden darf.

9.2 Änderung des Niedersächsischen Meldegesetzes

Das Niedersächsische Meldegesetz (NMG) wurde in einigen Bestimmungen geändert. Im Wesentlichen geht es um die Anpassung an bundesrechtliche Vorgaben im Melderechtsrahmengesetz (vgl. XIII 10.1). Aus Sicht des Datenschutzes ist über zwei positive Neuerungen zu berichten. Die Einrichtung oder Verlängerung einer Auskunftssperre ist nunmehr kostenfrei. So müssen z. B. Zeugen, die aufgrund ihrer belastenden Aussage in wichtigen Strafprozessen späteren Repressalien ausgesetzt sein könnten und sich deswegen vor einer Weitergabe ihrer Meldedaten an Dritte durch eine Auskunftssperre schützen, für die Sperre kein Geld mehr bezahlen. Des Weiteren konnten sich bisher z. B. Geheimdienste unter bestimmten Voraussetzungen von Krankenhäusern und Heimen das Verzeichnis über aufgenommene Patienten zuschicken lassen. Die geänderte Vorschrift lässt dieses Verfahren nicht mehr zu. Erlaubt ist nun nur noch eine auf den Einzelfall bezogene Auskunft des Krankenhauses. Die Neufassung des NMG wurde 1998 bekannt gemacht (Nds. GVBl. S. 57).

9.3 Rasterfahndung nach Rundfunkgebühren

Das Niedersächsische Meldegesetz (NMG) wurde ergänzt, um Schwarzhörer und –seher aufzuspüren. Eine neue Vorschrift verpflichtet die Meldebehörden, dem NDR bzw. der GEZ monatlich alle volljährigen Einwohner zu nennen, die

sich an- oder abgemeldet haben oder gestorben sind (vgl. § 34 a NMG – Regelmäßige Datenübermittlung an den Norddeutschen Rundfunk). Gemeldet werden folgende Daten: Familienname; Vornamen, unter Bezeichnung des Rufnamens; frühere Namen; Tag der Geburt; gegenwärtige, frühere und zukünftige Anschriften, Haupt- und Nebenwohnungen; Tag des Ein- und Auszugs; Familienstand, beschränkt auf die Angabe, ob verheiratet oder nicht; Sterbetag. Diese Angaben werden dann bei der GEZ mit den vorhandenen Gebührenkonten abgeglichen, um festzustellen, welche Meldepflichtigen kein Gebührenkonto haben – also in der Logik dieses Vorgehens Schwarzhörer sind. Die Gebührenkonten der Verstorbenen werden gelöscht.

Bei unbefangener Betrachtung wird man Verständnis für das Anliegen des NDR haben, Schwarzhörer zur Kasse zu bitten. Wenn ein flächendeckender Abgleich eingeführt wird, dann muss es Schwarzhörer in einer beträchtlichen Größenordnung geben. Öffentlich-rechtliche Rundfunkanstalten haben ja nicht nur einen Anspruch auf funktionsgerechte Finanzierung. Sie sind auch gehalten, Gebührengerechtigkeit herzustellen. Und doch bleibt angesichts der Massenhaftigkeit des Datentransfers ein gewisses Unbehagen zurück.

Die Skepsis ist nur allzu berechtigt. Die Gleichsetzung, jeder Meldepflichtige sei auch Gebührenschuldner, trifft nicht zu. Zudem stimmt das suggerierte Ergebnis nicht, das Verfahren zwinge jetzt alle zum Bezahlen.

Zunächst einige Fakten zur Situation. Wer sich ein Radio oder einen Fernseher kauft, weiß, dass er Rundfunkgebühren zahlen muss. Viele kommen der Zahlungspflicht auch nach. Die auf Haushalte bezogene Anmeldequote liegt bei 86 %, nach manchen Quellen liegt sie noch darüber. Eine wie ich meine sehr hohe Bereitschaft, die öffentlich-rechtlichen Rundfunkanstalten mitzufinanzieren, wenn man bedenkt, dass wegen des anonymen Kaufs niemand die tatsächlichen Verhältnisse kennt. Weiter zu berücksichtigen sind 7 % von der Gebührenpflicht Befreite und etwa 3 %, die gar kein Gerät besitzen. Mithin verbleiben ca. 4 % der Haushalte mit Schwarzhörern. Nach diesen – öffentlichen – Zahlen kann keine Rede davon sein, alle Meldepflichtigen seien Gebührenschuldner. Das Übermittlungsverfahren betrifft somit Menschen, die zwar meldepflichtig sind, sich aber offensichtlich ganz überwiegend gebührenmäßig korrekt verhalten. Die Funktion der regelmäßigen Datenübermittlung an die GEZ ist hiernach erkennbar eine Ausforschung, verbunden mit der Hoffnung, über eine Erfassung aller Meldepflichtigen vielleicht auf Schwarzhörer zu stoßen. Ein solches Verfahren kann ich aus Sicht des Datenschutzes nicht als verhältnismäßig bezeichnen.

Wird bei der GEZ durch einen Abgleich festgestellt, dass Meldepflichtige noch kein Gebührenkonto haben, so bedingt das Verfahren, sie für potentielle Schwarzhörer zu halten. Dieser Kreis erhält dann freundliche Aufforderungsschreiben, ggf. vorhandene Geräte anzumelden. Nach Erfahrungen aus anderen Bundesländern melden ca. 1/5 der Angeschriebenen daraufhin Geräte an. Erfolgt auch nach einem zweiten Schreiben keine Rückäußerung, dann passiert nichts mehr.

Wenn es – wie eingangs beschrieben – ca. 4 % Haushalte mit Schwarzhörern geben soll und der positive Rücklauf ca. 1/5 der Angeschriebenen ausmacht, dann bewirkt das massenhafte Abgleichverfahren eine zusätzliche Erfassung von 0,8 %.

9.4 Unmut über Datenverkäufe an Adressbuchverlage, Parteien u. a.

„Wie kommt meine Anschrift ohne meine Zustimmung ins Adressbuch? Ich bin damit überhaupt nicht einverstanden. Ich hatte doch gar nichts unterschrieben." „Kann die Verwaltung mit Daten, die der Bürger abgeben muss, machen was sie will? Eigentlich müsste es doch so sein, dass erst ein Einverständnis eingeholt und dann veröffentlicht wird". – Um die Jahreswende 1986/87 verschickte die CSU vor der Bundestagswahl 1 300 000 Wahlwerbebriefe an Rentner und Jungwähler. Die Kosten sollen 1 Million DM betragen haben. In der jüngeren Zeit war in den Zeitungen nachzulesen, wie DVU und NPD gezielt Briefkasten-Wahlkampf vor den Wahlen in Sachsen-Anhalt und Mecklenburg-Vorpommern betrieben.

Die Zitate aus an mich gerichteten Beschwerden belegen Unmut und Empörung. Nachdenklichkeit kommt auf, wenn man sieht, wie leicht offenbar der Zugang zu Daten über Menschen ist. Ein Weg ist im Melderecht verankert. Nach § 34 des Niedersächsischen Meldegesetzes (NMG) dürfen Meldeämter den Adressbuchverlagen, Parteien, parlamentarischen und kommunalen Mandatsträgern, der Presse und dem Rundfunk Angaben auf Anforderung überlassen. Es handelt sich immer um Vor- und Familiennamen, Doktorgrad und Anschriften. Sind Mandatsträger, Presse und Rundfunk Datenempfänger, so erhalten sie noch zusätzliche Informationen über Alters- und Ehejubiläen, nämlich Tag und Art des Jubiläums. Parteien bekommen die Auskünfte sechs Monate vor einem Wahltermin; der Auskunftsinhalt ist beschränkt auf nach dem Lebensalter bestimmte Gruppen. Die eingangs dargestellten Aktivitäten der Parteien sind also auch bei uns völlig legal. Adressbuchverlage müssen in Niedersachsen für jeden Datensatz über einen Menschen zwischen 4 und 40 Pfennig Gebühren bezahlen.

Die Privilegierung bestimmter gesellschaftlicher Gruppen bei der Beschaffung von Daten fällt auf. Aus Sicht des Datenschutzes ist das fehlende Einverständnis (Einwilligung) der Betroffenen vor den Datenübermittlungen zu kritisieren. Diese Position hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder noch einmal bekräftigt (vgl. Anlage 15). Das Meldegesetz räumt den Betroffenen lediglich ein Widerspruchsrecht ein. Diese Möglichkeit ist weithin unbekannt. Nach meinen praktischen Erfahrungen erreicht die Information über das Widerspruchsrecht die Menschen nicht. Zu der gleichen Feststellung kam auch der Bundesrat im Rahmen einer Änderung des Melderechtsrahmengesetzes des Bundes. Eine konsequente Umsetzung des Grundrechts auf informationelle Selbstbestimmung im Sinne von „Erst fragen – dann handeln" kann ich daher nicht sehen.

Das Niedersächsische Innenministerium sah keinen Anlaß, die bisherige Rechtslage zu ändern. Der Niedersächsische Landtag hat meine Empfehlung, derartige Datenübermittlungen von einer Einwilligung abhängig zu machen, bei der Änderung des NMG mit Mehrheit abgelehnt.

9.5 Übermittlung von Aussiedlerdaten an Parteien vor Wahlen

Nach Schilderung mehrerer niedersächsischer Meldebehörden war vor der Bundestagswahl das Interesse der politischen Parteien an den Daten der Aussiedler groß. Eine Partei beklagte sich bei mir über die Weigerung einer Meldebehörde, die Daten der dortigen Aussiedler zu übermitteln. Ich habe die Meldebehörden in ihrer ablehnenden Haltung unterstützt.

Nach § 34 Abs. 1 des Niedersächsischen Meldegesetzes (NMG) darf die Meldebehörde den politischen Parteien im Zusammenhang mit Wahlen Auskunft aus dem Melderegister über Wahlberechtigte erteilen. Dabei muss es sich jedoch um Gruppen von Wahlberechtigten handeln, die nach dem Lebensalter bestimmt

sind. Einziges Auswahlkriterium ist also das Lebensalter. Die begehrte Auskunft über Aussiedler ist nach dieser Vorschrift somit nicht zulässig. Da es sich bei dieser Vorschrift um eine spezielle Regelung für die Erteilung von Gruppenauskünften im Zusammenhang mit Wahlen handelt, ist eine Anwendung der allgemeinen Vorschrift über die Erteilung von Gruppenauskünften in diesem Fall ausgeschlossen. Zudem wäre auch die Kennzeichnung von Aussiedlern im Melderegister nicht zulässig. Der Inhalt des Melderegisters ist im NMG abschließend geregelt. Das Datum „Aussiedler“ ist dort nicht aufgeführt.

9.6 Gruppenauskunft über Haushaltsvorstände ab 45 Jahren

Eine niedersächsische Gemeinde hatte einem Verein Namen und Anschriften von Haushaltsvorständen ab 45 Jahren für Einladungen zu einer Informationsveranstaltung übermittelt, bei der das Gesamtkonzept eines geplanten Neubauprojektes für seniorenfreundliches Wohnen vorgestellt werden sollte. Ein Betroffener wunderte sich zunächst, woher der Verein seine Daten hatte, und ging der Sache auf den Grund. Er war empört über die Weitergabe seiner Daten, die er dem Einwohnermeldeamt angeben müsse.

Die Datenübermittlung aus dem Melderegister an den Verein war unzulässig. Sogenannte Gruppenauskünfte über eine Vielzahl nicht namentlich bezeichneter Personen dürfen nur erteilt werden, soweit sie im öffentlichen Interesse liegen. Für die Zusammensetzung der Personengruppe dürfen die im Gesetz genannten Daten (Geburtstag, Geschlecht, Staatsangehörigkeiten, Anschriften, Tag des Ein- und Auszugs, verheiratet oder nicht, Ehefrau/Ehemann, Kind, gesetzlicher Vertreter) herangezogen werden. Das Merkmal Haushaltsvorstand gehört nicht zu diesen Daten. Im übrigen ist eine Speicherung dieser Angabe im Melderegister auch nicht vorgesehen und somit unzulässig. Nach welchen Kriterien die Gemeinde den Haushaltsvorstand der einzelnen Familien bestimmt hat, ist mir nicht bekannt.

Ob ein öffentliches Interesse besteht, hängt von den konkreten Zwecken ab, denen die Gruppenauskunft dienen soll, sowie von der beabsichtigten Art der Verwendung der Daten. Ausgeschlossen ist die Erteilung einer Gruppenauskunft, wenn der verfolgte Zweck zwar im öffentlichen Interesse liegt, aber auf andere Weise ohne Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen erreicht werden kann. Selbst wenn die Einladung zu der Informationsveranstaltung im öffentlichen Interesse liegen sollte, wäre die Erteilung der Gruppenauskunft unzulässig, weil der Zweck z. B. durch öffentliche Aufrufe, Zeitungsanzeigen oder Postwurfsendungen ohne Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen hätte erreicht werden können.

10 Polizei

10.1 Tausche Freiheit gegen Sicherheit

„Der Staat muss doch in der Lage sein, zur Bewahrung der inneren Sicherheit Eingriffe in Freiheitsrechte vorzunehmen“. Solche und ähnliche Sätze sind zu hören, wenn es um die Erweiterung von Handlungsmöglichkeiten für Sicherheitsbehörden geht.

Private Risikovorsorge

Sicherheit ist ein schillernder Begriff. Wir alle streben danach und meinen damit familiäre, berufliche, finanzielle Sicherheit. Um finanzielle Risiken im Alter zu vermeiden, schließen manche eine Lebensversicherung ab. Bei Fälligkeit löst der Versicherer sein Leistungsversprechen ein und zahlt, und der Versiche-

rungsnehmer freut sich über das zusätzliche Geld. Das Risiko ist abgewendet, über zu wenig Mittel im Alter zu verfügen. Die Lebenserfahrung zeigt allerdings, dass eine Vermeidung von Risiken nur sehr begrenzt möglich ist. So schützen Ausbildung und erlernter Beruf leider nicht vor Arbeitslosigkeit. Selbst wenn die private Risikovorsorge klappt, hat sie zuweilen auch unangenehme Seiten. Eine Alarmanlage z. B. bietet Schutz vor Einbrechern. Doch derjenige, der sich in Sicherheit bringen will, schließt nicht nur andere aus, er schließt auch sich selber ein. Trotzdem: Private Risikovorsorge tut Not und ist gut.

Staatliche Risikovorsorge: Politik der „Inneren Sicherheit“

Fraglich ist, ob staatliche Risikovorsorge zur Herstellung von Sicherheit durch Sicherheitsbehörden ähnlich positiv zu sehen ist. Auch hier treten Nebenwirkungen ein, die es zu bedenken gilt. Nach dem Grundgesetz gibt es weder „die“ Staatsaufgabe Sicherheit noch ein Grundrecht auf Sicherheit. Die Brücke zu vorsorgenden Aktivitäten der Sicherheitsbehörden heißt „Innere Sicherheit“.

Das Programm hierfür wurde in den innen- und außenpolitisch unruhigen 70er Jahren entwickelt. Ziel war es, die freiheitlich demokratische Grundordnung des Staates, seinen Bestand sowie den Einzelnen vor Verbrechen zu schützen. Gefordert wurde die ständige Bereitschaft aller Sicherheitsbehörden, Störungen jenseits der Normallage abzuwenden. In jener Zeit schuf man ein Pendant zur „Äußeren Sicherheit“. Wesentlicher Inhalt des Programms war ein Methodenwechsel. Angesagt war nun ein operatives, vorsorgliches Vorgehen. Nicht mehr Reaktionen auf eingetretene Störungen waren im Blick, sondern aktive Vorfeldoperationen zur Vermeidung von Störungen. Innenpolitisch suggerierte das Programm das Versprechen, für umfassenden Schutz vor unterschiedlichsten Gefahren, Straftaten, extremistischen Bestrebungen und terroristischen Anschlägen zu sorgen. Die Vielschichtigkeit des Begriffs „Sicherheit“ wurde verkürzt auf Kriminalität. Zwischen Kriminalität und Sicherheit wird ein kausaler Zusammenhang behauptet, mit der Botschaft, durch mehr sicherheitsbehördliche Befugnisse weniger Kriminalität und damit Sicherheit herzustellen.

In den Folgejahren ging die Umsetzung des Programms nur schleppend voran. Ein richtiger, auch öffentlichkeitswirksamer Schub kam erst mit der Einführung des Begriffs „Organisierte Kriminalität (OK)“. Seine rechtliche Bedeutung ist zwar nach wie vor diffus. Offenkundig hat die kurze Bezeichnung aber die zu Zeiten der Wende aufkommende Unsicherheit in der Bevölkerung hervorragend aufgenommen. Diese Unsicherheit spiegelt sich in Umfragen zur Angst vor Kriminalität wider. Sie belegen eine immer stärkere Furcht vor Kriminalität, obwohl eine persönliche Betroffenheit nicht vorliegt. Das subjektive Sicherheitsgefühl hinkt den objektiven Zahlen hinterher. Die Erklärungsversuche dafür verweisen auf den Zusammenhang zwischen Kriminalitätsangst und allgemeiner Lebensangst. Zukunftsängste sollen erheblich zugenommen haben. „Risikogesellschaft“, „Globalisierung“ und „Standort Deutschland“ werden sehr persönlich erfahren als Verlust des Arbeitsplatzes, an Einkommen und Sozialabbau. Auch glaubt jeder angesichts entsprechender Informationen in den Medien über Kriminalität und Gegenkonzepte Bescheid zu wissen. So sind nach einer Studie 16 % aller Deutschland betreffenden Beiträge in den Hauptnachrichtensendungen von ARD, ZDF, RTL, SAT 1 und Pro Sieben solche über die innere Sicherheit. Die Darstellung über kriminelle Täter und sicherheitspolitische Konzepte erfolgte – mit Ausnahme zum „Großen Lauschangriff“ – nicht kontrovers. Zudem haben unentwegte Hinweise aus der Politik dafür gesorgt zu meinen, der Staat sei der „OK“ tendenziell unterlegen. Daher müsse nach weiteren Möglichkeiten zur adäquaten Bekämpfung gesucht werden. Über die gesellschaftlichen Ursachen für Kriminalität und Unsicherheit ist nach meiner Beobachtung in der Öffentlichkeit kaum noch nachgedacht worden. Das Kürzel „OK“ wurde der

Schlüssel für den weithin akzeptierten Ausbau von Kompetenzen der Sicherheitsbehörden.

„Leistungsbilanz“ der sicherheitsbehördlichen Risikovorsorge

Die Politik der inneren Sicherheit hatte in den letzten Jahren Hochkonjunktur. Der Türöffner „OK“ wurde bei der Befugniserweiterung zu Gunsten der Sicherheitsbehörden teilweise ausdrücklich genannt, teilweise war er Motiv. Diese Politik kann – was die geänderten Gesetze und Entwicklungen betrifft – eine Erfolgsbilanz aufweisen. Eine Liste:

1991
- Das Bundesamt für Verfassungsschutz (BfV) schlägt vor, seinen Aufgabenbereich auf „Organisierte Kriminalität“ auszudehnen.

1992
- Strafverfolgungsbehörden erhalten die Erlaubnis zur
  – Rasterfahndung und
  – polizeilichen Beobachtung (sie ermöglicht bundesweite Bewegungsbilder).
  Beide Methoden wurden in den 70er Jahren zur Terrorismusfahndung entwickelt. Gesetzlich zugelassen wurden auch der Einsatz
  – Verdeckter Ermittler und
  – technischer Mittel zur akustistischen und optischen Überwachung außerhalb von Wohnungen.
- Das Zollkriminalamt (Bundesbehörde) darf bereits vor dem Anfangsverdacht einer Straftat (sog. Vorfeld) Telefongespräche abhören.
- Das BfV tritt erneut mit Vorschlägen an die Öffentlichkeit:
  – Erweiterung seiner Kompetenzen, etwa bei der Bekämpfung der Organisierten Kriminalität
  – Umbenennung in „Bundessicherheitsamt“.

1994
- Die niedersächsische Polizei erhält mit Ausnahme von Rasterfahndung und Verdeckten Ermittlern die Befugnis, Vorfeldaufklärung zu betreiben, z. B.
  – in bestimmten Fällen Wohnung akustisch und optisch zu überwachen (sog. polizeilicher Lausch- und Spähangriff)
  – Einführung der niedersächsischen Variante der Schleierfahndung.
- Einbeziehung des Bundesnachrichtendienstes (BND) in die Bekämpfung der Organisierten Kriminalität. Ihm wird erlaubt, den internationalen Fernmeldeverkehr über Funkstrecken ohne konkreten Strafverdacht abzuhören und auszuwerten (Strategische „Rasterfahndung“).
- Der Bundesgrenzschutz (BGS) erhält Vorfeldkompetenzen und wird ermächtigt, das BfV funktechnisch zu unterstützen.
- Der bayerische Verfassungsschutz erhält die Aufgabe „Bekämpfung der Organisierten Kriminalität“.

1995
- Erweiterung der polizeilichen Beobachtung auf alle Schengen-Staaten (von Skandinavien bis Spanien)

1996
- Private Telekommunikationsanbieter werden verpflichtet, den Sicherheitsbehörden einen Online-Zugriff auf die Kundendaten zu ermöglichen; die Ausgestaltung muss so erfolgen, dass selbst die Anbieter den Abruf nicht bemerken.
- Die infolge der Digitalisierung vollständig aufgezeichneten Verbindungsdaten konnten schon vorher in „strafgerichtliche Verfahren“ verwendet werden.

1997
- Das BKA erhält umfassende Kompetenzen für Vorsorgedateien.
- Private Telekommunikationsanbieter werden zusätzlich verpflichtet, den Sicherheitsbehörden
  – das Abhören zu ermöglichen,
  – Verbindungs- und Bestandsdaten zur Verfügung zu stellen.

1998
- Dem BGS werden verdachtsunabhängige Kontrollen in Zügen und auf Flughäfen und Bahnanlagen erlaubt.
- Die niedersächsische Polizei erhält zusätzliche Vorfeldbefugnisse:
  – Wohnungen können im Vorfeld schneller abgehört und ausgespäht werden.
  – Erlaubt wird der Einsatz von Verdeckten Ermittlern.
- Strafverfolgungsbehörden erhalten die Befugnis zum „Großen Lauschangriff“ in Wohnungen.
- EUROPOL darf europaweit Vorsorgedateien einrichten.
- Es wird bekannt, dass allein die Zahl der Telefonüberwachungsanordnungen sich im Zeitraum von 1990 bis 1997 mehr als verdreifacht hat – von 2 494 auf 7776.

Wirkungen: Sicherheitsraum Deutschland

Wie steht es nun mit der Einlösung des Versprechens, innere Sicherheit herzustellen? Wie sicher ist sicher? Die zugespitzte Fragestellung macht deutlich, dass es keine befriedigende Antwort geben kann. Im Gegensatz zum eingangs genannten Beispiel der Risikoabwendung einer finanziellen Notlage durch Altersvorsorge fehlt es bei der Risikovorsorge durch innere Sicherheit schon an einer klaren Bestimmung dessen, was „Innere Sicherheit“ ist. Nach meiner Beobachtung scheint es jedenfalls mannigfache Auslegungsmöglichkeiten zu geben, die bei den Parteien noch durch die jeweilige Rolle – Regierung oder Opposition – geprägt sind.

Sicher sind hingegen andere Feststellungen. Prävention durch innere Sicherheit legitimierte zu Vorsorgeregeln, nach denen Sicherheitsbehörden flächendeckend private und öffentliche Räume überwachen können, und zwar heimlich. Wir leben gleichsam in einem Sicherheitsraum. Private Gespräche, Telefonate und Verhaltensweisen, die der Staat nicht belauschen oder beobachten könnte, sind nahezu unmöglich. Jeder kann als potentielles Risiko betrachtet werden. Zur konkreten Umsetzung des Programms der ständigen Bereitschaft aller Sicherheitsbehörden, Störungen jenseits der „Normallage“ abzuwenden, wurden zudem umfassende Datentransfers erlaubt und umfängliche Datensammlungen zur Vorsorge aufgebaut.

Eine Kontrolle der Vorsorgeaktivitäten ist nur schwerlich möglich. Die Kompetenzen eingerichteter parlamentarischer Kontrollgremien beziehen sich auf den jeweiligen gesetzlich bestimmten Einzelbereich; der Gesamtkomplex bleibt au-

ßen vor. Fachaufsichtsinstanzen werden unter dem Stichwort „Weg mit der Mißtrauensverwaltung“ ausgedünnt. Prüfungen der Datenschutzbeauftragten können angesichts der knappen personellen Ressourcen allenfalls den Charakter von Stichproben haben; sie beschränken sich zudem auf die Datenverarbeitung. Nachdenkliche Stimmen zum Ausbau der Vorfeldbefugnisse aus der Praxis bleiben in der Minderheit. So hält der Polizeiabteilungsleiter im Kieler Innenministerium die klassischen Eingriffsbefugnisse für ausreichend, 95 % aller polizeilichen Tätigkeiten abzuarbeiten. Er bezweifelt die Effektivität der seit 1992 neu eingeführten Befugnisse und plädiert für eine intelligente Polizeiarbeit ohne neue Grundrechtseingriffe, die den Grundkonsens rechtsstaatlicher Polizeiarbeit berühren. Diejenigen, die sich kritisch zum Ausbau der sicherheitsbehördlichen Befugnisse äußern oder nicht richtig mitziehen, erhalten eine Außenseiterrolle zugewiesen. Datenschützer werden Verhinderer, rechtsstaatliche Arbeitsweisen der Gerichte und Staatsanwaltschaften veranlassen Verbandsfunktionäre der Polizei, Richter und Staatsanwälte eine „ Gefahr für die innere Sicherheit“ zu nennen.

Vor allem aber stellt man bei einer Beschäftigung mit dem Thema immer wieder fest, dass eine seriöse Aussage zur Richtigkeit des eingeschlagenen Weges wegen mangelnder Informationen nicht möglich ist. Es fehlt an einer nachhaltigen Erfolgskontrolle. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deswegen die Überprüfung der Erforderlichkeit und Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien angemahnt (vgl. XIII 11.4 und Anlage 16).

Die „Innere Sicherheit“ scheint trotz aller Gesetzgebungsaktivitäten noch nicht hergestellt zu sein. Anders kann ich mir die Forderungen nach weiteren Eingriffsmethoden nicht erklären. Der „Große Lauschangriff“ – gerade eingeführt und kaum praktiziert – reicht nicht. Gefordert wird bereits die heimliche Video-Überwachung von Wohnungen. Eigentlich bleibt nur noch das „Restrisiko“ Mensch. Methoden zur Erkennung seiner Bausteine werden bereits erforscht. Insgesamt entwickeln sich die Dinge wie eine Spirale.

Zeit zum Besinnen

Es würde zu kurz greifen, Gefährdungen privater Räume ausschließlich beim Staat zu suchen. Umfassende Datenverarbeitung findet erst recht im privaten Bereich statt, und private Software-Firmen legen weltweit Regeln für die Kommunikation und die Zugänge fest. Jedoch bleibt festzuhalten, dass viele geneigt sind, vom Staat Sicherheit zu verlangen. Die Politik der „Inneren Sicherheit“ mit ihrer besonderen Ausprägung staatlicher Risikovorsorge zu Lasten von Freiheitsräumen erfährt weite Akzeptanz. Damit wird der Staat – wie es ein ehemaliger Kollege von mir ausdrückte – gleichsam zum Vater, der Schutz und Sicherheit verspricht, aber diese Erwartung gar nicht einlösen kann. Wer aber alles veranworten muss, der muss zumindest alles wissen, können und dürfen.

Die Hauptaufgabe des Datenschutzes liegt darin, die Würde und Persönlichkeit des Menschen in einer sich entwickelnden Informationsgesellschaft zu erhalten. Wer Datenschutz als opferbares Luxusgut betrachtet, verkennt wesentliche Funktionen des Grundrechts auf informationelle Selbstbestimmung: die informationelle Teilhabe am öffentlichen Leben und den Versuch, das private Leben von informationeller Überwältigung freizuhalten. Unsere freiheitliche Demokratie ist nicht auf Waffengleichheit mit Verbrechern angelegt. Nach dem Grundgesetz haben wir keinen Sicherheits-, sondern einen Freiheitsstaat. Kennzeichnend für einen solchen Staat ist nicht Allwissenheit, sondern die bewußte Beschränkung der Informationsherrschaft. Trotz vielfältiger technischer Möglichkeiten plädiere ich daher für die Bereitschaft, gegebenenfalls die Risiken un-

vollständiger Information zu akzeptieren, also auch den Informationsverzicht – so schwer es auch fallen mag – auszuhalten.

Der Preis für die Politik der „Inneren Sicherheit“ ist hoch. Der zu Beginn dieses Beitrages genannte Satz kann auch anders formuliert werden: „Der Staat zerstört Freiheitsrechte, wenn er sie den Bürgern nimmt“.

10.2 Abbau von Bürgerrechten im Niedersächsischen Gefahrenabwehrgesetz

Der Niedersächsisches Landtag hat am 12. November 1997 wesentliche Änderungen des Niedersächsischen Gefahrenabwehrgesetzes (NGefAG) beschlossen. Die Änderungen sind seit dem 6. Februar 1998 in Kraft. Angesichts der Vielzahl der Neuregelungen erfolgte im März 1998 eine Bekanntmachung der Neufassung des NGefAG (Nds. GVBl. S. 101).

Erklärtes Ziel der Novellierung war die Deregulierung und Entbürokratisierung des Datenschutzes unter Zugrundelegung praktischer Erfahrungen. Stattdessen werden zunächst erst einmal neue Vorfeldbefugnisse für heimliche Maßnahmen installiert. Sie sind zugleich verbunden mit einem Rückbau parlamentarischer Kontrollmöglichkeiten.

Die Zulässigkeit des heimlichen Abhörens von Wohnungen bereits vor dem Anfangsverdacht auf eine Straftat ist massiv erweitert worden. Zulässig ist nunmehr das Lauschen in Wohnungen auch zur Abwehr der Gefahr, jemand könne eine Straftat von erheblicher Bedeutung – Staatsschutzdelikte sind ausgenommen – begehen (vgl. § 35 Abs. 2 Nr. 2 NGefAG). Sachliche und praktische Gründe für die Notwendigkeit dieser Ausweitung wurden nicht vorgetragen. Anlass war allein der Wille, die zum Zeitpunkt der Beratungen noch in Planung befindliche Neufassung des Art. 13 GG auszuschöpfen. Die Offenheit der neuen Befugnis – und nur darauf kommt es mir hier an – ist frappierend. Es genügt, wenn sich zwei Jugendliche zusammentun, um Fahrräder zu stehlen.

Neu ist die Erlaubnis, Verdeckte Ermittler einsetzen zu dürfen (vgl. § 36 a NGefAG). Bisher war dies nur in Verfahren nach der Strafprozessordnung möglich. Verdeckte Ermittler sind Polizeibeamte, die unter einer auf Dauer angelegten falschen Identität in die Szene gehen. Sie sollen die Frühentstehungsphase bei Straftaten von erheblicher Bedeutung ergründen. Mit dieser neuen Befugnis macht das Gesetz für mich einen nicht mehr vertretbaren Riesenschritt in Richtung Geheimpolizei. Schwere bis nicht mehr lösbare Konflikte sind vorprogrammiert; die nachträgliche Kontrolle eines Geschehnisablaufs halte ich für kaum möglich. Denn wenn jemand auftragsgemäß in eine Szene eintaucht, dann wird sein bestimmendes Umfeld die „Gegenseite“. Will er nicht Außenseiter bleiben, dann muß er sich als zugehörig darstellen und verhalten. Es dürfte eine Verharmlosung sein anzunehmen, ein Verdeckter Ermittler müsse sich nur in Kleidung, Sprache und Gestik dem Milieu anpassen.

Gestrichen wurde zudem die Berichtspflicht der Landesregierung gegenüber dem Landtag zu Entwicklungen polizeilicher Vorfeldaktivitäten, insbesondere bei Kontrollstellen und beim Einsatz aller besonderen Mittel. Die Berichte waren öffentlich zugänglich. Dieses parlamentarische Überprüfungsinstrument war darauf angelegt, den Gesamtkomplex Vorfeldeingriffe zu erfassen und – soweit erforderlich – rechtzeitig gesetzgeberische Konsequenzen zu ziehen. Nunmehr gibt es einen Ausschuss zur Kontrolle besonderer polizeilicher Datenerhebungen (vgl. § 37 a NGefAG). In nicht-öffentlicher Sitzung nimmt der Ausschuss Unterichtungen des Innenministeriums entgegen. Unterrichtungsgegenstand sind nur noch Informationen über den Einsatz von vier besonderen Mitteln der Polizei, nämlich längerfristige Observation, technischer Mitteleinsatz, Verdeckter Ermittler und Kontrollmeldungen (vgl. auch 10.6).

Weggefallen sind etwa 2/3 aller Bestimmungen, die Grundrechtsschutz durch Verfahren sichern sollen, wie z. B. externe Anordnungskompetenzen (Richtervorbehalte) bei bestimmten besonderen Mitteln und die Unterrichtung Betroffener nach verdeckten Datenerhebungen. Richtervorbehalte sind umstritten. Für mich erfüllen externe Anordnungskompetenzen aber eine wichtige Funktion, weil sie das Defizit ausgleichen können, vor Grundrechtseingriffen nicht angehört zu werden. Die Vorbehalte sind also eine „korrigierende“ Gewährleistung dafür, dass mögliche Interessen vorher nicht gehörter Betroffener aus neutraler Sicht gewichtet werden. Das in der Begründung zum Gesetzentwurf genannte Argument, die Richtervorbehalte im NGefAG würden einen erheblichen Aufwand bei Polizei und Justiz bewirken, kann ich beim besten Willen nicht nachvollziehen. Bekannt war, dass im Zeitraum von Juni 1994 bis Mai 1997 38 richterliche Anordnungen erfolgten, also landesweit pro Monat etwa ein Verfahren stattfand. Gestrichen wurde auch die bisherige Unterrichtung Betroffener nach verdeckten Datenerhebungen. Nach heimlichen Datenerhebungen ist eine Unterrichtung Betroffener eigentlich eine Selbstverständlichkeit. Nur so erfährt ein Betroffener etwas über einen gegen ihn durchgeführten Grundrechtseingriff und kann sich überlegen, ob er gegebenenfalls Rechtsschutz in Anspruch nehmen will. Den mit der Unterrichtung verbundenen Rechtsschutz-Initiativeffekt hatte der Sächsische Verfassungsgerichtshof in seiner Entscheidung vom 14. Mai 1996 zum Sächsischen Polizeigesetz noch besonders betont. Die Begründung zum Gesetzentwurf enthält keine Hinweise zum tatsächlichen Aufwand für Unterrichtungen.

Bisher vorgesehene kurze Löschungsfristen für Daten Unbeteiligter gibt es nicht mehr. Folge der Deregulierung ist eine Vorschrift, die Speichermöglichkeiten für Daten Dritter nicht nur erweitert, sondern auch ermöglicht, nicht mehr erforderliche Angaben weiterhin aufzubewahren und verwenden zu können (vgl. § 38 Abs. 1 Satz 4 NGefAG). Erweitert wurde auch die Befugnis zur Kriminalaktenhaltung. Entgegen dem früheren Recht können nunmehr zur Person geführte Datensammlungen auch über Kinder angelegt werden, da das Gesetz nur noch auf die Begehung rechtswidriger Taten abstellt (vgl. §§ 39 Abs. 3, 2 Nr. 9 NGefAG). Ich hatte in meinem letzten Tätigkeitsbericht über solche Kinderakten berichtet (vgl. XIII 11.6.2). Meine Empfehlung lautete, über differenzierte Lösungen nachzudenken. Das Gesetz sieht jetzt eine pauschale Ermächtigung zur Aktenanlegung vor. Eine Differenzierung erfolgte auf der Ebene der Verwaltungsvorschriften. Nach der Kriminalakten-Richtlinie dürfen keine Akten über Kinder unter sieben Jahren angelegt werden. Zwischen 7 und 12 Jahren kann es eine Kriminalakte dann geben, wenn eine Beteiligung des Kindes an banden- oder gewerbsmäßigen Straftaten vorliegt oder das Kind im Einzelfall eine kriminelle Energie gezeigt hat, die weit über den altersgemäßen Rahmen hinausgeht. Die Aufzählung weiterer „verschlankter“ Vorschriften im NGefAG ließe sich fortsetzen.

Aus meiner Sicht erfolgte unter dem Deckmantel der Deregulierung schlicht ein Ausbau polizeilicher Befugnisse. Zugleich werden Schutzrechte Betroffener bzw. der Datenschutzstandard insgesamt deutlich abgesenkt. Bisher habe ich das NGefAG für einen weitgehend gelungenen Ausgleich zwischen staatlichen Eingriffsmöglichkeiten und datenschutzrechtlichen Sicherungen gehalten. Dieser Meinung bin ich nicht mehr. Ich habe auch Zweifel, ob die im Gesetz gepflegte hohe Schule abstrakter Formulierungen verbunden mit einer teilweisen neuen Systematik der richtige Weg ist, Anwendern und Betroffenen Klarheit über das Erlaubte zu geben. Ich bedauere diese Entwicklung. Die zum Teil komplizierten neuen Vorschriften waren aus meiner Sicht nicht erforderlich.

10.3 Die Wahrheit steht in der Zeitung – Über den diskreten Charme des Niedersächsischen Gefahrenabwehrgesetzes

Die Länder Bayern und Baden-Württemberg führten 1995 bzw. 1996 die Schleierfahndung ein. Damit sollte auf den Wegfall der Kontrollen an den Außengrenzen aufgrund des Schengener Abkommens reagiert werden. Die Länder hofften, durch diese neue Art von Polizeikontrollen besser gegen grenzüberschreitende Kriminalität vorgehen zu können. Die öffentliche Kritik an der Schleierfahndung war heftig und ging in Richtung Süden.

Viele erinnerten sich an das – über das Schengener Abkommen ja auch umgesetzte – Politikversprechen über ein Europa ohne Grenzkontrollen. Nun zeigte sich der Preis, der für den Abbau der Grenzkontrollen zu bezahlen war. Anstelle der Kontrollen an den Grenzen gab es nun Kontrollen im Land – die Schleierfahndung. Sie ist verdachts- und ereignisfrei zulässig. Die bisherige Voraussetzung für polizeiliches Handeln, das Vorliegen einer konkreten schadensstiftenden Situation, wurde fallen gelassen. Der Grundsatz, der Staat lässt den Bürger in Ruhe, wenn gegen ihn kein konkreter Verdacht besteht, war nur noch Historie. Jeder konnte nun in den beiden Ländern festgehalten und überprüft werden, ohne dass irgendetwas gegen ihn vorliegen musste. Die Schleierfahndung ist damit eine präventive Kontrolle mit dem Ziel, im Einzelfall erst zu prüfen, ob sich ein konkreter Verdacht begründen lässt. Aus Sicht des Datenschutzes begegnet das neue Prinzip „Jeder ist verdächtig“ schwerwiegenden Bedenken, weil kein konkreter Anlass für die Erhebung persönlicher Daten vorliegt.

Als im März 1998 Bundesinnenminister Kanther die bundesweite Einführung der Schleierfahndung forderte, konnten sich um den Rechtsstaat besorgte Niedersachsen entspannt zurücklehnen. Die Entwarnung kam vom Niedersächsischen Innenminister. Er verkenne nicht die Probleme grenzüberschreitender Kriminalität. Verdachtsunabhängige Personenkontrollen leisteten aber nur wenig im Kampf gegen die organisierte Kriminalität, würden jedoch einen nicht unerheblichen Grundrechtseingriff für eine Vielzahl von Bürgern bedeuten. Diese Meinung hörte ich als Datenschützer zwar gern, war allerdings auch ein wenig überrascht. Andere, die sich mit aus ihrer Sicht guten Gründen für den Weg der inneren Sicherheit entschieden hatten, waren eher beunruhigt. Versagt Niedersachsen im Kampf gegen die organisierte Kriminalität?

Wie so häufig kann ein Blick in das Gesetz Klarheit schaffen. Still und kaum wahrgenommen, fast klammheimlich, hatte Niedersachsen schon 1994 vor Bayern und Baden-Württemberg das Niedersächsische Gefahrenabwehrgesetz (NGefAG) ergänzt. Ein kleiner Absatz ermöglichte der Polizei, just solche verdachtslosen Kontrollen flächendeckend durchzuführen mit dem Ziel, Vermögensverschiebungen in das Ausland zu verhindern (vgl. § 12 Abs. 6 NGefAG i.d.F. der Bekanntmachung vom 14. April 1994, Nds. GVBl. S. 172). Das Ziel der Kontrollen wurde bei der jüngsten Änderung des Gesetzes noch umfassender formuliert. Nunmehr geht es um die Vorsorge für die Verfolgung oder Verhütung von Straftaten von erheblicher Bedeutung mit internationalem Bezug (vgl. § 12 Abs. 6 NGefAG i.d.F. der Bekanntmachung vom 20. Februar 1998, Nds. GVBl. S. 101).

Fazit: Niedersachsen war längst Spitze beim Abbau eines rechtsstaatlichen Grundsatzes, nur stand es nicht in der Zeitung.

10.4 Neukonzeption der INPOL-Datenbank

Die Polizei im Bund und in den Ländern setzt zur Unterstützung ihrer vollzugspolizeilichen Aufgaben das Informationssystem INPOL ein. Der Datenbestand von INPOL rekrutiert sich im wesentlichen aus den Daten der Landespolizeisysteme. Der zentrale Rechner für das INPOL-System steht im Bundeskriminalamt (BKA). Die INPOL-Daten stehen bundesweit den Polizeidienststellen in zahlreichen, nach unterschiedlichen Fachgebieten aufgebauten Dateien im online-Zugriff zur Verfügung.

Niedersachsen hatte die Regeln für die Anlieferung der Daten an das BKA im Niedersächsischen Gefahrenabwehrgesetz von 1994 festgelegt. Nunmehr gibt es auch gesetzliche Grundlagen für die Datenverarbeitung beim BKA. Das Gesetz über das Bundeskriminalamt ist seit dem 1. August 1997 in Kraft (BGBl. I 1997, S. 1650). Ich hatte über datenschutzrechtliche Aspekte und Auswirkungen auf das Bund-Länder-Verhältnis im Rahmen der Entstehungsgeschichte des Gesetzes berichtet (vgl. zuletzt XIII 11.3.2).

Das aktuelle INPOL-System stammt noch aus den siebziger Jahren. Es gilt in seiner polizeifachlichen und technischen Konzeption als veraltet. Aus diesem Grund wird z. Z. mit Hochdruck an einer Neukonzeption gearbeitet. „INPOL-neu“ soll im Gegensatz zum aktuellen Verfahren ein integriertes System mit einem einzigen Datenpool darstellen, in dem Mehrfacherfassungen und Recherchen in verschiedenen Datenbanken unnötig werden. Im Idealfall sollen direkt von der automatisierten Vorgangsbearbeitung in den Polizeidienststellen Daten in das Bundessystem übertragen und von dort abgerufen werden. Natürlich soll alles auch schneller, schöner und bedienungsfreundlicher werden. Um dieses ehrgeizige Vorhaben zu verwirklichen, ist der Aufbau einer modernen IuK-Infrastruktur mit UNIX-Rechnern und einer relationalen Datenbank geplant, die eine hohe Systemverfügbarkeit und Skalierbarkeit zulässt. Auch das neue zentrale INPOL-System wird im Bundeskriminalamt eingerichtet und betreut. Die Länder werden über eine einheitliche Schnittstelle mit der eigenen IuK-Technik auf das Bundessystem zugreifen. Für INPOL-neu werden z. Z. Feinkonzepte entwickelt und erste Tests durchgeführt. Projektabschluss und Systemeinführung sollen bis zum 1. Januar 2000 erfolgen.

Die fachliche und technische Neukonzeption von INPOL wirft viele Fragen auf, die den Datenschutz und die Datensicherheit sowohl auf Bundes- als auch auf Landesebene betreffen. Werden durch die Bildung eines Datenpools Zugriffe zugelassen, die über das bisherige Maß hinausgehen? Entstehen mit dem neuen System Verknüpfungen, bei denen z. B. Zeugen- und Täterdaten nicht mehr ausreichend unterscheidbar sind? Wird der Datenumfang insgesamt in unzulässiger Weise erweitert? Werden die datenschutzrechtlichen Vorgaben der Länder ausreichend berücksichtigt? Werden geeignete Sicherungsmaßnahmen gegen unberechtigte Zugriffe von Externen getroffen? Können Polizeibeamte aufgrund des Sicherungskonzeptes nur die Daten einsehen oder verändern, auf die sie aufgrund ihres Berechtigungsprofils Zugriff haben sollen?

Um diese und viele andere Fragen zu beantworten und das Projekt datenschutzrechtlich zu begleiten, haben die Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe gebildet. Auch ich nehme an dieser Arbeitsgruppe teil. Anfänglich war deren Arbeit mit einigen Irritationen verbunden, da das Bundesministerium des Innern (BMI) und die Leitung des BKA die Arbeitsgruppe nicht als Ansprechpartner für die datenschutzrechtliche Begleitung akzeptieren wollten, sondern nur dem Bundesbeauftragten für den Datenschutz diese Kompetenz zuerkannten. Die Arbeitsgruppe war daher auf die Informationen und Aktivitäten des Bundesbeauftragten angewiesen, was zu einigen

Schwierigkeiten und Verzögerungen geführt hat. Mittlerweile ist die Zusammenarbeit mit BKA und BMI aber als gut zu bezeichnen.

Die Arbeitsgruppe hat u. a. durch die Erörterung eines umfangreichen Fragenkatalogs auf die Datenschutzprobleme und -risiken bei der Neugestaltung von INPOL hingewiesen. Zu manchen Punkten zeichnen sich Entscheidungen ab, die von den Datenschutzbeauftragten begrüßt und mitgetragen werden. Hierzu gehört, dass eine Rechteverwaltung aufgebaut werden soll, um die Zugriffsrechte auf das erforderliche Maß zu beschränken. Die Berechtigungsvergabe soll allerdings im wesentlichen nicht von INPOL vorgenommen werden, sondern muss auf Landesebene realisiert werden. Ebenfalls erfreulich ist, dass sämtliche Daten bei der Übertragung zwischen der INPOL-Zentrale beim BKA und den Ländern verschlüsselt werden sollen.

Zu anderen Punkten, etwa zu den zahlreichen Erweiterungen im Datenbestand, zu den Fragen der Protokollierung oder dem anzuwendenden Recht bei Verbunddateien, sind noch Erörterungen erforderlich, um eine einvernehmliche Lösung zu finden. Bei vielen weiteren Punkten aber, etwa zum „erweiterten Besitzerprinzip“, zur Einführung einer „Alertfunktion“ oder zur genauen Ausgestaltung einer Sicherheitskonzeption, bestehen selbst in den INPOL-neu-Projektgruppen noch keine klaren Vorstellungen.

10.5 EUROPOL – Immunität für Polizisten?

Der Deutsche Bundestag hat dem EUROPOL-Übereinkommen zugestimmt (vgl. EUROPOL-Gesetz, BGBl. II 1997, S. 2150). Bei der angegebenen Fundstelle ist auch das Übereinkommen abgedruckt. Es ist am 1. Oktober 1998 in Kraft getreten. Ich hatte mich kritisch mit den nunmehr zulässigen Datenverarbeitungsmöglichkeiten auseinandergesetzt (vgl. XIII 11.3).

Die öffentliche Diskussion der letzten beiden Jahre befasste sich u. a. mit der Immunität der EUROPOL-Mitarbeiter. Hierdurch sollte die Unabhängigkeit und Funktionsfähigkeit von EUROPOL gewährleistet werden. Der Bundestag hat das EUROPOL-Immunitätenprotokollgesetz zwischenzeitlich beschlossen (BGBl. II 1998, S. 974). Nach dem Protokoll wird EUROPOL-Bediensteten Immunität vor jeglicher Gerichtsbarkeit für in Ausübung ihres Amtes vorgenommene strafbare Handlungen eingeräumt. In Deutschland gab es heftige Kontroversen über die rechtspolitischen und verfassungsrechtlichen Aspekte dieser Freistellung. Niemand käme etwa auf die Idee, eine Einschränkung der Funktionsfähigkeit des Landeskriminalamts Niedersachsen deswegen anzunehmen, weil die Mitarbeiter keine Immunität besitzen. Trotz der Bedenken wurde das Gesetz beschlossen, da der gewollte Tätigkeitsbeginn von EUROPOL von der Verabschiedung des Gesetzes abhing und Neuverhandlungen anstehen, wenn EUROPOL Exekutivaufgaben erhält. Kritische Stimmen sehen die Entwicklung gleichwohl mit Sorge. Anlass hierfür ist auch eine Äußerung des wahrscheinlich künftigen EUROPOL-Direktors. Offenbar gibt es Strömungen, die die Immunität nicht als Übergangsstadium betrachten, sondern sie eher als einen Einstieg in die Immunität auch nationaler Polizeibeamter und damit in eine generelle Zulassung sogenannter milieubedingter Straftaten ansehen. Die Äußerung lautet: „Vielleicht kommen wir ja, wenn die Gefährdungen für nationale Polizeien steigen, auch zu ähnlichen Immunitätsregelungen“.

Nach Art. 3 des Immunitätenprotokolls sind die Archive von EUROPOL unverletzlich. Dazu gehören alle Aufzeichnungen, Schriftwechsel und -stücke, Manuskripte, Computer- und Mediendaten, Fotografien, Filme, Video- und Tonaufzeichnungen. Es ist nicht auszuschließen, dass diese Bestimmung auch zu datenschutzrechtlich nachteiligen Folgen führt. Betroffenen, die zur Durchsetzung ihrer Individualansprüche auf Auskunft oder Löschung gegebenenfalls auf eine

Offenbarung von Unterlagen angewiesen sind, könnten unter Hinweis auf die Unverletzlichkeit abschlägig beschieden werden. Sie könnte auch zu Konflikten mit der Gemeinsamen Kontrollinstanz von EUROPOL führen (vgl. XIII 11.3.1). Dieser Instanz steht zwar ein Einsichtsrecht in Unterlagen und Akten von EUROPOL zu; aber was geschieht, wenn sich EUROPOL auf die Unverletzlichkeit beruft? Nach der deutschen Begründung zu Art. 3 des Protokolls soll das Recht der Gemeinsamen Kontrollinstanz auf Einsichtnahmen unberührt bleiben. Dies mag eine freundliche Meinung der deutschen Seite sein. Der Wortlaut des von allen Staaten abgezeichneten Protokolls trägt diese Auffassung leider nicht.

10.6 NoeP'se, Verdeckte Ermittler und weitere Befugnisse der Polizei im Vorfeldnebel

Ich hatte in meinem letzten Tätigkeitsbericht über meine Kontrolle eines polizeilichen Lauschangriffs zur Gefahrenabwehr in einer Wohnung berichtet (vgl. XIII 11.5). Zwischenzeitlich habe ich zwei weitere Einsätze besonderer Mittel im Vorfeld überprüft. Gegenstand meiner Kontrolle war die Verwendung eines Personenschutzsenders außerhalb von Wohnungen sowie eine Kontrollmeldung. Eine Überprüfung der Erfassung unbeteiligter Dritter war nicht möglich, weil Aufzeichnungen hierzu nicht vorlagen; sie sind gesetzlich auch nicht vorgesehen. Beide Fälle waren – wie schon der polizeiliche Lauschangriff – begleitet von Ermittlungsverfahren. Die Datenverarbeitung entsprach dem Gesetz. Zur Einordnung dieser Aussage ist es hilfreich, sich die Entwicklung und Überprüfbarkeit des Einsatzes besonderer Mittel und Methoden vor Augen zu führen.

Die Polizei ist seit Juni 1994 gehalten, Schwerpunkte von Aktivitäten im Vorfeldbereich und die sehr eingriffsintensiven und verdeckten Datenerhebungen unter Verwendung besonderer Mittel und Methoden darzustellen. Bis Mai 1997 zählten hierzu die Einrichtung von Kontrollstellen, längerfristige Observationen, der Einsatz von technischen Mitteln in und außerhalb von Wohnungen einschließlich Personenschutzsendern, die Verwendung von Vertrauenspersonen und Kontrollmeldungen (beobachtende Fahndung). Infolge der jüngsten Gesetzesänderung bezieht sich die Darstellung nur noch auf längerfristige Observationen, technische Mittel, Verdeckte Ermittler (neu eingeführt) und Kontrollmeldungen. Weggefallen sind Informationen über Schwerpunkte polizeilicher Arbeit im Vorfeldbereich und über Kontrollstellen und Vertrauenspersonen (vgl. 10.2). Eine weitere Folge war, dass Angaben zum Zeitraum Juni 1997 bis Januar 1998 nicht vorliegen. Zwischen Februar 1998 und Mai 1998 gab es - richterlich angeordnet - eine längerfristige Observation und einen technischen Mitteleinsatz; ein weiterer Einsatz eines technischen Mittels war behördlich angeordnet. Die nachfolgende Übersicht bezieht sich auf den Zeitraum Juni 1994 bis Mai 1997, für den veröffentlichte Daten zur Verfügung stehen.

Einsatz besonderer Mittel und Methoden einschl. Kontrollstellen

Zeitraum	Anordnungen			Fälle
	Richter	Behörden	Gesamt	
06/94-05/95	9	14	23	37
06/95-05/96	14	30	44	52
06/96-05/97	15	8	23	52
Gesamt - 3 Jahre -	**38**	**52**	**90**	**141**

Quelle: LT-Drs. 13/1638; 13/2533: 13/3329

Die Übersicht lässt eine erste Grobeinschätzung zu. In einem Zeitraum von drei Jahren wurden 90 Anordnungen zum Einsatz besonderer Mittel und Methoden getroffen. Die Anordnungen betrafen 141 Fälle. Quantitativ betrachtet würde ich bei landesweit durchschnittlich zwei bis drei Anordnungen pro Monat von einem maßvollen Gebrauch der 1994 gesetzlich neu eingeführten besonders eingriffsintensiven Befugnisse sprechen.

Auf den zweiten Blick kommen Fragen auf. Die Informationen über verdeckt eingesetzte Vorfeldmittel sollen der demokratisch gebotenen Transparenz staatlichen Handelns in für Grundrechtsverletzungen anfälligen Bereichen dienen und zugleich Kontrollinstanzen wie dem Innenministerium oder dem Parlament ermöglichen, auf gegebenenfalls eintretende Fehlentwicklungen zu reagieren. Ich habe große Zweifel, ob dieses Ziel mit den vorhandenen Daten erreicht werden kann.

Die Daten beziehen sich nur auf fünf bestimmte Eingriffsbefugnisse. Informationen über sonstige polizeiliche Vorfeldaktivitäten, wie z. B. über den Einsatz von nicht offen ermittelnden Polizisten (noeP‘se), fehlen. Die Angaben geben vor allem keine Auskunft über die Zahl der Betroffenen, insbesondere über die Zahl unbeteiligter Dritter. Die Größenordnung läßt sich nur erahnen, da nur selten Zahlen erfasst und bekannt werden. So führte z. B. 1 Anordnung zu 13 Kontrollstellen (Fälle) und zur Überprüfung von 2 600 Menschen. Hier trifft die auch schon bei Telefonüberwachungen gemachte Erfahrung zu: Die Zahl der Anordnungen ist relativ gering, die Anzahl der konkreten Fälle bzw. Verfahren schon größer; deutlich wird der Eingriffsumfang erst mit der überwiegend nicht bekannten Zahl der Betroffenen (vgl. 27.6).

Offen bleibt auch, ob das Ziel der Maßnahmen erreicht wurde, durch einen unerlässlichen Grundrechtseingriff eine Straftat zu verhüten. Nähere Angaben hierzu fehlen, etwa darüber, inwieweit Strafverfahren eingeleitet wurden oder Unterrichtungen Betroffener erfolgten. Zur Bewertung einer Einzelmaßnahme sind einordnende Angaben über den Gesamtkomplex nötig. Dazu gehören angesichts der häufig anzutreffenden Gemengelage Gefahrenabwehr/Strafverfolgung Informationen über parallel verlaufende verdeckte Maßnahmen nach der Strafprozessordnung (StPO) ebenso wie Aktivitäten des Verfassungsschutzes oder auch anderer Sicherheitsbehörden z. B. des Bundes. Unklar ist zudem, ob die einzelnen Mittel zur Abwehr der organisierten Kriminalität eingesetzt wurden. Mit diesem Zweck war ursprünglich die gesetzliche Einführung der besonderen Mittel und Methoden im Gefahrenabwehrrecht begründet worden. Eine Neuregelung in der StPO zeigt, dass einige dieser notwendigen Grundinformationen, jedenfalls nach dem Abhören von Wohnungen, für erforderlich gehalten werden. Danach sind auch Umfang (Erfassung unbeteiligter Dritter), Dauer, Zweckerreichen und Kosten der Maßnahme sowie Unterrichtungen Betroffener darzustellen (vgl. § 100 e StPO).

Das Ergebnis meiner eingangs dargestellten Kontrollen ist wegen der angesprochenen Informationslücken und meiner auf die Datenverarbeitung begrenzten Prüfkompetenz mithin auch nicht geeignet, Anworten zur tatsächlichen Wirkungsweise polizeilicher Vorfeldaktivitäten zu geben.

10.7 Schwarzer Fleck auf weißer Weste (MIKADO)

„Na, Sie haben ja schon einiges auf dem Kerbholz.“ „Da ist doch schon mal etwas gewesen.“ Diese Aussagen von Polizeibeamten, die aufgrund von Speicherungen im automatisierten Datenverarbeitungssystem MIKADO getroffen worden waren und sich später als falsch herausstellten, erregten den Unmut der Betroffenen. Ein anderer Bürger stellte anlässlich der Anzeige eines Einbruchs in seinen Pkw überrascht fest, dass er in MIKADO einen Eintrag als Beschuldigter

hatte. Das gegen ihn eingeleitete Ermittlungsverfahren war schon lange eingestellt worden, nachdem er die Anschuldigungen widerlegt hatte. Er war daher empört, dass diese Daten nach Auskunft des Polizeibeamten 5 Jahre im System gespeichert sind und er bei einem erneuten Kontakt mit der Polizei als „Wiederholungstäter“ eingestuft wird.

Die Fälle zeigen, dass es sich bei dem landesweit eingesetzten System MIKADO nicht nur um ein reines Vorgangsverwaltungssystem im Sinne eines Aktenfindungs-, Textverarbeitungs- und Dokumentationssystems handelt. MIKADO stellt Daten über Personen für die polizeiliche Arbeit bereit, auf deren Richtigkeit sich der ermittelnde Beamte verlassen können muss. Die Aktualisierung der Eintragungen ist also nicht nur aus Sicht des Datenschutzes unverzichtbar. In dem geschilderten Fall war der Eintrag ursprünglich richtig. Nach der Einstellung des Verfahrens hätte jedoch eine Korrektur der nunmehr unrichtigen Daten erfolgen müssen. Die Technik sah die Umsetzung des Rechts nicht vor. Das Datenfeld „Status“ (z. B. Beschuldigter, Zeuge) ist nicht einzeln änderbar. Eine Korrektur kann nur durch Löschung und Neueingabe des gesamten Datensatzes mit nunmehr geändertem Status erfolgen. Ein Status „zu Unrecht beschuldigt“ (weiße Weste) ist bei den 50 vorgegebenen Rollen nicht vorgesehen. Immerhin erfolgte aufgrund der Eingabe des Betroffenen eine Neuaufnahme des Datensatzes mit dem unverfänglichen Status „Zeuge“. Die mit der Qualifikation „Beschuldigter“ verknüpften Bewertungsmöglichkeiten waren damit vom Tisch. Eine ersatzlose Löschung der Personalien war wegen der erforderlichen Dokumentation des Vorgangs nicht möglich.

Die durch Beschwerden gesammelten Erfahrungen zeigen die Wichtigkeit der Aktualität der gespeicherten Daten und einer anwenderfreundlichen Technik. Das Statusfeld sollte einzeln änderbar sein und eine Rolle für Unbescholtene vorsehen.

11 Ausländerangelegenheiten

11.1 Vorlage der Asylbewerberakten für Ehefähigkeitszeugnisse

Eine deutsch-ausländische Initiative fragte an, ob es zulässig sei, die gesamte Akte des Asylbewerbers für die Entscheidung zur Ehefähigkeit dem Oberlandesgericht in Kopie zur Verfügung zu stellen und damit dem Gericht die Anhörungsprotokolle und das Asylverfahren zu offenbaren. Man vertrat die Auffassung, dass die in dieser Akte vorhandenen Anhörungsprotokolle mit der zu treffenden Entscheidung in keinem Zusammenhang stehen.

In der von mir angeforderten Stellungnahme führte das Oberlandesgericht aus: Ausländer haben vor einer Eheschließung ein sogenanntes „Ehefähigkeitszeugnis“ beizubringen (§ 10 Abs. 1 Ehegesetz). Der Präsident des Oberlandesgerichts kann unter bestimmten Voraussetzungen eine Befreiung von der Beibringung eines Ehefähigkeitszeugnisses erteilen (§ 10 Abs. 2 Ehegesetz). Er hat nach Vorbereitung des Antrags und Vorlage durch den zuständigen Standesbeamten eine Identitätsprüfung vorzunehmen und unter Zugrundelegung des jeweiligen ausländischen Rechts den Personenstand des Antragstellers so zuverlässig wie möglich festzustellen. Dabei tritt er quasi an die Stelle der Innenbehörde des Heimatlandes und muss den Sachverhalt im Hinblick auf Ehehindernisse von Amts wegen ermitteln und sich dabei der erforderlichen Beweismittel bedienen. In der Praxis geht es vornehmlich um die Frage, ob der Antragsteller bereits verheiratet ist, um einer bigamen Eheschließung vorzubeugen. Über die Notwendigkeit der Hinzuziehung von Ausländerakten wird nach Durchsicht der Aufgebotsunterlagen unter Beachtung des Verfahrenszwecks jeweils im Einzelfall entschieden. Bei konkreten Zweifeln an der Echtheit oder inhaltlichen Richtigkeit

vorgelegter Urkunden zur Überprüfung der darin enthaltenen Angaben werden entsprechende Akten angefordert. Weiterhin wird in die jeweilige Ausländerakte Einsicht genommen, wenn Unterlagen von Ausländern vorgelegt werden, deren Heimatstaaten kein bzw. kein geordnetes Personenstandswesen kennen, oder bekannt ist, dass Personenstandsnachweise aus diesen Staaten in nicht unerheblicher Anzahl gefälscht oder inhaltlich unrichtig sind, wenn also generelle Zweifel an der Richtigkeit derartiger Urkunden bestehen sollten.

In diesem konkreten Fall handelte es sich um einen Antragsteller aus Zaire. Nach Informationen des Oberlandesgerichts existiert in Zaire kein Melde- bzw. Personenstandswesen (mehr). Bescheinigungen dortiger Behörden würden schon aufgrund mündlicher Anfragen ohne tatsächliche Überprüfung erstellt bzw. seien käuflich zu erwerben. Die deutsche Botschaft habe mitgeteilt, 95 v.H. der vorgelegten Personenstandsurkunden seien gefälscht oder unrichtig. Von daher hielt das Oberlandesgericht eine Prüfung anhand vollständiger Akten für unumgänglich. Von Interesse seien dabei auch die in der Akte befindlichen Anhörungsprotokolle. Gerade darin fänden sich Schilderungen über die Lebensumstände des Antragstellers, die Aufschluss über den zu ermittelnden Personenstand gäben. Weitere Möglichkeiten der Prüfung stünden regelmäßig nicht zur Verfügung. Das Oberlandesgericht hat angemerkt, dass gerade die Überprüfung bei abgelehnten Asylbewerbern in nicht wenigen Fällen ergeben habe, dass bei Befragungen kurz nach der Einreise in die Bundesrepublik Deutschland andere Angaben zum Personenstand als in dem anhängigen Befreiungsverfahren gemacht worden seien. Entsprechende Anträge würden sich häufig nach diesbezüglichem Hinweis durch Rücknahme erledigen.

Abschließend wurde darauf hingewiesen, auf Seiten des Antragstellers habe offensichtlich ein besonderes Interesse an der beschleunigten Bearbeitung bestanden, so dass die Übersendung der Ausländerakte bereits vor Tätigwerden des Oberlandesgerichts veranlasst worden sei und innerhalb von 14 Tagen eine positive Entscheidung habe getroffen werden können.

Nach der Stellungnahme des Oberlandesgerichts war die Übermittlung personenbezogener Daten zur Erfüllung eigener Aufgaben (§ 10 Abs. 2 Ehegesetz) erforderlich. Die zweckändernde Nutzung der bereits erhobenen Daten ist gerechtfertigt, da nur auf dieser Grundlage Hinweise auf Ehehindernisse ermittelt oder geprüft werden können, insbesondere dann, wenn konkrete Zweifel an vorgelegten Urkunden bestehen oder die Heimatstaaten kein geordnetes Personenstandswesen kennen.

Aus datenschutzrechtlicher Sicht war daher das Vorgehen des Oberlandesgerichts weder bezogen auf den Einzelfall noch generell von mir zu beanstanden.

11.2 Was darf ein ausländischer Besucher über seinen Gastgeber wissen?

Ein Gastgeber, der Ausländer aus bestimmten Staaten einlädt, muss sich gemäß § 84 Ausländergesetz für die Erteilung eines Visums für Besuchszwecke gegenüber der zuständigen Ausländerbehörde verpflichten, die Kosten des Lebensunterhalts, der notwendigen medizinischen Versorgung und der Rückreise zu übernehmen, wenn der Ausländer selbst dazu nicht in der Lage ist.

Für die Erklärung wird ein bundeseinheitliches Formular verwendet, das das Bundesministerium des Innern mit Rundschreiben vom 6. November 1996 eingeführt hat. In dem Vordruck werden weitere Hinweise zur Verpflichtungserklärung gegeben. Es wird eine umfangreiche Bonitätsprüfung des sich verpflichtenden Gastgebers von der Ausländerbehörde vorgenommen und das Ergebnis auf dem Formular vermerkt. Als Belege kommen in Betracht: Mietvertrag, Einkommensnachweis, Bankbürgschaft, Versicherungsnachweise und Mitteilungen

über bereits abgegebene Verpflichtungserklärungen. Der Verpflichtungserklärende ist auf die Freiwilligkeit seiner Angaben sowie auf den Umfang der eingegangenen Verpflichtung hinzuweisen. Die Durchschrift des Formulars verbleibt bei der Ausländerbehörde als gegebenenfalls erforderlicher vollstreckbarer Titel. Das Original wird dem Verpflichtungserklärenden ausgehändigt zur Weiterleitung an den Ausländer, der die Verpflichtungserklärung im Rahmen des Visumverfahrens bei der zuständigen Auslandsvertretung vorlegt. Das Original verbleibt anschließend beim Ausländer zur Vorlage bei der Grenzkontrolle. Der Gastgeber bzw. der Ausländer sind vorab darüber zu belehren, dass der Ausländer eine Ablichtung der Verpflichtungserklärung bei der deutschen Auslandsvertretung abzugeben hat und daher vorher selbst eine Kopie des Originals fertigen sollte.

Die umfangreiche Datenerhebung und Weitergabe dieser Daten an Dritte begegneten bei etlichen Datenschutzbeauftragten erheblichen Bedenken:

– Für die Bonitätsprüfung werden Daten des Gastgebers erhoben, die nicht zur Erfüllung des Zwecks erforderlich sind (Beruf, Arbeitgeber, Miet- oder Eigentumswohnung, Wohnraumgröße, genaue Höhe des Einkommens/ Vermögens).

– Dritte – insbesondere der Gast – erhalten Kenntnis von der Einkommens- und Vermögenslage des Gastgebers, ohne dass dies für die Verpflichtungserklärung erforderlich ist.

– Die Daten werden jahrelang in den Ausländerbehörden aufbewahrt, obwohl die Verpflichtung des Gastgebers sich nur auf den Zeitraum der Einladung bezieht.

Der Bundesbeauftragte für den Datenschutz wies mit Schreiben vom 4. August 1997 und vom 29. Januar 1998 das Bundesministerium des Innern auf die erheblichen datenschutzrechtlichen Mängel hin. Insbesondere war ihm wichtig, dass die der Bonitätsprüfung durch die Ausländerbehörden zu Grunde liegenden Detailangaben nur dem sich Verpflichtenden und der Ausländerbehörde zugänglich sein dürfen. Diese Forderungen wurden auch teilweise von den Innenministerien und Senatsverwaltungen der Länder anerkannt und von der ad hoc Arbeitsgruppe Ausländerrecht am 21. April 1998 aufgenommen.

Mit Schreiben vom 16. Oktober 1998 hat der Bundesbeauftragte für den Datenschutz darauf aufmerksam gemacht, dass das Bundesministerium des Innern mit Schreiben vom 17. Oktober 1998 den Innenministerien und Senatsverwaltungen der Länder die endgültige Fassung der „Hinweise zur Verwendung des bundeseinheitlichen Formulars der Verpflichtungserklärung“ übersandt hat und dass darin seine Änderungswünsche weitgehend eingeflossen sind. Insbesondere wird künftig auf Detailangaben zu Wohn-, Einkommens- und Vermögensverhältnisse verzichtet, sodass ein ausländischer Besucher diese Angaben über seinen Gastgeber nicht mehr erfährt. Die Angabe des Berufes und des Arbeitgebers wird vom Bundesministerium des Innern weiterhin als notwendiges Kriterium für die Bonitätsprüfung angesehen.

Entgegen den Erfahrungen in anderen Ländern gab es in Niedersachsen nur vereinzelt Eingaben zu diesen Verpflichtungserklärungen. Sie bezogen sich insbesondere auf die Offenbarung der Einkommens- und Vermögensverhältnisse des Gastgebers gegenüber dem ausländischen Gast. In meinen Gesprächen mit dem Innenministerium habe ich volles Verständnis für die Einwände gefunden. Die Mitteilung von Detailangaben über die finanzielle Situation des Einladenden wird vom Ministerium nicht für erforderlich erachtet. Im Übrigen werden z. Z. die Hinweise für die Ausländerbehörden entsprechend den Vorgaben des Bundesministeriums des Innern überarbeitet.

12 Verfassungsschutz

12.1 40 Millionen Bundesbürger beim Verfassungsschutz registriert?

Natürlich stimmt die Zahl nicht. Sie spiegelt aber Vermutungen und vielleicht auch Ängste wider, die sich aus einer repräsentativen Bevölkerungsumfrage ergeben. Danach glauben 47 von 100 Befragten, sie seien beim Verfassungsschutz erfasst.

Vermutungen sind das eine, die Realität kann anders aussehen. Angesichts des datenschutzrechtlichen Auskunftsanspruchs kann der Datenschutz helfen, Vermutungen auf ihre Richtigkeit hin zu überprüfen. Jedem steht das Recht zu, sich bei Behörden zu erkundigen, ob persönliche Daten über ihn dort gespeichert sind. Die Antwort der Behörde ermöglicht dann weitere – jetzt allerdings begründbare – Überlegungen einschließlich der Frage, ob eventuell eine gerichtliche Durchsetzung eigener Positionen nötig ist. Hintergrund des datenschutzrechtlichen Auskunftsanspruchs ist demnach sowohl das Grundrecht auf informationelle Selbstbestimmung als auch die Rechtsschutzgarantie des Grundgesetzes.

Die Wegstrecke zum Auskunftsanspruch gegenüber dem Verfassungsschutz war lang, der Weg mühevoll. In den vergangenen Jahrzehnten war es nicht einfach, von Verwaltungsbehörden die entsprechenden Angaben zu erhalten. Für einen jedermann zustehenden Rechtsanspruch auf Auskunft über personenbezogene Daten sorgte erst das Datenschutzrecht, unterstützt vom „Volkszählungsurteil“ des Bundesverfassungsgerichts. Das Auskunftsrecht nach dem (früheren) Niedersächsischen Datenschutzgesetz von 1978 galt allerdings nicht gegenüber dem Verfassungsschutz. Dies änderte sich mit Inkrafttreten des Niedersächsischen Verfassungsschutzgesetzes vom 3. November 1992 (vgl. XI 14.1). Darin wurde das Recht auf Auskunft gegenüber dem Niedersächsischen Landesamt für Verfassungsschutz (NLfV) erstmalig normiert, wenn auch mit weit gefassten Ablehnungsmöglichkeiten. Äußerungen im Rahmen der Diskussion um die Einführung des Auskunftsrechts erweckten damals den Eindruck, das NLfV werde über „Wellen“ von Anfragen auf „kaltem Wege“ lahmgelegt. Interessierte Kreise könnten zudem durch die Auskünfte vieles über die Arbeitsweise dieses Amtes erfahren. Insgesamt werde das NLfV gleichsam zu einer Auskunftei degradiert. So gesehen war die Einführung des Auskunftsrechts schon fast revolutionär. Dabei handelte es sich nur um die selbstverständliche Umsetzung des Grundrechts auf informationelle Selbstbestimmung. Angesichts dieses historischen Prozesses lag es für mich auf der Hand, die praktische Handhabung des Auskunftsrechts zu begleiten und auch datenschutzrechtlich zu kontrollieren.

Zunächst ist positiv zu würdigen, daß die jährlichen Verfassungsschutzberichte aus Gründen gewollter Transparenz ab 1993 Angaben über Auskunftserteilungen und –ablehnungen enthalten. Insgesamt gab es seit 1993 bis August 1998 120 Auskunftsanfragen. Bei 97 Anfragen lag keine Registrierung beim NLfV vor. In den verbleibenden 23 Speicherungsfällen wurde vierzehnmal eine Auskunft erteilt. Bei neun Anfragen wurde eine Auskunft abgelehnt, verbunden mit dem gesetzlich vorgesehenen Hinweis, der Betroffene könne sich zur Überprüfung der Angelegenheit an mich wenden.

Nach diesen Zahlen aus einem Zeitraum von fast sechs Jahren kann festgestellt werden, dass bei durchschnittlich ein bis zwei Auskunftsanfragen pro Monat wahrlich keine Auskunftswellen über das NLfV hinweggefegt sind. Es ist ein Stück Normalität eingetreten. Normal ist die Möglichkeit, Speicherungen beim Verfassungsschutz zu erfahren, und das Verhalten des NLfV, von der Ausnahmeregelung über Ablehnungen deutlich weniger Gebrauch zu machen. Ich habe solche Ablehnungsfälle überprüft. Das Ergebnis war immer ein datenschutzrechtlich korrektes Verhalten des NLfV. Unter dem Strich meine ich, in diesem

Bereich einen spürbaren Gewinn an Transparenz und Gelassenheit sehen zu können.

12.2 Nachträgliche Information Betroffener über eingesetzte Geheimdienstmittel

Der zuvor angesprochene Auskunftsanspruch ist in seiner Wirkung begrenzt. Wer kommt schon auf die Idee, eine Auskunft über gespeicherte Daten von Behörden zu verlangen, wenn überhaupt kein konkreter Anlass hierfür besteht. Dennoch könnten gravierende Eingriffe in das Persönlichkeitsrecht erfolgt sein, von denen Betroffene nichts ahnen. Die vom Verfassungsschutz genutzten nachrichtendienstlichen Mittel zur Informationsbeschaffung sind alle heimlich. Es liegt in der Natur der Sache, dass diese Aktivitäten nicht erkannt werden sollen. Bei solch heimlichen Datenerhebungen würde ohne eine nachträgliche Information Betroffener die Rechtsschutzgarantie des Grundgesetzes leerlaufen. Geboten ist daher eine nachträgliche Offenlegung des heimlichen Informationseingriffs, um – wie bei den normalerweise offenen Vorgehensweisen des Staates – informierte Bürgerinnen und Bürger entscheiden zu lassen, ob sie gegebenenfalls Rechtsschutz in Anspruch nehmen wollen. Fachlich spricht man hier vom Rechtsschutz-Initiativeffekt, der mit der nachträglichen Information ausgelöst wird.

Der Wille des niedersächsischen Parlaments, für Rechtsschutzmöglichkeiten und Transparenz zu sorgen, zeigte sich auch in diesem diffizilen Bereich. Nach dem Verfassungsschutzgesetz ist das NLfV verpflichtet, von sich aus Betroffene über bestimmte schwerwiegende Eingriffe zu informieren, wenn die heimliche Aktion beendet und der Zweck der Maßnahme durch die Offenlegung nicht mehr gefährdet ist. Zu solch intensiven Eingriffen in das Persönlichkeitsrecht zählt das Gesetz bestimmte nachrichtendienstliche Mittel der Informationsbeschaffung, wie z. B. den Einsatz verdeckt ermittelnder Beamter, das Belauschen privater Gespräche mit technischen Mitteln oder auch längerfristige Observationen. Die Informationsverpflichtung gegenüber Betroffenen führt jedoch nicht zu einer umfassenden Offenlegung der nachrichtendienstlichen Aktivitäten. Die Formulierungen „bestimmte Eingriffe“ und „keine Gefährdung des Zwecks der Maßnahme“ weisen schon auf bestehende gesetzliche Einschränkungen der Informationsverpflichtung hin. Betroffene sind also nicht über alle eingesetzten nachrichtendienstlichen Mittel zu informieren, und die Gründe für ein Unterlassen der nachträglichen Information können vielfältig sein.

Ich habe das vom NLfV durchgeführte Mitteilungsverfahren datenschutzrechtlich kontrolliert. Meine Überprüfung erstreckte sich auf den Zeitraum 1993 bis Anfang August 1998. Während dieser Zeit wurden in 11 überprüfbaren Verfahren gegen insgesamt 24 Betroffene die oben beschriebenen nachrichtendienstlichen Mittel eingesetzt. Die Mitteilung über einen beendeten Informationseingriff erhielt ein Betroffener; bei einem weiteren ist eine erneute Prüfung der Mitteilung in absehbarer Zeit vorgesehen. Alle Entscheidungen des NLfV entsprachen aus meiner Sicht dem Gesetz. Sie waren aufgrund sorgfältig geführter Unterlagen nachvollziehbar. Als wohltuend im Vergleich zu manch anderen Bereichen habe ich empfunden, wie selbstverständlich die Dokumentation des eigenen Handelns erfolgt. Zu keinem Zeitpunkt wurde etwa behauptet, die rechtsstaatlich notwendige Dokumentation sei viel zu aufwändig.

Nun mag jede Leserin und jeder Leser die Zahlen aus einem Zeitraum von fast sechs Jahren interpretieren. Ich halte zwei Feststellungen für wesentlich: Mit der gesetzlichen Mitteilungspflicht ist ein prinzipiell richtiger Schritt getan worden und – das Verfahren funktioniert.

12.3 Kontrolle von Sicherheitsüberprüfungsakten

In meinem vorletzten Tätigkeitsbericht hatte ich über das Verfahren bei Sicherheitsüberprüfungen berichtet (vgl. XII 14.3 – Unglaubliche Personendossiers). Solchen Verfahren müssen sich Berufstätige unterziehen, die Umgang mit geheimen Unterlagen haben können. In den Verfahren wirkt das Niedersächsische Landesamt für Verfassungsschutz maßgeblich mit. Die Feststellung, der Überprüfte sei kein Risiko – kann also gleichsam Geheimnisträger sein -, ist bei den entsprechenden Arbeitsplätzen unerlässlich für die „Schicksalsfrage“ Einstellung/Beförderung im öffentlichen Bereich und in der Privatwirtschaft.

Ich habe erneut Akten aus dem strengsten Überprüfungsverfahren beim Niedersächsischen Landesamt für Verfassungsschutz kontrolliert. Bei diesen Verfahren geht es um Antragsteller, die Umgang mit als „Streng Geheim“ eingestuften Unterlagen haben können, sog. Ü 3-Verfahren. Meine stichprobenartige Kontrolle umfasste 20 Sicherheitsüberprüfungsakten aus den Jahren 1994 bis 1996. Alle Betroffenen kamen aus dem öffentlichen Bereich. Es handelte sich um Geheimschutzbeauftragte, Behördenleiter, Polizeibedienstete und Beschäftigte in der Geheimregistratur. Meine datenschutzrechtliche Bewertung orientierte sich im Wesentlichen an den Niedersächsischen Sicherheitsrichtlinien, da zum Zeitpunkt meiner um die Jahreswende 1996/97 vorgenommenen Prüfung noch kein Sicherheitsüberprüfungsgesetz vorlag.

Im Vergleich zu meiner 1994 durchgeführten Kontrolle habe ich eine durchgängig verbesserte Datenverarbeitung festgestellt, die sich deutlich am Grundsatz der Verhältnismäßigkeit orientierte. Die Erforderlichkeit der Sicherheitsüberprüfungsverfahren war nahezu immer nachvollziehbar. Unnötige Speicherungen ohne Bezug zum Verfahrensgegenstand habe ich praktisch nicht angetroffen. Pro Verfahren wurden Informationen über durchschnittlich acht Menschen eingeholt; bei meiner früheren Kontrolle erstreckten sich die Recherchen noch auf 15 Personen. Dementsprechend verringerte sich auch der durchschnittliche Aktenumfang pro Verfahren auf etwa die Hälfte. Weiter kontrovers blieben u. a. Fragen nach der Erforderlichkeit von Datenerhebungen über Verwandte und Referenzpersonen sowie bei Auskunftspersonen. Der niedersächsische Gesetzgeber hat die streitigen Punkte im Niedersächsischen Sicherheitsüberprüfungsgesetz zu Gunsten der Fachverwaltung entschieden.

12.4 Bürgerinnen und Bürger als Sicherheitsrisiko

Sicherheitsüberprüfungsverfahren sind nur ein schmaler Ausschnitt aus den Verfahren zur Überprüfung der staatsbürgerlichen Zuverlässigkeit. Es gibt eine Vielzahl weiterer Verfahren, die alle darauf abzielen festzustellen, ob berufstätige Niedersachsen mit als geheimhaltungsbedürftig bewerteten Informationen umgehen dürfen. Dazu zählen Zuverlässigkeitsüberprüfungen des Personals auf Flughäfen und bei Luftverkehrsunternehmen (vgl. XI 14.7, XII 14.8 – Flughafen Langenhagen -), der privaten Betreiber von Telekommunikationseinrichtungen und der Beschäftigten in der Atomindustrie (Anlagen und Transport, vgl. XII 13.5). Arbeitnehmer von ca. 140 Firmen in Niedersachsen werden nach dem sog. Geheimschutzverfahren für die Wirtschaft überprüft. Man könnte daher geneigt sein, die „Lage“ mit der eingangs genannten Überschrift zu kennzeichnen.

Die überspitzte Formulierung der Überschrift trifft selbstverständlich nicht zu. Leider gibt es keine Veröffentlichungen über die Gesamtzahl der in Niedersachsen überprüften Menschen, sondern lediglich Informationen über einen einzigen Bereich. Das Niedersächsische Innenministerium publiziert Zahlen für den Teilbereich Sicherheitsüberprüfungen. Ende 1997 gab es danach 9 866 Speicherungen. Diese Angabe bezieht sich auf Antragsteller und in die Sicherheitsüberprüfung einbezogene Ehegatten bzw. Lebenspartner. Die Zahl gibt

aber keine Auskunft über die im Rahmen der Sicherheitsüberprüfungen miterfassten Menschen aus dem Umfeld der Antragsteller. Nach meinen Feststellungen im Rahmen der Kontrolle von Sicherheitsüberprüfungsakten werden in jüngerer Zeit pro Ü 3-Verfahren Informationen über etwa acht Menschen eingeholt. Dieser Umstand und die Gesamtzahl der Sicherheitsüberprüfungen lassen die Annahme zu, dass allein bei den Sicherheitsüberprüfungsverfahren in Niedersachsen ca. 30 000 Menschen Betroffene waren. Diese Zahl kann ein Fingerzeig für die tatsächliche Größenordnung aller von Sicherheits-, Zuverlässigkeits- und Geheimschutzverfahren Betroffenen in Niedersachsen sein.

12.5 Verschlusssachen

Zentraler Anknüpfungspunkt für eine Sicherheitsüberprüfung nach dem Niedersächsischen Sicherheitsüberprüfungsgesetz ist der mögliche Umgang mit eingestuften Verschlusssachen. Das Gesetz setzt voraus, dass es sich um Verschlusssachen handelt. Es definiert zwar generalklauselartig die Geheimhaltungsgrade „VS–Vertraulich“, „Geheim“ und „Streng Geheim“, lässt aber offen, was im Einzelnen dahintersteckt. Dies ergibt sich erst aus einer internen Verwaltungsvorschrift, der Verschlusssachenanweisung (vgl. XII 14.3.4). Diese Anweisung steuert mit ihren 64 Paragraphen die Geheimhaltungspraxis staatlicher Instanzen. Damit gibt sich die Exekutive ihre eigenen Regeln. Wäre es nicht eigentlich Sache der Parlamente, näher festzulegen, was ein Staatsgeheimnis ist? Wie offensichtlich mit dem Geheimstempel demokratische Neugier abgeschottet und auch Politik gemacht wird, zeigte sich erst jüngst beim Plutonium-Untersuchungsausschuss des Deutschen Bundestages. Einer Mitteilung der Süddeutschen Zeitung vom 24. Juni 1998 zufolge erhielten sogar Zeitungsartikel (!) den Stempel „Verschlusssache – Nur für den Dienstgebrauch“. Wenn aber ein Regierungsvertreter Erklärungsbedarf hatte und auf einer Pressekonferenz auf vertrauliche Unterlagen zurückgreifen wollte, dann stufte der Bundesnachrichtendienst das als „VS–Vertraulich“ klassifizierte Material ganz schnell auf „Offen“ herab.

12.6 Niedersächsisches Sicherheitsüberprüfungsgesetz

Das Niedersächsische Sicherheitsüberprüfungsgesetz (Nds.SÜG) ist am 12. März 1998 in Kraft getreten (Nds. GVBl. S. 128).

Das Niedersächsische Sicherheitsüberprüfungsgesetz ist ein rechtsstaatlicher Gewinn. Die handelnden Bediensteten erhalten gesetzliche Grundlagen für den Umgang mit persönlichen Daten Dritter. Die Betroffenen wiederum bekommen einen Überblick über mögliche Datenerhebungen, Speicherungen und deren Dauer sowie über ihre Rechte. Der Überblick kann noch durch die ergänzenden Verwaltungsvorschriften (vgl. Nds. MBl. S. 1125) verfeinert werden. Das Gesetz regelt das Verfahren, mit dem festgestellt werden soll, ob Zweifel an der staatsbürgerlichen Zuverlässigkeit bestehen oder nicht. Wie bisher liegt der Ablauf des Verfahrens in der Verantwortung des Geheimschutzbeauftragten der Behörde (früher Sicherheitsbeautragter). Er leitet die Überprüfung ein und trifft die Schlussentscheidung. Die Funktion des Niedersächsischen Landesamtes für Verfassungsschutz liegt in der Mitwirkung, was nicht darüber hinwegtäuschen darf, dass das Amt die hauptsächliche Arbeit bei der Sicherheitsüberprüfung übernimmt.

Aus Sicht des Datenschutzes sind mit dem Sicherheitsüberprüfungsgesetz bedeutsame Fortschritte erzielt worden. Das Gesetz stellt unmissverständlich klar, dass die Einwilligung der betroffenen Personen Voraussetzung für die Sicherheitsüberprüfung ist. Niemand kann mehr gezwungen werden, das Überprüfungsverfahren mit all seinen Ausleuchtungen über sich ergehen zu lassen. An-

tragsteller und ggf. mit in die Überprüfung einbezogene Ehegatten bzw. Lebenspartner sind vor überraschenden Negativentscheidungen durch weitere Beteiligungsrechte geschützt. Sie müssen während des Verfahrens und im Rahmen einer Schlussanhörung zu Zweifeln an ihrer Zuverlässigkeit angehört werden. Die Betroffenen haben zudem einen unentgeltlichen – leider auch mit vielen Ablehnungsmöglichkeiten verbundenen – Auskunftsanspruch über zur Person gespeicherte Daten sowie ein Akteneinsichtsrecht, das es im Niedersächsischen Verfassungsschutzgesetz nicht gibt. Die Betroffenenrechte werden durch klare Regelungen zum Berichtigen, Löschen und Sperren von Daten vervollständigt. So werden z. B. fünf Jahre nach Ausscheiden aus der sicherheitsempfindlichen Tätigkeit alle Unterlagen vernichtet, automatisierte Speicherungen einschließlich derjenigen in Computersystemen der Verfassungsschutzbehörden werden gelöscht. Die im Rahmen einer Sicherheitsüberprüfung anfallenden, zum Teil intimen Angaben dürfen grundsätzlich auch nicht an die Pesonalstelle weitergeleitet werden. Das Gesetz sieht ausdrücklich eine personelle und organisatorische Trennung zwischen den Geheimschutzbeauftragten und der Personalverwaltung vor. Eine Ausnahme gibt es jedoch. Zu disziplinarrechtlichen sowie dienst- oder arbeitsrechtlichen Zwecken dürfen Daten an die Personalstelle weitergegeben werden, wenn dies zur Gewährleistung des Verschlusssachenschutzes erforderlich ist.

Einige datenschutzförderliche Bestimmungen, die im Vorfeld des Gesetzgebungsverfahrens noch vorgesehen waren, sind der Normensparsamkeit zum Opfer gefallen. Sie finden sich nunmehr in den Verwaltungsvorschriften, so z. B. das Gebot, die Gründe für die Erforderlichkeit der Sicherheitsüberprüfung aktenkundig zu machen, oder der klarstellende Hinweis, dass wegen der abschließenden Zuordnung der nachrichtendienstlichen Mittel im Verfassungsschutzgesetz der Einsatz solcher Mittel bei Sicherheitsüberprüfungen nicht zulässig ist. Befragungsberichte über Gespräche mit Referenz- und Auskunftspersonen müssen sich auf das sachlich notwendige Maß beschränken.

Nach dieser Übersicht bin ich der Meinung, dass viele Regelungen des Nds.SÜG datenschutzfreundlich sind. Gleichwohl trifft das Gesetz einige Grundentscheidungen, die aus meiner Sicht den bisher positiven Blick gravierend trüben. Hierzu zählen u. a. die Fülle an unbestimmten Rechtsbegriffen, die der Exekutive weite Handlungsspielräume einräumen. Bei bestimmten Verfahren soll der Ehegatte oder z. B. auch der Lebenspartner eines Antragstellers hinsichtlich seiner staatsbürgerlichen Zuverlässigkeit ebenfalls umfassend überprüft werden. Wer ist ein Lebenspartner? Rechnen hierzu auch Verlobte, die nicht zusammenleben und über keine gemeinsame Kasse verfügen? Unklar ist auch die Behandlung von Wochenendbeziehungen. Die Zahl der Paare, die eine Wochenend-Liebesbeziehung bevorzugen, soll sich z. B. in den Jahren 1985 bis 1995 auf 13 % verdoppelt haben.

Entgegen früheren politischen Absichtserklärungen, etwa den Kreis der von einer Sicherheitsüberprüfung betroffenen Personen zu verkleinern, erweitert das Niedersächsische Sicherheitsüberprüfungsgesetz den Anwendungsbereich von Sicherheitsüberprüfungen. Streng geheime Unterlagen waren bisher solche, deren Kenntnisnahme durch Unbefugte den Bestand des Staates gefährden können. Nunmehr gibt es noch die weitere Kategorie der „lebenswichtigen Interessen“. Die Begründung, das Bundesrecht habe eine gleichlautende Fassung, gibt keine Auskunft über Inhalt und Grenzen dieser neuen Kategorie. Klar ist nur die gewollte Erweiterung einzustufender Unterlagen mit der Folge des strengsten Überprüfungsverfahrens. Das Gesetz enthält überdies eine ganz bemerkenswerte Regelung. Sie fällt völlig aus dem System, weil sie zu Sicherheitsüberprüfungen führt, obwohl Betroffene überhaupt keinen Umgang mit Verschlusssachen haben. Behörden oder Teile von Ihnen können zu sog. „Sicherheitsbereichen“ erklärt werden. Damit sei man in der Lage, kurzfristig oder örtlich begrenzt insbe-

sondere auf unvorhersehbare Ereignisse zu reagieren, so die Begründung des Innenministeriums. Welche Ereignisse das sein können, bleibt dunkel. Hell sind hingegen die weiteren Folgen. Sicherheitsbereiche sind abgeschottet. Die Öffentlichkeit wird es schwer haben zu erfahren, was in den zu Sicherheitsbereichen erklärten Behörden passiert.

Ein weiterer Kritikpunkt ist die erhebliche Ausweitung erlaubter Datenweitergaben. Immerhin handelt es sich um ein Verfahren, das zu weitgehenden Eingriffen in die Persönlichkeitssphäre und in das persönliche Umfeld führen kann und auch auf eine sehr vertrauensvolle Zusammenarbeit angewiesen ist. Am Ende steht nun wegen der Weitergabemöglichkeiten die Aussicht, dass doch nicht alles vertraulich bleibt. Mir leuchtet z. B. die Regelung ein, nach der erhaltene Informationen erforderlichenfalls auch zur Spionageabwehr genutzt werden können. Die durchgängig mögliche Weiterleitung etwaiger Hinweise an Strafverfolgungsbehörden vermag ich aber nicht nachzuvollziehen, zumal sich eine praktische Notwendigkeit hierfür in den letzten Jahren nicht ergeben hat. Das Gesetz erlaubt nunmehr umfassende Informationsweitergaben an Strafverfolgungsbehörden; ausgenommen sind praktisch nur Hinweise auf Bagatelldelikte. In der Begründung zur bisher geltenden (Teil)regelung im Verfassungsschutzgesetz hieß es zu solchen Datenübermittlungen noch, sie müssten auf das Unerlässliche begrenzt werden. Demzufolge war es nur erlaubt, den Strafverfolgungsbehörden Hinweise auf eine Verletzung hochrangiger Schutzgüter, wie Verrat und Gefährdung des demokratischen Rechtsstaats, zu geben. Von einer solchen Beschränkung auf das Unerlässliche kann jetzt nicht mehr die Rede sein.

In einer datenschutzrechtlichen Gesamtschau verdient das neue Sicherheitsüberprüfungsgesetz dennoch Anerkennung. Die vielen Bestimmungen zu Beteiligungs- und Informationsrechten der Betroffenen bieten eine gute Chance, auf das Überprüfungsverfahren Einfluss zu nehmen und zu erfahren, was mit den persönlichen Daten geschieht.

13 Personalangelegenheiten

13.1 Neue Datenschutzregelungen im Beamtenrecht

Mit dem Dritten Gesetz zur Änderung dienstrechtlicher Vorschriften vom 17. Dezember 1997 (Nds. GVBl. S. 528) hat Niedersachsen datenschutzgerechte Regelungen zur Verarbeitung der Daten von Beschäftigten im öffentlichen Dienst erhalten. Der Gesetzgeber hat sich mit dieser Anpassung an das Beamtenrechtsrahmengesetz (BRRG) des Bundes zwar lange Zeit gelassen, die einschlägigen Bundesvorschriften stammen bereits aus dem Jahre 1992, sich andererseits aber nicht lediglich auf eine bloße Übernahme der Rechtsvorschriften des BRRG beschränkt, sondern in Einzelfragen zugunsten der Angehörigen des öffentlichen Dienstes datenschutzfreundlichere Lösungen gefunden.

Die bisherige Unübersichtlichkeit beim Ineinandergreifen von dienstrechtlichen und allgemeinen datenschutzrechtlichen Regelungen ist damit beseitigt. Die neuen Rechtsvorschriften gelten nicht nur für Beamte, sondern auch für Tarifbedienstete, sofern vorgehende tarifvertragliche Bestimmungen nicht entgegenstehen (vgl. § 261 Abs. 1 Nr. 2 NBG). § 24 NDSG als bisherige Grundvorschrift zur Datenverarbeitung in Dienst- und Beschäftigungsverhältnissen konnte deshalb gestrichen werden.

Ich hoffe, dass die neuen Vorschriften, die erstmals auch für die Kommunen und die übrige mittelbare Landesverwaltung die Verarbeitung von Beschäftigtendaten umfassend regeln, dazu beitragen, die in der Vergangenheit (vgl. XIII 14.) und auch im Berichtszeitraum immer wieder festgestellten Rechtsverstöße in diesem Bereich entscheidend zu reduzieren.

Durch die Abweichungen der jetzigen Fassung des NBG von den rahmenrechtlichen Regelungen sind die Verwaltungsvorschriften zum NBG vom 25. November 1992 (Nds. MBl. S. 13) z. T. überholt. Vor ihrer Anwendung muss jeweils geprüft werden, ob die seinerzeit zugrunde gelegte Rechtslage noch fortbesteht oder inzwischen geändert worden ist. Um Rechtsunsicherheiten zu vermeiden, sollte das Innenministerium die Verwaltungsvorschriften umgehend der geänderten Rechtslage anpassen.

Für die Verwaltungspraxis möchte ich auf folgende Punkte aufmerksam machen:

Daten von Angehörigen

Neben den personenbezogenen Daten über Bewerber, Bedienstete, frühere Bedienstete und deren Hinterbliebene verarbeiten die Personal verwaltenden Stellen auch Daten der Angehörigen (z. B. für Bezüge - und Beihilfeberechnung). Eine eigenständige Rechtsgrundlage für die Verarbeitung dieser Daten hat der Gesetzgeber nicht geschaffen. Er geht vielmehr davon aus, dass Daten der Angehörigen, die im Personalbereich im Zusammenhang mit dem Beschäftigungsverhältnis des Bediensteten verarbeitet werden, auch als dessen personenbezogene Daten anzusehen sind. Diese Daten werden zudem bei den Beschäftigten, nicht bei den Angehörigen selbst, erhoben. Die Regelungen des NBG zur Verarbeitung der „Daten über Beamte“ erfassen deshalb grundsätzlich auch die Verarbeitung von Daten der Angehörigen. Selbstverständlich muss auch die Verarbeitung dieser Daten für Zwecke der Personalverwaltung oder Personalwirtschaft erforderlich sein. Bezüglich der Daten von volljährigen Angehörigen geht der Gesetzgeber davon aus, dass der Beamte sie mit deren Zustimmung der Personalstelle mitteilt.

Bewerbungsunterlagen

Im Falle einer erfolglosen Bewerbung – sei es, dass der Bewerber in den öffentlichen Dienst aufgenommen werden möchte, sei es, dass er sich als Angehöriger des öffentlichen Dienstes um eine höherwertige Stelle bewirbt – sind alle aus Anlass der Bewerbung verarbeiteten personenbezogenen Daten unverzüglich zu löschen, sobald der Fehlschlag der Bewerbung feststeht (§ 101 Abs. 4 NBG). Dies bedeutet nicht nur, dass die Bewerbungsunterlagen an den Betroffenen zurückzugeben sind und das Bewerbungsschreiben zu vernichten ist, auch die Unterlagen über den Auswahlvorgang dürfen nicht länger aufbewahrt werden.

Gegen die Vernichtung auch der Unterlagen des Auswahlvorgangs ist bei den Gesetzesberatungen eingewandt worden, dass damit eine spätere Prüfung des Auswahlverfahrens, etwa im Falle einer Petition, unmöglich gemacht werde und dass bei späteren personellen Entscheidungen nicht mehr auf eine Zusammenfassung des Ergebnisses der früheren Bewerbungverfahren zurückgegriffen werden könne. Der Gesetzgeber hat diese Einwände nicht aufgegriffen.

Die unverzügliche Löschung der Bewerbungsunterlagen darf erst erfolgen, wenn die Auswahlentscheidung unanfechtbar ist; erst dann steht fest, dass das vom Bewerber angestrebte Dienstverhältnis nicht zustande gekommen ist. Den Belangen eines unterlegenen Mitbewerbers ist damit hinreichend Rechnung getragen. Ein Erfordernis, aus anderen Gründen die Bewerbungsunterlagen weiter aufzubewahren, hat der Gesetzgeber nicht gesehen.

Beihilfedaten

Die besonders sensiblen Beihilfedaten unterliegen einer besonders engen Zweckbindung. Für andere als Beihilfezwecke dürfen sie nur verarbeitet werden, wenn eine Einwilligung der Betroffenen vorliegt oder die Einleitung oder

Durchführung eines behördlichen Verfahrens, das mit dem Beihilfeantrag im Zusammenhang steht, dies erfordert. Im Gegensatz zum Beamtenrechtsrahmengesetz hat es der niedersächsische Gesetzgeber nicht für sachgerecht angesehen, zusätzlich Auskünfte aus Beihilfeakten zur Abwehr erheblicher Nachteile für das Gemeinwohl, unmittelbar drohender Gefahren für die öffentliche Sicherheit oder einer schwerwiegenden Rechtsbeeinträchtigung Dritter (§ 56 a Satz 4 BRRG) zuzulassen. Der Gesetzgeber ist meiner Einschätzung gefolgt, dass eine solche Regelung, die sich ohnehin nur auf Extremfälle beziehen kann, der Beihilfestelle schwierige Abgrenzungsfragen aufbürden würde, die diese in der Regel überfordern dürfte. Zudem hätte eine derartige Vorschrift auch deshalb kaum praktische Bedeutung, weil Unterlagen, aus denen die Art der Erkrankung hervorgeht, dem Antragsteller nach der Entscheidung über den Beihilfeantrag unverzüglich zurückzugeben sind (§ 101 g Abs. 2 Satz 2 NBG). Die Beihilfestelle wäre deshalb praktisch kaum in der Lage, entsprechende Auskunftwünsche zu erfüllen.

Unbegründete Beschwerden

In meinem XIII. Tätigkeitsbericht habe ich unter 14.6 auf die unterschiedliche Behandlung von unbegründeten Beschwerden gegen Beschäftigte hingewiesen. Stellt sich erst nach Aufnahme in die Personalakte heraus, dass eine Beschwerde oder Behauptung unzutreffend war, mussten nach der bisherigen Rechtslage die Unterlagen auf Antrag des Beamten vernichtet werden. Der Bedienstete war damit vor etwaigen nachteiligen Auswirkungen unbegründeter Vorwürfe wirksam geschützt. Anders wurden dagegen Beschwerden behandelt, deren Unbegründetheit von vornherein klar war. Sie wurden zwar nicht zur Personalakte, aber zur Sachakte genommen und konnten damit u. U. noch zum Nachteil des Beamten herangezogen werden.

Ich habe auf eine Beseitigung der unterschiedlichen Behandlung unbegründeter Vorwürfe gedrungen und gefordert, auch Unterlagen über Vorwürfe, die von vornherein als unzutreffend erkannt werden, zu vernichten. Leider ist der Gesetzgeber meinen Anregungen nicht gefolgt; er hat stattdessen eine Angleichung der bisherigen Verfahrensweisen zum Nachteil der Bediensteten vorgenommen. Eine sofortige Vernichtung von zur Personalakte genommenen Unterlagen über unbegründete Vorwürfe ist nach neuem Recht nicht mehr zulässig. Die entsprechenden Aktenbestandteile werden zwar aus der Personalakte entfernt, jetzt aber in einer Sachakte für ein Jahr aufbewahrt (§ 101 f Abs. 1 Satz 1 Nr. 1 und Satz 2 NBG).

Der Gesetzgeber ist davon ausgegangen, auch bei unbegründeten Beschwerden könnte es notwendig werden, die Vorgänge nochmals zu überprüfen, wenn z. B. später erneut Vorwürfe gegen den Beamten erhoben würden. Dahinter steht offenbar die Vorstellung, bei neuen späteren Beschwerden könne sich ein früher als unbegründet angesehener Vorwurf doch noch als zutreffend erweisen. Man darf diese Regelung als Illustration der alten Volksweisheit „etwas bleibt immer hängen“ ansehen.

Weiter bestehen bleibt zunächst auch die Diskrepanz bei den Aufbewahrungsfristen unbegründeter Beschwerden (vgl. XIII 14.6). Die von vornherein haltlose Beschwerde wird nach der Niedersächsischen Aktenordnung fünf Jahre, die erst später als unrichtig erkannte ein Jahr in der Sachakte aufbewahrt. Das Innenministerium hat zwar erklärt, die Aufbewahrungsfrist bei einer Überarbeitung der Aktenordnung einheitlich auf ein Jahr festlegen zu wollen. Ich fürchte jedoch, dass eine grundlegende Revision der Aktenordnung, die ich schon in der Vergangenheit angemahnt habe, weiter verschleppt wird.

13.2 Ärztliche Gutachten über Dienstfähigkeit / Polizeidienstfähigkeit

Die Dienstfähigkeit von Beamten wird aufgrund eines amtsärztlichen Gutachtens durch den unmittelbaren Dienstvorgesetzten - nicht, wie vielfach angenommen wird, durch den untersuchenden Arzt - festgestellt. Bei Polizeivollzugsbeamten kann zur Feststellung der Polizeidienstfähigkeit z. B. ein beamteter Arzt herangezogen werden.

Im Zusammenhang mit der Anforderung und Erstattung solcher ärztlicher Gutachten haben sich häufig Probleme ergeben. Mehrfach haben Amtsärzte die Frage aufgeworfen, welche Unterlagen über den zu untersuchenden Beamten ihnen zur Verfügung gestellt werden dürfen. Zum Teil ist die Vorlage der „gesamten“ Personalakte verlangt worden; ein Amtsarzt hat z. B. Einsicht in die Beihilfeakte verlangt.

Noch größere Unsicherheiten haben sich bei der Frage gezeigt, welche personenbezogenen Daten über die untersuchten Personen an die Dienststellen zu übermitteln seien. In den mir bekannt gewordenen Gutachten sind zum Teil eine Fülle von Aussagen zur Lebensgeschichte der Untersuchten und medizinische Details über weit zurückliegende Beschwerden und Krankheiten festgehalten, bei denen ein Bezug zur Frage der Dienstunfähigkeit sich oft nicht mehr erkennen ließ. So fanden sich z. B. in ärztlichen Gutachten zur Frage der Polizeidienstfähigkeit bei einer Polizeidirektion u. a. folgende Aussagen zur Lebensgeschichte: „warmherzige, mitfühlende und hilfsbereite Mutter“, „Liebesheirat“, „geringe Motivation für die Schule“, „schläft abends vor dem Fernseher ein“, „im Grunde immer leichte Kontaktaufnahme zu Frauen“, „Spaß am Segeln und Surfen“. Zur medizinischen Vorgeschichte wurden u. a. Details wie „1986 Stauchung Mittelgelenk vierter Finger rechts“, „1976 Bissverletzung“, „1964 Spreizfußbeschwerden“, „1965 Bronchitis“ festgehalten. Daneben befanden sich zum Teil eingehende Angaben über Art und Menge von in der Vergangenheit verabreichten Medikamenten in den Gutachten.

Fragen nach dem notwendigen Inhalt amtsärztlicher Gutachten sind auch dadurch ausgelöst worden, dass das Niedersächsische Finanzministerium, das nach seinem Runderlass vom 24. Juni 1996 (Nds. MBl. S. 1090) bei einer vorzeitigen Versetzung von Beamten und Richtern vor Vollendung des 58. Lebensjahres in den Ruhestand zu beteiligen ist (vgl. XIII. 14.7.4), dieser Maßnahme häufiger widersprochen hat. Offenbar hat dies zu einer gewissen Verunsicherung bei den betroffenen Amtsärzten geführt. Da Niedersachsen – im Gegensatz zu anderen Ländern – bislang kein Gesundheitsdienstgesetz erlassen hat, das den begutachtenden Amtsärzten entsprechende Hinweise geben könnte, habe ich angeregt, die dienstrechtlichen Vorschriften über die Versetzung in den Ruhestand im NBG datenschutzgerecht auszugestalten und zudem eine Verwaltungsvorschrift zu diesem Problembereich zu erlassen. Dies ist inzwischen geschehen.

Im Gemeinsamen Runderlass des Ministeriums für Frauen, Arbeit und Soziales sowie des Innenministeriums vom 25. Februar 1998 (Nds. MBl. S. 605) wird im Einzelnen geregelt, welche Unterlagen dem Gesundheitsamt für die Erstellung des Gutachtens zur Verfügung zu stellen sind. Damit wird der datenschutzrechtliche Erforderlichkeitsgrundsatz konkretisiert. Aus der Personalakte dürfen lediglich Auszüge übersandt werden, die für die Erstellung des Gutachtens im Einzelfall erforderlich sind. Eine Einsicht in Beihilfeakten kommt nicht in Betracht. Die in § 101 b Satz 4 NBG festgelegte enge Zweckbindung lässt die Verwendung der Beihilfeakte für andere Zwecke nur zu, wenn dies zur Einleitung oder Durchführung eines behördlichen oder gerichtlichen Verfahrens erforderlich ist, das mit dem Beihilfeantrag im Zusammenhang steht, oder wenn der Beihilfeberechtigte oder die betroffenen Angehörigen im Einzelfall in die Verwendung zu anderen Zwecken einwilligen.

In seinem Gutachten darf der Amtsarzt wiederum der entscheidenden Behörde nur die Daten übermitteln, die für die Beurteilung der Dienstfähigkeit oder ggf. eines anderen Einsatzes des Beamten erforderlich sind. Dazu gehören das Ergebnis der Untersuchung sowie die Darstellung der Auswirkungen gesundheitlicher Beeinträchtigungen auf die dienstliche Tätigkeit. Darüber hinaus dürfen Einzelergebnisse der Anamnese, ergänzende Befunde etc. nur übermittelt werden, wenn dies im Einzelfall für die behördliche Entscheidung erforderlich ist. Für den Fall, dass Zusatzgutachten eingeholt werden müssen, gelten die gleichen Beschränkungen. Das Zusatzgutachten verbleibt grundsätzlich beim Gesundheitsamt. Nur die daraus erforderlichen Angaben werden ergänzend übermittelt. Die bisher manchmal ausufernden Gutachtendarstellungen gehören bei Beachtung dieser Vorschriften der Vergangenheit an.

Der genannte Runderlass gilt allerdings nicht für die Beurteilung der Dienstfähigkeit von Polizeivollzugsbeamten. Für diesen Personenkreis ist das Verfahren in der Polizeidienstvorschrift (PDV) 300 geregelt. Das Innenministerium hat mir jedoch zugesagt, die Polizeiärzte in einem gesonderten Erlass auf die Rechtslage hinzuweisen. Das medizinisch umfassende Gutachten, einschließlich eventuell vorliegender Zusatzgutachten anderer Ärzte, sowie Untersuchungsergebnisse, wie z. B. Laboranalysen und EKG-Befunde, verbleiben somit auch im Polizeibereich künftig beim untersuchenden Arzt.

Der Amtsarzt oder beamtete Arzt, der sich in seinem Gutachten auf die erforderlichen personenbezogenen Angaben beschränkt, ist zur Datenübermittlung befugt. Eine Entbindung von der ärztlichen Schweigepflicht durch den untersuchten Beamten ist nicht notwendig. Werden dagegen medizinische Daten übermittelt, die für die behördliche Entscheidung über die Dienstunfähigkeit nicht erforderlich sind, kann dieses Verhalten den Tatbestand des § 203 StGB (Verletzung von Privatgeheimnissen) erfüllen.

Die Neuregelung macht die Situation auch für den betroffenen Beamten transparent. Er ist vor der Untersuchung auf die Übermittlungsbefugnisse des Amtsarztes hinzuweisen und erhält auf Verlangen eine Abschrift des ärztlichen Gutachtens (§ 59 a Abs. 3 NBG).

13.3 Freie Heilfürsorge

Bei meiner Prüfung einer Polizeidirektion habe ich folgende Verfahrensweise bei der Gewährung von Leistungen der Freien Heilfürsorge an Polizeivollzugsbeamtinnen und –beamte festgestellt: Die vorgelegten Rechnungen über die erbrachten Leistungen werden geprüft und die Rechnungsbeträge – zumeist durch Sammelauszahlungsanordnungen – über die Regierungsbezirkskasse ausgezahlt. Den förmlichen Kassenanweisungen werden dabei gemäß VV Nr. 101 zu § 70 LHO im Einvernehmen mit dem Landesrechnungshof die begründenden Unterlagen nicht (mehr) beigefügt. Sie verbleiben beim Entwurf der Kassenanweisung in der Verwaltung unter Verschluss und werden erst nach Ablauf der durch Haushalts- und Aktenrecht vorgesehenen Fristen vernichtet.

Dagegen werden bei der Beihilfe bereits seit Jahren auszahlungsbegründende Unterlagen weder der Auszahlungsanordnung noch deren Entwurf beigefügt. Zudem bestimmt § 101 g Abs. 2 Satz 2 NBG seit Inkrafttreten der Rechtsänderung, dass Unterlagen, aus denen die Art einer Erkrankung ersichtlich ist, unverzüglich zurückzugeben sind, wenn sie zu dem Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden. Dies betrifft nicht nur Unterlagen der Freien Heilfürsorge, die bisher in der zu führenden Teilakte für fünf Jahre aufbewahrt werden durften (vgl. Nr. 9.2 der VV zu § 101 NBG). Die geänderte Rechtslage muss sich auch auf die Unterlagen auswirken, die aus haushalts- und kassenrechtlicher Sicht entstehen.

Das Innenministerum hat dazu bemerkt, die Abrechnungsverfahren im Beihilfe- und im Heilfürsorgebereich seien nicht vergleichbar. Während bei der Beihilfe die Beamtinnen und Beamten selbst zahlungspflichtig seien und ihre Aufwendungen ihnen anschließend erstattet würden, würden bei der Freien Heilfürsorge die entstehenden Kosten überwiegend direkt mit Krankenhäusern, Apotheken und anderen Leistungserbringern abgerechnet. Zudem müssten im Polizeivollzugsdienst zahlungsbegründende Unterlagen auch zur Abwicklung von Dienstunfällen und von Schadensersatzfällen aufbewahrt werden. Schließlich sei die Notwendigkeit einer Aufbewahrung solcher Unterlagen aus haushaltsrechtlichen Gründen noch zu prüfen.

Ich vermag z. Z. nicht zu erkennen, dass die Unterschiede zwischen Beihilfe und Freier Heilfürsorge den bisherigen Verbleib der zahlungsbegründenden Unterlagen bei der Abrechnungsstelle rechtfertigen können. Mit der Feststellung und Überweisung des Zahlungsbetrages verlieren diese Unterlagen ihre Bedeutung für die Verwaltung ebenso wie bei der Beihilfe. Auf sie braucht nicht mehr zurückgegriffen zu werden. Auch die Argumentation, die Unterlagen müssten – quasi vorsorglich – bei der Abrechnungsstelle verbleiben, weil sich herausstellen könnte, dass ein Dienstunfall vorgelegen habe, leuchtet mir nicht ein. Dies könnte allenfalls in solchen Ausnahmefällen in Betracht kommen, in denen nicht von vornherein feststeht, ob ein Dienstunfall vorliegt oder nicht. Sobald diese Frage geklärt ist, sind die einschlägigen Unterlagen aber zurückzugeben. Haushaltsrechtliche Gründe schließlich können für eine weitere Aufbewahrung nicht herhalten. Darüber bestand im Gesetzgebungsverfahren Einigkeit.

Das Innenministerium will die aufgeworfenen Fragen durch eine Arbeitsgruppe prüfen lassen.

13.4 Automatisierte Verarbeitung von Beihilfedaten

Im Rahmen der Verwaltungsreform hat das Finanzministerium ein neues System der automatisierten Beihilfeabrechnung für Landesbedienstete (samba) – vgl. Nr. 4.12.3 - entwickelt, das das bisherige Großrechner basierte DV-Verfahren ablösen soll. Mit Hilfe des neuen Verfahrens wird die dem Beihilfeberechtigten zustehende Leistung errechnet, der Beihilfebescheid erstellt und die Auszahlung im Datenträgeraustausch mit den Geldinstituten veranlasst. Im Ergebnis soll die Fallbearbeitung weitgehend ohne Beihilfeakte durchgeführt werden können.

Zum Schutz des Persönlichkeitsrechts setzt § 101 h Abs. 1 NBG der automatisierten Verarbeitung von medizinischen Daten allerdings Schranken. Medizinische und psychologische Befunde dürfen nicht in automatisierter Form verarbeitet werden. Zugelassen ist nur eine vorübergehende automatisierte Speicherung dieser Daten, die einen Zeitraum von drei Monaten nicht überschreiten darf. Zudem hat der Gesetzgeber die Aufbewahrungsfristen für Beihilfeunterlagen in herkömmlicher Form eingeschränkt. Unterlagen, aus denen die Art einer Erkrankung ersichtlich ist, sind unverzüglich zurückzugeben, wenn sie für den Zweck, für den sie vorgelegt worden sind, nicht mehr benötigt werden (§ 101 g Abs. 2 NBG). Dieser Zweck erschöpft sich in der Abrechnung der jeweils konkret geltend gemachten Aufwendungen, er kann nicht etwa in einer vom Einzelfall losgelösten Verwendung für Beihilfezwecke allgemein liegen. Wenn der Gesetzgeber eine Datenverarbeitung in Akten für unzulässig erklärt, kann diese im Rahmen eines automatisierten Verfahrens erst recht nicht zugelassen werden.

Probleme ergeben sich nach dieser Rechtslage insbesondere bei der automatisierten Verarbeitung von Gebührenziffern, Angaben über Sehstärken und Indikationen bei Sehhilfen (z. B. Kunststoffgläser, Tönung) sowie bei Diagnosen bei Langzeittherapien oder Dauerverordnungen für Medikamente und Hilfsmittel.

Wenn die geltend gemachten Aufwendungen im Einzelfall nicht beihilfefähig sind, wird die beantragte Leistung entsprechend der einschlägigen Gebührenziffer, insbesondere der Gebührenordnungen für Ärzte und Zahnärzte, gekürzt. Die Gebührenziffern lassen oft Rückschlüsse auf das Krankheitsbild zu (Beispiel: GOÄ Nr. 1761 Operation eines Wasserbruchs). Eine nicht nur vorübergehende automatisierte Verarbeitung dieser Daten scheidet deshalb aus. Aus dem gleichen Grund konnte die vom Finanzministerium zunächst gewünschte Speicherung der Daten über abgerechnete Zahnersatzmaßnahmen (Zahnschema) nicht realisiert werden. Auch Angaben über Sehstärken und Indikationen bei Sehhilfen sowie Diagnosen bei Langzeittherapien sind als Befunddaten anzusehen, deren Speicherung grundsätzlich untersagt ist.

In Erörterungen mit den zuständigen Stellen konnte jedoch im Ergebnis eine zufriedenstellende Lösung dieser Probleme gefunden werden. Künftig soll der Beihilfebescheid in einen Berechnungsteil (mit Rechtsbehelfsbelehrung) und einen Erläuterungsteil (Anlage) gegliedert werden. In den Erläuterungsteil können auch Gebührenziffern und sonstige Angaben mit dem Charakter von Befunddaten aufgenommen werden. Dieser Teil wird für eine etwaige Auskunftserteilung und Widerspruchsbearbeitung lediglich für drei Monate vorgehalten und dann gelöscht. Von einer Speicherung der Daten für das ursprünglich geplante Zahnschema wird abgesehen. Diese Datenverarbeitung hat sich als nicht erforderlich erwiesen. Für Befunddaten, die wie bei einer Dauerverordnung, Indikationen für Sehhilfen etc. über den konkreten Beihilfefall hinaus benötigt werden, wird eine Zustimmung des Beihilfeberechtigten zur automatisierten Speicherung eingeholt. Eine Einwilligung der Angehörigen bezüglich der sie betreffenden Daten ist nach der Konzeption des NBG (vgl. Nr. 13.1) nicht notwendig. Über Sinn und Zweck dieser Datenverarbeitung kann der Berechtigte zugleich mit dem Beihilfebescheid unterrichtet werden. Versagt er seine Einwilligung, muss er bei späteren Anträgen selbst die notwendigen Unterlagen vorlegen. Ich gehe davon aus, dass die weitaus überwiegende Zahl der Beihilfeberechtigten der in ihrem Interesse liegenden Speicherung zustimmen wird.

Technisch basiert das Verfahren auf einer Client-Server-Architektur. Für die Datenhaltung und die Transaktionsverarbeitung kommt ein Informix-Datenbankssystem zum Einsatz. Als Datenbankserver wird ein leistungsfähiger UNIX-Server eingesetzt, der ausschließlich für das Verfahren samba genutzt wird. Die Anwendung wird auf Clients mit dem Betriebssystem Windows NT Workstation ausgeführt, die über das LAN mit dem Datenbankserver kommunizieren. Die Netzwerkverwaltung übernimmt ein Windows NT Server. Alle Clients der Beihilfestelle sind Mitglied der Domäne, die für zentral organisierte Verwaltung und Sicherheit sorgt. Die Daten werden durch die Beihilfesachbearbeiter eingegeben und zentral gespeichert. Bei dem Verfahren samba handelt es sich um eine Eigenprogrammierung der Projektgruppe „Beihilfe neu“ des Niedersächsischen Landesamtes für Besoldung und Versorgung (NLBV).

Das Datenschutz- und Datensicherungskonzept für samba ist bisher nicht ausreichend verwirklicht. Meine Forderung einer verschlüsselten Datenübertragung ist bisher nicht umgesetzt worden. Dabei handelt es sich um Daten der Schutzstufe D, deren Vertraulichkeit während der Übertragung nicht gewährleistet ist. Vertraulichkeit, Integrität und Authentizität der Daten sind nicht ausreichend sichergestellt, solange Manipulation, unbefugte Kenntnisnahme und Fehler während des Transportes nicht ausgeschlossen werden können. Im Hinblick auf die Sensibilität der personenbezogenen Daten bei der Kommunikation im IZN-net halte ich eine Verschlüsselung auch weiterhin für dringend geboten.

Die in diesem Projekt vorgesehene externe Administration und Wartung der eingesetzten IuK-Technik durch das IZN (Fernadministration) bedarf der datenschutzrechtlichen Ausgestaltung. Dabei hat die datenverarbeitende Stelle folgende Datenschutzpflichten zu beachten:

– Eine Wartung der Datenverarbeitungsanlagen durch externe Personen oder Stellen sollte nur dann gewählt werden, wenn eine eigene Wartung nur eingeschränkt oder gar nicht möglich ist.

– Externe Personen oder Stellen, die mit der Wartung oder Systembetreuung von Einrichtungen zur automatisierten Datenverarbeitung betraut sind, haben nach den Weisungen des Auftraggebers zu arbeiten. Der Auftraggeber hat vor Beginn der Arbeiten sicherzustellen, dass der Auftragnehmer personenbezogene Daten nur zur Kenntnis nehmen kann, soweit dies unvermeidbar ist. Ziel muss es sein, den Zugriff auf personenbezogene Daten auszuschließen. Hiervon darf nur abgewichen werden, wenn der Zugriff auf personenbezogene Daten im konkreten Einzelfall unerlässlich ist.

– Die Auftragnehmer haben die technischen und organisatorischen Maßnahmen nach § 9 BDSG bzw. § 7 NDSG zu treffen, die erforderlich sind, um eine datenschutzgerechte Verarbeitung personenbezogener Daten sicherzustellen.

Eine Beauftragung des IZN darf nur erfolgen, wenn die oben aufgeführten Datenschutzpflichten durch technische und organisatorische Maßnahmen erfüllt werden können.

13.5 Pfändungs- und Überweisungsbeschlüsse /Abtretungserklärungen

Die geprüfte Polizeidirektion erhält von der Besoldungsstelle ihrer Bezirksregierung Kopien von Pfändungs- und Überweisungsbeschlüssen und von Abtretungserklärungen, die Gläubiger gegen Bedienstete der Polizeibehörde erwirkt haben. Die Mitteilung erfolgt vordruckmäßig ohne Rücksicht auf die Höhe des gepfändeten bzw. abgetretenen Betrages oder etwaige besondere Umstände, wie das Vorliegen früherer Pfändungen und Abtretungen. Mit dieser Verfahrensweise lebt offenbar eine Verwaltungspraxis fort, die ein inzwischen außer Kraft getretener Runderlass des Finanzministeriums vom 31. August 1981 (Nds. MBl. S. 804) angeordnet hatte. Die Polizeidirektion nimmt die entsprechenden Unterlagen zu einer Sammelakte (Sachakte), in der seit 1982 Pfändungsbeschlüsse und Abtretungserklärungen chronologisch abgeheftet werden.

Ich halte diese undifferenzierte Verfahrensweise nicht für zulässig. Für mich ist nicht ersichtlich, zu welchem Zweck die genannten Unterlagen unterschiedslos zur Sachakte genommen und dort offenbar auf unbestimmte Dauer aufbewahrt werden. Pfändungs- bzw. Abtretungsunterlagen können zwar im Hinblick auf die dienstliche Verpflichtung der Beamtinnen und Beamten zu „würdigem Verhalten“ (§ 62 NBG) im Einzelfall von Belang sein. So kann ein „leichtfertiges Schulden machen“ ein Dienstvergehen darstellen.

Dabei ist allerdings zu beachten, dass von Beamtinnen und Beamten bei außerdienstlichem Verhalten keine Vorbildfunktion (mehr) verlangt wird. Das Beamtenrecht stellt vielmehr ausdrücklich auf die Achtung und das Vertrauen ab, „die der Beruf erfordert“ (vgl. § 62 Satz 2 NBG). Ein Dienstvergehen liegt bei außerdienstlichem Verhalten nach § 85 Abs. 1 Satz 2 NBG nur vor, wenn es im Einzelfall geeignet ist, das Vertrauen in die pflichtgemäße Amtsführung nachhaltig zu beeinträchtigen. Mit dieser 1994 getroffenen Regelung hat der Gesetzgeber bewusst eine Einschränkung der außerdienstlichen Pflichten von Beamten vorgenommen. Ein außerdienstliches Fehlverhalten, das für andere Beschäftigtengruppen im Hinblick auf ihr Dienstverhältnis keine Nachteile mit sich bringt, soll danach auch bei Beamten nur unter erschwerten Voraussetzungen noch als Dienstpflichtverletzung angesehen werden können. Es kommt hiernach nicht (mehr) darauf an, ob das Verhalten einen Verlust des Ansehens des Beamten-

tums nach sich ziehen könnte; vielmehr muss in jedem Einzelfall ein konkreter Bezug zum jeweiligen Amt hergestellt werden.

Nach meiner Einschätzung kann nicht davon ausgegangen werden, dass jede Pfändung und jede Abtretung bei Polizeibeamtinnen und –beamten dienstrechtliche Relevanz in diesem Sinne besitzen. Deshalb darf eine uneingeschränkte Weitergabe entspechender Informationen vom Besoldungsdezernat der Bezirksregierung an die Polizeidirektion nicht erfolgen (vgl. BVerwG, NJW 1987, 1214). Das Gleiche gilt für die Unterrichtung anderer Besoldungsstellen über Pfändungs- und Überweisungsbeschlüsse und Abtretungserklärungen. Die Datenweitergabe und die anschließende Speicherung sind im derzeitigen Umfang zur Aufgabenerfüllung der Personalstelle nicht erforderlich. Soweit im Einzelfall eine Übermittlung derartiger Unterlagen zulässig ist, sind die Pfändungsbeschlüsse und Abtretungserklärungen als Unterlagen, die für den Beamten ungünstig sind oder ihm nachteilig werden können, auf seinen Antrag hin grundsätzlich nach drei Jahren zu vernichten (§ 101 f Abs. 1 Satz 1 Nr. 2 NBG). Eine unbefristete Aufbewahrung in einer Sachakte ist nicht zulässig.

13.6 Tilgung von Disziplinarvorgängen

Bei der Tilgung von Disziplinarvorgängen musste ich häufiger Unzulänglichkeiten feststellen.

13.6.1 Listen über Disziplinarmaßnahmen

Nach Ablauf der Tilgungsfrist sind die Vorgänge aus der Personalakte zu entfernen und zu vernichten. Dabei wird leicht übersehen, dass die Tilgung auch Auswirkungen auf personenbezogene Listen haben muss, die in der Praxis offenbar in vielfältiger Weise über die Disziplinarverfahren einer Behörde geführt werden.

So befand sich in der von mir geprüften Polizeibehörde eine Aufstellung über verhängte Disziplinarmaßnahmen, die alle seit 1962 getroffenen Disziplinarmaßnahmen mit dem Namen der Betroffenen und der Art der disziplinaren Reaktion enthielt, auch wenn die Maßnahmen inzwischen längst getilgt waren.

Eine solche Verwaltungspraxis unterläuft die Tilgungsvorschriften. Nach Ablauf der Tilgungsfristen müssen die Namen der Betroffenen in der zur Fristüberwachung oder aus sonstigen Gründen geführten Liste geschwärzt werden. Vorrangig ist jedoch zu prüfen, ob eine solche Listenführung überhaupt erforderlich ist. Die angesprochene Polizeibehörde kam nach meiner Prüfung zu dem Schluss, dass dies nicht der Fall war.

13.6.2 Tilgungsunterlagen

Auch nach der Tilgung sind die über die Tilgung selbst entstandenen Vorgänge aufzubewahren (§ 5 Abs. 3 TilgVO). Sie sind in einem verschlossenen Umschlag zu einer Sammelakte zu nehmen und verbleiben auch bei einem späteren Dienststellenwechsel des Beamten bei der Dienststelle, bei der sie entstanden sind. Auf diese Unterlagen darf nur zurückgegriffen werden, soweit im Einzelfall Anlass zu einer Überprüfung des Tilgungsverfahrens besteht. Eine Regelung über die Aufbewahrungsdauer enthalten die Tilgungsvorschriften nicht.

Da die Vorgänge als Sachakten anzusehen sind, gelten für sie die Bestimmungen der Niedersächsischen Aktenordnung. Diese sieht vor, dass derartige Vorgänge fünf Jahre aufzubewahren sind. Die Aufbewahrungsfristen beginnen grundsätzlich mit Ablauf des Jahres, in dem die Akten geschlossen worden sind (§ 18

Abs. 4 Nds.AktO). Dies heisst in der Verwaltungspraxis allerdings nicht, dass ein Beamter, gegen den eine Disziplinarmaßnahme verhängt wurde, hoffen kann, nach Ablauf von insgesamt acht oder zehn Jahren (drei bzw. fünf Jahre Tilgungsfrist für Verweis/Geldbuße bzw. Gehaltskürzung zuzüglich fünf Jahre Aufbewahrung der Tilgungsverhandlungen) seien alle Unterlagen über sein früheres Fehlverhalten endlich beseitigt. Denn die Niedersächsische Aktenordnung hat bei der Festlegung der Aufbewahrungsfristen Einzelakten im Auge; den Begriff der Sammelakte kennt sie nicht. Im Falle der als Sammelakte geführten Tilgungsverhandlungen beginnt deshalb nach Ansicht des Innenministeriums die Aufbewahrungsfrist erst mit Ablauf des Kalenderjahres zu laufen, in dem die Sammelakte geschlossen wird. Da die Sammelakte aber auf fortwährende Ergänzungen angelegt ist, wird ein Fristablauf möglicherweise über Jahre hin nicht in Gang gesetzt. Der einzelne Beamte wird damit bezüglich der Vernichtung seiner Tilgungsvorgänge dadurch belastet, dass immer neue, andere Bedienstete betreffende Vorgänge zur Akte hinzukommen können.

Die von mir dagegen erhobenen Bedenken teilt das Innenministerium nicht. Es ist der Meinung, den berechtigten Interessen des Beamten werde dadurch Rechnung getragen, dass die Vorgänge bei der Dienststelle, bei der sie entstanden sind, verbleiben und zudem in einem verschlossenen Umschlag aufbewahrt werden. Außerdem bestünden bezüglich des Inhalts Verwertungsverbote nach den Disziplinarrechts- und Tilgungsvorschriften. Trotz dieser Einschätzung will das Innenministerium der Problematik im Rahmen einer grundlegenden Überarbeitung des Disziplinarrechts nachgehen.

Ich habe der Auffassung, das derzeitige Verfahren beeinträchtige datenschutzrechtliche Belange nicht, entschieden widersprochen. Eine „sichere Aufbewahrung“ und ein Verwertungsverbot können selbstverständlich eine Speicherung personenbezogener Daten nicht rechtfertigen, wenn deren Aufbewahrung überhaupt nicht erforderlich ist. In der Praxis führt die Argumentation des Ministeriums dazu, dass selbst Tilgungsverhandlungen über Bedienstete, die längst aus dem öffentlichen Dienst ausgeschieden oder verstorben sind, weiter unbegrenzt aufbewahrt werden dürfen. Bei der Polizeibehörde habe ich z. B. in einem Fall Tilgungsverhandlungen über einen Beamten gefunden, der vor mehr als zehn Jahren bei der Behörde tätig war und bereits vor Jahren aus dem Landesdienst ausgeschieden ist. Aus Datenschutzsicht ist eine solche Praxis unhaltbar.

Nicht nur der Beginn der Aufbewahrungsfrist von Unterlagen, sondern auch die in der Niedersächsischen Aktenordnung festgelegte Dauer müssen geändert werden. Eine Aufbewahrungsfrist von fünf Jahren steht in keinem angemessenen Verhältnis zur Aufbewahrung der Disziplinarvorgänge. So ist insbesondere nicht einsehbar, warum Disziplinarakten über Verweise und Geldbußen zwei Jahre, die Tilgungsverhandlungen darüber aber fünf Jahre aufbewahrt werden müssen. Das Beispiel zeigt, dass hier Wertungsentscheidungen des Verordnungsgebers im Bereich der Vorschriften zur Aktenführung nicht nachvollzogen worden sind.

Aus meiner Sicht sollte die Lösung des Tilgungsproblems nicht bis zu einer umfassenden Überarbeitung des Disziplinarrechts aufgeschoben werden. Vor einer solchen Rechtsänderung, die möglicherweise noch lange Zeit in Anspruch nehmen wird, sollte das Innenministerium die Frage des Beginns der Aufbewahrungsfrist, die nicht durch Rechtsvorschriften bestimmt wird, kurzfristig im Verwaltungswege datenschutzgerecht lösen.

13.7 Schutz von Telefonverbindungsdaten

Im letzten Tätigkeitsbericht (XIII 14.14) hatte ich darauf hingewiesen, dass Telefonverbindungsdaten über dienstlich geführte Telefonate von Berufsgruppen, die einer besonderen beruflichen Verschwiegenheitspflicht unterliegen, nicht

vollständig erfasst werden dürfen. Das Finanzministerium hatte seinerzeit in Aussicht gestellt, diese Probleme bei einer Überarbeitung der Vorschriften über die Einrichtung und Benutzung dienstlicher Fernmeldeanlagen – Dienstanschlussvorschriften - zu berücksichtigen. Von dieser Überarbeitung wurde Abstand genommen. Die Dienstanschlussvorschriften sind nach der in Niedersachsen geltenden Verfallsautomatik für Verwaltungsvorschriften mit Ablauf des Jahres 1996 außer Kraft getreten. Das Finanzministerium hat jedoch in einem nicht veröffentlichen Schreiben vom 22. Juli 1997 den übrigen Ressorts mitgeteilt, dass die Zielnummern der dienstlichen Telefongespräche von freigestellten Personalratsvorsitzenden/-mitgliedern und solchen, die aus dienstrechtlichen Gründen auf eine Freistellung verzichten, sowie von Frauenbeauftragten und Vertrauensleuten der Schwerbehinderten nicht erfasst und gespeichert werden dürfen. Dies gilt auch für andere Personen im öffentlichen Dienst, die gemäß § 203 StGB einer besonderen beruflichen Geheimhaltungspflicht unterliegen (z. B. Ärzte, Psychologen etc.). Darüber hinaus betont das Finanzministerium, dass die Zielrufnummern der von Bediensteten geführten Privatgespräche in den zu Abrechnungszwecken erstellten Einzelausdrucken um die letzten drei Ziffern zu verkürzen sind. Die Ressorts haben die Dienststellen ihrer Geschäftsbereiche entsprechend unterrichtet.

Nach den dargestellten Grundsätzen ist auch im Bereich der Kommunen und der übrigen mittelbaren Landesverwaltung zu verfahren

14 Kommunalverwaltung

14.1 Öffentliche Auslegung des Schlussberichtes des Rechnungsprüfungsamtes

Nach § 120 Abs. 4 NGO sind die Gemeinden verpflichtet, den um die Stellungnahme des Hauptverwaltungsbeamten ergänzten Schlussbericht des Rechnungsprüfungsamtes öffentlich auszulegen und dabei die Belange des Datenschutzes zu beachten. Mehrere Kommunen haben sich mit der Frage an mich gewandt, wie diese Forderung zu erfüllen ist.

Eine Gemeinde hat die Auffassung vertreten, die Nennung personenbezogener Daten im Schlussbericht sei bis zu dessen Veröffentlichung unverzichtbar, um die geschilderten Sachverhalte nachvollziehen zu können. Ohne personenbezogene Daten sei der Hauptverwaltungsbeamte nicht in der Lage, einen Beanstandungsfall zu bearbeiten und die erforderliche Stellungnahme abzugeben. Auch der Rat habe einen Anspruch darauf, alle mit der Beanstandung zusammenhängenden Fakten – einschließlich der personenbezogenen Daten – zur Kenntnis zu nehmen. Unmittelbar vor der Auslegung könne dann eine Schwärzung erfolgen. Von kommunalen Rechnungsprüfern ist auch die Möglichkeit angesprochen worden, zwei Ausfertigungen des Schlussberichts zu erstellen, eine mit personenbezogenen Daten für die verwaltungsinterne Bearbeitung und eine ohne diese Angaben für die öffentliche Auslegung. In Nordrhein-Westfalen soll in dieser Weise verfahren werden.

Beide Lösungen können nicht befriedigen. Trotz geschwärzter Daten kann nicht selten aus dem textlichen Zusammenhang auf Personen geschlossen werden, so dass diese Vorgehensweise keinen sicheren Datenschutz gewährleistet. Zudem setzt sie voraus, dass eine personenbezogene Darstellung im Schlussbericht zunächst notwendig ist. Die Erstellung von zwei Ausfertigungen des Berichts ist anders als z. B. in der Gemeindeordnung Nordrhein-Westfalens in der NGO nicht vorgesehen. § 120 Abs. 3 NGO verpflichtet das Rechnungsprüfungsamt, seine Bemerkungen in einem Schlussbericht zusammenzufassen.

Ich habe mich in dieser Sache an das Innenministerium gewandt, das wiederum die Arbeitsgemeinschaft der kommunalen Spitzenverbände eingeschaltet hat, um einen Überblick über die in der Praxis gewählten Verfahrensweisen zu erhalten. Dabei hat sich die übereinstimmende Einschätzung ergeben, dass keine Notwendigkeit besteht, einschlägige Sachverhalte im Schlussbericht personenbezogen darzustellen.

Der Schlussbericht des Rechnungsprüfungsamtes soll nach Ablauf eines Rechnungszeitraumes einen Einblick in die von der Kommune abgewickelten Finanzleistungen geben. Einzelfälle, die nicht von herausragender Bedeutung sind, dürften regelmäßig nicht Gegenstand der Ausführungen sein. Sofern im Schlussbericht Einzelfälle aufgeführt werden, müssen sie von solchem Gewicht sein, dass der Rat hierüber – um seine Entscheidung über die Entlastung treffen zu können – unterrichtet werden sollte. Für diesen Fall kann im Schlussbericht zur Anonymisierung beispielsweise auf die Belegnummern, nach denen die Kassenbelege geordnet werden, hingewiesen werden. Eine personenbezogene Unterrichtung des Rats ist grundsätzlich nicht erforderlich.

Eine nach Anzahl und geleisteten Gesamtsummen gebündelte Angabe von Beschaffungs-, Auftragsvergabe- oder Zahlfällen dürfte grundsätzlich ausreichen, die Ausgabenstruktur und –höhe des kommunalen Haushaltes sowie dessen korrekter Abwicklung zu verdeutlichen. Sollten die Hauptverwaltungsbeamtin oder der Hauptverwaltungsbeamte oder der Rat zur Erfüllung ihrer Aufgaben (Stellungnahme nach § 120 Abs. 4 Satz 1 NGO oder Entlastung nach § 101 NGO) im Einzelfall ausnahmsweise personenbezogene Daten benötigen, reicht eine mündliche Erläuterung z. B. in der Schlussbesprechung aus.

14.2 Hähnchendreck und Akteneinsicht

Eine Bürgerinitiative setzte sich gegen die Planungen für einen Hähnchenmastbetrieb mit ca. 40 000 Tieren zur Wehr. Sie überreichte eine Liste mit etwa 1 200 Unterschriften von Gegnern des Vorhabens einem Vertreter der Gemeinde, in der der Betrieb errichtet werden sollte. Die gleiche Liste wurde dem Landkreis zugeleitet. Die Bürgerinitiative protestierte u. a. dagegen, dass die Bevölkerung über den geplanten Mastbetrieb, der eine erhebliche Geruchsbelästigung mit sich bringen werde, nicht unterrichtet worden sei und die Gemeinde dem Bauvorhaben gegenüber der Baugenehmigungsbehörde nicht widersprochen habe. Der Bauherr wandte sich daraufhin an die Gemeinde und erbat Einsicht in die Unterschriftenliste. Nach seiner Darstellung wollte er überprüfen, ob tatsächlich eine so hohe Zahl von betroffenen Bürgerinnen und Bürgern gegen das Vorhaben protestiert habe, ob diese volljährig seien und ob der bekundete Widerstand auf generelle tierschutzrechtliche oder konkrete nachbarliche Befürchtungen hinsichtlich Geruchs- und anderer Belästigungen zurückzuführen sei. Zur Akteneinsicht, die die Gemeinde ohne Umstände gewährte, brachte der Bauherr als „Berater“ einen Landwirt mit, der in einem Nachbarort einen vergleichbaren Hähnchenmastbetrieb betreiben soll. Die Bürgerinitiative war über die Akteneinsicht empört.

Die Zulässigkeit der Akteneinsicht beurteilt sich nach § 1 NdsVwVfG i. V. m. § 29 VwVfG. Eine Akteneinsicht nach § 16 NDSG kommt hier schon deshalb nicht in Betracht, weil der Bauherr nicht die zu seiner Person gespeicherten Daten, sondern die Daten der Hähnchenmastgegner einsehen wollte. § 29 VwVfG gibt den Beteiligten eines Verwaltungsverfahrens bis zu dessen Abschluss ein Recht auf Akteneinsicht, soweit die Vorgänge nicht u. a. wegen der berechtigten Interessen der Beteiligten oder Dritter geheim gehalten werden müssen. Bei dem Verwaltungsverfahren handelt es sich um das Baugenehmigungsverfahren, das allerdings vom Landkreis als Baugenehmigungsbehörde betrieben wird. Die

Gemeinde wirkt an der Entscheidung zur Erteilung der Baugenehmigung nur insoweit mit, als ihr Einvernehmen nach § 36 Baugesetzbuch erforderlich ist. Diese Mitwirkung ist ein behördeninterner Vorgang, der allein der Vorbereitung der Entscheidung über den Bauantrag dient. Zur Gewährung der Akteneinsicht war deshalb nur der Landkreis als Akten führende Behörde befugt (§ 29 Abs. 3 Satz 1 VwVfG).

Ein Anspruch auf Akteneinsicht besteht nur, soweit die Aktenkenntnis zur Geltendmachung oder Verteidigung der rechtlichen Interessen eines Beteiligten erforderlich ist. Ein rechtliches Interesse ist vor allem dann gegeben, wenn die Einsichtnahme bezweckt, eine tatsächliche Unsicherheit über ein Rechtsverhältnis (z. B. den Nachbarstatus) zu klären, ein rechtlich relevantes Verhalten zu regeln oder eine gesicherte Grundlage für die Verfolgung eines Anspruches zu erhalten. Das Recht nach § 29 VwVfG dient nicht dazu, einem Verfahrensbeteiligten allgemein Kenntnis von Behördeninterna zu verschaffen. Aktenbestandteile, die nicht im genannten Sinn zur Rechtsverfolgung notwendig sind, kann die Baugenehmigungsbehörde daher von der Einsicht ausschließen.

Bei Einwendungen gegen ein Bauvorhaben hat die Baugenehmigungsbehörde zu prüfen (vgl. § 73 Absatz 5 NBauO), ob ein Einwender die Nachbareigenschaft besitzt und durch die beantragte Baugenehmigung ggf. in seinen subjektiv-öffentlichen Rechten verletzt ist oder ob er bloß einem allgemeinen Protest gegen das Vorhaben Ausdruck geben will. Bei mangelnder Nachbareigenschaft bleiben Einwendungen unberücksichtigt; ein rechtliches Interesse des Bauantragstellers an der Kenntnis der Identität solcher Einwender ist nicht ersichtlich. Deshalb ist insbesondere bei Unterschriftenlisten durch die Baugenehmigungsbehörde (nicht durch die mitwirkende Gemeinde) zu prüfen, in welchem Umfang Akteneinsicht gewährt werden kann und welche Daten geschwärzt werden müssen.

Die Aufgabe, Bauherren oder Antragsteller von Nachbareinwendungen zu unterrichten (§ 73 Abs. 5 NBauO), obliegt nur dem Landkreis als zuständiger Behörde.

Das Niedersächsische Ministerium für Frauen, Arbeit und Soziales teilt meine Rechtsauffassung.

14.3 Frauenbeauftragte laden ein – am besten mit Einwilligung!

Eine kommunale Frauenbeauftragte fügte der Einladung zu einem Frauentreffen eine Liste mit Namen, Anschriften und Telefonnummern von mehr als 50 anderen, ebenfalls eingeladenen Frauen bei. Die Angaben stammten im Wesentlichen aus einer Übersicht über Teilnehmerinnen einer längere Zeit zurückliegenden Veranstaltung. Die Liste sollte den Eingeladenen zum einen zeigen „wer denn noch so kommen könnte“, zum anderen die Möglichkeit eröffnen, sich über eine Teilnahme abzustimmen Fahrgemeinschaften zu bilden etc.

Leider hat die Frauenbeauftragte bei ihrem sicher gut gemeinten Vorgehen das Datenschutzrecht außer Acht gelassen. Das Versenden der Adressenliste ist eine Übermittlung personenbezogener Daten an Personen außerhalb des öffentlichen Bereichs. Sie ist schon deshalb unzulässig, weil sie zur Aufgabenerfüllung der Frauenbeauftragten nicht erforderlich ist (§ 13 Abs. 1 Satz 1 Nr. 1 NDSG). Das Zustandekommen des Treffens hängt nicht davon ab, dass einer eingeladenen Frau auch Namen und Anschriften der übrigen Eingeladenen mitgeteilt werden. Auch die sonstigen Erlaubnistatbestände des § 13 NDSG waren nicht erfüllt.

Um Ärger zu vermeiden, sollten sich Frauenbeauftragte in solchen Fällen die Einwilligung (§ 4 NDSG) von Teilnehmerinnen ihrer Veranstaltungen geben lassen, auch für später beabsichtigte Treffen auf deren Adressdaten zurückgreifen zu können. Soll jede eingeladene Person mit der Einladung zugleich über die übrigen Eingeladenen unterrichtet werden, muss sich die Einwilligung auch hierauf erstrecken.

15 Niedersächsisches Wassergesetz

Mit dem Elften Gesetz zur Änderung des Niedersächsischen Wassergesetzes (NWG) vom 11. Februar 1998 ist nach langer Diskussion eine Regelung über die Verarbeitung personenbezogener Daten in das Gesetz aufgenommen worden. Nach § 171 NWG findet das NDSG für die Verarbeitung personenbezogener Daten Anwendung. Zur Vermeidung einer Doppelerhebung ist in Abs. 2 in Durchbrechung der strengen Zweckbindung des NDSG die Verarbeitung einmal erhobener Daten auch zu weiteren Zwecken erlaubt.

Ursprünglich hatte ich eine in ihrer Aussage wesentlich differenziertere, die verschiedenen Schritte der Verarbeitung beschreibende Norm gefordert, um so eine für die Bürger nachvollziehbare und für die Verwaltung problemlos umsetzbare Regelung zu treffen, wie sie bereits in anderen Landesgesetzen, z. B. in Schleswig-Holstein und Hessen, zu finden ist. Damit konnte ich mich leider nicht durchsetzen. Nachdem dann jedoch das Fachressort in Abstimmung mit dem Innenministerium eine Art Pauschalklausel zur Diskussion stellte, die aus meiner Sicht wegen ihrer mangelnden Konkretheit in keiner Weise den verfassungsrechtlichen Anforderungen an eine normenklare bereichsspezifsche Regelung entsprach, habe ich im Rahmen des weiteren Gesetzgebungsverfahrens die Verweisung auf das NDSG vorgeschlagen, um zumindest deutlich zu machen, nach welchen Regelungen der Datenschutz zu erfolgen hat. Diesem Vorschlag ist der Gesetzgeber weitgehend gefolgt, indem er § 171 in der nunmehr vorliegenden Form verabschiedete.

16 Bau-, Wohnungs- und Vermessungswesen

16.1 Selbstauskunft gegenüber einem Wohnungsbauunternehmen

Auf Bitten einer Abgeordneten des Niedersächsichen Landtags habe ich das Selbstauskunftsverfahren eines hannoverschen Wohnungsbau-unternehmens bei der Vergabe von Sozialwohnungen überprüft. Der Fragebogen des Unternehmens enthielt einige Angaben, die für die Vergabe der Wohnungen nicht erforderlich waren und daher datenschutzrechtlich bedenklich schienen. So wurde das Datum der Eheschliessung bzw. der Verwitwung erfragt und eine pauschale Zustimmung zur Übermittlung der Daten an eine Auskunftei sowie ihre Überprüfung durch die Auskunftei gefordert. Der notwendige Hinweis auf die Freiwilligkeit der Angaben fehlte ganz.

Ich konnte erreichen, dass die kritisierten Fragen und die Einwilligung zur Datenübermittlung an die Auskunftei aus dem Fragebogen entfernt wurden. Das Unternehmen sagte zu, zukünftig auf die Freiwilligkeit der Angaben in der Selbstauskunft hinzuweisen.

16.2 Wo bleibt das neue Vermessungs- und Katastergesetz?

Die längst überfällige Anpassung des Vermessungs- und Katastergesetzes an die Grundsätze des Volkszählungsurteils steht noch immer aus. Dateninhalt, Nutzung und automatisierter Abruf müssen normenklar geregelt werden. Die Zusage des Innenministeriums zur Novellierung wurde bisher nicht eingehalten.

17 Finanzverwaltung

17.1 Datenschutz in der Abgabenordnung – kein „happy end“ in Sicht

Die langjährigen Bemühungen der Datenschutzbeauftragten des Bundes und der Länder um konkrete Datenschutzregelungen in der Abgabenordnung sind trotz zugesagter Unterstützung des Niedersächsischen Finanzministeriums auf Bundesebene gescheitert. Dabei hatten sich die Datenschutzbeauftragten viel Mühe gemacht und auf 21 Seiten ihre Vorschläge detailliert dargelegt und begründet. Die Steuerverwaltung vertritt jedoch mehrheitlich die Auffassung, mit dem Steuergeheimnis in § 30 Abgabenordnung (AO) seien alle Vorkehrungen für den Datenschutz hinreichend vorhanden. Die Rechtsprechung des Bundesverfassungsgerichts zum Volkszählungsgesetz sei nicht auf den Bereich der Steuerverwaltung übertragbar, weder das Bundesverfassungsgericht noch der Bundesfinanzhof hätten bisher Vorschriften der Abgabenordnung aus datenschutzrechtlicher Sicht beanstandet. Jede Änderung des Wortlauts der AO werfe die Frage auf, ob die seit nahezu 80 Jahren zum alten Wortlaut ergangene Rechtsprechung Makulatur geworden sei.

Das Bundesverfassungsgericht hat es allerdings in seiner Entscheidung zum Flick-Untersuchungsausschuss (BVerfGE 67, 100) ausdrücklich offen gelassen, ob alle Tatbestände des § 30 AO den verfassungsrechtlichen Anforderungen an den Schutz individualisierter und individualsierbarer steuerlicher Daten genügen (a.a.O. S.144). In seinen Erwägungen zu den Grenzen zulässiger Kontrollmitteilungen berücksichtigt der Bundesfinanzhof ebenfalls datenschutzrechtliche Grundsätze (Urteil vom 18.02.1997, NJW 1997, 2067, 2072). Ausgangspunkt der Vorschläge der Datenschutzbeauftragten zur Regelung dieses Bereichs war der Gesetzentwurf des Bundes zur Änderung der Abgabenordnung (AOÄG 1994). Dieser Entwurf begründete – wie schon der vorangehende Entwurf für ein AOÄG 1993 – die darin vorgeschlagenen bereichsspezifischen Regelungen der Abgabenordnung im Wesentlichen damit, sie seien Ausdruck einer Interessenabwägung zwischen dem durch das Recht auf informationelle Selbstbestimmung garantierten Schutz personenbezogener Daten und der Verpflichtung der Finanzbehörden, die Steuern nach Artikel 3 GG gleichmäßig festzusetzen. Im Laufe der Arbeiten am Gesetzentwurf änderte das Bundesfinanzministerium seine Auffassung hinsichtlich des weiteren Regelungsbedarfs datenschutzrelevanter Fragen in der Abgabenordnung grundlegend, reduzierte die vorgesehenen Vorschriften auf Ergänzungen des § 30 AO und sah schließlich ganz von einer Änderung ab.

Fortschreitende technische Entwicklungen im Bereich der automatisierten Datenverarbeitung, die Öffnung neuer Informations- und Kommunikationstechniken auch für die Steuerfestsetzung im online-Betrieb sowie die sich abzeichnenden Nutzungsmöglichkeiten des Internet zur elektronischen Kommunikation zwischen den Finanzbehörden untereinander und mit den Steuerpflichtigen erfordern neue datenschutzrechtliche Maßnahmen. Die technischen Möglichkeiten zum schnellen Datenaustausch und -abgleich machen auch aus Gründen des Schutzes des Steuergeheimnisses Vorkehrungen notwendig, die nicht nur die Glaubwürdigkeit der Steuerverwaltung im Umgang mit den ihr anvertrauten Daten untermauern helfen, sondern auch den neuen Risiken für die Persönlich-

keitsrechte der betroffenen Steuerpflichtigen begegnen. Nicht zuletzt auch die Umsetzung der EU-Datenschutzrichtlinie gibt Anlass, die Abgabenordnung aus der Sicht des Datenschutzes zu überprüfen.

17.2 Vereinfachte Besteuerung oder Überwachung der Berater

Niedersächsische Steuerberater haben sich an mich gewandt und Bedenken gegen die geplante Einführung einer Beraterdatei der Finanzverwaltung geäußert. Die neue Beraterdatei hat zum einen die Aufgabe, die Adressdaten der Steuerberater für die Steuerbearbeitung durch die Finanzbehörden zu speichern. Zugleich soll aber auch eine Überwachung der fristgerechten und zulässigen Bearbeitung durch Angehörige der steuerberatenden Berufe und der Lohnsteuerhilfevereine ermöglicht werden. Das Niedersächsische Finanzministerium begründet die Überwachungsfunktion mit dem Hinweis auf § 80 Abs. 5 i. V. m. §§ 5 bis 7 Steuerberatungsgesetz. Diese Rechtsvorschrift begründet jedoch nur eine Aufgabenzuweisung und kann nicht als eine ausreichende Rechtsgrundlage angesehen werden. Eine solche Rechtsgrundlage muss Art der personenbezogenen Daten sowie Zweck und Erforderlichkeit der Datenverarbeitung normenklar festlegen und den Grundsatz der Verhältnismässigkeit erfüllen.

Ich habe keine grundsätzlichen Bedenken gegen eine Verwendung der Beraterdatei zu Zwecken der eigentlichen Steuersachbearbeitung. Auch anonyme Auswertungen der Beratungsfälle wären datenschutzrechtlich unbedenklich. Dagegen sehe ich die Auswertung und Auflistung aller erledigten und unerledigten Steuerfälle eines Beraters als unzulässig an. Für die betroffenen Steuerpflichtigen und die an der Steuererklärung beteiligten Berater ist nicht ausreichend klar erkennbar, in welcher Weise ihre Daten ausgewertet und genutzt werden. Meine Umfrage bei den Datenschutzbeauftragten des Bundes und der Länder hat ergeben, dass entsprechende Beraterdateien nur in vier Ländern eingeführt worden sind. In keinem der vier Bundesländer wurde eine so weitgehende Zweckbestimmung gewählt.

Das Niedersächsische Finanzministerium hat sich meine Bedenken in einem Gespräch erläutern lassen und eine intensive Prüfung vor einer endgültigen Entscheidung zugesagt. Die Entscheidung steht noch aus.

17.3 Öffentlicher Pranger der Steuerberaterkammer

Die Steuerberaterkammer Niedersachsen – eine Körperschaft des öffentlichen Rechts - veröffentlicht regelmäßig in ihren Mitteilungsblättern personenbezogene Daten von Personen, gegen die die Steuerberaterkammer wegen unerlaubter Hilfe in Steuersachen oder unerlaubter Werbung rechtlich vorgegangen ist. Veröffentlicht werden Verurteilungen und strafrechtliche Unterlassungserklärungen mit Angabe von Name, Anschrift, Aktenzeichen und Grund. Übereinstimmend mit den Datenschutzbeauftragten der Länder vertrete ich die Ansicht, dass dies unzulässig ist. Die Mitteilungen stellen datenschutzrechtlich „ein Übermitteln personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs“ dar. Steuerberater und andere Mitglieder der Steuerberaterkammer sind als Dritte anzusehen. Sie sind nicht Mitarbeiter der Kammer, sondern Selbstständige, die der Aufsicht der Kammer unterliegen und deren Interessen von der Kammer vertreten werden. Dies gilt auch für Rechtsanwälte, die gemäß § 3 Abs. 1 Nr. 2 Steuerberatungsgesetz (StBerG) zu unbeschränkter Hilfeleistung in Steuersachen befugt sind und auf Anfrage die Kammermitteilungen erhalten.

Nach § 4 Abs. 1 NDSG ist die Verarbeitung personenbezogener Daten zulässig, wenn die Betroffenen eingewilligt haben oder das NDSG oder eine andere Rechtsvorschrift dies vorsieht. Eine Einwilligung scheidet hier aus. Auch bereichsspezifische Vorschriften, die eine derartige Veröffentlichung ausdrücklich erlauben würden, sind nicht erkennbar. Selbst der vielfach genannte § 76 StBerG scheidet aus, da es sich bei dieser Regelung nur um eine gesetzliche Aufgabenzuweisung und nicht um eine datenschutzrechtliche Befugnisnorm handelt. Ein Eingriff in das verfassungsrechtlich geschützte Recht auf informationelle Selbstbestimmung erfordert eine normenklare Ermächtigungsgrundlage. Die bloße gesetzliche Aufgabenzuweisung an eine Behörde verleiht dieser keine Befugnis zur Datenweitergabe an Dritte.

Auch § 23 des Gesetzes gegen den unlauteren Wettbewerb (UWG) scheidet als generelle Bekanntmachungsnorm aus, weil diese Vorschrift eine ausdrückliche gerichtliche Anordnung verlangt. Wegen des Richtervorbehalts läßt sich die Vorschrift auch nicht auf solche Fälle anwenden, in denen das Gericht eine entsprechende Anordnung nicht getroffen hat bzw. in denen gar kein gerichtliches Verfahren stattgefunden hat.

Die fragliche Veröffentlichung in den Mitteilungsblättern läßt sich auch nicht mit dem Niedersächsischen Datenschutzgesetz rechtfertigen. § 13 Abs. 1 NDSG läßt die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs nur dann zu, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Daten nach § 10 verarbeitet werden dürfen,
2. 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, oder
3. sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und die Betroffenen in diesen Fällen der Übermittlung nicht widersprochen haben.

Keine der Zulässigkeitsalternativen trifft zu. Erforderlich ist eine Übermittlung nur dann, wenn ohne sie die Aufgabe überhaupt nicht, nicht vollständig, nicht rechtzeitig oder nur mit unverhältnismässigen Schwierigkeiten erfüllt werden kann. Dabei ist wegen des bei Eingriffen in das Recht auf informationelle Selbstbestimmung zu beachtenden Grundsatzes der Verhältnismäßigkeit ein strenger Maßstab anzulegen. Bei einer „Veröffentlichung zur Überwachung“ erhält eine unbestimmte Vielzahl von Personen, die keineswegs nur Kammermitglieder sind, Kenntnis von Sanktionen gegen Betroffene. Die Veröffentlichung entfaltet damit eine erhebliche und unzulässige Prangerwirkung. Auch kann nicht davon ausgegangen werden, dass die Betroffenen nach verhängten Maßnahmen weiterhin gegen einschlägige Vorschriften über die Ausübung des Steuerberaterberufs verstoßen werden. Auswertungen in Schleswig-Holstein zeigen nämlich, dass bei jährlich erstrittenen ca. 60 Unterlassungserklärungen nur ca. 5 Wiederholungsfälle auftreten. Dabei konnte nicht festgestellt werden, dass die Anzeigen durch Kammerveröffentlichungen initiiert worden sind.

Die praktizierte Veröffentlichung ist nach diesen Betrachtungen nicht gerechtfertigt. Nach übereinstimmender Ansicht der Datenschutzbeauftragten der Länder verstößt die Veröffentlichung gegen das Recht auf informationelle Selbstbestimmung der Betroffenen. Die Steuerberaterkammern in Berlin, Sachsen-Anhalt und Schleswig-Holstein haben nach Beanstandungen ihrer Landesdatenschutzbeauftragten die problematische namentliche Veröffentlichung eingestellt.

In den übrigen Ländern sind die Diskussionen noch im Gange. Entscheidungen stehen noch aus.

Ich habe die Steuerberaterkammer Niedersachsen aufgefordert, künftig von derartigen Veröffentlichungen abzusehen. Meiner Forderung wurde inzwischen gefolgt; eine Veröffentlichung von Namen wird nicht mehr erfolgen. Allerdings konnte sich die Steuerberaterkammer den Hinweis nicht „verkneifen“, dass damit eine Rechtspflicht nicht anerkannt werde.

17.4 Aktenanforderung durch Gerichte

Der Versand der vollständigen Akte eines Versorgungsempfängers nach undifferenzierter Aktenanforderung des Niedersächsischen Finanzgerichts war erneut Anlass einer Anrufung. Die Akte enthielt neben den für den anhängigen Rechtsstreit bedeutsamen Teilen auch eine ganze Reihe von irrelevanten, sehr persönlichen Daten des Petenten. Die Versendung vollständiger Versorgungsakten widerspricht geltenden Datenschutzvorschriften und steht im Widerspruch zum Sozialgeheimnis.

Meine Bitte an das Niedersächsische Finanzgericht, trotz meiner fehlenden Kontrollzuständigkeit zu dem allgemeinen Problem der Aktenübersendung und zu dem konkreten Beschwerdevorgang Stellung zu nehmen, wurde mit dem Hinweis auf das Steuergeheimnis nach § 30 Abgabenordnung abgelehnt. Dadurch hat sich die Beantwortung der Bürgeranrufung verzögert. Der Hinweis auf das Steuergeheimnis geht von einer unrichtigen Beurteilung der Rechtslage aus. Die Datenschutzkontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. § 24 Abs. 2 Satz 1 BDSG nennt als Beispielsfall ausdrücklich das Steuergeheimnis, das somit Auskünften an den Bundesbeauftragten für den Datenschutz nicht entgegengehalten werden kann. Für die Landesbeauftragten für den Datenschutz gilt die Vorschrift nach § 24 Abs. 6 BDSG entsprechend.

Mein Eingreifen hat dazu geführt, dass im Bereich der Versorgungsverwaltung der besondere Aspekt des Datenschutzes bei der Übersendung von Versorgungsakten an Gerichte deutlich mehr Gewicht erhält. Im Bereich der Justiz ist man bemüht, dieses Thema bei der richterlichen Fortbildung verstärkt zu berücksichtigen. Eine befriedigende und datenschutzfreundliche Lösung wird nur zu erreichen sein, wenn die Gerichte die Anforderung von Akten auf das notwendige Mass beschränken und die abgebenden Behörden prüfen, inwieweit die Akten für den entsprechenden Rechtsstreit überhaupt von Bedeutung sind.

17.5 Datenübermittlung zwischen Finanzbehörden und Deichverbänden

Bereits seit längerer Zeit übermitteln Finanzämter den Deichverbänden für im Verbandsgebiet gelegene Grundstücke die jeweiligen Einheitswerte in automatisierter Form. Mehrere Eingaben haben mich auf dieses Verfahren aufmerksam gemacht. Auch wenn rechtlich gegen dieses Verfahren keine Einwände zu erheben sind, zeigen die Eingaben der betroffenen Bürger, dass es erhebliche Informationsdefizite gibt. Die Tatsache der Datenübermittlung war in der vorgelegten Satzung nur am Rande erwähnt, so dass Unklarheiten über die rechtliche Zulässigkeit fast zwangsläufig auftreten mussten. Es ist sicher verwaltungsökonomisch und kostensparend, wenn benötigte Daten im Rahmen der geltenden Gesetze zwischen Behörden unmittelbar ausgetauscht werden; dennoch sollte es seitens der beteiligten Behörden eine Selbstverständlichkeit sein, diesen praktizierten Datenaustausch den Betroffenen offenzulegen und ihnen die rechtlichen Grundlagen zu erläutern. Ich habe das zuständige Fachministerium gebeten, in diesem Sinne auf die entsprechenden Verbände einzuwirken.

18 Soziales

18.1 Einschränkung des Sozialdatenschutzes

Seitdem die öffentlichen Kassen leer sind, reißt die Diskussion darüber, wie ein Missbrauch von Sozialleistungen verhindert werden kann, nicht ab. Spektakuläre Einzelfälle, über die in den Medien berichtet wird, beflügeln diese Diskussion, die auch von Politikern oft in sehr populistischer Weise geführt wird. Gefordert werden insbesondere zunehmende Datenabgleiche zwischen den unterschiedlichsten Behörden und sonstigen Stellen, durch die man einem vermuteten Sozialleistungsbetrug auf die Spur kommen will. Dass es in diesem wie in anderen Lebensbereichen – man denke nur an Steuerhinterziehungen – auch Missbräuche gibt, kann nicht bestritten werden. Über ihr Ausmaß bestehen jedoch weit voneinander abweichende Auffassungen. Verlässliches Zahlenmaterial, das auch nur eine ungefähre Einschätzung der Größenordnung dieses Problems zuließe, gibt es nicht. Keine Frage: Es ist die Pflicht des Staates, unberechtigtem Leistungsbezug entgegenzutreten. Dies muss jedoch in einer Weise geschehen, die diejenigen, die auf Sozialleistungen angewiesen sind, nicht von vornherein als potentielle Betrüger behandelt und ohne konkreten Anlass einer umfassenden Missbrauchskontrolle unterwirft. Alle Maßnahmen, die zur Bekämpfung von Leistungsmissbrauch ergriffen werden, müssen den verfassungsmäßigen Grundsatz der Verhältnismäßigkeit beachten. Unter diesem Gesichtspunkt sind Datenabgleiche, die für Kontrollmaßnahmen ohne konkreten Verdacht im Einzelfall durchgeführt werden, besonders problematisch. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1994 ihre Besorgnis über diese Entwicklung, die zu einem immer dichteren Datenverbundsystem im Sozialleistungsbereich und damit zu immer stärkeren Eingriffen in das Recht der Betroffenen auf informationelle Selbstbestimmung führt, geäußert (vgl. XII, Anlage 12).

Sozialhilfedatenabgleichsverordnung

Schon das Gesetz zur Umsetzung des föderalen Konsolidierungsprogramms hat 1993 in § 117 BSHG die Grundlage geschaffen, dass Sozialhilfeträger untereinander sowie mit der Bundesanstalt für Arbeit und den Trägern der gesetzlichen Unfall- und Rentenversicherung regelmäßig Daten über erbrachte Sozialleistungen abgleichen können. Die erforderliche Verordnung zur Umsetzung dieser Vorschrift ist jedoch erst am 1. Januar 1998 in Kraft getreten. Danach können die Sozialleistungsträger regelmäßig einen Datensatz mit Angaben über Name, Geburtsort, Nationalität, Geschlecht, Anschrift und Versicherungsnummer an eine zentrale Vermittlungsstelle bei der Dienststelle der Rentenversicherungsträger übermitteln. Der Datenabgleich zeigt, ob und ggf. welche Sozialleistungen für die betreffende Person im Leistungszeitraum von anderen Sozialleistungsträgern erbracht worden sind.

Da diese Verfahrensweise keinen konkreten Missbrauchsverdacht im Einzelfall voraussetzt, greift sie erheblich in das Grundrecht der Betroffenen auf Datenschutz ein. Immerhin soll auf Drängen des Bundesbeauftragten für den Datenschutz durch ein Sozialforschungsinstitut eine Untersuchung mit dem Ziel einer Erfolgskontrolle dieses Verfahrens durchgeführt werden. Ein entsprechender Bericht wird für Mitte 1999 erwartet. Er soll Erkenntnisse über Effizienz und Verhältnismäßigkeit derartiger Verfahren bringen. Es bleibt zu hoffen, dass mit dem Bericht auch eine geeignete Grundlage für eine Versachlichung der Diskussion über das Problem des Leistungsmissbrauchs im Sozialbereich zur Verfügung stehen wird.

Geplante weitere Datenabgleiche

Schon bevor der Datenabgleich nach § 117 Abs. 1 und 2 BSHG möglich wurde, hatte die Konferenz der Arbeits- und Sozialminister (ASMK) im Herbst 1995 eine Arbeitsgruppe „Verbesserter Datenaustausch bei Sozialleistungen“ eingesetzt, die weitere Möglichkeiten zur Ausweitung von Datenabgleichen prüfen soll. Zu dem Bericht der Arbeitsgruppe hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die als Anlage 6 beigefügte Entschließung gefasst.

Sozialleistungsmissbrauchs-Ermittler

In der Diskussion um die Bekämpfung des Missbrauchs bei Sozialleistungen ist in jüngster Zeit häufiger der Einsatz von „Sozialdetektiven“, „Sozialleistungskontrolleuren“ u. Ä. gefordert worden. Dabei bleibt oft unklar, ob hiermit Außendienstmitarbeiter gemeint sind, die vor Ort die Berechtigung einer bestimmten Sozialleistung überprüfen sollen und in diesem Zusammenhang Feststellungen treffen, oder ob es um die gezielte Überprüfung vermuteten Leistungsmissbrauchs geht. In diesem Zusammenhang weise ich auf folgende zu beachtende datenschutzrechtliche Grundsätze hin:

1. Der Sozialleistungsträger darf (beim Betroffenen) angemessene Zeit nach Bewilligung einer Sozialleistung auch ohne Anhaltspunkte für einen Leistungsmissbrauch prüfen, ob die Anspruchsvoraussetzungen noch erfüllt sind. Dazu wird in der Regel eine schriftliche Befragung des Leistungsempfängers, dessen Vorladung oder ein Datenabgleich nach § 117 BSHG ausreichen.

2. Der Einsatz eines „Missbrauchsermittlers“ kann – als stärkere Beeinträchtigung der Betroffenen – nur in Betracht kommen, wenn diese Möglichkeiten keinen Erfolg versprechen und konkrete Anhaltspunkte für einen Leistungsmissbrauch im Einzelfall vorliegen. Dagegen wäre es nicht erforderlich und damit unzulässig, einen „Missbrauchsermittler“ einzusetzen, um erst Anhaltspunkte für einen möglichen Missbrauchsverdacht (Verdachtschöpfung) zu gewinnen.

3. Der „Missbrauchsermittler“ hat ohne Einwilligung des Hilfeempfängers keinen Zutritt zu dessen Wohnung. Der Außendienstmitarbeiter muss seinen Prüfauftrag offen legen und den Betroffenen darauf hinweisen, ob er zur Auskunft verpflichtet ist und welche Folgen sich bei einer verweigerten Mitwirkung ergeben. Eine Datenerhebung bei anderen als Leistungsträgern (z. B. Hauseigentümern, Vermietern, Nachbarn) darf der Ermittler nur unter den Voraussetzungen des § 67 a Abs. 2 Nr. 2 SGB X vornehmen. Dabei dürfen durch die Erhebung keine überwiegenden schutzwürdigen Interessen des Betroffenen verletzt werden.

4. Grundsätzliche Bedenken bestehen gegen eine „verdeckte“ Beobachtung von Sozialhilfeempfängern. Ein Ausspähen von Hilfeempfängern ist im Sozialgesetzbuch nicht vorgesehen. Die besondere Schwere eines solchen Eingriffs in das Persönlichkeitsrecht des Betroffenen liegt neben der Heimlichkeit der Vorgehensweise darin, dass dem Ermittler eine Vielzahl von Daten aus der Privatsphäre zur Kenntnis gelangen würde, die zur Prüfung eines Leistungsmissbrauchs nicht erforderlich sind.

5. Bei Einsatz eines „Missbrauchs-Ermittlers“ ist der Ablauf des Ermittlungsverfahrens aktenmäßig so festzuhalten, dass das Vorgehen des Sozialamtsmitarbeiters überprüft werden kann.

Sozialbehörden als Außenstellen der Polizei

Unter dem Titel „Erstes Gesetz zur Änderung des Medizinproduktegesetzes“ hat der Deutsche Bundestag 1998 das Sozialgeheimnis weiter eingeschränkt. Bei den Ausschussberatungen zu diesem Gesetz ist kurzfristig eine Änderung des § 68 SGB X eingefügt worden. Der zuständige Fachausschuss wurde dabei nicht beteiligt. Die Rechtsänderung, irreführend als „Klarstellung“ bezeichnet, greift die in letzter Zeit häufig diskutierte Frage auf, ob Sozialämter der Polizei oder der Staatsanwaltschaft auf deren Ersuchen hin mitteilen dürfen, ob sich ein Leistungsempfänger im Sozialamt aufhält. Zu diesem Problembereich habe ich mich im XIII. Tätigkeitsbericht unter 19.6 geäußert. Nach meiner Auffassung durfte bereits nach der bisherigen Rechtslage der momentane Aufenthalt eines Hilfeempfängers in einer Sozialbehörde mitgeteilt werden. Auskünfte über geplante zukünftige Aufenthalte, z. B. einen vereinbarten Gesprächstermin, durften dagegen nur gegeben werden, wenn z. B. ein Sozialhilfebetrug oder eine entsprechende richterliche Anordnung im Strafverfahren wegen eines Verbrechens oder einer anderen Straftat von erheblicher Bedeutung vorlagen. Dies ist auf Kritik gestoßen.

Aus meiner Sicht hätte durchaus in Erwägung gezogen werden können, Sozialbehörden zu verpflichten, die notwendigen Daten von mit Haftbefehl gesuchten Sozialleistungsempfängern an die Strafverfolgungsbehörden weiterzugeben. Die jetzige Änderung des § 68 SGB X sieht dagegen vor, dass sämtliche Sozialleistungsträger, neben den Sozialämtern z. B. auch Jugendämter, Arbeitsämter, gesetzliche Krankenkassen, Berufsgenossenschaften, Versorgungsämter Auskunft über die derzeitige Anwesenheit oder künftige Vorsprachetermine Ratsuchender zu geben haben. Zwar spricht das Gesetz nur von einer Befugnis zur Datenübermittlung, die entsprechende Verpflichtung hierzu ergibt sich jedoch aus den Amtshilfevorschriften des SGB X. Das Vertrauensverhältnis, das vor allem aus fachlicher Sicht immer wieder als grundlegende Voraussetzung einer erfolgreichen Arbeit der Sozialleistungsträger genannt wird und das in den einzelnen Aufgabenfeldern des Sozialbereichs unterschiedlich ausgeprägt ist, hat der Gesetzgeber mit dieser undifferenzierten Regelung unberücksichtigt gelassen. Eine Differenzierung enthält das Gesetz auch nicht im Hinblick auf die Aufgaben, für die die Daten verarbeitet werden dürfen. Polizeibehörden, Staatsanwaltschaften, Gerichte, Behörden der Gefahrenabwehr und Justizvollzugsanstalten können die in Rede stehenden Daten für ihre sämtlichen Aufgaben fordern. Vorgeschrieben ist selbst eine Datenübermittlung für die Durchsetzung öffentlich-rechtlicher Ansprüche in Höhe von mindestens 1 000,-- DM. Die Regelung ist zwar primär für die Zusammenarbeit zwischen Polizei und Sozialämtern gedacht, der Einfachheit halber hat sie der Gesetzgeber aber auf zahlreiche öffentliche Stellen erstreckt. Den Hilfesuchenden wird sich der Eindruck aufdrängen, die Sozialleistungsträger seien insgesamt Teil des polizeilichen Fahndungsapparates.

Wie wenig der Gesetzgeber die Rechtsänderung durchdacht hat, zeigt sich auch in Folgendem: Nach § 73 Abs. 2 und 3 SGB X kann der Richter zur Durchführung eines Strafverfahrens wegen einer Straftat, die weder als Verbrechen noch als Straftat von erheblicher Bedeutung anzusehen ist, die Übermittlung von Sozialdaten anordnen. In diesem Falle darf der künftige Aufenthalt des Sozialleistungsempfängers nicht mitgeteilt werden. Bei einer bloßen Ordnungswidrigkeit ist diese Übermittlung dagegen nach der Neufassung des § 68 SGB X zulässig.

18.2 Pflegeversicherung

Einer Pflegekasse habe ich mitgeteilt, dass gegen die Übermittlung der im Rahmen der Durchführung des Pflegeversicherungsgesetzes erhobenen Daten zur Erstattung einer Strafanzeige gegen Leistungsmissbrauch, soweit nur die erforderlichen Daten übermittelt werden, keine datenschutzrechtlichen Bedenken bestehen. Diese Datenübermittlung ist gemäß § 69 Abs. 1 Ziff. 1, 2. Fall SGB X (Erfüllung sonstiger eigener Aufgaben der übermittelnden Stelle) zulässig.

18.3 Amtshilfeersuchen einer Landesversicherungsanstalt

Bei der Bearbeitung von Schadensersatzforderungen, die durch Schuldanerkenntnis oder einen anderen Titel festgestellt worden sind, geht eine Landesversicherungsanstalt (LVA) in Niedersachsen wie folgt vor: Da Anfragen beim Schuldner nach seinen Einkommens- und Vermögensverhältnissen – so die Darstellung der Behörde - „in aller Regel“ erfolglos bleiben und ein Antrag beim zuständigen Amtsgericht auf Abgabe einer eidesstattlichen Versicherung im Interesse des Schuldners möglichst vermieden werden soll, wendet sich die LVA an die Wohnortgemeinde des Schuldners und bittet diese, die erforderlichen Daten beim Schuldner zu erheben. In der Regel wird der Schuldner dazu vom Ordnungsamt der betreffenden Gemeinde vorgeladen und dort ein Fragebogen über seine Einkommens- und Vermögensverhältnisse mit ihm ausgefüllt. Die LVA hat dieses Vorgehen mit Hinweis auf die Amtshilfevorschriften begründet.

Diese sind hier allerdings nicht anwendbar. Bei der Ermittlung eines Sachverhalts im Sozialleistungsbereich treten die Amtshilfevorschriften gegenüber den speziellen Regelungen zur Datenerhebung im SGB X zurück. Zudem liegen aus meiner Sicht die Voraussetzungen für eine Amtshilfe nicht vor. Die LVA ist insbesondere weder aus rechtlichen noch aus tatsächlichen Gründen gehindert, selbst die in Rede stehenden Daten zu erheben. Allein der Umstand, dass sich die LVA von der Befragung des Schuldners durch die Gemeinde eine nachhaltigere Wirkung verspricht als bei einer entsprechenden schriftlichen Aufforderung an den Schuldner, die notwendigen Angaben zu machen, stellt noch keine Rechtfertigung für eine Amtshilfe dar.

Der Sache nach handelt es sich bei dem praktizierten Verfahren um eine Datenerhebung im Auftrag. Es ist zweifelhaft, ob diese nach den Bestimmungen des SGB X (§ 80) zulässig ist. Die Vorschrift spricht nur von der Verarbeitung oder Nutzung von Sozialdaten im Auftrag, die Datenerhebung ist nach dem Wortlaut der Vorschrift nicht einbezogen. Bei der vergleichbaren Problematik im Rahmen des § 11 BDSG wird wohl überwiegend angenommen, die Nichterwähnung der Erhebung stelle ein Redaktionsversehen des Gesetzgebers dar, so dass im Wege der Auslegung die Erhebung als miterfasst angesehen werden müsse. Da § 80 SGB X seine derzeitige Fassung jedoch zu einem Zeitpunkt erhalten hat, zu dem diese Problematik bereits bekannt war, ist umstritten, ob man auch hier noch von einem Redaktionsversehen ausgehen kann oder vielmehr annehmen muss, der Gesetzgeber habe die Erhebung bewusst nicht in die Regelung aufgenommen. Da inzwischen Entwürfe zur BDSG-Novellierung jedoch die Ergänzung der Datenerhebung im Auftrag in § 80 SGB X vorsehen, halte ich – auch im Hinblick auf die zu erwartende Erweiterung der Vorschrift – die praktizierte Verfahrensweise grundsätzlich für tolerierbar.

18.4 Bildschirmunterstützte Aufnahme von Anträgen auf Rentenleistungen durch die Versicherungsämter

Der Verband Deutscher Rentenversicherungsträger (VDR) hat sich mit einer Initiative zu Einrichtung eines EDV-Verfahrens, das die bildschirmunterstützte Aufnahme von Anträgen auf Rentenversicherungsleistungen durch Versicherungsämter und Gemeinden ermöglichen soll, an das Bundesministerium für Arbeit und Sozialordnung gewandt.

Die Einräumung eines Online-Zugriffs für die Versicherungsämter ist von erheblicher datenschutzrechtlicher Tragweite. Gegenwärtig ist ein solcher Zugriff den Auskunfts- und Beratungsstellen der gesetzlichen Rentenversicherungsträger möglich; dies sind insgesamt ungefähr 350 Abfragestellen bundesweit. Nach Eröffnung des Online-Zugriffs auch für die Versicherungsämter und Gemeinden könnte sich diese Zahl auf über 15 000 Abfragestellen erhöhen. Allein schon mit einer solchen Vervielfachung ist ein Risiko missbräuchlicher Zugriffe verbunden. Zudem ist zu berücksichtigen, dass die Abrufe durch Stellen außerhalb der gesetzlichen Rentenversicherungsträger erfolgen sollen, wobei durch § 67 Abs. 9 SGB X nur eine begrenzte Abschottung gewährleistet ist. Die Eröffnung eines Online-Zugriffs für die Versicherungsämter und Gemeinden halte ich daher keinesfalls für bedenkenfrei. Die Eröffnung des Online-Zugriffs tastet den gesetzlich abgesicherten, angemessen hohen Standard des Sozialdatenschutzes in der gesetzlichen Rentenversicherung an. Der Gesetzgeber hat im Bewusstsein des hohen Schutzbedarfs der Stammsatzdatei beim VDR und der Rentenversicherungskonten bei den Rentenversicherungsträgern Online-Zugriffe von einer gesetzlichen Zulassung abhängig gemacht. Sie ist bisher selten erfolgt. Ich halte es für unbedingt erforderlich, nachhaltige datenschutzrechtliche Absicherungen gegen die mit der erheblichen Ausweitung des Kreises Online zugriffsberechtigter Abfragestellen verbundenen Risiken gesetzlich zu verankern.

Der vorgesehene Online-Zugriff ist ein automatisiertes Abrufverfahren nach § 79 SGB X. Von der individuellen Zulassung jedes einzelnen Versicherungsamtes und jeder Gemeinde kann nicht abgesehen werden, weil die Umstände des Einzelfalles zu berücksichtigen sind. Dabei halte ich insbesondere die Berücksichtigung folgender Kriterien für erforderlich:

- Ein Online-Zugriff kann nur für Versicherungsämter oder Gemeinden in Betracht kommen ,die ein hinreichendes Aufkommen an Rentenversicherungsanträgen haben, so dass die Einrichtung des Online-Zugriffs angemessen ist.
- Der Online-Zugriff muss ausgeschlossen bleiben, wenn die Funktion des Versicherungsamtes von anderen Aufgabenbereichen der Gebietskörperschaften nicht personell und organisatorisch abgeschottet ist, insbesondere dann, wenn die Funktion des Versicherungsamtes den zuständigen Amtsträger nicht auslastet und dieser daher in Personalunion zugleich für andere Aufgaben zuständig ist.
- Die Versicherungsämter und Gemeinden, soweit sie die Funktion eines Versicherungsamtes ausüben, sind in den Katalog der dem Sozialgeheimnis verpflichteten Stellen in § 35 SGB I aufzunehmen.
- Der Online-Zugriff ist auf die in der Praxis tatsächlich benötigten Datenfelder des Rentenversicherungskontos zu beschränken (vgl. § 79 Abs. 2 Satz 2 Nr. 3 SGB X).
- Tatsache, Zeitpunkt und Inhalt eines jeden erfolgten Abrufs sind im Rentenversicherungskonto oder der Akte des Versicherten so zu dokumentieren, dass Auskunftsersuchen der Versicherten über die erfolgten Online-Abrufe entsprochen werden kann.

– Die Abrufe sind bei den Rentenversicherungsträgern lückenlos zu protokollieren.

– Auf Verlangen des Versicherten ist im Rentenversicherungskonto ein Kennzeichen zu setzen, das sein Konto vom Online-Zugriff ausschließt.

– Der Online-Zugriff soll technisch erst dann erfolgen, wenn sich der Versicherte durch Vorlage seines Lichtbildausweises identifiziert und einen schriftlichen Antrag gestellt hat.

Da weder § 148 Abs. 3 SGB VI noch § 69 SGB X ein Abrufverfahren zu Gunsten der Versicherungsämter vorsehen, bedürfte es einer Gesetzesänderung. Nach meiner Auffassung regelt § 148 Abs. 3 SGB VI den Kreis der beteiligten Stellen spezialgesetzlich und somit vorrangig. § 79 SGB X kommt nur als – zudem neuere – Querschnittsregelung ergänzend zur Anwendung. Hiervon ausgehend müsste nicht nur § 35 Abs. 1 SGB I um die Versicherungsämter ergänzt werden, sondern auch § 148 Abs. 3 SGB VI. Diese Auffassung wird vom Niedersächsischen Ministerium für Frauen, Arbeit und Soziales (MFAS) geteilt. Meines Erachtens sollte auch § 150 Abs. 4 SGB VI insofern geändert werden, dass über die Zulassung einzelner Versicherungsämter und Gemeinden zum Online-Zugriff anhand der bereits genannten Kriterien jeweils individuell zu entscheiden ist.

18.5 Gegenseitige Beauftragung der Träger der gesetzlichen Rentenversicherung mit der Versichertenbetreuung (Dialogverfahren)

Die Datenschutzbeauftragten des Bundes und der Länder befassen sich seit geraumer Zeit mit dem Problem der gegenseitigen Beauftragung der Träger der gesetzlichen Rentenversicherung mit der Versichertenbetreuung (Dialogverfahren).

Die gesetzlichen Rentenversicherungsträger speichern nur über die bei ihnen versicherten Personen Daten. Benötigt der Versicherte Auskünfte zu seinem Versicherungskonto, musste er sich bisher an den zuständigen Rentenversicherungsträger wenden. Da oftmals Versicherte in den Zuständigkeitsbereich eines anderen Rentenversicherungsträgers umziehen oder in unterschiedlichen Orten leben und arbeiten, entstand das Bedürfnis, den Versicherten die Möglichkeit einzuräumen, auch bei nicht zuständigen Rentenversicherungsträgern Auskünfte über das Versicherungskonto zu erhalten und sich die Angaben erläutern zu lassen. Hierzu haben die Landesversicherungsanstalten und die Bundesversicherungsanstalt für Angestellte Vereinbarungen über „die gegenseitige Beauftragung nach § 88 SGB X mit der Erstellung, Anforderung, Aushändigung und Erläuterung von Versicherungsverläufen, Rentenauskünften, Lückenauskünften und Auskünften über Beitragserstattungen sowie über die dafür erforderliche Bearbeitung und Nutzung von Sozialdaten im Auftrag nach § 80 SGB X“ abgeschlossen. Danach wird allen Rentenversicherungsträgern technisch die Möglichkeit eingeräumt, auf die Versichertenkonten der jeweils unzuständigen Rentenversicherungsträger zum Zweck der Auskunftserteilung und Erläuterung bei Anfragen des Versicherten zuzugreifen.

Die Frage, ob es sich um eine Auftragsdatenverarbeitung oder um ein automatisiertes Abrufverfahren handelt, ist bisher nicht zweifelsfrei geklärt. Ich neige der Ansicht zu, dass es sich hierbei nicht um eine Auftragsdatenverarbeitung handelt. Insofern halte ich eine gesetzliche Regelung für dieses Dialogverfahren für angebracht. Unabhängig von dieser Rechtsfrage bin ich der Auffassung, dass es angesichts der Zugriffsmöglichkeiten auf die Daten aller Versicherten in der Rentenversicherung, die den Mitarbeitern der Rentenversicherungsträger im Rahmen der gegenseitigen Betreuung eingeräumt werden, darauf ankommt, die erforderlichen technisch-organisatorischen Maßnahmen nach § 78 a SGB X zu

schaffen. Die Rentenversicherungsträger haben insbesondere zu verhindern, dass Datenträger unbefugt gelesen und personenbezogene Daten zur Kenntnis genommen werden können. Die innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Ein Verfahren, auf das der Versicherte keine Einflussmöglichkeit hat, halte ich für rechtswidrig. Zahlreiche Versicherte sind betroffen, die diesen Service niemals in Anspruch nehmen werden. Es bestünde die Möglichkeit, eine entsprechende Einwilligung einzuholen, z. B. bei neuen Versicherten anlässlich der erstmaligen Versendung der Rentenversicherungsnummer. Auch bei bereits Versicherten ist die Einwilligung möglich. Sollte man dies aus Kostengründen und anderen wichtigen Gesichtspunkten nicht für angemessen halten, müsste den Versicherten wenigstens ein Widerspruchsrecht dergestalt eingeräumt werden, die Möglichkeit, auf einzelne Versichertenkonten extern zuzugreifen, technisch auszuschließen. Die Versicherten wären auf die Widerspruchsmöglichkeit hinzuweisen. Bei einem solchen Verfahren müssten die technischen Möglichkeiten dafür geschaffen werden, dass im Falle eines Widerspruchs die Freischaltung der Kontenanforderung verhindert werden kann.

Der Verband Deutscher Rentenversicherungsträger hat dem Bundesbeauftragten für den Datenschutz mitgeteilt, eine entsprechende Möglichkeit werde geschaffen.

Ich halte es aus Dokumentations- und Kontrollzwecken für notwendig, dass der Versicherte und nicht der Mitarbeiter des Rentenversicherungsträgers durch seine Unterschrift dokumentiert, dass die Anforderung des Versicherungskontos beim Konto führenden Rentenversicherungsträger von ihm beantragt worden ist. Dies kann formularmäßig erfolgen. Die niedersächsischen Landesversicherungsanstalten haben den Vorschlag aufgegriffen und werden zur Sicherstellung der Kontrolle ein entsprechendes Formular einsetzen.

Für erforderlich halte ich ferner eine Identitätsprüfung des Antragstellers durch Vorlage eines Lichtbildausweises. Dies liegt auch im Interesse des Versicherten. Eine entsprechende Identitätsprüfung ist auch dann möglich, wenn sich der Versicherte durch Dritte vertreten lässt. So kann der Lichtbildausweis z. B. auf die Rückseite der schriftlich vorzulegenden Vollmacht des Betroffenen kopiert werden. Hierzu haben mir die niedersächsischen Landesversicherungsanstalten mitgeteilt, eine Identitätsprüfung erfolge in allen Beratungsgesprächen, die persönliche Auskünfte aus dem Versicherungskonto enthalten.

Die Landesversicherungsanstalten in Niedersachsen und Bremen sind am Dialogverfahren beteiligt. Die Berechtigung für die Dialogisierung wurde nur an ausgewählte Mitarbeiter im Auskunfts- und Beratungsdienst und an die mit der technischen Durchführung des Dialogverfahrens betrauten Mitarbeiter erteilt. Die Berechtigten wurden auf ihre besonderen Verpflichtungen in diesem Verfahren ausführlich hingewiesen. Jede Kontoanforderung wird beim zuständigen Kontoführer maschinell protokolliert und vom anfordernden Versicherungsträger schriftlich dokumentiert. Diese Dokumentationslisten werden über mehrere Jahre aufbewahrt.

18.6 Übersendung von Sozialhilfeakten beim Umzug des Hilfeempfängers

Einige Kommunen haben sich mit dem Problem der Übersendung von Sozialhilfeakten befasst. Dabei trat die Frage auf, ob es zulässig ist, die vollständigen Sozialhilfeakten zu übersenden

a) beim Umzug eines Sozialhilfeempfänger innerhalb eines Landkreises

b) beim Umzug in den Bereich eines anderen Landkreises.

Ein Wohnortwechsel zwischen Gemeinden innerhalb eines Landkreises führt nicht zu einem Wechsel des Sozialhilfeträgers. Nach der Legaldefinition des § 12 SGB I sind Leistungsträger die in §§ 18 bis 29 SGB I genannten Körperschaften, Anstalten und Behörden. Zuständig für die Leistungen der Sozialhilfe sind nach § 28 Abs. 2 SGB I u. a. die Kreise und kreisfreien Städte; die kreisangehörigen Gemeinden sind nicht genannt. Da die Heranziehung kreisangehöriger Gemeinden oder Samtgemeinden gemäß § 4 Nds. AG BSHG diese nicht zu Leistungsträgern i.S. von § 35 Abs. 1 SGB I macht, bleibt der jeweilige Landkreis örtlicher Träger der Sozialhilfe. Daraus folgt, dass es bei einem Umzug eines Sozialhilfeempfängers innerhalb eines Landkreises zulässig ist, die Sozialhilfeakte zu übersenden. Dies kann nach meiner Auffassung allerdings nicht für Akten gelten, deren Sachverhalte in der Vergangenheit abgeschlossen wurden und die keine Wirkungen für die Zukunft mehr entfalten können.

Bei einem Umzug eines Sozialhilfeempfängers in den Zuständigkeitsbereich eines anderen Landkreises tritt ein Wechsel des Trägers der Sozialhilfe ein. In diesem Fall dürfen nur die zur Aufgabenerfüllung des neu zuständigen Sozialhilfeträgers erforderlichen Sozialdaten übermittelt werden.

18.7 Übermittlung personenbezogener Daten bei der Festsetzung von Unterhaltsleistungen im Rahmen der Sozialhilfegewährung

Häufig ist die Frage aufgeworfen worden, ob die Unterrichtung eines anteilig Unterhaltsverpflichteten durch die Sozialhilfeträger über die Unterhaltsquoten der parallel zum Unterhalt Verpflichteten zulässig ist. Von betroffenen Kommunen wird darauf hingewiesen, dass bei der beabsichtigten Heranziehung von unterhaltspflichtigen Kindern zu Sozialhilfeaufwendungen für in Einrichtungen untergebrachte Angehörige die Unterhaltspflichtigen häufig grundsätzlich durchaus mit der Heranziehung zur Unterhaltsleistung (Heimpflegekosten) einverstanden seien. Sie wollten jedoch prüfen, ob die eigene Unterhaltsquote im Verhältnis zur Quote von Mitverpflichteten zutreffend festgesetzt worden sei. Verweigere der Sozialhilfeträger diese Angaben im Verwaltungsverfahren und beschreite den Klageweg, so habe er mit der Klageerhebung die zuvor verweigerten Angaben über die wirtschaftlichen Verhältnisse der zum Unterhalt mitverpflichteten Geschwister zu machen, weil die Klage andernfalls nicht schlüssig sei. Wenn der Beklagte daraufhin die Quotenfestsetzung anerkenne, fielen dem klagenden Sozialhilfeträger die Prozesskosten nach § 93 ZPO zur Last.

Ich halte die Übermittlung der bei einem Sozialleistungsträger vorhandenen Angaben über die Unterhaltsquoten (und deren Festsetzung) von anteilig Unterhaltsverpflichtigten im Falle eines Anspruchsüberganges nach § 91 BSHG an weitere unterhaltspflichtige Geschwister für zulässig. Die in Rede stehenden Daten sind Sozialdaten. Sie müssen im Hinblick auf Aufgaben nach dem SGB verarbeitet werden. Die Geltendmachung von übergegangenen Unterhaltsansprüchen steht im Zusammenhang mit der Gewährung der Sozialhilfe und ist damit zum Aufgabenbereich des Sozialhilfeträgers zu rechnen. Der Umstand, dass der Anspruch seinen rechtlichen Charakter durch die Überleitung durch § 91 BSHG nicht ändert, ein zivilrechtlicher Anspruch also durch den Rechtsübergang nicht zum öffentlich-rechtlichen wird, ist dabei aus meiner Sicht in diesem Zusammenhang nicht von Belang.

Zwar scheidet eine Datenübermittlung nach § 74 Satz 1 Nr. 1 Buchst. a SGB X aus, da sie hiernach u. a. nur für ein gerichtliches, nicht aber für ein Verwaltungsverfahren zugelassen ist. Allerdings sind die Voraussetzungen des § 74 Satz 1 Nr. 2 Buchst. a SGB X erfüllt, da auch der Betroffene zivilrechtlich zur Auskunft über die zur Geltendmachung eines Unterhaltsanspruchs erforderlichen Daten verpflichtet ist. Die in dieser Vorschrift ausdrücklich genannten

Auskunftspflichten zwischen Verwandten gerader Linie nach § 1605 BGB, getrennt lebenden Ehegatten nach § 1361 Abs. 4 Satz 4 BGB, geschiedenen Ehegatten nach § 1580 Satz 2 BGB, dem nichtehelichen Kind, dem Vater bzw. der Mutter nach § 1615 a BGB sowie der Mutter und dem Vater aus Anlass der Schwangerschaft und Geburt eines Kindes nach § 1615 Abs. 3 Satz 1 BGB jeweils i. V. m. § 1605 BGB sind zwar nicht einschlägig. Diese Auskunftsansprüche sind jedoch, wie der Wortlaut der Bestimmung zeigt („insbesondere"), nicht abschließend.

Bezüglich des in Rede stehenden Auskunftsanspruchs zwischen Geschwistern zur Feststellung ihrer jeweiligen Unterhaltspflicht gegenüber einem oder beiden Elternteilen wird vereinzelt die Ansicht vertreten, dass in analoger Anwendung des § 1605 BGB auch zwischen diesen Unterhaltsverpflichteten eine Auskunftspflicht bestehe. Die überwiegende Auffassung in der Literatur geht dagegen davon aus, dass eine Erstreckung der Vorschrift auf Verwandte in der Seitenlinie nicht möglich ist. Auch nach dieser Ansicht ist ein Auskunftsanspruch zwischen Geschwistern jedoch nicht ausgeschlossen. Auskunftsansprüche zur Feststellung der Unterhaltspflicht wurden ursprünglich von der Rechtsprechung aus § 242 BGB abgeleitet. Nachdem der Gesetzgeber in den erwähnten Fällen derartige Ansprüche ausdrücklich normiert hat, ist jedoch im Übrigen ein Rückgriff auf diese Vorschrift weiterhin möglich. Der Bundesgerichtshof (BGH) hat den Grundsatz betont, dass dann ein Auskunftsanspruch besteht, wenn zwischen den Beteiligten besondere rechtliche Beziehungen vertraglicher oder außervertraglicher Art bestehen, die es mit sich bringen, dass der Auskunftsbegehrende entschuldbar über das Bestehen oder den Umfang seines Rechts im Unklaren und deshalb auf die Auskunft des Verpflichteten angewiesen ist. In der genannten Entscheidung hat der BGH mit dieser Erwägung den Auskunftsanspruch eines Elternteils, der von einem Kind auf Unterhalt in Anspruch genommen wurde, gegenüber dem nach § 1606 Abs. 3 Satz 1 BGB anteilig verpflichteten anderen Elternteil bejaht. Da diese Vorschrift auch für die Unterhaltspflicht zwischen Geschwistern gilt, hat aufgrund dieser rechtlichen Sonderbeziehung ebenfalls jeder Teil ein berechtigtes Interesse daran, die Einkommensverhältnisse der neben ihm anteilig Verpflichteten zu erfahren. Der Auskunftsanspruch ergibt sich somit aus § 242 BGB.

Das MFAS teilt diese Rechtsauffassung.

18.8 Übermittlung von Mieterdaten an Sozialämter

Wohnungsbaugesellschaften machen häufig den örtlichen Sozialämtern Mitteilung darüber, dass keine Miete gezahlt wird bzw. die Einleitung einer Räumungsklage angestrebt wird. Gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist eine Übermittlung zulässig, soweit sie zur Wahrung berechtigter Interessen der Wohnungsbaugesellschaften erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung überwiegt. Ich halte in derartigen Fällen eine Unterrichtung des Betroffenen über die beabsichtigte Übermittlung seiner Daten an das Sozialamt für angebracht. Dieses könnte in der Weise geschehen, dass der Betroffene von der Wohnungsbaugesellschaft darauf hingewiesen wird, einen Antrag auf Sozialhilfe beim zuständigen Leistungsträger zu stellen. Kommt er dieser Aufforderung nicht nach, so habe ich keine Bedenken, dass die erforderlichen Daten an das Sozialamt übermittelt werden.

In diesem Zusammenhang weise ich auf die Änderung des § 15 a BSHG hin. Nach Abs. 2 dieser Vorschrift teilt das Gericht, bei dem eine Klage auf Räumung von Wohnraum im Falle der Kündigung des Mietverhältnisses nach § 554 des BGB eingeht, dem zuständigen örtlichen Träger der Sozialhilfe unverzüglich bestimmte Daten mit. Die Übermittlung unterbleibt, wenn die Nichtzahlung des Mietzinses offensichtlich nicht auf Zahlungsunfähigkeit des Mieters beruht.

18.9 Arbeit statt Sozialhilfe

Die in den §§ 18 ff. BSHG geregelten Aufgaben der örtlichen Sozialhilfeträger bezüglich der Hilfe zur Arbeit haben im Berichtszeitraum immer größere Bedeutung erlangt. Sozialhilfeträger haben z. T. selbst versucht, beschäftigungslose Sozialhilfeempfänger in Arbeitsverhältnisse zu vermitteln, andere haben Beschäftigungsgesellschaften gegründet oder haben sich privater Stellen bedient.

Datenschutzrechtlich unbedenklich ist in allen Fällen die folgende Vorgehensweise:

1. Das Sozialamt stellt diejenigen Sozialhilfeempfänger fest, die für ein Beschäftigungsverhältnis in Frage kommen, und erhebt eventuell in diesem Zusammenhang zusätzlich benötigte Daten.
2. Eine Datenübermittlung an eine Beschäftigungsgesellschaft oder an eine private Einrichtung ist gemäß § 69 Abs. 1 Nr. 1, 2. Fall SGB X zulässig. Dabei hat sich der Umfang der zu übermittelnden Daten an dem Erforderlichkeitsgrundsatz zu orientieren. Einer Einwilligung der Betroffenen in diese Datenübermittlung bedarf es nicht. Für datenschutzfreundlich halte ich es, wenn die Betroffenen über die Datenübermittlung und das Gesamtverfahren informiert werden.

18.10 Akteneinsicht/Auskunftsanspruch

Gemäß § 83 SGB X ist dem Betroffenen auf Antrag Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Hierzu gehört auch die Auskunft über die in Akten gespeicherten Daten. Eine Auskunft muss nach § 83 Abs. 4 Nr. 3 SGB X unterbleiben, soweit die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Wird nach dieser Rechtsvorschrift keine Auskunft erteilt, so habe ich auf Verlangen des Auskunftsberechtigten zu prüfen, ob die Ablehnung der Auskunftserteilung rechtmäßig war (§ 83 Abs. 6 SGB X).

Ein Akteneinsichtsrecht besteht nach § 25 SGB X nur für Beteiligte eines laufenden Verwaltungsverfahrens, jedoch gemäß § 25 Abs. 3 SGB X nicht, wenn die Vorgänge wegen der berechtigten Interessen der Beteiligten oder dritter Personen geheim gehalten werden müssen.

Da mich zu dieser Problematik in letzter Zeit häufiger Anfragen von Kommunen erreicht haben, will ich hierzu an dieser Stelle grundsätzlich Stellung nehmen.

Bei der Interessenabwägung im Rahmen des § 83 Abs. 4 Nr. 3 bzw. § 25 Abs. 3 SGB X sind die Belange der auskunftsberechtigten Personen, das Geheimhaltungsinteresse der Personen, über deren Verhalten Auskunft erteilt werden soll, und die besonderen Belange der Behörde (§ 83 Abs. 4 Nr. 1) zu berücksichtigen. Das Interesse z. B. eines Informanten, der seinen Namen nicht preisgeben will, und das gegenläufige Interesse des Auskunftsberechtigten liegen auf der Hand. Gegenüber diesen Einzelbelangen gibt es oft ein herausgehobenes Interesse der Verwaltung daran, von der Bevölkerung so weit wie möglich Hinweise für die

Aufgabenwahrnehmung zu erhalten. Würde z. B. bekannt, dass ein Jugendamt die Namen von Anzeigeerstattern bei vermuteter Kindesmisshandlung ohne weiteres preisgibt, würde die Bereitschaft in der Bevölkerung zu sachdienlichen Hinweisen sinken und die Aufgabenerledigung der Behörde damit erheblich erschwert. Der grundsätzliche Schutz des Informanten muss allerdings begrenzt werden, wenn Anhaltspunkte dafür bestehen, dass dieser die Behörde wider besseres Wissen oder leichtfertig falsch über den Betroffenen informiert oder gar den Tatbestand einer falschen Verdächtigung (§ 164 StGB) oder der Beleidigung bzw. üblen Nachrede (§§ 185 f. StGB) erfüllt hat. Dagegen kann allein der Umstand, dass eine gegebene Information sich nach entsprechender Überprüfung als unrichtig herausstellt, im Hinblick auf eine möglichst effektive Aufgabenwahrnehmung der Behörde noch nicht zur Preisgabe der Informanten führen (s. a. 20.1):

18.11. Verschlüsselung von Diagnosen, ICD-10-Schlüssel

Die in XIII 9.8 geschilderte Erprobung des ICD-10-Schlüssels hat in Pilotprojekten in Niedersachsen und Sachsen-Anhalt stattgefunden. In Niedersachsen hat die Kassenärztliche Vereinigung zum 1. April 1997 mit ca. 2 500 Ärzten aus allen Fachgruppen den Modellversuch begonnen.

Einen Zwischenbericht hat die Kassenärztliche Vereinigung am 15. Dezember 1997 dem Bundesministerium für Gesundheit vorgelegt. Darüber hinaus hat das Zentralinstitut der Kassenärztlichen Versorgung in der Bundesrepublik Deutschland einen Ergebnisbericht über die erste Arztbefragung zur Praktibilität und Funktionalität der Diagnoseverschlüsselung erstellt.

Ich habe mich gemeinsam mit meinem Kollegen aus Sachsen-Anhalt und dem Bundesbeauftragten für den Datenschutz intensiv mit den damit zusammenhängenden datenschutzrechtlichen Fragen beschäftigt. Auf eine Darstellung der Probleme soll hier verzichtet werden, weil das Bundesministerium für Gesundheit im Juni 1998 mitgeteilt hat, eine verbindliche Einführung der Verschlüsselung der Diagnosen (ursprünglich geplant zum 1. Januar 1998) sei z. Z. nicht absehbar.

18.12 Daten für den Medizinischen Dienst

Für die Durchführung der Beratung und die Begutachtung durch den Medizinischen Dienst der Krankenversicherung (MDK) ist es erforderlich, dass die Leistungsträger im Einzelfall sämtliche relevanten Unterlagen vorlegen.

Die Zurverfügungstellung der notwendigen Unterlagen muss zeitnah geschehen, damit im Begutachtungs- und Verwaltungsverfahren keine Nachteile aus eventuellen Verzögerungen entstehen und negative Auswirkungen auf die Leistungsgewährung für die Versicherten vermieden werden.

Nach § 100 SGB X sind die Krankenkassen berechtigt, vom Arzt oder Angehörigen eines anderen Heilberufes bzw. vom Krankenhaus oder der Vorsorge- und Rehabilitationseinrichtung im Einzelfall Auskunft zu verlangen, soweit es für die Durchführung der Aufgaben nach dem Gesetz erforderlich und gesetzlich zugelassen ist oder der Betroffene im Einzelfall eingewilligt hat. Sind die Daten aufgrund dieser Einwilligung erhoben worden, darf eine Übermittlung an den MDK wiederum nur mit Einwilligung erfolgen. Eine Einwilligung ist außerdem dann erforderlich, wenn Krankenkassen Unterlagen, die ihnen der Versicherte über seine Mitwirkungspflicht hinaus freiwillig selbst überlassen hat, an den MDK übermittelt werden sollen (§ 276 Abs. 1 SGB V).

Die Krankenkassen bieten den betroffenen Ärzten, Krankenhäusern und anderen Stellen an, die medizinischen Unterlagen entweder direkt an den MDK zu übersenden oder im verschlossenen Umschlag über die Krankenkasse an den MDK weiterzuleiten.

Stellt der Gutachter des MDK fest, dass für die gutachterliche Stellungnahme und Prüfung weitere medizinische Unterlagen erforderlich sind, fordert der MDK diese ergänzenden Unterlagen selbstständig bei den Leistungserbringern an (§ 276 Abs. 2 Satz 1, 2. Halbsatz SGB V).

Die beschriebenen Abläufe zur Begutachtung durch den MDK finden im Rahmen der Pflegeversicherung entsprechende Anwendung. Hinsichtlich der Erhebung, Speicherung und Nutzung von Sozialdaten gelten die Vorschriften des Zweiten Kapitels des SGB X i. V. m. §§ 93, 94, 97 SGB XI.

Nach § 18 Abs. 4 SGB XI sind die Pflege- und Krankenkassen sowie die Leistungserbringer verpflichtet, dem MDK die für die Begutachtung erforderlichen Unterlagen vorzulegen und Auskünfte zu erteilen.

Der MDK soll die behandelnden Ärzte des Versicherten, insbesondere die Hausärzte, in die Begutachtung einbeziehen und ärztliche Auskünfte und Unterlagen über die für die Begutachtung der Pflegebedürftigkeit wichtigen Vorerkrankungen sowie Art, Umfang und Dauer der Hilfebedürftigkeit einholen, soweit der Versicherte eingewilligt hat (§ 18 Abs. 3 SGB XI).

18.13 Fehlbelegungsprüfungen in Krankenhäusern durch den Medizinischen Dienst

Gemäß § 17 a Krankenhausfinanzierungsgesetz (KHG) wirken die Krankenkassen insbesondere durch gezielte Einschaltung des Medizinischen Dienstes der Krankenversicherung (MDK) darauf hin, dass Fehlbelegungen vermieden und bestehende Fehlbelegungen zügig abgebaut werden. Zu diesem Zweck darf der MDK Einsicht in die Krankenunterlagen nehmen. Der MDK verarbeitet insofern Sozialdaten. Die Krankenkassen dürfen den MDK nach § 17 a Abs. 2 KHG i. V. m. § 275 Abs. 4 SGB X mit einzelfallübergreifenden, wohl auch mit hinsichtlich der Versicherten stichprobenartigen, allerdings nicht mit flächendekkenden Überprüfungen von Krankenhäusern beauftragen. Auswahllisten zur Vorbereitung einer Stichprobe dürfen mangels Erforderlichkeit keine Patientennamen enthalten. Fälle von privat versicherten Patienten oder Fälle von Sozialhilfeempfängern dürfen nicht mitgeteilt werden.

18.14 Hilfe bei Schwangerschaftsabbrüchen

Nach einer Verwaltungsvereinbarung zur Durchführung des Verfahrens der Kostenerstattung zwischen dem Land Niedersachsen und den Landesverbänden der gesetzlichen Krankenkassen übersenden die Krankenkassen Kopien/Durchschriften der Abrechnungsbelege der Ärztinnen/Ärzte, Krankenhäuser oder Einrichtungen, die Schwangerschaftsabbrüche durchgeführt haben, dem Niedersächsischen Landesamt für Zentrale Soziale Dienste (NLZSA). Die Abrechnungsbelege enthalten nach dem mir vorliegenden Muster Namen, Vornamen und Geburtsdatum der Patientinnen. Die Abrechnung erfolgt damit nicht fall-, sondern personenbezogen.

Gegen dieses Verfahren habe ich Bedenken. Es wird der Forderung des § 3 Abs. 5 des „Gesetzes zur Hilfe für Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen“ hinsichtlich der Beachtung des Persönlichkeitsrechts der betroffenen Frauen nicht gerecht. Ich habe das damalige Niedersächsische Frauenministerium darauf hingewiesen und gebeten, sich für eine anonymisierte Kostenerstattung einzusetzen.

Meiner Forderung nach Anonymisierung ist insbesondere entgegengehalten worden, die ordnungsgemäße Durchführung des Abrechnungsverfahrens verlange die Angabe von Namen und Vornamen der Patientinnen. Andernfalls könnten Kostenerstattungsanträge, die weder dem Grunde noch der Höhe nach gerechtfertigt seien, nicht zurückgewiesen werden. So würden z. T. Erstattungsanträge für Frauen gestellt, die weder ihren Wohnsitz noch ihren gewöhnlichen Aufenthalt in Niedersachsen haben, Leistungen abgerechnet, die nicht in die Kostenerstattungspflicht der gesetzlichen Krankenkassen fallen, oder Abrechnungen für Schwangerschaftsabbrüche nach der 13. Kalenderwoche vorgelegt, ebenso Doppelabrechnungen für denselben Schwangerschaftsabbruch.

Nach mehrfachem Schriftwechsel habe ich die Angelegenheit mit dem Niedersächsischen Frauenministerium und dem NLZSA erörtert. Die Besprechung hat zu der übereinstimmenden Einschätzung geführt, dass die angeführten Gesichtspunkte einer fallbezogenen Abrechnung nicht entgegengehalten werden können. Bei den genannten Fallkonstellationen sind nicht Name und Vorname der Frau, sondern jeweils andere Kriterien (wie Wohnsitz, Schwangerschaftswoche etc.) für die Prüfung der Erstattungsfähigkeit von Bedeutung. Um den für Abrechnungszwecke nicht erforderlichen Personenbezug zu vermeiden, sollte deshalb eine Kennziffer, die sich z. B. aus dem Institutionskennzeichen der Krankenkasse und der Krankenversichertennummer zusammensetzen könnte, verwendet werden.

In einem Schreiben an die Landesverbände der gesetzlichen Krankenkassen habe ich angemahnt, die Verwaltungsvereinbarung entsprechend zu ändern und die verwendeten Formulare zu überarbeiten.

Nach ca. einem halben Jahr haben mir die Verbände der gesetzlichen Krankenkassen in Niedersachsen mitgeteilt, die von mir vorgeschlagene umfassende Anonymisierung sei aus Sicht der Krankenkassen nicht durchführbar. Nach Auffassung der Verbände der gesetzlichen Krankenkassen in Niedersachsen ist sie auch nicht erforderlich. Da alle Mitarbeiter der Krankenkassen zur Verschwiegenheit verpflichtet seien, könne kein Unbefugter Kenntnis von den persönlichen Daten der Betroffenen erlangen. Die Verbände gehen auch davon aus, dass das NLZSA als Erstattungsstelle für zahlreiche Vorgänge, in denen personenbezogene Daten eine Rolle spielen, grundsätzlich der Verschwiegenheitspflicht unterliegt. Aus diesen Gründen halten die Verbände eine Änderung der Verwaltungsvereinbarung nicht für sinnvoll.

Folgt man dieser Argumentation, so wären datenschutzrechtliche Regelungen im öffentlichen Bereich überhaupt nicht vonnöten, da alle Bediensteten einer Verschwiegenheitspflicht unterliegen. Das Unverständnis der Verbände der gesetzlichen Krankenkassen für datenschutzrechtliche Belange der Schwangeren ist bemerkenswert. Ich werde weiter mit Nachdruck darauf drängen, dass die derzeitige Praxis geändert wird.

19 Gesundheit

Weitergabe von Patientendaten an die Rechtsabteilung eines Krankenhauses

Ein Krankenhauspatient beklagte sich darüber, dass seine Patientendaten von der behandelnden Fachabteilung an eine nicht medizinische Abteilung des Krankenhauses weitergegeben worden seien.

Das von mir um eine Stellungnahme gebetene Krankenhaus teilte mit, der Leiter der Fachabteilung sei gezwungen gewesen, zahlreiche Patientenprobleme und die Betreuung der Patienten mit einem Vertreter der Rechtsabteilung des Krankenhauses zu besprechen. Üblicherweise nenne die Fachabteilung in solchen Fällen nicht den Namen des Patienten, sondern nur seine Initialen. In dem Falle des Patienten, der sich an mich gewandt hatte, habe der Mitarbeiter der Rechtsabteilung jedoch Einsicht in die Patientenunterlagen nehmen müssen. Es würden jedoch von nun an Patientennamen nicht mehr an die Rechtsabteilung weitergegeben.

Aufgrund dieser Stellungnahme gehe ich davon aus, dass in Zukunft die Rechtsabteilung nur im erforderlichen Umfang, etwa bei einer Vertretung des Krankenhauses in einem gerichtlichen Verfahren, Kenntnis vom Namen des Patienten erhält.

20 Kinder- und Jugendhilfe

20.1 Vertrauliche Behandlung von Anzeigen durch Mitarbeiter des Jugendamtes

Bei den Jugendämtern gehen häufig Hinweise aus der Bevölkerung auf ein möglicherweise auch strafrechtlich relevantes Verhalten von Eltern ein. Auf solche Informationen sind die Behörden zur Gewährleistung einer sachgerechten Sozialarbeit dringend angewiesen. In diesen Fällen wird häufig um vertraulichen Umgang mit den Daten gebeten, insbesondere legen die Anzeigeerstatter Wert darauf, dass ihre Person der betroffenen Familie nicht bekannt wird. Stellt sich im Rahmen der Nachforschungen des Jugendamtes heraus, dass dieses aufgrund entsprechender Informationen handelt, versuchen die Betroffenen möglicherweise durch eine Strafanzeige, etwa wegen übler Nachrede, den jeweiligen Hinweisgeber in Erfahrung zu bringen. In der ganz überwiegenden Zahl der Fälle sind derartige Straftatbestände jedoch nicht erfüllt. Die Anzeigeerstatter haben vielmehr in berechtigter Sorge Beobachtungen über Verhaltensauffälligkeiten von Kindern, Anzeichen von Verletzungen und andere Wahrnehmungen, die Anlass zur Vermutung geben, dass Übergriffe gegenüber Kindern oder Jugendlichen stattgefunden haben könnten, an das Jugendamt weitergegeben. In einer Vielzahl der Fälle dürfte hier auch der Rechtfertigungsgrund des § 193 StGB erfüllt sein. Bisher wurde auch bei einer Einstellung des strafrechtlichen Ermittlungsverfahrens wegen eines Ehrverletzungsdelikts dem Anzeigeerstatter der Name der Person mitgeteilt, gegen die ermittelt wurde. Der Hinweisgeber, der sich im guten Glauben an das Jugendamt gewandt hatte, wurde damit aus seiner Sicht bloßgestellt.

Um dies zu vermeiden und so Bürgerinnen und Bürger nicht von notwendigen Informationen gegenüber dem Jugendamt abzuhalten, hat der Landkreis Osnabrück sich mit der dortigen Staatsanwaltschaft auf folgende Verfahrensweise verständigt: Wenn ein Anzeigeerstatter um vertraulichen Umgang mit seinen Informationen bittet, wird mit ihm vereinbart, dass das Jugendamt im Fall eines staatsanwaltschaftlichen Ermittlungsverfahrens zur Aufklärung der Vorwürfe nur den Inhalt der Aussagen an die Staatsanwaltschaft weitergibt. Sollte sich daraufhin ein Verfahren wegen übler Nachrede oder eines anderen Ehrverlet-

zungsdelikts anschließen, geben die Mitarbeiter des Jugendamts eine dienstliche Erklärung über den Inhalt der Anzeige ab bzw. bekunden diese als Zeugen. Ergeben die Ermittlungen keinen Tatverdacht, wird das Verfahren „gegen unbekannt“ eingestellt. Die Staatsanwaltschaft behält sich allerdings vor, den Anzeigeerstatter zu vernehmen, soweit dies im Rahmen der geführten Ermittlungen erforderlich sein sollte. In diesem Fall erwirkt die Staatsanwaltschaft beim zuständigen Amtsgericht einen Beschluss nach § 73 SGB X zur Übermittlung der notwendigen Sozialdaten für Strafverfahrenszwecke.

Sollte im Einzelfall ein hinreichender Tatverdacht gegen einen Anzeigeerstatter bestehen, werden ebenfalls aufgrund richterlichen Beschlusses die Angaben zur Person des Anzeigeerstatters an die Staatsanwaltschaft weitergegeben.

Ich halte diese Verfahrensweise zur vertraulichen Behandlung von Anzeigen für einen datenschutzfreundlichen und nachahmenswerten Weg, um die Anonymität von Anzeigeerstattern so lange zu wahren, wie der Ermittlungsstand es zulässt. Das Justizministerium hat gegen diese Vorgehensweise keine Bedenken erhoben.

20.2 Übermittlung personenbezogener Daten für die Durchführung von Strafverfahren

Über eine Übermittlung von Sozialdaten zur Durchführung eines Strafverfahrens ist durch richterliche Anordnung zu entscheiden (§ 73 Abs. 3 SGB X). Vor Erlass eines Beschlagnahme- oder Durchsuchungsbeschlusses hat der Richter die materiell-rechtlichen Voraussetzungen zu prüfen, insbesondere, ob hinreichende Anhaltspunkte für ein Verbrechen oder Vergehen vorliegen, ob der Datenumfang sich an der Art der Straftat (Verbrechen oder Vergehen) orientiert, ob die Übermittlung der Sozialdaten für die Durchführung des Strafverfahrens erforderlich ist und ob der Grundsatz der Verhältnismäßigkeit gewahrt ist.

Die SGB-Stellen haben nicht die Aufgabe, richterliche Anordnungen umfassend zu überprüfen. Sie wären hierzu auch nicht in der Lage. Ergeben sich bei einer Schlüssigkeitsprüfung Zweifel an der Rechtmäßigkeit der richterlichen Anordnung (z. B. weil die Einschränkung der Übermittlungsbefugnis nach § 73 Abs. 2 oder § 76 SGB X nicht berücksichtigt worden ist), ist der Angelegenheit weiter nachzugehen.

Ich halte es für sachgerecht, in einem solchen Falle etwa die Polizeibeamten auf die Rechtswidrigkeit eines Durchsuchungs- oder Beschlagnahmebeschlusses hinzuweisen und darauf hinzuwirken, dass die angeordnete Datenübermittlung zunächst unterbleibt. Geben sich die Beamten jedoch hiermit nicht zufrieden, ist nach der Rechtslage die SGB-Stelle verpflichtet, die von ihr als unzulässig angesehene Datenübermittlung vorzunehmen. Im Konfliktfalle können Zweifel an der Rechtmäßigkeit der richterlichen Anordnung letztlich nur durch den Rechtsbehelf der Beschwerde nach §§ 304 ff. StPO geltend gemacht werden. Die Beschwerde hat keine aufschiebende Wirkung (§ 307 Abs. 2 StPO), so dass daneben die Aussetzung des Vollzugs beantragt werden muss.

Eine große Bundesbehörde hat hierzu folgende Regelung getroffen, die auch für die niedersächsischen SGB-Stellen richtungsweisend sein kann:

„Soweit Durchsuchungs- und Beschlagnahmebeschlüsse im Sinne der Strafprozessordnung vollzogen werden sollen, obwohl eine Übermittlung von Sozialdaten nicht zulässig ist, ist gegen diese Beschlüsse im Hinblick auf § 35 Abs. 3 SGB I gemäß § 306 Strafprozessordnung Beschwerde einzulegen und das Beschwerdegericht um Aussetzung des Vollzuges zu ersuchen.

Sofern Strafverfolgungsbehörden oder Gerichte vollständige Akten beschlagnahmen wollen und auf deren Herausgabe bestehen, obwohl nur die Übermittlung einzelner Sozialdaten erfolgen darf, ist die Akte in verschlossenem Umschlag unter gesonderter Beifügung der Beschwerde nach Abs. 1 auszuhändigen."

In diesem Zusammenhang weise ich auf einen Beschluss des OLG Celle vom 30. Juli 1997 – 2 Ws 157/97 – (NJW 1997, 2964) hin, in dem festgestellt wird, dass es objektiv willkürlich ist, wenn der Tatrichter zur Durchsetzung eines Auskunftsbegehrens gegenüber einer Sozialbehörde, das als besonders eilig angesehen wird, statt einer richterlichen Anordnung nach § 73 SGB X einen Durchsuchungs- und Beschlagnahmebeschluss erlässt.

20.3 Datenübermittlung vom Jugendamt an das Sozialamt

Eine große Kommune hat die Frage aufgeworfen, ob bei folgender Fallkonstellation eine unaufgeforderte Datenübermittlung vom Jugendamt an das Sozialamt zulässig ist: Einem Jugendlichen aus einer Familie, die Hilfe zum Lebensunterhalt erhält, werden Jugendhilfeleistungen gewährt, die mit einer Fremdunterbringung verbunden sind. Vom Beginn dieser Leistung an ist der Jugendliche bei der Gewährung der Sozialhilfe nicht mehr zu berücksichtigen. Das Jugendamt soll in solchen Fällen dem Sozialamt unaufgefordert mitteilen, dass der Jugendliche nicht mehr Mitglied der sozialhilferechtlichen Bedarfsgemeinschaft ist und insoweit Hilfe zum Lebensunterhalt nicht mehr gezahlt werden muss. Eine Mitteilung an das Sozialamt über die einzelne Jugendhilfemaßnahme ist nicht beabsichtigt.

Eine Datenübermittlung nach § 69 SGB X setzt im Bereich der Jugendhilfe zunächst voraus, dass hierdurch der Erfolg der gewährten Jugendhilfeleistung nicht in Frage gestellt wird (§ 64 Abs. 2 SGB VIII). Damit ist eine „Übermittlungsautomatik" von vornherein ausgeschlossen. Zudem muss vor einer Datenübermittlung im Einzelfall geprüft werden, ob hierdurch ein besonderer Vertrauensschutz gefährdet würde (§ 65 SGB VIII). Geht man davon aus, dass diese Gesichtspunkte hier einer Datenübermittlung nicht entegenstehen, so ist dennoch eine generelle Übermittlung der in Rede stehenden Daten an das Sozialamt nicht erforderlich.

Die Argumentation der Kommune, die Erforderlichkeit ergäbe sich bereits aus dem Umstand, dass die Gewährung der Jugendhilfeleistung sich hier unmittelbar auf die Höhe des Sozialhilfeanspruchs auswirke, trifft nicht zu.

Da das Grundrecht auf informationelle Selbstbestimmung den Einzelnen schützt, muss die Erforderlichkeit in jedem Einzelfall vorliegen. Teilt der Empfänger der Jugendhilfeleistung – wie es seiner Rechtspflicht entspricht – die Leistungsgewährung dem Sozialamt mit, ist ein Erfordernis für eine Unterrichtung dieses Amtes durch das Jugendamt nicht gegeben. Da das Jugendamt in der Regel keine Kenntnis darüber haben dürfte, ob das Sozialamt von der Veränderung in den Lebensverhältnissen des Sozialhilfeempfängers bereits Kenntnis erlangt hat, darf es die in Rede stehenden Daten nicht etwa im Hinblick darauf, dass ein gewisser Teil der Betroffenen möglicherweise seiner Mitteilungspflicht nicht genügt, die Informationen weitergeben. Aus diesem Grunde scheidet eine generelle Unterrichtung des Sozialamtes nach § 69 Abs. 1 Nr. 1, 3. Alt. SGB X in diesen Fällen aus. Eine Datenübermittlung ist allerdings dann zulässig, wenn im Einzelfall konkrete Anhaltspunkte dafür vorliegen, dass die Familie, die Jugendhilfeleistungen bezieht, ihrer Pflicht zur Unterrichtung des Jugendamtes nicht nachkommt.

Da die Datenübermittlung auch nicht auf eine andere Befugnisnorm gestützt werden kann, käme nur in Betracht, die Betroffenen – etwa im Zusammenhang mit einer Belehrung über ihre Mitteilungspflichten – um eine Einwilligung zu bitten, dass das Jugendamt (im Rahmen der Erforderlichkeit) die Unterrichtung des Sozialamtes für sie übernimmt.

Das Kultusministerium und das Ministerium für Frauen, Arbeit und Soziales, die ich wegen der grundsätzlichen Bedeutung der Angelegenheit um ihre Stellungnahme gebeten habe, teilen meine Auffassung. Sie haben zusätzlich darauf hingewiesen, dass die Erforderlichkeit der Datenübermittlung auch dann entfalle, wenn die Daten bei den Betroffenen erhoben werden können. Dem ist zwar grundsätzlich zuzustimmen. Bei der vorliegenden Fallkonstellation scheidet diese Möglichkeit allerdings aus, weil das Sozialamt regelmäßig keine konkreten Anhaltspunkte für die Gewährung der jeweiligen Jugendhilfeleistung haben dürfte.

21 Forschung

21.1 Forschung und Datenschutz: Unvereinbare Gegensätze?

Von manchen Forschern wird immer wieder die Behinderung der Forschung durch datenschutzrechtliche Vorgaben angeprangert. Dieses Thema wird auch in einer Denkschrift der Deutschen Forschungsgemeinschaft (DFG) aus dem Jahre 1996 aufgegriffen, in der einerseits auf positive Entwicklungen bei der Vereinbarkeit dieser gegensätzlichen Bereiche hingewiesen wird, andererseits aber zu weit gehende Behinderungen durch Datenschutzregelungen in den Bereichen Sozialwissenschaften, Erziehungswissenschaften, Kriminologie, Geschichtswissenschaften und der medizinischen Forschung aufgeführt werden. Die Datenschutzbeauftragten sind bereits in der Vergangenheit auf diese Kritik eingegangen und haben darauf hingewiesen, dass zwischen den Grundrechten der Forschungsfreiheit und der informationellen Selbstbestimmung ein vernünftiges Gleichgewicht beibehalten werden muss und dass die Einschränkung der Forschung durch datenschutzrechtliche Regelungen weitaus geringer ist, als von manchen Kritikern behauptet wird (vgl. XIII 22).

Die Erfahrungen aus meiner Datenschutzpraxis zeigen, dass in konkreten Projekten weit weniger Probleme auftreten, als die öffentliche Kritik suggerieren will (siehe 21.2). Vielfach sehen die Forscher selbst die Datenschutzprobleme und suchen nach vernünftigen Lösungen. Auch sind sie oft auf die freiwillige Mithilfe der Betroffenen angewiesen und haben von daher schon das Bestreben, ein datenschutzrechtlich unangreifbares Konzept anzubieten.

Dass nach pragmatischen Lösungen gesucht wird, zeigen die gemeinsamen Aktivitäten der Deutschen Arbeitsgemeinschaft für Epidemiologie (DAE) und des Arbeitskreises Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. In gemeinsamen Workshops wurden Probleme bei der epidemiologischen Forschung durch datenschutzrechtliche Restriktionen untersucht und Lösungswege gefunden. Ergebnis ist das Arbeitspapier „Epidemiologie und Datenschutz“, das Lösungsansätze zu folgenden Problemfeldern liefert:

- Zweckbindung von personenbezogenen Daten,
- Löschung der Daten nach Beendigung des Forschungsvorhabens,
- Weitergabe anonymisierter Daten,
- Gestaltung der Einverständniserklärung,
- Verknüpfung personenbezogener Datensätze z. B. bei Kohortenstudien,

– Nutzung der amtlichen Statistik,

– Aufbewahrung von Daten der amtlichen Statistik,

– Nutzung von Krebsregistern für Fall-Kontroll-Studien,

– Datenschutzfragen bei bundesweiten Studien.

Das Arbeitspapier kann über das Internet-Angebot des Hessischen Datenschutzbeauftragten (www.hessen.de/hdsb), der den Vorsitz im Arbeitskreis Wissenschaft innehat, abgerufen oder bei mir angefordert werden. Die Suche nach pragmatischen Lösungen ist der richtige Weg, um die von Kritikern angeführten Forschungshindernisse aus dem Weg zu räumen oder zumindest zu minimieren. Dieser Weg sollte auch in anderen Spezialgebieten der Forschung beschritten werden.

Bestimmte Forscherkreise, insbesondere die Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften (AWMF), gehen aber über die Suche nach pragmatischen Lösungen weit hinaus. Sie fordern grundsätzliche Gesetzesänderungen, etwa die Einführung eines medizinischen Forschungsgeheimnisses und die Ersetzung der staatlichen Kontrolle durch eine Selbstkontrolle der Forscher. Solche Gesetzesänderungen brächten aber nicht nur eine deutliche Verschlechterung der Datenschutzrechte der Betroffenen mit sich. Sie wären auch eine Gefahr für das Grundrecht auf Forschungsfreiheit, wenn beispielsweise nur bestimmten, „genehmen“ Forschern das medizinische Forschungsgeheimnis zugestanden würde oder die Gremien der Selbstkontrolle aufgrund ihrer Tätigkeit nicht unbefangen die Vorhaben ihrer Kollegen bewerten könnten. Ich stehe solchen Entwicklungen eher skeptisch gegenüber und plädiere dafür, die bestehenden gesetzlichen Regelungen im Grundsatz beizubehalten.

21.2 Datenschutzaufsicht im Forschungsbereich: Mehr Beratung als Kontrolle

Auch wenn das Interesse der Forschung in den meisten Fällen nicht personenbezogenen Daten gilt, so wird doch das Recht auf informationelle Selbstbestimmung der betroffenen „Probanden“ durch beinahe jedes Forschungsvorhaben berührt. Der Gesetzgeber hat daher die Datenverarbeitung zu Forschungszwecken in den Datenschutzgesetzen besonders berücksichtigt. § 25 NDSG regelt als allgemeine „Forschungsklausel“ die Verarbeitung personenbezogener Daten für wissenschaftliche Zwecke durch öffentliche Stellen, die Forschung betreiben, sowie die Übermittlung von öffentlichen Stellen an Forschende. Nach § 25 Abs. 2 NDSG dürfen in wissenschaftlichen Forschungsvorhaben personenbezogene Daten, die für andere Zwecke oder für ein anderes Forschungsvorhaben erhoben oder gespeichert worden sind, nur verarbeitet werden, wenn die Betroffenen eingewilligt haben, eine Rechtsvorschrift dies vorsieht oder Art und Verarbeitung der Daten darauf schließen lassen, dass ein schutzwürdiges Interesse der Betroffenen der Verarbeitung der Daten für das Forschungsvorhaben nicht entgegensteht oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens das schutzwürdige Interesse der Betroffenen erheblich überwiegt. Beim Zugang zu personenbezogenen Informationen sollte zusätzlich der Grundsatz der Datensparsamkeit beachtet werden. Jeder Forschende sollte methodisch gezwungen sein, mit möglichst wenig Daten auszukommen und sie zum frühestmöglichen Zeitpunkt zu anonymisieren. Dies verhindert die viel zitierten „Datenfriedhöfe“.

Ich stehe mit vielen Forschenden im ständigen Dialog. Dabei fungiere ich in erster Linie als Berater, der Gestaltungshilfen gibt, um das wissenschaftliche Vorgehen auf einen größtmöglichen Schutz der Persönlichkeitsrechte der Betroffenen auszurichten. Nach diesen Beratungen bedanken sich die Forschenden häufig bei mir, weil sie neben Informationsmaterialen einfache, datenschutzfreund-

lichere Wege zum Forschungsziel genannt bekommen haben, ohne Qualitätsverluste der Forschungsergebnisse befürchten zu müssen. Sicherlich ist auch eine positive datenschutzrechtliche Bewertung eines Projektes durch mich eine wichtige Voraussetzung, um Probanden zur Teilnahme zu bewegen. Auf diese Weise können datenschutzrechtlich bedenkliche Schritte von vornherein vermieden werden. Mir sind keine Beispiele bekannt, bei denen sich dieses Vorgehen als falsch erwiesen hätte.

In den Jahren 1997/98 war ich bei insgesamt 40 Forschungsvorhaben beteiligt. Ich habe in keinem einzigen Fall ein Forschungsvorhaben formell beanstanden müssen. Bei den meisten Vorhaben wurden Einwilligungen der Probanden eingeholt. Hierzu habe ich eine Muster-Einwilligung entwickelt, der den Forschenden im Rahmen der Beratungsgespräche übergeben wurde.

Lediglich zweimal wurde eine Abwägung zwischen den schutzwürdigen Interessen der Betroffenen und dem öffentlichen Interesse an der Durchführung des Forschungsvorhabens vorgenommen. Für eine solche Abwägung lassen sich keine allgemeinen Regeln aufstellen. Sie muss für jedes Forschungsprojekt gesondert getroffen werden. Hierbei sollten folgende Aspekte untersucht und dargestellt werden:

- Zielsetzung und Begründung des Projektes,
- Art und Umfang der im Forschungsvorhaben zu erfassenden personenbezogenen Daten,
- Anzahl der Betroffenen,
- Zeitpunkt der Pseudonymisierung/Anonymisierung,
- Güte der Anonymisierung,
- Ablauf des Projektes,
- Art und Weise der Auswertung,
- Anzahl der Forschenden,
- Zeitraum der Vorhaltung personenbezogener Daten,
- Datensicherung.

Ich gehe davon aus, dass auch in Zukunft der Dialog mit mir geführt wird und mein Beratungsangebot Zuspruch findet. Ich stehe hierfür auch mit den behördlichen Datenschutzbeauftragten, insbesondere den Datenschutzbeauftragten der Hochschulen, in Kontakt, die im Rahmen der letzten Novellierung des NDSG stärker in die datenschutzrechtliche Kontrolle von Forschungsvorhaben eingebunden wurden.

22 Hochschulen

22.1 Telefon- und Vorlesungsverzeichnisse im Internet?

Im Hochschulbereich wird das Internet so intensiv wie in kaum einem anderen Bereich genutzt. Schwerpunkt ist natürlich der Austausch von Forschungsergebnissen. Der Besuch der Hochschul-Homepages macht aber schnell deutlich, dass darüber hinaus in den schillerndsten Variationen auch personenbezogene Daten von Hochschulbediensteten und Studenten präsentiert werden. Es finden sich Telefonlisten, Vorlesungsverzeichnisse, Namenslisten mit Gruppen- und Einzelbildern, Lebensläufe, Klausurergebnisse und vieles mehr. Häufig sind Daten von den betroffenen Personen selbst oder auf deren Veranlassung hin eingestellt worden. Dies trifft aber längst nicht immer zu. Viele Mitarbeiter oder Studenten

werden durch diese Praxis und durch die weltweite Verbreitung des Internets erheblich in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt.

Ich habe mich zu dieser Problematik in meinem letzten Tätigkeitsbericht geäußert (XIII 23.1). Offenbar bestand aber immer noch viel Unsicherheit in dieser Sache, die dazu führte, dass beim letzten Verfahren zur Novellierung des Niedersächsischen Hochschulgesetzes der Wunsch an den Gesetzgeber herangetragen wurde, die Veröffentlichung von „Vorlesungs- und Institutionenverzeichnissen“ im Internet pauschal für zulässig zu erklären. Einer solchen Regelung konnte ich nicht zustimmen, da sie das Recht der Betroffenen auf informationelle Selbstbestimmung viel zu weitreichend eingeschränkt hätte. Ergebnis der Gesetzesberatungen war, auf eine Regelung im Gesetz zu verzichten und auf dem Erlasswege eine klare Richtschnur für alle niedersächsischen Hochschulen zur Verfügung zu stellen.

Dieser Erlass ist inzwischen mit mir abgestimmt und im Niedersächsischen Ministerialblatt (1998 S. 984) veröffentlicht worden. Er führt aus, dass eine Veröffentlichung im Internet zulässig ist, soweit es sich um folgende Daten handelt:

- Forschungsergebnisse unter Nennung der Autorinnen und Autoren sowie der Forschungseinrichtung,
- Ankündigungen und Berichte von Tagungen mit Namen der Referentinnen und Referenten und Kontakadressen,
- Namen, Kontaktadressen und Forschungsgebiet der unmittelbar in Forschung und Lehre tätigen Bediensteten,
- Sprechzeiten sowie Bezeichnungen und Termine von Lehrveranstaltungen der lehrenden Bediensteten,
- Private Kontaktadressen nur, wenn die vorgenannten Bediensteten sonst dienstlich nicht erreichbar sind.

Weitere Angaben dürfen nur mit schriftlich erklärter Einwilligung der Betroffenen veröffentlicht werden. Die Veröffentlichung von Studentendaten ohne Einwilligung ist grundsätzlich unzulässig.

Der Erlass stellt eine pragmatische Vorgabe dar, die den Bedürfnissen der Hochschulen weitgehend gerecht werden sollte, ohne die Datenschutzrechte der Betroffenen über das zulässige Maß hinaus zu beeinträchtigen. Seit der Veröffentlichung des Erlasses gibt es praktisch keine Nachfragen oder Beschwerden mehr zu diesem Problembereich, ein klares Indiz dafür, dass hier der richtige Weg eingeschlagen wurde.

22.2 Gemeinsamer Bibliotheksverbund norddeutscher Länder

Zum Gemeinsamen Bibliotheksverbund (GBV) mit der Verbundzentrale in der Niedersächsischen Staats- und Universitätsbibliothek Göttingen gehören inzwischen die Freie Hansestadt Bremen, die Freie und Hansestadt Hamburg sowie die Länder Mecklenburg-Vorpommern, Niedersachsen, Sachsen-Anhalt, Schleswig-Holstein und der Freistaat Thüringen. Rechtsgrundlage des Niedersächsischen Bibliotheksverbundes sind §§ 129 und 130 des Niedersächsischen Hochschulgesetzes (NHG). Darüber hinaus enthält der Runderlass des Niedersächsischen Ministeriums für Wissenschaft und Kultur vom 25. August 1992 (Nds. MBl. 1992 S. 1386) nähere Verfahrensregeln und Festlegungen zum Datenkatalog. Der Erlass ist auch nach Aussage des Ministeriums für Wissenschaft und Kultur dringend überarbeitungsbedürftig.

Der Zugang zu den zentralen Nachweisdatenbanken erfolgt in aller Regel über das Internet. Für die kostenpflichtige Fernleihe von Literatur aus anderen Bibliotheken wurde ein Verfahren entwickelt, das einen unabstreitbaren Nachweis über Bestellungen und Besteller liefert sowie eine sichere Abrechnung ermöglicht. Zu den hierfür benötigten personenbezogenen Daten gehören Name, Anschrift, Abrechnungskonto und Identifikationsnummer (Passwort). Die Zuteilung der Bestellberechtigung kann nach zwei alternativen Verfahren erfolgen. Ich empfehle die Alternative der „anonymen Zugangsnummer". Dabei muss der Benutzer allerdings bei seiner ersten Bestellung Name und Adresse angeben, soweit es für eine ordnungsgemäße Zustellung der Literaturlieferung notwendig ist. Bei der Alternative der Verwendung lokaler Benutzernummern wird der Datenbestand der lokalen Nutzerdatei an die Verbundzentrale übermittelt. Für die Übermittlung der vorhandenen Nutzerdaten an die Verbundzentrale ist eine informierte, schriftliche Einwilligung der Nutzer erforderlich. In der Unterrichtung wird der Nutzer auch über die Folgen einer Verweigerung aufgeklärt.

Für die Angabe von Zugangsnummer und Passwort zur Vornahme einer Bestellung habe ich eine Verschlüsselung gefordert. Die Verschlüsselung erfolgt bereits jetzt bei einer Bestellung über allgemein zugängliche Fernleih-PC in den Bibliotheken. Ungesichert war bisher allerdings die ebenfalls zugelassene Bestellung über einen privaten PC aus häuslicher Umgebung. Die Verbundzentrale hat mir erklärt, dass für diese Bestellart ein JAVA-Applet in Vorbereitung sei, das eine verschlüsselte Übertragung sicherstellen wird. Ich habe gefordert, die Fernleih-Benutzer auf die bestehende Unsicherheit hinzuweisen. Eine aktuelle Unterrichtung über den Stand der Sicherungstechnik steht noch aus.

22.3 Lokaler Bibliotheksverbund in Oldenburg

Im Raum Oldenburg ist eine engere Zusammenarbeit zwischen der Landesbibliothek Oldenburg, der Fachhochschule Oldenburg und der Universitätsbibliothek der Carl-von-Ossietzky-Universität vereinbart worden. Hierfür war die Ausgabe eines gemeinsamen Bibliotheksausweises vorgesehen. Die Einführung dieses Systems ist von mir durch Beratung zu datenschutzrechtlichen Aspekten des Bibliotheksverbundes begleitet worden. Meinen Empfehlungen wurde in vollem Umfang gefolgt; die Realisierung einzelner Teilaspekte wie die Datenverschlüsselung bei der Übertragung personenbezogener Daten über öffentliche Netze musste jedoch wegen fehlender Haushaltsmittel zurückgestellt werden, obwohl die Erforderlichkeit erkannt war.

23 Schulen

23.1 Regelmäßige Datenübermittlungen

Wie bereits unter 6.1 Nr. 5 ausgeführt, ist durch die Streichung des § 12 Abs. 6 NDSG das Erfordernis einer Rechtsverordnung für regelmäßige Datenübermittlungen entfallen. Die nach Wegfall der Ermächtigungsgrundlage gegenstandslosen Regelungen der Verordnung über regelmäßige Datenübermittlungen und automatisierte Abrufverfahren im Geschäftsbereich des Kultusministeriums sind durch Verordnung vom 29. September 1998 (Nds GVBl. S. 639) aufgehoben worden. Dies bedeutet – insbesondere für die Schulen – nicht, dass die darin geregelten regelmäßigen Datenübermittlungen generell unzulässig werden. Die Zulässigkeit der Übermittlung ergibt sich aus den dafür geltenden allgemeinen Regelungen (§ 31 NSchG i. V. m. den §§ 11 und 13 NDSG). Hiernach dürfen z. B. die in § 2 der bisherigen Verordnung angesprochenen Daten von Schülerinnen, Schülern und Erziehungsberechtigten an Schulträger und an Mitschüler sowie deren Erziehungsberechtigte weiterhin übermittelt werden.

23.2 Aufbewahrung von Schriftgut in Schulen

Das MK hat mit Runderlass vom 28. Februar 1996 (Nds. MBl. S. 591) die Aufbewahrung von Schriftgut in Schulen und die Löschung personenbezogener Daten nach § 17 Abs. 2 NDSG geregelt. Unterschieden wird hierbei nach der Art des Schriftgutes. Grundsätzlich ist das Schriftgut nach Ablauf der jeweils bestimmten Frist, spätestens jedoch 30 Jahre nach der letzten inhaltlichen Bearbeitung, dem zuständigen Staats- oder Kommunalarchiv zur Übernahme anzubieten. Wird das Schriftgut nicht von einem Archiv übernommen, ist es nach Ablauf der im Erlass bestimmten Frist zu vernichten oder, wenn es sich um maschinenlesbare Datenträger handelt, zu löschen. Die Archive müssen sich innerhalb von zwei Jahren nach der Veröffentlichung des Runderlasses bei den von ihnen zu bestimmenden Schulen melden und mitteilen, welches Schriftgut zur Übernahme anzubieten ist. Erfolgt eine solche Meldung nicht, vernichtet die Schule das Schriftgut.

23.3 Übermittlung eines Beratungsgutachtens an den Vorsitzenden des Schulelternrates

Ein schulpflichtiges behindertes Kind eines Petenten wurde einer sonderpädagogischen Begutachtung unterzogen. Danach stellten die Eltern dieses Kindes an einer Grundschule einen Antrag auf integrative Beschulung. Gemäß § 23 Abs. 4 NSchG können im ersten bis zehnten Schuljahrgang der allgemeinbildenden Schulen Integrationsklassen eingerichtet werden, in denen Schülerinnen und Schüler, die einer sonderpädagogischen Förderung bedürfen, gemeinsam mit anderen Schülerinnen und Schülern unterrichtet werden und in denen die Leistungsanforderungen der unterschiedlichen Lernfähigkeit entsprechen. Das Beratungsgutachten wurde mit Einverständnis der Eltern an die zuständige Grundschule geschickt. Diese leitete eine Abschrift dem Vorsitzenden des Schulelternrats zu. Der Petent war über die Weitergabe des Gutachtens erstaunt. Er stellte die Frage, wozu der Schulelternrat das Beratungsgutachten benötige.

Der Schulelternrat wirkt bei der Entscheidung, ob eine Integrationsklasse eingerichtet wird, mit. Hierbei ist zu prüfen, ob die betreffende Schule die spezifischen Anforderungen an eine integrative Beschulung erfüllt. Das Verfahren ist im Erlass des Kultusministeriums „Einrichtung von vollen Halbtagsschulen und Integrationsklassen“ vom 30. September 1993 geregelt. Für seine Meinungsbildung benötigt der Schulelternrat Informationen über die personellen, sächlichen und organisatorischen Voraussetzungen für die Einrichtung einer Integrationsklasse. Diese können durch den Schulleiter gegeben werden. Die Kenntnis des Beratungsgutachtens ist dagegen für den Schulelternrat nicht erforderlich.

Dieses Gutachten soll eine Kind-Umwelt-Analyse enthalten. Die Persönlichkeitsentwicklung eines Kindes ist unter Einbeziehung des familiären und außerschulischen Umfeldes zu beschreiben. Das Gutachten ist eine Entscheidungshilfe für die Schulbehörde bei der Feststellung, ob ein sonderpädagogischer Förderungsbedarf im Einzelfall besteht. Zur Vorbereitung dieser Entscheidung können von einer Förderkommission Empfehlungen erarbeitet werden. Die Mitglieder der Förderkommission und die Schulbehörde müssen deshalb Kenntnis von dem Gutachten haben, der Schulelternrat dagegen nicht.

23.4 Beurteilung von Lehrkräften durch Elternvertreter

Auf Initiative von Elternvertretern wurden an einer Schule ausgewählte Lehrkräfte durch Schüler einer bestimmten Klasse beurteilt. Dazu hatten die rührigen Elternvertreter Fragebögen entwickelt und ausgewertet. Nach Darstellung des Personalrats waren lediglich der Schulleiter und ein Klassenlehrer in die Aktion eingeweiht. Die beurteilten Lehrkräfte erfuhren erst nach der Auswertung davon, als ihnen ein Mitglied der Elternvertretung die ihren Unterricht betreffenden Ergebnisse mitteilte.

Der hierüber ausbrechende Unmut im Lehrerkollegium war nicht nur wegen der Art und Weise, in der die Beurteilung vorgenommen wurde, berechtigt. Die Elternvertretung hatte sich Befugnisse angemaßt, die ihr nicht zustehen.

Die Mitwirkungsrechte der Elternvertretungen umfassen gemäß § 69 NSchG das Recht, schulische Fragen zu erörtern sowie vor grundsätzlichen Entscheidungen gehört zu werden und die erforderlichen Auskünfte von Lehrkräften und der Schulleitung zu erhalten. Die Befragung von Schülerinnen und Schüler im Rahmen eines „Feed-back-Verfahrens“ gehört nicht dazu. Sie ist daher gemäß § 31 Abs. 2 NSchG i. V. m. § 4 Abs. 1 Nr. 2 NDSG ohne Einwilligung der Betroffenen nicht zulässig.

24 Landwirtschaft und Forsten

24.1 Tierschutzgesetz

In XIII 25.1 hatte ich von der Initiative Niedersachsens berichtet, eine Änderung des Tierschutzgesetzes herbeizuführen. Inzwischen ist in das am 25. Mai 1998 (BGBl. I S. 1094) neu gefasste Tierschutzgesetz mit § 16 Abs. 6 eine datenschutzrechtliche Regelung aufgenommen worden, die zumindest inhaltlich meinem ursprünglichen Vorschlag entspricht. Damit enthält das Gesetz nunmehr eine hinreichende Datenverarbeitungsnorm. Durch eine Verordnungsermächtigung wird das Bundesministerium für Ernährung, Landwirtschaft und Forsten ermächtigt, weitere datenschutzrelevante Bestimmungen zu treffen. Ich begrüße aus grundsätzlichen Erwägungen die Schaffung dieser Rechtsgrundlage für die Datenverarbeitung in der Erwartung, dass die entsprechende Verordnung baldmöglichst folgt.

24.2 Tierzuchtgesetz

War die Zusammenarbeit mit dem Fachressort im Falle der Novellierung des Tierschutzgesetzes (vgl. 24.1) ein äußerst positives Beispiel für eine konstruktive Zusammenarbeit mit mir durch rechtzeitige Information, so wurde ich bei dem Verfahren zur Änderung des Tierzuchtgesetzes nicht beteiligt. Auch dieses Gesetz ist kürzlich geändert worden. Es hätte sich aus datenschutzrechtlicher Sicht ebenfalls angeboten, Regelungen zur Datenverarbeitung vorzusehen. Dies ist leider unterblieben.

24.3 Petri Heil

Ein Angler beschwerte sich darüber, dass ein Fischereiaufseher seine Daten wie Name, Anschrift und Geburtstag notierte, obwohl die Kontrolle seiner Fischereipapiere und Fanggeräte keine Beanstandung ergeben hatte. Mit dem Ministerium für Ernährung, Landwirtschaft und Forsten (ML) bin ich der Auffassung, dass keinerlei Grund besteht, bei einer Fischereikontrolle, die keinen Anlass zu

Beanstandungen ergibt, Name, Anschrift und Geburtsdatum des Anglers zu notieren.

In diesem Zusammenhang ist zu begrüßen, dass das ML den Einzelfall zum Anlass genommen hat, den Landessportfischerverband Niedersachsen e.V. und den Landesfischereiverband Weser-Ems anzuschreiben, um dort eine Sensibilisierung bezüglich der Datenerhebung und -speicherung zu erreichen. Ferner hat es die Fischereiverbände gebeten, die Mitgliedsvereine ihres Verbandes, besonders die Gewässerwarte und die von diesen betreuten Fischereiaufseher, auf dieses Problemfeld hinzuweisen und möglicherweise erhobene und noch vorhandene personenbezogene Daten von Fischereikontrollen (ohne Beanstandungen) zu vernichten. Die Verbände sind schließlich vom ML gebeten worden, im Rahmen von Schulungen und Fortbildungen für Fischereiaufseher und Gewässerwarte auf dieses Problem hinzuweisen. Aus datenschutzrechtlicher Sicht ein erfreuliches Beispiel für nachgehenden und präventiven Datenschutz.

25 Wirtschaft

25.1 Bekanntgabe der Erteilung von Reisegewerbekarten an Industrie- und Handelskammern

Einzelne Gewerbebehörden übermitteln Daten der Reisegewerbekarten an die Industrie- und Handelskammern. Für diese Datenweitergabe gibt es keine Rechtsgrundlage. § 14 Abs. 5 Gewerbeordnung (GewO) lässt sich nicht heranziehen, da dort abschließend der Bereich des stehenden Gewerbes geregelt ist. Da auch weitere Regelungen der Gewerbeordnung als Rechtsgrundlage für die Datenübermittlung der Reisegewerbekarten an die Industrie- und Handelskammern ausscheiden, ist diese unzulässig. In dieser Rechtsauffassung bin ich mir mit dem zuständigen Niedersächsischen Ministerium für Wirtschaft, Technologie und Verkehr einig. Von dort ist mir auf meine Nachfrage mitgeteilt worden, dass derzeit bundesweit bei den zuständigen Ministerien erwogen wird, § 55 GewO um einen neuen Abs. 4 zu erweitern, der § 14 Abs. 5 GewO auch für das Reisegewerbe für anwendbar erklären soll. Darüber hinaus soll im Vorfeld dieser Überlegungen geklärt werden, ob ein Bedarf auch anderer Stellen an einer solchen Datenweitergabe in Betracht käme. Damit ist bis zu einer etwaigen Neuregelung die Übermittlung der Daten der Reisegewerbekarten an die Industrie – und Handelskammern unzulässig.

25.2 Weitergabe von Mitgliederadressen an Innungsmitglieder

Datenschutzrechtliche Probleme gab es, als sich eine Handwerksinnung aus datenschutzrechtlichen Gründen weigerte, einem ihrer Mitglieder die Adressen der übrigen Innungsangehörigen mitzuteilen. Das Innungsmitglied beabsichtigte, sich an die Innungsmitglieder direkt zu wenden, um sie für die Einberufung einer außerordentlichen Innungsversammlung zu gewinnen. Eine solche ist laut Satzung möglich, wenn ein Viertel der stimmberechtigten Mitglieder die Einberufung beantragt.

Nach Auffassung des Niedersächsischen Ministeriums für Wirtschaft, Technologie und Verkehr (MW) war eine Übermittlung der Daten auf der Grundlage des § 13 Abs. 1 Nr. 2 NDSG zulässig. Die Innung war gehalten, dem Petenten die gewünschten Adressen herauszugeben, da er auf andere Weise nicht die satzungsmäßig vorgegebene Bedingung für die Einberufung einer außerordentlichen Innungsversammlung hätte herbeiführen können. Er musste in die Lage versetzt werden, mindestens ein Viertel der übrigen Mitglieder für eine entsprechende Antragsstellung zu erreichen. Dem steht – so das MW - auch kein über-

wiegendes schutzwürdiges Interesse der übrigen Innungsmitglieder an der Geheimhaltung ihrer Namen und Adressen gegenüber dem eigenen Innungsmitglied entgegen. Ich habe mich dieser Begründung nicht verschlossen, weil sie mir vertretbar und angemessen erscheint.

25.3 Datenschutz als Reformmotor

Zur Vorbereitung örtlicher Eichtage, an denen regelmäßig Nacheichungen von Messgeräten vorzunehmen sind, übersandte in Niedersachsen das Eichamt die Daten der Eichpflichtigen den örtlichen Gemeinden, damit diese dann die jeweils Betroffenen anschrieben und auf die örtlichen Eichtage hinwiesen. Begründet wurde dieses Vorgehen damit, dass die Eichämter aufgrund ihrer personellen und sachlichen Ausstattung nicht in der Lage seien, selbst die entsprechenden Mitteilungsschreiben an die betroffenen Eichpflichtigen zu versenden.

Bei meiner datenschutzrechtlichen Überprüfung habe ich die Erforderlichkeit dieser Datenübermittlung vom Eichamt an die Gemeinden in Zweifel gezogen. Als Begründung für den beschriebenen Organisationsablauf hat mir das zuständige Ministerium für Wirtschaft, Technologie und Verkehr (MW) mitgeteilt, die Eichämter hätten die Gemeinden lediglich zur eigenen Verwaltungserleichterung die Aufforderungsschreiben fertigen lassen, weil sie sich dazu aufgrund ihrer Ausstattung selbst nicht in der Lage sahen. Schlechte personelle und sachliche Ausstattung kann aber keine datenschutzrechtliche Erforderlichkeit für eine Datenübermittlung begründen.

In verschiedenen Gesprächen konnte ich das MW davon überzeugen, dass das Einschalten der Gemeinden den datenschutzrechtlichen Ansprüchen nicht genügt und das Verfahren geändert werden muss. Das MW sah sich aufgrund meines Hinweises veranlasst, schnellstmöglich dafür Sorge zu tragen, dass eine direkte Benachrichtigung der Eichpflichtigen in Niedersachsen durch die Eichverwaltung selbst erfolgt.

Inzwischen wird die Eichverwaltung umorganisiert und mit neuer IuK-Technik ausgestattet. Im Zuge dieser Umorganisation soll auch das Benachrichtigungsverfahren in der Weise umgestellt werden, dass eine Benachrichtigung der Eichpflichtigen direkt durch die Eichverwaltung erfolgt. Damit ist ein Verwaltungsweg gespart, die Bekanntmachung der Eichtage erfolgt schneller, und das Verfahren genügt den datenschutzrechtlichen Ansprüchen. Die konkstruktive Zusammenarbeit zeigt, dass richtig angewandter Datenschutz durchaus innovativ wirken kann.

26 Verkehr

26.1 Änderung des Straßenverkehrsgesetzes und anderer Gesetze

Das Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze vom 24. April 1998 (BGBl. I S. 747) sieht aus Sicht des Datenschutzes wesentliche Neuerungen vor, die am 01. Januar 1999 in Kraft treten werden. Einige möchte ich im Folgenden nennen:

Neu eingeführt wird beim Kraftfahrt-Bundesamt (KBA) neben dem schon bestehenden Zentralen Fahrzeugregister (ZFR) und dem Verkehrszentralregister (VZR) - das Zentrale Fahrerlaubnisregister (ZFER). Da alle Fahrerlaubnisinhaber gespeichert werden, handelt es sich um ein Register mit fast 50 Millionen Datensätzen. Erfasst werden die unveränderbaren Personalien und Führerscheindaten der Betroffenen. Die Anschriften werden nicht gespeichert. Damit wird auf die Einführung eines neuen bundesweiten „Melderegisters“ von Führer-

scheininhabern verzichtet. Zusätzlich werden in das ZFER die Daten über die Fahrlehrer und die Kraftfahrzeugsachverständigen übernommen, die bisher beim KBA in eigenständigen Fahrlehrer- und Kraftfahrzeugsachverständigenregistern geführt wurden. Neben zahlreichen deutschen Stellen erhalten viele öffentliche Stellen der EU-Mitgliedstaaten im automatisierten Verfahren Zugriff auf das ZFER.

Die Kritik der Datenschutzbeauftragten hinsichtlich einer Doppelspeicherung der Führerscheininhaber im ZFER und in den örtlichen Fahrerlaubnisregistern hat gewirkt (vgl. XIII 27.1). Die örtlichen Register müssen bis zum 31. Dezember 2005 aufgelöst sein. Damit wird das Nebeneinander des ZFER und der örtlichen Fahrerlaubnisregister auf einen Übergangszeitraum von höchstens 7 Jahren beschränkt. Insgesamt bin ich aber nach wie vor von der Notwendigkeit eines Zentralen Fahrerlaubnisregisters im Sinne eines überwiegenden Allgemeininteresses nicht überzeugt. Angesichts der zahlreichen europaweiten Abrufmöglichkeiten öffentlicher Stellen besteht mit der Einrichtung des zentralen Registers jederzeit die Möglichkeit, ein umfassendes elektronisches Überwachungssystem nicht nur für den Verkehrsbereich zu schaffen. Ein europäisches Verkehrszentralregister, das der Kontrolle durch die Landesdatenschutzbeauftragten entzogen wäre, könnte dann am Ende der Entwicklung stehen.

Bisher wurden Abrufe aus dem VZR und dem ZFR protokolliert und durften nur für Zwecke der Datenschutzkontrolle genutzt werden. Nunmehr wird die Nutzung der Protokolldaten über Abrufe aus dem VZR, dem ZFR und dem ZFER auch zur Aufklärung oder Verhütung von schwerwiegenden Straftaten gegen Leib, Leben und Freiheit einer Person zugelassen. Die Aufbewahrungsfrist der Protokolldaten wird aufgrund der bisherigen Erfahrungen von drei auf sechs Monate verlängert. Damit erhalten die Protokolldateien den Charakter polizeilicher Fachdateien.

Aus datenschutzrechtlicher Sicht zu begrüßen ist, dass für die Datenverarbeitung in Führerscheinakten erstmalig gesetzliche Festlegungen getroffen worden sind, auch wenn sie leider nicht umfassend sind. Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse sind nunmehr nach spätestens zehn Jahren zu vernichten, es sei denn, die Unterlagen stehen im Zusammenhang mit einer Eintragung im VZR oder im ZFER. Unterlagen in „Altakten“ müssen allerdings erst dann berichtigt werden, wenn die Fahrerlaubnisbehörde aus anderem Anlass mit dem Vorgang befasst ist. Fünfzehn Jahre nach Inkrafttreten des Gesetzes sollen alle Akten auf „Vernichtenswertes“ überprüft sein.

Positiv zu erwähnen ist auch die Korrektur der bislang möglichen lebenslangen Verwendung von Informationen über Entscheidungen, die sowohl im Bundeszentralregister als auch im VZR eingetragen waren. In Verfahren, die die Erteilung oder Entziehung einer Fahrerlaubnis zum Gegenstand haben, galt bisher eine unbefristete Verwertungsmöglichkeit, selbst wenn die Eintragungen in den beiden Registern getilgt waren (vgl. § 52 Abs. 2 Bundeszentralregistergesetz). Nunmehr dürfen die Tat und die Entscheidung dem Betroffenen nach der Tilgung im VZR im Verfahren über die Erteilung oder Entziehung der Fahrerlaubnis nicht mehr vorgehalten werden.

Außerdem sieht das Gesetz, im Gegensatz zu früheren Entwürfen, eine kostenfreie Auskunft über die eigenen Daten vor (vgl. §§ 30 Absatz 8, 58 Straßenverkehrsgesetz).

26.2 Fahrerlaubnis-Verordnung

Die Fahrerlaubnis-Verordnung (FeV) vom 18. August 1998 tritt am 01. Januar 1999 in Kraft (BGBl. I S. 2214). Da bisher wesentliche Fragen der Datenverarbeitung im Zusammenhang mit Fahrerlaubnissen nicht geregelt waren, ist die Neufassung des Fahrerlaubnisrechts grundsätzlich zu begrüßen.

Positiv zu erwähnen ist, dass für die ärztliche Bescheinigung, durch die Bewerber um eine Fahrerlaubnis zur Fahrgastbeförderung ihre körperliche und geistige Eignung nachzuweisen haben, ein bundeseinheitliches Muster vorgegeben wird. Wie ich in meinem letzten Tätigkeitsbericht dargelegt habe (vgl. XIII 27.2), gab es bisher keine Regelungen darüber, welchen Inhalt und Umfang das z. B. von Bus- und Taxifahrern vorzulegende ärztliche Zeugnis haben muß. Dies hatte dazu geführt, dass Ärzte detaillierte Angaben zur Krankengeschichte von Bewerbern aufgelistet hatten, die die Erlaubnisbehörden nicht kennen mussten. Das durch die FeV vorgegebene Muster für die ärztliche Bescheinigung gliedert sich in zwei Teile. Der erste Teil mit einzelnen Untersuchungsergebnissen verbleibt beim Arzt und nur der zweite Teil mit den Schlußfolgerungen des Arztes wird dem Bewerber zur Vorlage bei der Erlaubnisbehörde ausgehändigt.

Die im Straßenverkehrsgesetz neu geschaffene gesetzliche Grundlage für das Verfahren zur Anforderung medizinisch-psychologischer Gutachten über die Eignung der Betroffenen zur Führung von Kraftfahrzeugen und die damit verbundenen Datenverarbeitungsschritte, die sich bisher nur auf Verwaltungsvorschriften stützten, wird durch die FeV konkretisiert. Ich begrüße grundsätzlich die Regelung der Datenverarbeitung, zumal die fehlenden Rechtsgrundlagen in der Vergangenheit immer wieder zu Eingaben führten. Ich bedauere jedoch, dass eine vollständige normenklare Regelung unterblieben ist. So wird zwar die Datenübermittlung der Fahrerlaubnisbehörden festgelegt, hinsichtlich der Datenverarbeitung und Datenübermittlung der begutachtenden Stellen fehlen jedoch nähere Angaben. Zudem fällt auf, dass bisher erforderliche Einwilligungen der Betroffenen durch gesetzliche Bestimmungen ersetzt werden. Außerdem geht die Verordnung hinsichtlich der Übersendung der Unterlagen an die begutachtenden Stellen über die Ermächtigungsgrundlage hinaus. Während das Straßenverkehrsgesetz lediglich die Übermittlung der Daten vorsieht, die zur Aufgabenerfüllung benötigt werden, bestimmt die FeV die Übersendung der vollständigen Unterlagen.

27 Rechtspflege

27.1 Fehlende bereichsspezifische Regelungen bei der Justiz

15 Jahre nach dem Volkszählungsurteil fehlt es im Bereich der Justiz weitgehend immer noch an bereichsspezifischen gesetzlichen Grundlagen für die dort umfangreich anfallende Datenverarbeitung. Lediglich in Teilbereichen sind inzwischen Gesetze geschaffen worden. So enthalten das Vierte Gesetz zur Änderung des Strafvollzugsgesetzes vom 26. August 1998 (BGBl. I S. 2461) Regelungen für die Datenverarbeitung im Bereich des Strafvollzuges und das Justizmitteilungsgesetz vom 18. Juni 1997 (BGBl. I S. 1430) Regelungen für den Bereich der Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen. Beide Gesetze habe ich kritisch begleitet (vgl. 28.1 und XIII 28.2).

Für den umfangreichen Bereich der Strafverfolgung fehlt es jedoch immer noch an Datenverarbeitungsregelungen, sodass die dort anfallenden hochsensiblen personenbezogenen Daten ohne Rechtsgrundlage verarbeitet werden. Das seit vielen Jahren in Arbeit befindliche Strafverfahrensänderungsgesetz (StVÄG), mit dem bisher fehlende Datenverarbeitungsregelungen im Bereich der Strafverfolgung geschaffen werden sollen, ist in der letzten Legislaturperiode wieder nicht verabschiedet worden. Im Übrigen erfüllt die z. Z. vorliegende Fassung ohnehin nicht die datenschutzrechtlichen Anforderungen (vgl. XII 31.3 sowie Anlage 1).

Aber auch der Bereich der Bewährungs- und Gerichtshilfe sowie der Führungsaufsicht muss weiterhin ohne die erforderlichen Rechtsgrundlagen zur Datenverarbeitung auskommen. Bereits im letzten Tätigkeitsbericht habe ich unter Nr. 28.8 auf die Problematik hingewiesen. Während das Justizministerium damals noch an eine Gesetzesinitiative zur Novellierung des Landesgesetzes über Bewährungshelfer vom 25. Oktober 1961(Nds. GVBl. S. 315) dachte, verwies die Landesregierung in ihrer Stellungnahme zu meinem XIII. Tätigkeitsbericht (vgl. Drs. 13/2500 S. 14) auf § 483 des Entwurfs des StVÄG 1996. Dort ist jedoch lediglich die Speicherung, Veränderung und Nutzung personenbezogener Daten geregelt. Für die Erhebung und Übermittlung der Daten hätte es immer noch an einer gesetzlichen Grundlage gefehlt. Hierauf habe ich das Niedersächsische Justizministerium aufmerksam gemacht.

Dieser normfreie Zustand in weiten Bereichen der Justiz kann nicht länger hingenommen werden. Es bedarf einer zügigen Schaffung gesetzlicher Regelungen für die Datenverarbeitung. Die Datenschutzbeauftragten des Bundes und der Länder haben hierzu am 5./6. Oktober 1998 die in Anlage 13 beigefügte Entschließung verabschiedet.

27.2 Das Zentrale Staatsanwaltschaftliche Verfahrensregister geht ans Netz – echter Betrieb

Das beim Bundeszentralregister in Berlin angesiedelte Zentrale Staatsanwaltschaftliche Verfahrensregister (ZStV) wird am 1. Januar 1999 seinen Echtbetrieb aufnehmen. In dem ZStV sollen Ermittlungsdaten aller Strafverfahren aus der Bundesrepublik Deutschland vorgehalten werden, die der Bund für die Länder als „Serviceleistung“ – gegen Geld - auf Abruf bereithält. Hierfür ist die Anlieferung der entsprechenden Daten an das ZStV durch die einzelnen Staatsanwaltschaften vor Ort notwendig. In Niedersachsen werden dazu von jeder Staatsanwaltschaft die notwendigen Daten an einen Kopfstellenrechner StA, der noch im Zuständigkeitsbereich Niedersachsens liegt, mit Hilfe des bei den niedersächsischen Staatsanwaltschaften eingeführten EDV-Systems SIJUS-STRAF übermittelt. Von dort aus gehen die Daten dann weiter an das ZStV nach Berlin.

Dieses für eine effektive Verbrechensbekämpfung sicherlich grundsätzlich begrüßenswerte Großprojekt wird Niedersachsen allein in der Aufbauphase ca. 4,2 Millionen DM kosten. Bedenkt man die Größenordnung dieses Systems, sollte es sowohl tatsächlich als auch rechtlich auf festem Grund stehen. Bei der Fülle der zu verarbeitenden hochsensiblen Daten bedarf es dringend einer klaren Gesetzesgrundlage. Daran aber fehlt es immer noch.

Für die Datenverarbeitung durch die Staatsanwaltschaften mit Hilfe des Verfahrens SIJUS-STRAF ist z. Z. eine hinreichende rechtliche Grundlage nicht vorhanden. Hierin bin ich mir mit dem Justizministerium einig. Es bedarf klarer Regelungen, in welchem Umfang und in welcher Weise die notwendigen Daten erhoben und verarbeitet werden dürfen (vgl. XIII 28.3). Datenverarbeitungsvorschriften sollten mit dem Strafverfahrensänderungsgesetz (StVÄG) geschaffen

werden. Dieses ist jedoch – wie oben ausgeführt - bedauerlicherweise immer noch nicht zustande gekommen.

Ich habe das Niedersächsische Justizministerium seit vielen Jahren immer wieder auf dieses Problem aufmerksam gemacht. Dessen ungeachtet hat sich das Justizministerium nicht veranlasst gesehen, die Entscheidungsgremien, die über die für die Anlieferung der Daten an das ZStV notwendigen Investitionen beschliessen müssen, über die fehlende rechtliche Grundlage zu informieren. Offensichtlich soll hier wieder einmal erst der technische Rahmen geschaffen werden und danach die rechtliche Begründung, nach dem Motto: Technik vor Recht.

Ein anderes Problem ist die Verschlüsselung der hochsensiblen Daten bei der Übermittlung von den Staatsanwaltschaften über die Kopfstelle StA an das ZStV. Sämtliche Beteiligte sind sich darüber einig, dass es dringend geboten ist, die Daten verschlüsselt zu übermitteln. Es sei sogar unverzichtbar, formuliert das Niedersächsische Justizministerium selbst in einem Schreiben an mich. Da man sich jedoch noch nicht endgültig auf ein bundeseinheitliches System hat verständigen können und auch die endgültige Kostenfrage für die Verschlüsselung und die damit verbundene technische „Nachrüstung“ noch nicht geklärt ist, wird nach dem Motto verfahren: „Es wird schon gut gehen, fangen wir mal freudig an“ – auch ohne Verschlüsselung. Mittelfristig wird mit einer Verschlüsselung erst in zwei bis drei Jahren gerechnet und das, obwohl alle Beteiligten die Verschlüsselung für dringend geboten halten! Sind die übermittelten Daten in diesen Jahren doch nicht so sensibel und gefährdet?

27.3 Zeugenschutzgesetz

Schon seit einigen Jahren wird darüber diskutiert, in welcher Weise die Stellung von Zeugen im Strafverfahren verbessert werden kann, ohne dass wichtige rechtsstaatliche Prinzipien des Verfahrensrechtes aufgegeben werden. Dabei haben sich schwerpunktmäßig zwei Problemkreise herausgebildet.

Zum einen geht es um Kinder als Zeugen, deren Aussage häufig im Zusammenhang mit Sexualdelikten steht und deren Mehrfachvernehmung und direkte Konfrontation mit dem Angeklagten verhindert werden sollten. Zum anderen geht es um Zeugen aus dem Bereich der schweren Drogenkriminalität oder anderer schwerer, häufig als Bande begangener Delikte. Solche Zeugen müssen unter Umständen mit erheblichen Nachteilen für Leib oder Leben rechnen, wenn sie eine umfassende Aussage machen.

In diesem Zusammenhang ist es in verschiedenen - auch spektakulären Prozessen - bereits einvernehmlich zum Einsatz von Videotechnik bei Zeugenvernehmungen gekommen. Nach Vorlage und Diskussion verschiedener Gesetzesentwürfe wurde jetzt das „Gesetz zum Schutz von Zeugen bei Vernehmungen im Strafverfahren und zur Verbesserung des Opferschutzes; Zeugenschutzgesetz – ZSchG“ vom 30. April 1998 (BGBl. I S. 820) verabschiedet. Das Gesetz ist am 1. Dezember 1998 in Kraft getreten.

Aufgrund des nun vorliegenden Gesetzes wird besonders schutzwürdigen Zeugen gestattet, sich bei ihrer Vernehmung in einem anderen Raum oder sogar an einem anderen Ort aufzuhalten. Die Vernehmung soll dann per „Video-Standleitung“ durch die übrigen Verfahrensbeteiligten, die sich weiterhin im Gerichtssaal befinden, erfolgen. Auf diese Weise müssen die besonders schutzwürdigen Zeugen, beispielsweise Kinder, nicht mehr im Gerichtssaal anwesend sein. Des Weiteren dürfen Zeugenvernehmungen unter bestimmten Voraussetzungen bereits im staatsanwaltschaftlichen Ermittlungsverfahren auf Video aufgezeichnet und später in der Hauptverhandlung verwertet werden. Damit sollen belastende Mehrfachvernehmungen vermieden werden.

Da Aufzeichnungen einer Vernehmung im Strafverfahren – per Video - einen erheblichen Eingriff in das Persönlichkeitsrecht des Zeugen darstellen, wäre es dringend geboten gewesen, als Zulässigkeitsvoraussetzung für die Videoaufzeichnungen, die ja zum Schutze des Zeugen gefertigt werden sollen, dessen Einwilligung einzuholen und ihn vorher über die Möglichkeit des Widerrufs der Einwilligung zu informieren. Auf diese Voraussetzung wurde jedoch verzichtet. Auch findet sich keine Regelung, die die Vervielfältigung der Aufzeichnungen verbietet oder limitiert. Damit besteht die Gefahr des Missbrauchs einer Videokopie etwa durch Veröffentlichung in den Medien (vgl. hierzu die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997, Anlage 8). Insgesamt bleibt abzuwarten, ob und wie sich die neue technische Möglichkeit im Strafverfahren bewährt.

27.4 Großer Lauschangriff

Mit dem Gesetz zur Änderung des Grundgesetzes (Artikel 13) vom 26. März 1998 (BGBl. I S. 610) ist nunmehr das Abhören von Wohnungen zum Zwecke der Strafverfolgung erlaubt. Zur Umsetzung des Großen Lauschangriffs regelt das „Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität“ vom 4. Mai 1998 (BGBl. I S. 845) durch neue Bestimmungen in verschiedenen Gesetzen, unter anderem auch in der Strafprozessordnung (StPO), im Einzelnen die Voraussetzungen für den Einsatz technischer Mittel zur akustischen Überwachung von Wohnungen.

Damit ist ein letzter unantastbarer Bereich der Privatsphäre – die Wohnung – dem Bedürfnis einer effektiven Strafverfolgung geopfert worden.

Das neue Instrument stellt einen besonders schweren Eingriff in das Persönlichkeitsrecht des Bürgers dar und ist von mir grundsätzlich abgelehnt worden. Dies habe ich wiederholt gegenüber dem Niedersächsischen Justizministerium, dem Innenministerium sowie der Staatskanzlei deutlich zum Ausdruck gebracht (XI-II 28.5). Bei aller Anerkennung der Notwendigkeit offensiver Kriminalitätsbekämpfung darf dies nicht dazu führen, dass die letzte Rückzugsmöglichkeit der Bürgerinnen und Bürger angetastet wird. Die Unantastbarkeit der Wohnung hat einen hohen verfassungsrechtlichen Rang. Das verabschiedete Gesetz erfüllt nicht hinreichend die Anforderungen, die unter Abwägung aller Interessen an ein Gesetz zu stellen sind, das dieses hohe Rechtsgut einschränkt.

Zwar ist es gelungen, mit Hilfe der Datenschutzbeauftragten des Bundes und der Länder in einigen Details die Entscheidung des Gesetzgebers zu beeinflussen, sodass verschiedene verfahrenssichernde Regelungen getroffen wurden. So liegt die Anordnungskompetenz für die Überwachungsmaßnahme bei einer Kammer des jeweiligen Landgerichts, also einem Kollegialgericht. Auch besteht eine Benachrichtigungspflicht gegenüber den Betroffenen nach Abschluss der Maßnahme. Schließlich muss nach amerikanischem Vorbild die Bundesregierung jährlich das Parlament über die durchgeführten Maßnahmen unterrichten (Wiretap Report).

Jedoch sollte nicht vergessen werden, dass der Große Lauschangriff als Maßnahme zur Bekämpfung der organisierten Kriminalität, also „schwerster Verbrechen“, gedacht war. Nun aber ist der Katalog der Anlasstaten, der Taten also, die einen Eingriff erlauben, viel zu umfangreich. Er umfasst auch Taten, die nur schwerlich als „schwerste Verbrechen“ anzusehen und dem Bereich der organisierten Kriminalität – was auch immer man darunter versteht – zuzuordnen sind. So fällt auch Bandendiebstahl unter die Katalogtaten. Stehlen zwei Freunde eine Zeit lang Fahrräder, so können sie bereits diesen Tatbestand erfüllen und es darf in ihren Wohnungen abgehört werden.

In der politischen Diskussion wurde immer wieder, insbesondere vom Bundeministerium des Innern, betont, die Abhörmaßnahme betreffe doch nur „Gangsterwohnungen“, ein Begriff, der ebenso inhaltsleer wie unsachlich ist. Entgegen dieser lautstarken Behauptung dürfen nunmehr jedoch Wanzen und Abhörgeräte auch in Wohnungen nicht Tatverdächtiger, also unschuldiger Personen, eingebaut werden, wenn nämlich Tatsachen die Annahme rechtfertigen, dass der Beschuldigte sich dort aufhält. Also bei den Eltern, der Freundin? Werden diese Wohnungen bereits zu „Gangsterwohnungen“, weil sich dort ein Verdächtiger aufhält?

Der Eingriff ist bereits bei einer sehr niedrigen Verdachtsstufe möglich. So bedarf es lediglich eines Anfangsverdachtes, der schnell erreicht ist und der der Bedeutung des Eingriffs nicht gerecht wird.

Die durch den Großen Lauschangriff erlangten Informationen dürfen nicht nur für Zwecke eines Strafverfahrens, sondern auch zur Abwehr einer im Einzelfall bestehenden Gefahr für Leben, Leib oder Freiheit einer Person oder für erhebliche Sach- oder Vermögenswerte verwendet werden (§ 100 f Abs. 1 StPO-neu). Damit dürfen Daten aus einem Strafermittlungsverfahren auch für Zwecke der Gefahrenabwehr genutzt werden. § 100 f Abs. 2 StPO läßt zu, dass Abhörergebnisse, die aufgrund polizeirechtlicher Maßnahmen erlangt worden sind, auch zur Aufklärung einer der in § 100 c Abs. 1 Nr. 3 StPO genannten Katalogtaten dient. Diese Zweckänderung und die ausgeweitete Verwendungsmöglichkeit sind in der Öffentlichkeit ebenfalls kaum deutlich gemacht worden. Dort wurde nur der Strafverfolgungszweck betont.

Nun ist das begehrte Instrument des Großen Lauschangriffs in die Hand der Ermittlungsbehörden gegeben worden, und man sollte erst einmal in Ruhe beginnen, damit zu arbeiten, und dann zu prüfen, ob es ein für das gesetzte Ziel tatsächlich geeignetes Mittel darstellt. Aber schon hört man - wie zu erwarten – den Ruf nach noch weiteren Eingriffsmöglichkeiten in die Privatsphäre der Bürger: „Die optische Überwachung muss her“. Die nach Art. 13 Abs. 1 GG geschützten Wände der Wohnungen werden dünner und dünner.

27.5 Genomanalyse im Strafverfahren

27.5.1 DNA-Analysegesetz (genetischer Fingerabdruck)

Durch das Strafverfahrensänderungsgesetz - DNA-Analyse („Genetischer Fingerabdruck“) – (StVÄG) vom 17. März 1997 (BGBl. I S. 534) ist mit den neu eingefügten §§ 81 e und 81 f Strafprozeßordnung (StPO) eine Rechtsgrundlage für diese in vielen Strafverfahren inzwischen so wichtig gewordene neue Untersuchungsmethode von menschlichen Körperzellen geschaffen worden. Die DNA-Analyse dient aufgrund ihrer differenzierten Aussagekraft der Aufklärung von schweren Straftaten. Grundsätzlich ist es zu begrüßen, wenn Spuren und Beweismittel einer Person eindeutig zugeordnet werden können. Die DNA-Analyse ist um ein vielfaches genauer als der herkömmliche Fingerabdruck, sodass aus datenschutzrechtlicher Sicht keine pauschale Ablehnung der Nutzung dieser modernen Technik zur Strafverfolgung erfolgt.

In das Gesetz haben einige wichtige datenschutzrechtliche Forderungen Eingang gefunden. So muss die Untersuchungsanordnung von einem Richter getroffen werden. An dieser wichtigen Voraussetzung, die im Übrigen während des Gesetzgebungsverfahrens von niemandem ernsthaft angezweifelt wurde, darf selbst unter dem Eindruck der sich immer weiter ausbreitenden Anwendung der DNA-Analyse im Strafverfahren nicht gerüttelt werden. Sie ist im Hinblick auf die besondere Aussagekraft der molekulargenetischen Untersuchung und der strengen gesetzlichen Zweckbindung ein unverzichtbarer rechtsstaatlicher Bestandteil

dieser Maßnahme. Der Richtervorbehalt dient als vertrauensbildende Maßnahme, die nicht aus Gründen der besseren Praktikabilität in der Praxis geopfert werden darf. Gerade auf dem Hintergrund der sich ständig ausweitenden Anwendungspraxis der DNA-Analyse im Strafverfahren einerseits und im Hinblick auf die sich rasant entwickelnde Genforschung andererseits bedarf es in diesem sensiblen Bereich auch in Zukunft der rechtsstaatlichen Kontrolle durch den Richtervorbehalt.

Weiterhin sieht das neue Gesetz vor, dass das Untersuchungsmaterial anonymisiert dem Sachverständigen zugeleitet wird. Den Datenschutzbeauftragten ist ausdrücklich eine weitgehende Kontrollbefugnis eingeräumt worden, gleichgültig, wo die Proben untersucht werden. Die DNA-Analyse darf nur zum Zweck der Abstammungs- oder Identitätsfeststellung erfolgen. Mit dieser Zweckbindung wird erreicht, dass das Material nicht zu anderen Zwecken mit der Folge weiterer Aussagen über die betroffene Person untersucht wird. Diese Zweckbindung gilt auch nach Abschluss des Verfahrens, sodass etwa noch vorhandenes Material nicht im Rahmen eines späteren Verfahrens oder zu einem anderen Zweck als die Abstammungs- oder Identitätsfeststellung untersucht werden darf.

Der datenschutzrechtlichen Forderung nach einer strikten Eingrenzung der Verwendung des entnommenen Materials auf das dem Zweck der Entnahme zugrunde liegende Verfahren wurde nicht gefolgt. So darf das Material auch zum Zweck der Abstammungs- und Identitätsfeststellung zwar nicht in einem späteren, jedoch in einem anderen anhängigen Strafverfahren verwendet werden. Auch wäre eine klarere Vernichtungsregelung sowohl hinsichtlich des Zeitpunkts als auch des Umfangs wünschenswert gewesen. Jetzt heisst es lediglich allgemein, dass das Untersuchungsmaterial unverzüglich zu vernichten ist, wenn es nicht mehr zu den im Gesetz genannten Zwecken erforderlich ist. Es fehlen Vernichtungsregelungen über die Ergebnisse der Untersuchung. Diese sollen als Aktenbestandteil in der Regel nicht der Vernichtung unterliegen. Regelungen zu anfallenden Spurenextrakten sind im Gesetz nicht vorhanden .

27.5.2 DNA-Massenreihenuntersuchungen an 17 900 Männern

Aufgrund des DNA-Analysegesetzes kann jetzt Zellmaterial von Beschuldigten im Strafverfahren unter den dort genannten Voraussetzungen einer DNA-Analyse unterzogen werden. Für die Probenentnahme und Untersuchung von Unverdächtigen gibt es jedoch keine Rechtsgrundlage. Diese Tests müssen ausschließlich auf freiwilliger Basis vorgenommen werden. Gerade in Niedersachsen ist es in den letzten Jahren nach schweren Straftaten zu einigen spektakulären Massenreihenuntersuchungen bei Unverdächtigen gekommen. Die bisher umfangreichste Massenreihenuntersuchung erfolgte im Rahmen der Ermittlungen der Soko „Nelly“ der Polizeiinspektion (PI) Cloppenburg nach dem Tod des Kindes Christina. Für mich war diese Reihenuntersuchung Anlass zu einer datenschutzrechtlichen Kontrolle. Diese erstreckte sich schwerpunktmäßig auf die Speichelprobenentnahme bei den insgesamt ca. 17 900 Männern und die durch das Landeskriminalamt Niedersachsen (LKAN) durchgeführten DNA-Analysen an 13 078 Proben.

Ca. 2 500 Männer wurden aufgrund sogenannter „KT“ (kriminaltechnische Spuren) ermittelt. Sie waren bereits früher polizeilich in Erscheinung getreten oder wiesen andere verdachtsrelevante Merkmale auf. Gegen 1 366 Männer dieser Gruppe ergingen unter Bejahung der Beschuldigteneigenschaft richterliche Anordnungsbeschlüsse für die Durchführung der DNA-Analyse gemäß §§ 81 e und 81 f Strafprozeßordnung (StPO). 15 400 Männer wurden per öffentlichem Aufruf zur Speichelprobenabgabe veranlasst. Der angesprochene Kreis ergab

sich insbesondere aufgrund der Kriterien Alter, Wohn-Lebensraum und Ortskenntnis. Bei beiden Gruppen erfolgte die Abgabe der Speichelproben freiwillig.

Der Fall gibt mir Anlass, erneut auf die Grenzen einer tatsächlichen Freiwilligkeit bei der Einwilligung aufmerksam zu machen. Aus meiner Sicht ist nicht auszuschliessen, dass es in Zukunft immer mehr zu Massenreihenuntersuchungen kommen wird, die dann mangels einer Rechtsgrundlage freiwillig aufgrund Einwilligung des Einzelnen zu erfolgen haben. Mit der Einwilligung soll der Betroffene selbst darüber entscheiden, wer zu welchem Zweck welche seiner Daten verwenden darf. Sie muss konsequenterweise dann ausscheiden, wenn sich der Betroffene in einer Situation befindet, die ihm keine Möglichkeit zu einer eigenen selbstständigen Entscheidung lässt und ihm insoweit keine andere Wahl bleibt. Gerade auch der von mir geprüfte Fall zeigt, dass es verschieden intensive Faktoren gibt, die auf die Willensentscheidung des Einzelnen einwirken können. So ist der Grad der Freiwilligkeit bei der Gruppe der Männer, gegen die bereits richterliche Anordnungsbeschlüsse für die Untersuchung nach § 81 f StPO vorgelegen haben, anders einzuschätzen als bei den übrigen Männern. Bei der zuerst genannten Gruppe hätte die Möglichkeit bestanden, bei nicht freiwilliger Abgabe der Speichelprobe den betreffenden Mann darauf hinzuweisen, dass gegen ihn bereits ein richterlicher Beschluss vorliegt, in dem er als Beschuldigter und damit der Tat Verdächtiger angesehen wird. Aber auch andere Faktoren beeinflussen in vergleichbaren Fällen die freie Entscheidung. Dies reicht von dem sozialen Druck bis hin zu dem Wunsch, an der Aufklärung einer schweren Straftat konstruktiv mitzuwirken. Freiwilligkeit kann nicht auf Dauer Grundlage für zukünftige Massenreihenuntersuchungen Unverdächtiger sein. Anderenfalls besteht die Gefahr, dass gesetzliche Verfahrenssicherungen, wie sie insbesondere in den neuen Gesetzen, die sich mit der DNA-Analyse befassen, enthalten sind, ausgehöhlt werden und wichtige rechtsstaatliche Prinzipien wie die richterliche Anordnung sowohl der Probenentnahme als auch der Untersuchung der Probe nicht mehr hinreichend Berücksichtigung finden. Über die „Freiwilligkeit“ könnte gewissermaßen ein neues Strafverfolgungsrecht entstehen, das die Strafprozessordnung in diesem Bereich ablöst. Es muss ein vernünftiger Ausgleich zwischen dem berechtigten und auch von mir nicht bestrittenen Interesse an schnellstmöglicher Aufklärung schwerer Straftaten mit Hilfe einer neuen erfolgversprechenden Methode und dem Recht auf informationelle Selbstbestimmung geschaffen werden.

Bei der von mir kontrollierten Massenuntersuchung ist offensichtlich versucht worden, diesem Gedanken in der Weise Rechnung zu tragen, dass das weitere Verfahren unter Beachtung wichtiger rechtsstaatlicher Grundsätze durchgeführt wurde. So sind sämtliche Speichelproben in anonymisierter Form an das LKAN zur Untersuchung gesandt worden. Zwar erfolgte die Anonymisierung in unterschiedlicher Weise. Die Proben der „KT“ wurden mit Vorname und erstem Buchstaben des Nachnamens versehen, während die übrigen 15 400 Proben lediglich mit einem Zahlencode verschlüsselt wurden, eine Form der Anonymisierung, die ich wiederholt gefordert habe und der ich den unbedingten Vorzug gebe. In jedem Falle aber konnte die Deanonymisierung der einzelnen Proben nur durch die ermittelnde Polizei vorgenommen werden. Außerdem sind inzwischen bis auf die tat- und täterrelevanten Spuren sämtliche Daten und Materialien, die im Zuge der Untersuchung angefallen sind und die einen Rückschluss auf eine Person zuließen, also auch Untersuchungsergebnisse, vernichtet und gelöscht worden. Auch damit wird eine wesentliche datenschutzrechtliche Forderung erfüllt.

Die Untersuchung an dem Zellmaterial selbst erfolgte im System D1S80, da auch dieses System bei den am Opfer gefundenen Spuren festgestellt werden konnte. Dabei handelt es sich um ein beim Menschen vergleichsweise selten vorkommendes System. Außerdem ist es nach bisherigem Forschungsstand nicht

Träger irgendwelcher Erbinformationen. Es zeichnet sich lediglich durch eine typische Form sich immer wiederholender Strichmuster, etwa vergleichbar mit dem Strichcode auf Waren für Scannerkassen, aus. Dieses Muster ist von Mensch zu Mensch sehr unterschiedlich und lässt damit bei Übereinstimmung von Spur und Probe einen äußerst sicheren Rückschluss auf die Identität des Spurenlegers zu. Irgendwelche Aussagen über die Persönlichkeitsstruktur oder genetisch bedingte Eigenschaften lassen sich diesem so festgestellten Muster in dem untersuchten System D1S80 mit der derzeitig angewandten Methode und nach Kenntnis der Wissenschaft z. Z. nicht entnehmen.

Da es inzwischen zur vollständigen Löschung und Vernichtung sämtlicher personenbezogener Daten und Unterlagen inklusive der Untersuchungsergebnisse und Spurenextrakte gekommen ist, stellt sich hier nicht das datenschutzrechtliche Problem einer unverhältnismäßig langen Speicherung der Daten in irgendwelchen Dateien.

Auch wenn zeitweilig in der Öffentlichkeit – gewollt oder ungewollt – der Eindruck entstanden ist, die Massenreihenuntersuchung im Falle der Christina in Strücklingen habe irgendetwas mit der zeitgleich geführten Diskussion über die Einrichtung einer Gendatei zu tun, so handelt es sich doch um zwei völlig unterschiedliche Vorgänge. Diese Tatsache ging teilweise in der öffentlichen Diskussion um die Gendatei unter. Für eine Speicherung der Ergebnisse der auf Freiwilligkeit basierenden Massenreihenuntersuchung und der „KT“-Spuren fehlt es an jeglicher Rechtsgrundlage. Das galt bereits während der Diskussion über die Gendatei und gilt auch heute nach Inkrafttreten des DNA-Identitätsfeststellungsgesetzes (vgl. 27.5.3). Es ist aber nicht auszuschließen, dass bedauerlicherweise die Vorgänge um die Massenreihenuntersuchung die Diskussion um die Errichtung der Gendatei indirekt beeinflusst haben und eine ruhige und gründliche Erörterung der damit verbundenen Fragen zeitweilig fast unmöglich hat erscheinen lassen.

27.5.3 Gendatei – DNA-Identitätsfeststellungsgesetz

Nachdem mit dem Gesetz „Genetischer Fingerabdruck“ (vgl. 27.5.1) die DNA-Analyse im Rahmen bereits anhängiger Strafverfahren erlaubt worden war, fehlte es an einer gesetzlichen Grundlage für die Anwendung dieser neuen Untersuchungsmethode zur Aufklärung künftiger Strafverfahren. Eine gesetzliche Regelung wurde erst durch das DNA-Identitätsfeststellungsgesetz vom 7. September 1998 (BGBl. I S. 2 646) nach einem ungeheuer schnellen und hektischen Gesetzgebungsverfahren geschaffen, mit dem u. a. ein neuer § 81 f in die Strafprozessordnung (StPO) eingefügt wurde. Das Gesetz ist seit dem 11. September 1998 in Kraft. Trotz einer bis dahin fehlenden Rechtsgrundlage hat das Bundesministerium des Innern bereits zuvor eine zentrale Gendatei durch schlichte Verwaltungsanordnung beim Bundeskriminalamt (BKA) einrichten lassen.

Die Datenschutzbeauftragten hatten bereits Anfang 1997 wesentliche datenschutzrechtliche Fragestellungen und Forderungen zur Errichtung einer Gendatei formuliert (vgl. Anlage 2). Ich habe gegenüber dem Niedersächsischen Justizministerium Stellungnahmen zu den verschiedenen vorgelegten Gesetzesentwürfen abgegeben. Dabei habe ich deutlich gemacht, dass ich die DNA-Analyse zur Aufklärung von schweren Straftaten im Einzelfall keinesfalls ablehne. Die Methode der DNA-Analyse ist zur eindeutigen Zuordnung von Spuren und Beweismitteln um ein Vielfaches genauer als der herkömmliche Fingerabdruck. Dies darf aber nicht über die erheblichen Zukunftsrisiken einer zentralen Gendatei hinwegtäuschen.

Mit der Errichtung einer DNA-Datei wird ein Bestand von hochsensiblen Daten aufgebaut. Angesichts der weltweiten intensiven Forschung zur Entschlüsselung des menschlichen Genoms ist es nicht auszuschließen, dass die gespeicherten DNA-Merkmale künftig auch die Erstellung von Persönlichkeitsprofilen ermöglicht. Auf diesem Hintergrund ist es eine wesentliche datenschutzrechtliche Forderung gewesen, den Betrieb der Gendatei erst aufzunehmen, wenn hierzu eine einwandfreie gesetzliche Grundlage nach parlamentarischer Beratung geschaffen worden ist. Nur sie ermöglicht eine breite öffentliche Diskussion über diesen wichtigen Bereich.

Wesentliche datenschutzrechtliche Forderungen haben in das nun gültige Gesetz zwar Eingang gefunden. So bestehen insbesondere eine strikte Zweckbindung, eine Vernichtungsregelung für die entnommenen Körperzellen und die Voraussetzung einer richterlichen Anordnung für die Materialentnahme bei den Betroffenen. Dennoch darf nicht übersehen werden, dass mit dem neuen Gesetz eine weitere erkennungsdienstliche Maßnahme ohne Bezug zu einem anhängigen Strafverfahren „zum Zwecke der Vorsorge für künftige Strafverfahren“, ein Begriff aus dem materiellen Polizeirecht, aufgenommen wurde. Diese Entwicklung wird noch dadurch unterstrichen, dass die Datei beim BKA angesiedelt ist. Die zart aufkeimende Diskussion während des Gesetzgebungsverfahrens über eine anderweitige Ansiedlung, z. B. beim Bundeszentralregister, wurde durch das Schlusstempo der Beratungen und den forcierten Wunsch des BMI, nun endlich mit dem Dateibetrieb zu beginnen, koste es was es wolle, niedergestreckt. Das Hauptproblem sehe ich jedoch darin, dass für die Datenverarbeitung in dem neuen Gesetz keine hinreichend normenklare Regelung vorhanden ist. In dem Gesetz wird lediglich in § 3 darauf verwiesen, dass die Verarbeitung und Nutzung der gewonnenen Ergebnisse nach dem Gesetz über das Bundeskriminalamt (BKAG) erfolgen kann. Der pauschale Verweis auf dieses Gesetz bedeutet eine problematische Ausweitung der Verarbeitungs- und Nutzungsbefugnisse hinsichtlich der besonders sensiblen Daten aus der DNA-Analyse. Damit gelten nämlich auch die Übermittlungsregelungen der §§ 10, 14 BKAG. Danach ist nicht auszuschließen, dass eine Übermittlung an Strafverfolgungsbehörden auch zum Zwecke der Strafverfolgung wegen anderer als der in dem neuen § 81 g Abs. 1 StPO genannten Straftaten erfolgt. Auch kann eine Übermittlung der beim BKA dann gespeicherten Daten an „sonstige öffentliche Stellen“ erfolgen, was unter Umständen dazu führt, dass eine Datenübermittlung an Sozialämter, Ausländerbehörden u. Ä. vorgenommen wird. Schließlich eröffnet § 14 BKAG eine Übermittlungsbefugnis gegenüber öffentlichen Stellen anderer Staaten sowie zwischen- und überstaatlichen Stellen. Im Übrigen erscheint eine Weitergabe durch das BKA an Europol nicht ausgeschlossen, da das BKA auch zentrale Stelle für die Anlieferung von Daten an diese Stelle ist. Aus diesen Gründen hätte es einer klaren Einschränkung der Zugriffs- bzw. Übermittlungsbefugnisse bedurft. Dies habe ich ausdrücklich gegenüber dem Niedersächsischen Justizministerium gefordert.

Wieder einmal sind wichtige datenschutzrechtliche Belange einer schnellen und vermeintlich einfachen Lösung geopfert worden, ohne dass diese, wie mir scheint, in allen Konsequenzen durchdacht wurde.

27.6 Telefonüberwachung

27.6.1 Zahlenspiele

Die Telefonüberwachung (TÜ) als die „Urmutter“ und der Prototyp der Heimlichkeit im Strafverfahren ist seit ihrer Einführung längst den Kinderschuhen entwachsen. Sie ist eine etablierte Ermittlungmethode erheblichen Ausmaßes geworden. Und Deutschland liegt bei der Anzahl der durchgeführten Telefonüberwachungen an einsamer Spitze mit immer noch steigender Tendenz.

Bundesweit wurde nach Auskunft der Bundesregierung 1997 in 2 384 Verfahren eine TÜ-Maßnahme gemäß §§ 100 a und 100 b StPO angeordnet. Diese Zahl besagt jedoch noch nichts, weil pro Verfahren häufig mehrere Anschlüsse abgehört werden. Die genaue Zahl der abgehörten Anschlüsse war von der Bundesregierung bedauerlicherweise nicht zu erfahren. Wurde sie für 1996 für den Bereich Festnetz und Mobilfunk noch mit insgesamt 8 112 angegeben, fehlten für 1997 Angaben für den Bereich des Festnetzes. Allein im Bereich des Mobilfunks betrugen sie 1997 bereits 4 009. Berücksichtigt man, dass im Jahre 1996 nur im Bereich des Festnetzes 6 183 Anschlüsse betroffen waren, kann man sich vorstellen, wieviele es im Jahre 1997 insgesamt waren. Wenn schon keine aussagekräftigen Zahlen für die Anzahl der abgehörten Anschlüsse vorhanden sind, zeigen die Zahlen der richterlichen Anordnungen deutlich eine steigende Tendenz. Betrugen sie 1996 noch 6 428, so waren es 1997 bereits 7 776, wobei allerdings die Zahlen für 1997 wiederum nur auf den Angaben der Regulierungsbehörde nach § 88 Abs. 5 Telekommunikationsgesetz beruhen. Das Bundeskriminalamt und der Generalbundesanwalt haben 1997 die Zahl der überwachten Anschlüsse und nicht der Anordnungen angegeben, wie es noch im Jahr zuvor der Generalbundesanwalt mit 104 getan hat. Aber auch die Zahl der erfolgten Anordnungen sagt noch nichts aus über die Anzahl der tatsächlich abgehörten Gespräche oftmals völlig unbeteiligter Dritter, zumal wenn man sich vor Augen hält, dass sich unter diesen abgehörten Anschlüssen auch solche in Gaststätten, Firmen und Telefonzellen (vgl. XIII 28.12.1) befinden. Rechnet man realistischerweise auf der Grundlage einer Hochrechnung aus den USA (Wiretap Report 1993 bis 1997) mit 150 betroffenen Personen pro abgehörter Leitung, so wird erst das Ausmaß der von TÜ Betroffenen, zumeist völlig unbeteiligter Personen, deutlich. Dies bedeutet, dass jährlich schätzungsweise 1 166 400 Personen von den angeordneten Telefonüberwachungen betroffen sind – eine Stadt etwa doppelt so groß wie Hannover.

Da der Straftatenkatalog des § 100 a StPO jedoch kontinuierlich erweitert wird – zuletzt durch das Gesetz vom 4. Mai 1998, mit dem der Große Lauschangriff eingeführt wurde - ist noch mit einer weiteren Erhöhung der Zahl Unbeteiligter zu rechnen. Eine Telefonüberwachungsmaßnahme bedeutet ein erhebliches und sich offensichtlich rechtlich und tatsächlich ständig erweiterndes Eingriffsinstrument in Rechte Dritter. Daher bedarf es dringend einer effektiven Erfolgskontrolle. Nur so läßt sich prüfen, ob dieses Eingriffsinstrument tatsächlich im vorliegenden Umfang notwendig und geeignet ist. Dies ist von mir wiederholt und eindringlich gefordert worden. An einer solchen effektiven Erfolgskontrolle der bestehenden Eingriffsinstrumente aber fehlt es völlig, wie bereits leicht aus dem oben aufgezeigten Zahlenwirrwarr erkennbar ist .

Die nunmehr von den Landesjustizverwaltungen seit drei Jahren eingeführte Berichtspflicht hilft auch nicht weiter. Sie entspricht in keiner Weise den datenschutzrechtlichen Vorstellungen. Die in dem Erfassungsbogen festzuhaltenden Daten geben lediglich Auskunft über die Anzahl der Verfahren, die Anzahl der Betroffenen im Sinne des § 100 a Satz 2 StPO und die Verdachtstaten des Katalogs des § 100 a Satz 1 StPO. Damit fehlt es an einer geeigneten, differenzierenden Aussage über den tatsächlichen Umfang, die Erforderlichkeit und die

Effizienz der angeordneten Maßnahmen. Ich habe vor Erstellung des Erfassungsbogens eindringlich die Führung einer tatsächlich aussagekräftigen Statistik gefordert, damit eine wirklich effektive Erfolgskontrolle durchgeführt werden kann. So hätte es dringend einer differenzierten Angabe über Zahl und Art der abgehörten Anschlüsse, über die Dauer der Maßnahme und die Anzahl der aufgezeichneten Telefonate bedurft. Aber auch Angaben zum Ermittlungserfolg wären nötig gewesen. Meine Forderungen sind jedoch sämtlich unter Hinweis auf die hohe Arbeitsbelastung der Staatsanwaltschaften abgelehnt worden. Die Landesjustizverwaltungen haben sich bedauerlicherweise auf die eher rudimentäre Ausgestaltung des nunmehr benutzten jährlichen Berichtsbogens verständigt. Die Erfahrungen der letzten drei Jahre zeigen jetzt jedoch deutlich deren geringe Aussagekraft. So bleibt völlig offen, wieviele Gespräche abgehört wurden, wieviele Unbeteiligte von der Maßnahme betroffen waren und wieviele TÜ-Maßnahmen inzwischen im Mobilfunkbereich in Niedersachsen durchgeführt werden (XIII 28.12.1). Auch können keine Angaben darüber gemacht werden, ob und in welcher Weise Erkenntnisse aus der Telefonüberwachung für das Ermittlungsergebnis überhaupt bedeutsam waren, ob sie also etwa zur Überführung oder Entlastung des Beschuldigten oder zur Gewinnung weiterer Ermittlungsansätze geführt haben.

Um das niedersächsische Zahlenwerk wenigstens ein wenig weiter zu erhellen und dessen Aussagekraft zu steigern, habe ich versucht, die beim Landeskriminalamt geführten statistischen Zahlen über TÜ-Maßnahmen der letzten Jahre zu erhalten. Diese wurden mir auch zur Verfügung gestellt. Sie sind mir jedoch nicht zur Veröffentlichung freigegeben worden. Aus meiner Sicht hätte die Verwertung des dortigen Zahlenmaterials zur Transparenz dieser das Grundrecht vieler auch unbeteiligter Menschen einschränkenden Maßnahme beigetragen. Sie wäre ein weiterer Schritt für die notwendige Erfolgskontrolle gewesen, da es sich um eine zusätzliche Erkenntnisquelle handelt, die auch Angaben zu der Anzahl der abgehörten Anschlüsse macht, was in dem Erfassungsbogen der Justizverwaltung nicht der Fall ist. Eine Gefährdung der Interessen der Bundesrepublik Deutschland und ihrer Länder - dies sind die Voraussetzungen für die Nichtfreigabe - sehe ich durch eine Veröffentlichung dieser Zahlen in keiner Weise. Bei der Bedeutung einer TÜ-Massnahme in Bezug auf die Grundrechte des Betroffenen sollten alle öffentlichen Stellen um größtmögliche Transparenz und Offenheit bemüht sein.

27.6.2 Benachrichtigungspflicht - Was ich nicht weiß, macht mich nicht heiß

Nach § 101 StPO sind alle von einer Telefonüberwachung betroffenen Personen nachträglich von der Durchführung dieser Maßnahme zu benachrichtigen. Sinn solcher Benachrichtigungsregelungen ist es, dem von einem Grundrechtseingriff Betroffenen zumindest nachträglich im Sinne einer gebotenen Folgenminimierung die Möglichkeit zu geben, seine Rechte aus Art. 19 Abs. 4 GG auf Rechtsschutz in Anspruch zu nehmen. Informationsbeschaffung durch verdeckte Maßnahmen geschieht sachnotwendig heimlich. Sie ist ein Eingriff in das informationelle Selbstbestimmungsrecht der Kommunikationspartner. Den Beteiligten muss zumindest nachträglicher Rechtsschutz ermöglicht werden. Dies muss sowohl für den Beschuldigten als auch für weitere von der Maßnahme betroffene Personen gelten. Der Beschuldigte, gegen den Anklage unter Verwertung der durch die Telefonüberwachung erlangten Erkenntnisse erhoben wird, wird in der Regel zu diesem Zeitpunkt, spätestens in der Hauptverhandlung, Kenntnis von der Maßnahme erhalten, auch wenn er nicht ausdrücklich bei Abschluss der Ermittlungen durch die Staatsanwaltschaft benachrichtigt wurde. Problematischer ist es, wenn die ursprüngliche Telefonüberwachung für die schließlich anklagerelevanten weiteren Ermittlungen keine Rolle mehr spielt und der Tatverdacht sich durch herkömmliche Beweismittel hat erhärten lassen oder wenn das Ver-

fahren nach § 170 Abs. 2 StPO mangels hinreichenden Tatverdachtes eingestellt wird.

Es sind aber auch Fälle zu berücksichtigen, in denen sich die Überwachungsmaßnahme gegen Telefonanschlussinhaber richtet, die nicht Beschuldigte sind. Hier ist mir im Rahmen einer Kontrolle ein Fall bekannt geworden, in dem eine Benachrichtigung zunächst unterblieben ist. Diese wurde dann jedoch unverzüglich nachgeholt, sodass es letztendlich zu keiner Beanstandung meinerseits kam. Dies gab mir jedoch Veranlassung zu einer Nachfrage beim Niedersächsischen Justizministerium, in welcher Weise und in welchem Umfang in Niedersachsen die Benachrichtigungen nach § 101 StPO von den Staatsanwaltschaften durchgeführt werden. Diese Anfrage wurde wiederum mit dem Hinweis auf die hohe Arbeitsbelastung der Staatsanwälte dahingehend beantwortet, dass es hierzu keine landesweiten Erkenntnisse im Justizministerium gebe. Ich wurde lediglich auf die Zahlen aus dem Berichtsformular hinsichtlich Telefonüberwachungsmaßnahmen der letzten drei Jahre verwiesen (s. o.). Die dort aufgeführten Zahlen sind jedoch im Zusammenhang mit der Benachrichtigungspflicht gemäß § 101 StPO gerade in keiner Weise aussagekräftig – wie ich bereits oben gezeigt habe. Dies zeigt einmal mehr, dass eine effektive Erfolgskontrolle und Evaluation der sich ständig erweiternden verdeckten Ermittlungsmöglichkeit durch Telefonüberwachung mangels tatsächlicher Grundlagenkenntnis z. Z. nicht möglich ist.

27.7 Gerichtsaushänge in nicht öffentlichen Verfahren

Gerichtsaushänge, mit denen an den Eingängen zu Verhandlungsräumen auf Termine hingewiesen wird, können datenschutzrechtlich problematisch sein. Dies ist in besonderer Weise bei nicht öffentlichen Verfahren der Fall. Die Nennung des Namens auf der öffentlich ausgehängten Terminsrolle beseitigt, ohne dass ich deren Erforderlichkeit erkennen kann, einen wesentlichen Teil der Nichtöffentlichkeit. Wenn z. B. auf der Terminsrolle im Gericht im Verfahren zur Abgabe der eidesstattlichen Versicherung der Name des Schuldners genannt wird, erlangen Dritte Kenntnis, wer zu ihrer Abgabe verpflichtet ist. Sie könnten daraus berechtigte oder unberechtigte Schlüsse ziehen.

Ich habe mich mit dem Niedersächsischen Justizministerium in Verbindung gesetzt und auf dieses Problem hingewiesen. Leider sieht man sich dort nicht veranlasst, unmissverständlich deutlich zu machen, dass bei nicht öffentlichen Sitzungen der Name des Betroffenen nicht genannt wird. Demgegenüber ist in Nordrhein-Westfalen ausdrücklich geregelt, dass auf einer Terminsrolle einer nicht öffentlichen Sitzung lediglich der Terminstag, die Terminsstunde, das Aktenzeichen, die Bezeichnung der Vorsitzenden bzw. des Vorsitzenden, die Namen der mitwirkenden Richterinnen und Richter einschließlich der Laienrichterinnen und Laienrichter sowie die Saal- bzw. Raumnummer aufzuführen sind. In Niedersachsen hofft man offensichtlich, dass sich das Problem durch die neuerdings veränderte Zuständigkeit erledigt haben könnte. Mit der Zweiten Zwangsvollstreckungsnovelle geht nämlich die Zuständigkeit für die Abnahme der eidesstattlichen Versicherung vom 1. Januar 1999 an auf den Gerichtsvollzieher über. Bisher war hierfür der Rechtspfleger zuständig.

Weshalb sich damit das Problem der Veröffentlichung von Daten Verfahrensbeteiligter durch Gerichtsaushänge bei nicht öffentlichen Verhandlungen erledigt haben sollte, ist mir nicht recht erfindlich. Nicht öffentliche Sitzungen finden nicht nur bei der Abgabe der eidesstattlichen Versicherung, sondern auch in einer Vielzahl anderer Fälle statt. Außerdem ist mit der allgemeinen Verschiebung der Zuständigkeit durch das neue Gesetz nicht gesagt, dass die Gerichtsvollzieher die eidesstattliche Versicherung nicht weiterhin im Gerichtsgebäude

abnehmen und nicht etwa – wie wohl das Justizministerium annimmt – im Haus des Schuldners oder in anderen Räumen. Ich würde es begrüßen, wenn auch in Niedersachsen das Problem in gleicher Weise wie in Nordrhein-Westfalen gelöst werden könnte.

27.8 Das offene Grundbuch

Ein Petent erwarb gemeinsam mit einer Gruppe weiterer Personen Miteigentumsanteile an einem Grundstück. Alle wurden ins Grundbuch eingetragen. Nach § 55 Abs. 1 Grundbuchordnung (GBO) soll jedem eingetragenen Eigentümer jede Eintragung bekannt gemacht werden. Der Petent erhielt jedoch eine umfassende Eintragungsmitteilung, in der sämtliche Miteigentümer, deren Geburtsdaten sowie die auf den jeweiligen Grundstücksanteilen lastenden Hypotheken, Grundschulden etc. enthalten waren. Wegen dieser weitgehenden Mitteilung wandte er sich an mich und bat um Prüfung. Diese Prüfung ergab: Die Eintragungsnachricht entsprach der früheren Rechtslage. Von dem um Stellungnahme gebetenen Amtsgericht wurde eingeräumt, dass die umfassende Eintragungsnachricht an die Miteigentümer im Hinblick auf die inzwischen geltende Vorschrift des § 55 Abs. 2 GBO nicht mehr hätte erfolgen dürfen. Danach ist bei Miteigentum die Bekanntmachung nur gegenüber den Miteigentümern vorzunehmen, auf deren Anteil sich die Eintragung bezieht. Auf diese Weise hat der Gesetzgeber die zu weit gehende Kenntnisnahme sensibler Daten Dritter verhindern wollen. Das Amtsgericht hat für die Zukunft sichergestellt, dass Eintragungsnachrichten in der nunmehr gebotenen Weise ergehen.

Diese eingeschränkte Mitteilungspflicht darf jedoch nicht darüber hinwegtäuschen, das das Grundbuch dennoch für viele ein offenes Buch ist. Eine vollständige Blattabschrift erhält nämlich nach § 12 GBO jeder, der ein berechtigtes Interesse daran darlegt. Dies wird bei Miteigentümern in der Regel leicht der Fall sein.

Immer wieder führt das Einsichtsrecht des Notars in Grundbücher bei Petenten zu Irritationen. Wie bereits oben gesagt, ist nach § 12 GBO jedem Einsicht in das Grundbuch zu gestatten, der ein berechtigtes Interesse darlegt. Notare sind jedoch von dieser Darlegungspflicht befreit. Sie müssen zwar ebenfalls wie jede andere Person ein berechtigtes Interesse an der Einsichtnahme haben, müssen es jedoch dem zuständigen Beamten gegenüber nicht darlegen. Allein seine Notareigenschaft reicht hier aus. Diese Erleichterung entspricht der besonderen Aufgabe und Rechtsstellung des Notars, insbesondere bei Grundstücksgeschäften. Erst wenn sich konkrete Anhaltspunkte ergeben, dass der Notar mit seiner Akteneinsicht unzulässige Zwecke verfolgt oder aus bloßer Neugierde Einsicht nehmen will, ohne in amtlicher Funktion zu handeln, muss ihm die Einsicht in das Grundbuch verwehrt werden.

27.9 Datenübermittlung von Anzeigeerstattern im OWi-Verfahren

Hat jemand einen anderen wegen einer vermeintlichen Verkehrsordnungswidrigkeit bei der Polizei angezeigt, so hat der Anzeigende häufig das Interesse, vorerst namentlich nicht in Erscheinung zu treten. Andererseits hat der Betroffene einen Anspruch darauf, vor einer Entscheidung durch die Verwaltung zu dem ihm gemachten Vorwurf umfassend angehört zu werden. In einem langwierigen Schriftwechsel mit dem Niedersächsischen Innenministerium und dem Niedersächsischen Justizministerium konnte eine beide Belange hinreichend berücksichtigende Regelung gefunden werden. Nach einer Anzeige durch eine Privatperson soll in dem schriftlichen Anhörungsbogen dem Beschuldigten erst einmal der neutrale Hinweis gegeben werden, dass als Beweismittel „Zeugenangaben“

zur Verfügung stehen. Die vollständige Angabe von Vor- und Zuname des Zeugen ist in diesem frühen Verfahrensstadium noch nicht erforderlich. Erst wenn der Betroffene nach Erhalt des Anhörungsbogens nachfragt, soll ihm der vollständige Vor- und Zuname des Zeugen mitgeteilt werden. Diese Vorgehensweise wird sowohl den Belangen des Betroffenen als auch des Anzeigeerstatters in hinreichender Weise gerecht. Ich halte diese Regelung – gemessen an der Praxis der Vergangenheit – für eine datenschutzrechtliche Verbesserung.

27.10 Datenübermittlung durch das Nachlassgericht - Es muss nicht jeder alles wissen

Zu einer Petition sah sich eine Bürgerin veranlasst, als das Amtsgericht nach dem Tode ihres Ehemannes das vollständige Testament jedem der darin Bedachten übersandte, ohne die Teile unkenntlich zu machen, die den einzelnen Bedachten nicht betrafen. Auf diese Weise wurden z. B. persönliche Anweisungen und Ratschläge des Verstorbenen an seine Ehefrau und andere höchstpersönliche Angaben Dritten bekannt, die diese gar nichts angingen. Die Bekanntgabe des vollständigen Inhalts des Testaments an sämtliche Beteiligte entsprach nicht der Rechtslage. Das Nachlassgericht hat zwar die Beteiligten, die bei einer Eröffnung des Testamentes nicht zugegen gewesen sind, von dem Inhalt des Testaments in Kenntnis zu setzen. Jedoch beschränkt sich diese Bekanntmachung ausdrücklich nur auf den Teil des Testaments, der den einzelnen Beteiligten betrifft (§ 2262 BGB). Die Weitergabe des vollständigen Testaments an sämtliche Beteiligte nur zum Zwecke der Benachrichtigung, dass sie in einem Testament bedacht worden sind, war danach nicht zulässig. Hiervon zu unterscheiden ist jedoch das Einsichtsrecht derjenigen, die ein rechtliches Interesse an dieser Akteneinsicht glaubhaft machen. Ihnen ist nach Eröffnung des Testaments zu gestatten, das vollständige Testament einzusehen oder eine Abschrift des gesamten Testaments oder einzelner Teile zu fordern (§ 2264 BGB). Damit soll die Möglichkeit einer Überprüfung etwaiger Rechtsansprüche gegeben werden. Hiergegen ist auch aus datenschutzrechtlicher Sicht nichts einzuwenden.

28 Strafvollzug

28.1 Datenschutzrechtliche Regelungen im Bereich des Strafvollzugs

Mit dem Vierten Gesetz zur Änderung des Strafvollzugsgesetzes vom 26. August 1998 (BGBl. I S. 2461) ist wider Erwarten nun doch noch in der 13. Legislaturperiode das schon so lange diskutierte Gesetz verabschiedet worden, mit dem datenschutzrechtliche Regelungen im Bereich des Strafvollzugs geschaffen werden sollten.

Dem Gesetz ist das Bemühen nicht abzuerkennen, die Eingriffe in das Recht auf informationelle Selbstbestimmung auf das im Rahmen des Strafvollzuges erforderliche Maß zu beschränken. Dies gilt gerade auch für die Verwendung von Daten innerhalb des Strafvollzuges. Dies Anliegen wird jedoch praktisch zunichte gemacht, wenn nunmehr in § 180 Abs. 4 StVollzG eine Generalklausel zur Datenübermittlung für vollzugsfremde Zwecke eingeführt worden ist. Nachdem in Satz 1 einzelne Übermittlungsbefugnisse aufgezählt werden, die sich weitgehend im Rahmen des Strafvollzuges bewegen, sieht Satz 2 eine Übermittlung auch für andere Zwecke vor, soweit dies in anderen Vorschriften gesetzlich geregelt ist und sich ausdrücklich auf personenbezogene Daten über Gefangene bezieht. Die Notwendigkeit einer solchen generellen Öffnung ist mir weder ersichtlich noch ist sie normenklar.

Einem weiteren datenschutzrechtlichen Anliegen wurde aus meiner Sicht nicht hinreichend Rechnung getragen. So sollten Akten nach der Entlassung des Gefangenen nur so lange aufbewahrt werden, wie dies aus nachvollziehbaren Gründen erforderlich ist, weil andernfalls eine erhebliche Datenspeicherung auf Vorrat erfolgt. In dem Gesetz beträgt jetzt die Aufbewahrungsfrist für Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter 20 Jahre und für Gefangenenbücher 30 Jahre. Ich hatte eine Aufbewahrungsfrist von 10 bzw. 20 Jahren als hinreichend lange angesehen und vorgeschlagen.

Als weitere Datenspeicherung über den Entlassungszeitpunkt hinweg sieht das Gesetz nunmehr vor, dass die von Gefangenen während des Vollzuges angefertigten Lichtbilder (XIII 29.2) sowie die Beschreibungen von körperlichen Merkmalen von der Vernichtung nach der Entlassung ausgenommen sind. Auch dies stellt aus meiner Sicht eine unzulässige Datenspeicherung auf Vorrat dar.

28.2 Folgen überalterter Strafregisterauszüge

Ein Strafgefangener beschwerte sich darüber, dass er im Vollzug so behandelt würde, als sei er vorbestraft. Aus diesem Grunde sei von der Justizvollzugsanstalt seine Aussicht auf vorzeitige Entlassung zum Zwei- Drittel-Zeitpunkt als gering eingeschätzt worden.

Was war geschehen? Die Strafvollstreckungsbehörde hatte bei Einleitung der Vollstreckung der Justizvollzugsanstalt einen fast zwei Jahre alten Bundeszentralregisterauszug zugesandt, der noch fünf Eintragungen enthielt. Zum Zeitpunkt der Urteilsverkündung waren diese Vorstrafen jedoch bereits getilgt, und der Gefangene hatte als unbestraft zu gelten. Nach § 31 Abs. 1 Buchst. b Strafvollstreckungsordnung hätte der beigefügte Bundeszentralregisterauszug möglichst nicht älter sein sollen als sechs Monate. Mit der Übersendung des überalterten Strafregisterauszuges hat die JVA zu Unrecht Kenntnis von bereits getilgten Eintragungen erhalten. Wie sich im Laufe meiner Kontrolle jedoch herausstellte, hat im konkreten Falle der Strafgefangene entgegen seiner Annahme letztendlich keine Nachteile durch diese Fehlinformation erleiden müssen.

Das Niedersächsische Justizministerium hat anläßlich dieses Falles in seiner neuen Allgemeinen Verfügung zur Vorbereitung der Entlassung aus der Strafhaft vom 21. April 1997 (Nds. Rpfl. S. 93), geregelt, dass die Staatsanwaltschaft in Vorbereitung der vorzeitigen Entlassung zur Bewährung ihrem Antrag an die Strafvollstreckungskammer u. a. auch einen aktuellen Bundeszentralregisterauszug des Gefangenen beifügen soll. Auf diese Weise ist zumindest gewährleistet, dass dem zuständigen Gericht nur der aktuelle Stand der Vorstrafen übermittelt wird.

28.3 Übermittlung von Gefangenendaten an Optiker

Die Annahme eines Gefangenen, die Justizvollzugsanstalt habe mit einem Brillenantrag (Formular Reg.Nr. 18) Daten zu seiner Haft (z. B. Haftbeginn und -ende, Hausgeld usw.) an den Optiker übermittelt, erwies sich als richtig. Die Anstalt hatte, wie sie einräumte, mit diesem Formular personenbezogene Daten erfasst und an den Optiker übermittelt, die nicht erforderlich waren, um Gefangene mit Sehhilfen durch den Optiker auszustatten. Es handelte sich dabei um ein altes Formblatt, das entweder aus Nachlässigkeit oder falschverstandener Sparsamkeit - dies ließ sich letztendlich nicht aufklären - verwendet worden war. Ich habe von einer datenschutzrechtlichen Beanstandung dieser rechtswidrigen Datenübermittlung abgesehen, da die Justizvollzugsanstalt inzwischen nur noch die Neufassung des Formblattes benutzt. Dieses enthält die im alten Vordruck noch vermerkten persönlichen Gefangenendaten nicht mehr.

Datenschutz im nicht-öffentlichen Bereich (§ 22 Abs. 6 Satz 3 NDSG)

29 Grundsätzliches zum Datenschutz in der Wirtschaft

Die im letzten Tätigkeitsbericht (XIII 31) angesprochene Expansion des Aufgabengebiets „Datenschutz im nicht-öffentlichen Bereich“ hält an. Die Datenverarbeitung in diesem Bereich ist außerordentlich vielgestaltig, und die privatwirtschaftlich angelegten Datensammlungen entwickeln sich wildwuchsartig. Das derzeitige Datenschutzrecht – geregelt im Wesentlichen im Dritten Abschnitt des BDSG – ist nach wie vor schwach ausgestaltet; die Betroffenen haben wenig Schutz, und die Sanktionsmöglichkeiten bei Rechtsverletzungen sind dürftig. Die Hoffnungen der Datenschutzbeauftragten des Bundes und der Länder sind auf eine kurzfristige Umsetzung der EU-Datenschutzrichtlinie gerichtet; eine solche kurzfristige Umsetzung wurde in der Bonner Koalitionsvereinbarung vom 20. Oktober 1998 festgelegt. Die Zügigkeit darf aber nicht zu Lasten materieller Substanz gehen.

30 Kontrolltätigkeit: Zahlen, Fakten und Erfahrungen

30.1 Meldepflicht nach § 32 BDSG

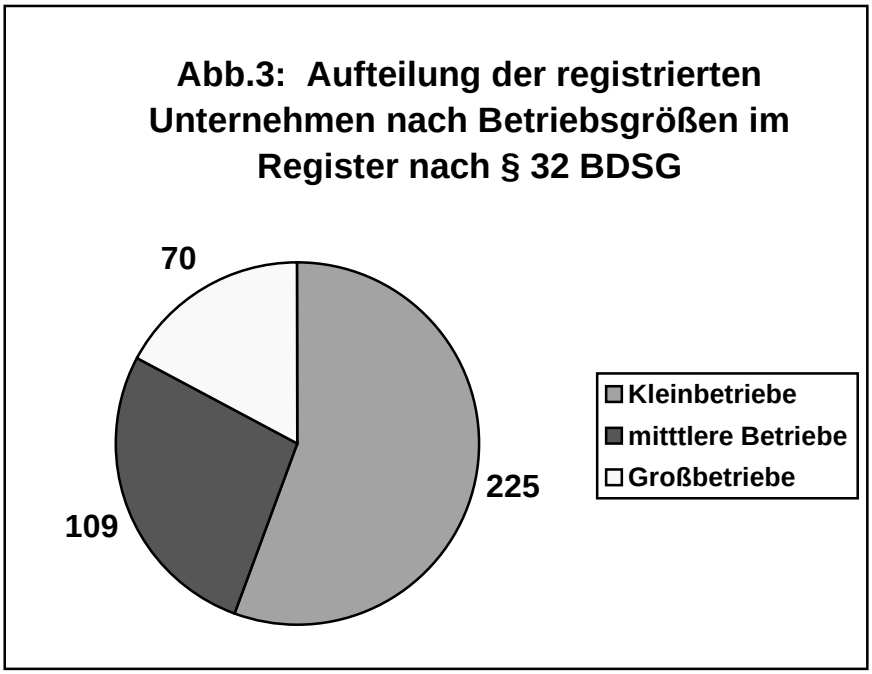
Unternehmen der Wirtschaft, die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung, zum Zwecke der anonymisierten Übermittlung oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen, haben mir die Aufnahme oder Beendigung ihrer Tätigkeit mitzuteilen.

Am 1. Oktober 1998 waren insgesamt 404 Firmen zum Register gemeldet. Dies entspricht einer Zunahme gegenüber Ende 1996 von knapp 20%; damals waren 338 Firmen registriert.

Die genaue Aufteilung nach Betriebsarten und deren Veränderung gegenüber 1992 zeigt die folgende Tabelle.

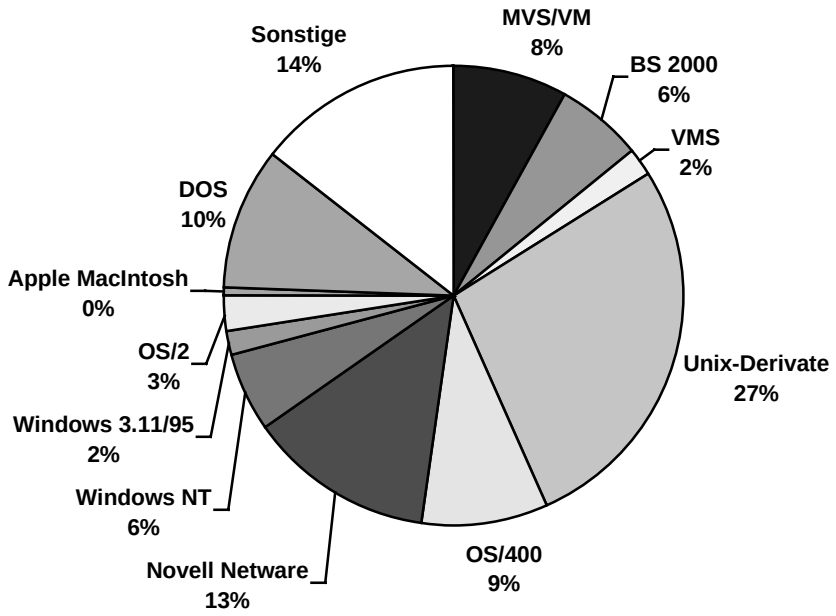
Betriebsarten	Anzahl			
	1992	1994	1996	1998
Service-Rechenzentren	65	85	114	128
Rechenzentren	66	70	72	90
Aktenvernichtungsunternehmen	9	26	45	59
Datenerfassungsunternehmen	28	37	40	40
Auskunfteien	27	29	31	33
Datenarchivierung	14	17	21	22
Adressverlage	3	3	5	16
Mailboxen	0	0	5	6
Markt- und Meinungsforschung	2	2	4	4
Telefon-Marketing	0	0	0	4
Lettershops	0	0	0	2
Internetprovider	0	0	0	1

Seit dem 1. Januar 1992 sind insgesamt 89 Firmen aus dem Register gelöscht und 308 Firmen neu aufgenommen worden. Nach wie vor stellen die Kleinbetriebe mit 55% den größten Anteil der gemeldeten Unternehmen.



Die Datensicherheit wird in besonderem Maße von dem verwendeten Betriebssystem beeinflusst. Eine Auswertung des Registers nach Betriebssystemen zeigt große Unterschiede in diesem Bereich (siehe Abb. 4). Ein genauerer Blick in das Register macht jedoch auch deutlich, dass die Vielfalt der Betriebssysteme nicht so groß ist, wie sie auf den ersten Blick zu sein scheint. Die vier Betriebssysteme MVS/VS, UNIX, Novell Netware und DOS/Windows decken bereits ca. 2/3 aller Systeme ab. Diese Informationen benutze ich bei der Planung meiner Aufsichtstätigkeit. So ist z. B. die Erstellung meiner Prüfkonzepte aufgrund dieser Zahlen erfolgt. Auch die Prüfungen vor Ort berücksichtigen diese Daten.

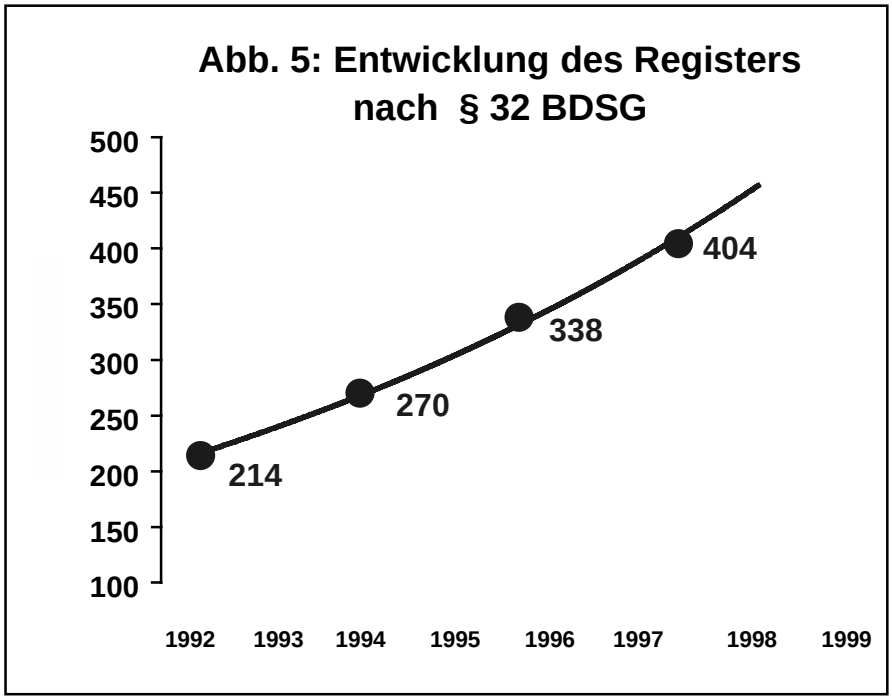
Abb. 4: Betriebssysteme gemeldeter Unternehmen



30.2 Kontrolle vor Ort

In den Jahren 1997 und 1998 habe ich im Rahmen meiner Aufsichtstätigkeit im Bereich der Wirtschaft 16 Prüfungen vor Ort bei niedersächsischen Unternehmen durchgeführt. Vier dieser Prüfungen waren „Anlassprüfungen“ nach § 38 Abs. 1 BDSG, die anderen „Routineprüfungen“ nach § 38 Abs. 2 BDSG. Damit habe ich den Schnitt an Prüfungen gegenüber den letzten Vorjahren in etwa wieder erreicht, was mir nur durch die Optimierung des Prüfungsablaufs möglich war (vergl. 30.2.2). Diese Stagnation auf niedrigem Niveau halte ich für unbefriedigend, insbesondere wenn diese Zahlen im Licht der steigenden Registermeldungen gesehen werden (Abb. 5).

Theoretisch beträgt damit der Abstand zwischen zwei Prüfungen bei einem Unternehmen mittlerweile 67 Jahre. Von regelmäßigen Prüfungen mit einem „Prüfrhythmus“ kann nicht mehr die Rede sein; vielmehr ist die Prüfungstätigkeit in weiten Teilen zu einem reinen Stichprobenverfahren geworden. Ein stärkeres Engagement war mir aber leider wegen der geringen Personalkapazitäten nicht möglich.



Prüfungsschwerpunkt im nicht-öffentlichen Bereich war die Kontrolle der Datensicherungsmaßnahmen beim Einsatz von MVS, dem wichtigsten Großrechner-Betriebssystem von IBM (vgl. 30.2.1).

30.2.1 Erfahrungen aus Prüfungen des Betriebssystems MVS

Die oft als Dinosaurier bezeichneten Großrechner sind noch lange nicht ausgestorben. Solche Systeme werden noch über Jahre ihren Dienst bei bewährten "Altverfahren" versehen. Deshalb habe ich für den Bereich der IBM-Betriebssysteme MVS und VM ein detailliertes Prüfkonzept entwickelt. MVS und VM bieten einige Sicherheitsmechanismen, die jedoch nicht ausreichen, um einen angemessenen Schutz zu gewährleisten. Zusatz-Softwareprodukte wie RACF von IBM, ACF2 und TOP SECRET von Computer Associates oder VMSECURE von Systems Center bieten zusätzliche Sicherheit; sie kommen bei den meisten IBM-Großrechnern zum Einsatz.

Das MVS/VM-Prüfkonzept unterstützt den Systemadministrator beim Erstellen seines Sicherheitskonzepts. Zunächst weist der Katalog auf Gefahren und Risiken hin. Es folgen Maßnahmeempfehlungen, die den Sicherheitsrisiken wirksam entgegenwirken. Das Prüfkonzept ist als Checkliste gestaltet und liefert nach Durcharbeiten eine Aufstellung der noch zu treffenden Maßnahmen. Das Konzept ist mittlerweile fertiggestellt und z. B. über mein Internet-Angebot abrufbar. Dieses Konzept war die Grundlage für sieben Prüfungen von Großrechnersystemen, fast ausschließlich im nicht-öffentlichen Bereich.

Großrechnersysteme sind komplexe Systeme mit einer großen Anzahl an Benutzern, Programmen und Daten. Dementsprechend komplex sind auch die erforderlichen Sicherungsmaßnahmen für diese Systeme. Die Ergebnisse meiner Prüfungen zeigen eine Vielzahl unterschiedlicher Sicherheitslücken auf. Anzahl und Art der Defizite variieren stark, einige Punkte finden sich aber bei fast allen auf der Mängelliste.

– Das AUDITOR-Attribut wurde zumeist nicht so genutzt, wie es von IBM vorgesehen ist. Dieses Attribut soll in erster Linie der Einrichtung einer Überwachungsstelle dienen, die weit mehr als etwa bei Unix oder Windows NT eine Kontrolle der ansonsten unkontrollierbaren Administration ermöglicht. Fast ausnahmslos wurde diese Kontrolle aber nicht von einer besonderen Auditor-Person, etwa dem Datenschutzbeauftragten, wahrgenommen. Vielmehr hatten die RACF-Administratoren meist sich selbst diese Rechte zugestanden.

– Eine der wichtigsten Maßnahmen zur Datensicherung, die Protokollierung von sicherheitsrelevanten Vorgängen, lässt sich zwar mit MVS/RACF hervorragend einrichten, wurde aber von vielen Unternehmen stiefmütterlich behandelt. Insbesondere die Kontrolle der produzierten Protokolle wurde nachlässig gehandhabt. Dies steht im Zusammenhang mit der Einrichtung der oben erwähnten Auditor-Funktion.

– Wie bei den PC sind auch im Großrechnerbereich die Mängel bei der Einrichtung sicherer Passwortverfahren und Pausenfunktionen ein Dauerbrenner. Obwohl technisch möglich, fehlten verschiedene wichtige Elemente für ein sicheres Passwortverfahren, mal war es die technisch erzwungene Passwortmindestlänge von sechs, besser acht Zeichen, mal war es die Passwortalterung, die Begrenzung der Fehlversuche oder die Zeichenmischung.

– Regelmäßig angesprochen habe ich auch die Frage nach der Verschlüsselung von Daten bei der Übertragung oder Speicherung. Im Gegensatz zu den anderen aufgeführten Punkten hakt es hier bereits bei den Möglichkeiten einer technischen Umsetzung. Eine umfassende Verschlüsselung ist nur mit Zusatzsoftware möglich.

Hinzu kamen verschiedene betriebssystemspezifische Mängel, etwa bei der Verwendung des SPECIAL-Attributs, beim Umgang mit dem RVARY-Befehl, bei der Kontrolle selbstgeschriebener Supervisor Calls, beim Freigabeverfahren für APF-Bibliotheken oder bei der Zugriffsbeschränkung mit der Befehlszeile „UNIVERSAL ACCESS = NONE“.

Nur bei einem Unternehmen waren die von mir angesprochenen Mängel so minimal, dass ich die Prüfung ohne Nachforderungen abschließen konnte. Bei den anderen Unternehmen habe ich die aufgedeckten Mängel, wie auch sonst bei meinen Prüfungen, mit den jeweiligen Unternehmensvertretern erörtert und im Prüfprotokoll festgehalten. Häufig wurde mir bereits während der Prüfung zugesichert, dass die Mängel umgehend beseitigt werden. Meine Nachfragen zu diesen Prüfungen sind noch nicht abgeschlossen. Schon jetzt lässt sich aber sagen, dass mit dem MVS/VM-Prüfkonzept und mit den durchgeführten Prüfungen in einem nach wie vor besonders wichtigen Bereich der automatisierten Datenverarbeitung viel für eine Verbesserung der Datensicherheit getan werden konnte.

30.2.2 Prüfungsablauf

Mit meinen Checklisten konnte der Prüfungsablauf effizienter und effektiver gestaltet werden. Die Prüfunterlagen wurden teilweise schon vor dem eigentlichen Prüftermin zur Verfügung gestellt, um den Unternehmen Gelegenheit zu geben, ihr Sicherheitskonzept selbst zu testen und zu korrigieren. Das korrigierte Sicherheitskonzept wurde mir vor der Prüfung zurückgesandt und von mir ausgewertet. Prüfungsablauf und -schwerpunkt wurden der zu prüfenden Stelle frühzeitig mitgeteilt. Bei meinen technischen Prüfungen im nicht-öffentlichen Bereich werde ich durch das Informatikzentrum Niedersachsen (IZN) unterstützt.

Das folgende Schema stellt den typischen Ablauf einer Prüfung im nicht-öffentlichen Bereich dar.

Ablauf einer Prüfung im nicht-öffentlichen Bereich			
Nr.	**Thema**	**Festlegung**	**Termin**
1	Prüfungsan-schreiben	Der LfD fertigt das Prüfungs-anschreiben und fordert Unter-lagen (Checklisten) an. – Terminbestätigung (7 Tage nach Eingang) – Unterlagen bis 4 Wochen vor der Prüfung	
2	Mitteilung	IZN bekommt Bestätigung des Prüfungstermins	10 Tage nach Ab-sendung der Prü-fungsmitteilung
3	Prüfungsunter-lagen	IZN bekommt Kopie oder Ori-ginal der Prüfungsunterlagen zum frühestmöglichen Zeit-puntk und Mitteilung über Schwerpunkt der Prüfung	Spätestens eine Wo-che vor der Prüfung
4	Abstimmungsge-spräch	Gespräch über den Prüfungsin-halt zwischen IZN und LfD	3 Werktage vor der Prüfung
5	Prüfung	Teilnehmer IZN und LfD. Im Vorfeld wird der Firma ein Ablauf- und Zeitplan der Prü-fung übersandt.	
6	Prüfprotokoll	IZN entwirft ein Prüfprotokoll (incl. Empfehlungen und Bean-standungen)	3 Werktage nach der Prüfung
7	Abstimmungsge-spräch	In einem Abstimmungsge-spräch zwischen IZN und LfD wird das Protokoll besprochen	4. Werktag nach der Prüfung
8	Endgültiges Protokoll	IZN übergibt endgültiges Prüf-protokoll	Je nach Arbeitsanfall
9	Anschreiben an das Unternehmen	Das Prüfprotokoll wird der Firma übersandt.	

Durch diese abgestimmte Zusammenarbeit wurden das Datenschutzverständnis und der Datenschutzstandard in der Wirtschaft wesentlich gestärkt.

31 Adressenhandel und Markt- und Meinungsforschung

31.1 Unerwünschte Kreditangebote

Einem Bürger, der eine eidesstattliche Versicherung abgegeben hatte, wurde von mehreren „Finanzservice-Unternehmen“ ein Angebot über einen Kredit zugesandt, und zwar, wie betont wurde, ohne Schufa-Eintragung. Der Betroffene äußerte die von mir geteilte Befürchtung, Personen in einer finanziellen Notlage würden durch solche Angebote möglicherweise in noch größere finanzielle Bedrängnis geraten. Er bat mich zu prüfen, wie diese Unternehmen an seinen Namen und seine Anschrift gelangt waren.

Es stellte sich heraus, dass die Anbieter unterschiedliche Quellen nutzten. Ein Unternehmen, dessen Sitz sich nicht in Niedersachsen befindet, teilte der von mir um Hilfe gebetenen Aufsichtsbehörde mit, es beziehe von ca. 1 900 Maklern Daten, werte jedoch, anders als von mir erwartet, nicht das Schuldnerverzeichnis aus. Die Herkunft der Daten des Petenten konnte nicht festgestellt werden, sodass ich mich damit begnügen musste, ihm zu raten, gegenüber diesem Unternehmen gemäß § 28 Abs. 3 BDSG der Nutzung seiner Daten für Werbezwecke zu widersprechen.

Bei einem in Niedersachsen ansässigen Finanzdienstleister ergab die Prüfung, dass er die Daten von einem Unternehmen erhalten hatte, das selbst Kredite vermittelte, darüber hinaus jedoch auch Daten potentieller Kreditnehmer an andere Finanzdienstunternehmen verkaufte. Die für seine Direktwerbung und die für den Weiterverkauf bestimmten Daten bezog er von einer Finanzagentur, die sich ihrerseits, wie sie mir mitteilte, bei überregionalen Anbietern bediente.

Dieses Beispiel zeigt, welchen Umfang der Adresshandel selbst bezüglich solcher Personen angenommen hat, bei denen man meinen sollte, dass sie für die Wirtschaft keine attraktive Zielgruppe darstellen.

31.2 Das Geschäft mit den „Haushaltsumfragen“

In der letzten Zeit erfolgen bundesweit von verschiedenen Firmen „Befragungen“ und „Haushaltsumfragen“. Darin werden weit über 100 Fragen mit sehr sensiblen Daten über das Urlaubs- und Reiseverhalten, Freizeitaktivitäten, Auto, Gesundheit, Finanzsituation, Wohnung, Kauf- und Kosumverhalten, Schulbildung und Berufsausübung gestellt.

Als „Dankeschön“ für das Ausfüllen des Fragebogens lockte die Teilnahme an einer Verlosung.

Diese Befragungen haben zu einer Vielzahl von telefonischen und schriftlichen Eingaben von verunsicherten Bürgerinnen und Bürgern geführt. Die Firmen verwenden häufig Firmennamen, die zunächst vertrauenserweckende Assoziationen auslösen. Bei den Befragungen handelte es sich aber nicht, wie von vielen vermutet, um reine Marktforschung. Die von den Bürgerinnen und Bürgern offenbarten Daten werden langfristig gespeichert und personenbezogen für alle denkbaren Direktwerbe-Zwecke verwendet. Das Ausfüllen des Bogens führt zwangsläufig dazu, dass die Betroffenen verstärkt persönliche Werbepost zugesandt bekommen. Mit den erfragten Persönlichkeitsprofilen soll eine gezielte, „kundenorientierte“ Ansprache erfolgen.

Ich habe wiederholt darauf hingewiesen, dass niemand verpflichtet ist, solche Fragebogen auszufüllen. Selbst wenn eine schriftliche Einwilligung per Unterschrift eingeholt wird – dies ist ein mit allen obersten Aufsichtsbehörden für den Datenschutz abgestimmtes Erfordernis -, bleibt die Offenbarung über „Ehepartner/Partner“, „Kinder“ oder sonstige Dritte datenschutzrechtlich problematisch. Wer erst später wegen der Auswertung seiner Daten Bedenken bekommt, kann deren Nutzung auch nachträglich widersprechen. Diese dürfen dann personenbezogen nicht mehr genutzt werden. Wer etwas gegen die Nutzung seiner Daten für Marketingzwecke tun will, sollte den Bogen in den Papierkorb werfen. Ein weitergehender Schutz vor direkt adressierter Werbung wird durch eine Eintragung in die „Robinson-Liste“ des Deutschen Direktmarketing Verbandes (Telefon 07156/951010) erreicht. Umstritten ist die Frage, ob die werbenden Unternehmen verpflichtet sind, ihren Adressbestände mit der Robinson-Liste abzugleichen. Nach meinen Erfahrungen wird dieser Abgleich aber in den meisten Fällen praktiziert.

In meinem Merkblatt „Tips zum Adressenhandel“ zeige ich auf, was man gegen die Werbepapierflut im Briefkasten unternehmen kann. Es kann bei mir angefordert oder über mein Internet-Angebot abgerufen werden.

32 Kundendaten und Werbung

Unverlangte Werbung per Telefax für ein Radarwarngerät

Zahlreiche Petenten beschwerten sich darüber, dass sie per Telefax unverlangte Werbung für ein Radarwarngerät, das angeblich auf eine Radarkontrolle der Polizei hinweist, erhalten hatten.

Vertrieben wurde dieses Gerät von zwei Unternehmen in meinem Zuständigkeitsbereich. Abgesandt hatte die Werbung jedoch ein Unternehmen in den Niederlanden.

Telefaxe waren bundesweit verschickt worden; selbst meine Dienststelle hatte solche Sendungen erhalten. Einem Teil der Petenten waren sie kurz nach Einleitung eines Bußgeldverfahrens wegen einer Geschwindigkeitsübertretung zugestellt worden. Der Verdacht, die Polizei, eine Straßenverkehrsbehörde oder das Kraftfahrtbundesamt könnten Daten herausgegeben haben, ließ sich jedoch nicht erhärten.

Es bestand Anlass zur Vermutung, dass die beiden in derselben Stadt ansässigen Händler und das Unternehmen aus den Niederlanden eng miteinander verbunden waren. Um die verworrenen Hintergründe zu klären, habe ich eine Reihe von Fragen gestellt, u. a. nach der Verbindung dieser Unternehmen, nach den für die Datenverarbeitung zuständigen Personen, ob eine Liste mit Angaben derjenigen, die einer Nutzung ihrer Daten zu Werbezwecken widersprochen hatten, geführt wurde und ob eine Information des Unternehmens in den Niederlanden sichergestellt wurde, sodass der Widerspruch beachtet wird.

Meine Fragen wurden nur unvollständig beantwortet. Auch die Beteiligung des Datenschutzbeauftragten der Niederlande führte nicht weiter. Er hatte von dem niederländischen Unternehmen die Antwort erhalten, die Adressen stammten aus der CD-ROM „Telefaxbuch für Deutschland“. Ich habe schließlich ein Bußgeld wegen der Auskunftsverweigerung verhängt. Das Verfahren wurde allerdings vom Amtsgericht gemäß § 47 Abs. 2 des Ordnungswidrigkeitengesetzes eingestellt. Dennoch werde ich weiter versuchen, eine vollständige Antwort zu erhalten.

33 Schufa

Personenverwechselung bei Auskünften

Die bisherige gute Zusammenarbeit mit der Schufa Nord setzte sich fort. Noch nicht gelöst ist das Problem einer Personenverwechselung (vgl. XIII 35).

Der Antrag eines Kunden, der einen Vertrag über ein Funktelefon abschließen wollte, wurde mit dem Hinweis auf eine negative Schufaauskunft abgelehnt. Dank der gemeinsamen Bemühungen des Unternehmens, das die Auskunft eingeholt hatte, und der Schufa wurde schnell geklärt, dass eine Verwechselung mit einer Person mit gleichem Namen, Vornamen und Geburtsdatum vorlag. Ich suche zurzeit gemeinsam mit der Schufa nach einem Weg, solche Verwechselungen in Zukunft zu vermeiden.

34 Auskunfteien

Ein nicht unerheblicher Teil der Eingaben bezog sich, wie nicht anders zu erwarten, auf Auskunfteien.

Bezweifelt wurde von Betroffenen, dass Auskunfteien ohne Einwilligung Daten übermitteln dürfen. Ich muss in solchen Fällen auf § 29 Abs. 2 Nr. 1 a BDSG hinweisen, nach dem eine Übermittlung zulässig ist, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der personenbezogenen Daten glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Ein solches berechtigtes Interesse des Empfängers liegt z. B. vor, wenn er sich vor dem Abschluss eines Kaufvertrags oder der Vergabe eines Kredits über die wirtschaftlichen Verhältnisse des Kunden orientieren will.

Andere Petenten wünschen Informationen, unter welchen Voraussetzungen sie Auskunft über die von der Auskunftei gespeicherten Daten verlangen können. Nicht selten richten sich Beschwerden auch gegen eine Übermittlung unrichtiger Daten durch die Auskunftei.

Einen ersten Überblick über die genannten Fragen gibt das Merkblatt „Handels- und Wirtschaftsauskunfteien“, das ich gemeinsam mit dem Berliner Datenschutzbeauftragten, dem Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen und dem Hamburgischen Datenschutzbeauftragten herausgegeben habe. Es kann bei mir und den anderen genannten Stellen angefordert werden.

35 Finanzwirtschaft

Verwendung der EC-Karte bei der Parkplatzbenutzung

Ein Bürger teilte mit, eine Bank beabsichtige, auf ihrem Kundenparkplatz eine Schranke zu installieren, die nur mit der EC-Karte betätigt werden könne. Beim Verlassen des Parkplatzes müsse der Kunde seine EC-Karte in das Schrankenterminal einführen. Die Parkgebühr werde dann von seinem Konto abgebucht.

Der Petent befürchtete, die Bank könne auf diese Weise die auf dem Magnetstreifen gespeicherten Daten auch anderer Banken lesen und für interne Zwecke gebrauchen. Auch lasse sich das Verhalten des Benutzers genau nachvollziehen. Nähere Angaben zu dem Schrankensystem konnte er zunächst nicht machen.

Die bisherigen Funktionen der EC-Karte sind durch Aufnahme eines Chips erweitert worden, sodass die EC-Karte seit dem 1. Januar 1998 auch als Geldkarte genutzt werden kann.

Der Sachverhalt ist im vorliegenden Fall noch nicht eindeutig geklärt. Ich gehe jedoch davon aus, dass die Verwendung als Geldkarte geplant ist. Andere Anwendungen würden die Eingabe der PIN oder im Lastschriftverfahren eine Unterschrift erfordern und wären damit für den Betrieb der Parkplatzschranke zu umständlich.

In dem Chip können Guthaben von bis zu 400,-- DM gespeichert werden. Für die Zahlungsvorgänge richten die Banken spezielle Börsenverrechnungskonten ein. Durch Einschieben der Geldkarte in das Abbuchungsgerät des Händlers können Waren des täglichen Bedarfs oder Dienstleistungen bargeldlos bezahlt werden. Der Händler übermittelt die Abrechnungsdaten an eine Clearingstelle, die sog. Evidenzzentrale, die eine Gutschrift auf dem Händlerkonto veranlasst und den entsprechenden Betrag vom Börsenverrechnungskonto abbucht. Dieses Konto weist nur den jeweiligen Saldo aus.

Daneben wird jedoch bei der Evidenzzentrale ein zweites Konto geführt, das sog. Schattenkonto. In ihm sind die vom Händler übermittelten Daten gespeichert: die Kartennummer, der Kaufbetrag, das Kaufdatum, die Kaufzeit, der Händlerschlüssel und der Saldo des Börsenverrechnungskontos zum Kaufzeitpunkt. Das Schattenkonto soll Sicherheitskontrollen zur Verhinderung des Kartenmissbrauchs ermöglichen.

Die Bank kann also nicht, wie von dem Petenten befürchtet, nach dem Einführen der Karte in das Schrankensystem Eintragungen anderer Institute lesen oder ein Benutzerprofil erstellen. Allerdings kann aufgrund des Schattenkontos durch ein Zusammenwirken zwischen Evidenzzentrale und Bank über die Kontennummer ein Personenbezug hergestellt werden. Möglich ist ebenfalls eine Auswertung des Schattenkontos. Auch wenn diese zweckwidrige Nutzung des Schattenkontos nicht unterstellt werden soll, haben die Datenschutzbeauftragten des Bundes und der Länder sich wiederholt dafür ausgesprochen, Geldkarten anzubieten, die ein anonymes Bezahlen ermöglichen, sog. White Cards. Zumindest sollte der Kunde darüber informiert werden, dass das Bezahlen mit der EC-Karte nicht anonym erfolgt.

Die Datenschutzbeauftragten werden die weitere Entwicklung aufmerksam verfolgen.

36 Versicherungen

Immer wieder richten sich Eingaben gegen eine Datenübermittlung, die im Rahmen eines Kooperationsvertrags zwischen Versicherungen und Vertragspartnern aus anderen Bereichen stattfindet. Zwei Beispiele seien dafür genannt.

36.1 Zusammenarbeit zwischen einer Versicherung und einer Gewerkschaft

Ein Gewerkschaftsmitglied hatte ein Schreiben von einer Versicherung erhalten, in dem sie unter Bezugnahme auf einen Kooperationsvertrag mit der Gewerkschaft auf ihre Angebote hinwies und den Besuch ihres Bezirksleiters ankündigte. Das Gewerkschaftsmitglied fürchtete, dass sein Name und seine Anschrift von der Gewerkschaft an die Versicherung weitergegeben worden seien.

Die von mir um Stellungnahme gebetene Versicherung antwortete, sie habe die Daten des Betroffenen inzwischen gelöscht.

Der Bundesvorstand der Gewerkschaft, für den ich örtlich nicht zuständig bin, teilte der von mir eingeschalteten zuständigen Aufsichtsbehörde mit, aufgrund des Kooperationsvertrags informiere die Versicherung in den Publikationen der Gewerkschaft über ihr Angebot und lege in deren Geschäftsstellen Prospekte aus. Der Kooperationsvertrag habe jedoch nicht zum Inhalt, dass die Gewerkschaft Mitgliederdaten übermittele. Nur in einem bestimmten Bezirk, zu dem der Petent gehörte, seien in einem Fall Mitgliederdaten durch Angestellte der Gewerkschaft unter Verstoß gegen arbeitsvertragliche Pflichten herausgegeben worden. Man habe sichergestellt, dass in Zukunft eine solche Weitergabe unterbleibe.

Diese Erklärung wurde von der Aufsichtsbehörde und von mir akzeptiert.

36.2 Zusammenarbeit zwischen einer Versicherung und einem Verkehrsbetrieb

Ein Unternehmen des öffentlichen Personennahverkehrs informierte seine Abonnenten darüber, dass in Zusammenarbeit mit einer renommierten Versicherung ein „exklusiver Sondertarif“ in der Kraftfahrzeugversicherung angeboten werden könne. Viele Abonnenten besäßen zwar ein Auto, würden es jedoch zumeist im besonders unfallträchtigen Berufsverkehr nicht benutzen. Dieses deutlich geringe Schadensrisiko zahle sich aus.

Dem Schreiben beigefügt war ein Fragebogen, den die Abonnenten an den Verkehrsbetrieb zurückschicken sollten, um auf diese Weise ein Angebot der Versicherung einzuholen, das einen Vergleich mit der derzeitgen Kraftfahrzeugversicherung der Abonnenten ermöglichte.

Ich habe den Verkehrsbetrieb um Auskunft gebeten, ob er gezielt Abonnenten angeschrieben habe, von denen bekannt sei, dass es sich um Kraftfahrzeughalter oder –benutzer handelte, und, falls dies zutreffen sollte, woher die Informationen stammten. Weiterhin habe ich um Mitteilung gebeten, ob die Versicherung erst dadurch, dass der Abonnent den Fragebogen zurückschickte, Informationen über ihn erhielt oder ob bereits vorher Daten über die als Versicherungskunden in Betracht kommenden Personen vorlagen. Auf Letzteres deutete hin, dass der Fragebogen eine „Angebotsnummer“ enthielt.

Der Verkehrsbetrieb antwortete, er habe alle Abonnenten angeschrieben, weil ihm Informationen über Personen mit Autobesitz nicht vorlägen. Es sei aber statistisch festgestellt worden, dass rund 50 % der Abonnenten über ein Auto oder Motorrad verfügten. Daten über Abonnenten, die als Kunden der Versicherung in Betracht kommen, lägen der Versicherung nicht vor. Sie erhalte erst nach Einsendung des Fragebogens Kenntnis von den Abonnenten. Die Angebotsnummer werde der Versicherung erst nach Einsendung bekannt. Sie diene allein der Ermittlung der Rücklaufquote.

Insoweit war die Antwort des Verkehrsbetriebs zufriedenstellend. Noch nicht abschließend geklärt ist allerdings ein weiteres Problem. In dem Fragebogen wurde nämlich auch nach der Mitgliedschaft in einem Umweltschutzverband gefragt und darüber hinaus die Angabe der Mitgliedsnummer erbeten, was zu Verärgerung bei Adressaten des Schreibens geführt hatte. Laut Mitteilung im Fragebogen wurde diese Angabe, die einen sehr persönlichen Lebensbereich betrifft, unbedingt für die Erstellung eines Vergleichsangebotes benötigt.

Dazu führte der Verkehrsbetrieb aus, es bestehe eine Kooperation zwischen der Versicherung und dem Umweltschutzverband mit dem Ziel, Versicherungsprodukte zu entwickeln, die ein umweltorientiertes Verhalten der Versicherungsnehmer förderten. Im Zuge dieser Kooperation erhielten Mitglieder des Verbands gesonderte Preisnachlässe in der Kraftfahrzeugversicherung, weil sie sich u. a. durch defensives Autofahren auszeichneten und damit ein geringes Schadensrisiko verursachten. Damit dieser Vorteil bei der Angebotserstellung berücksichtigt werden könne, benötige die Versicherung die Mitgliedsnummer als Nachweis, da ansonsten wettbewerbsrechtliche Bedenken geltend gemacht werden könnten.

Ich habe empfohlen, die Abonnenten im Anschreiben über diesen Grund für die Frage nach der Mitgliedschaft im Umweltschutzverband zu informieren. Dies dürfte auch in ihrem Interesse liegen, um Kritik derjenigen, die man als Kunden werben will, an übergroßer Neugierde zu vermeiden.

37 Arbeitnehmerdatenschutz

Übermittlung von Arbeitnehmerdaten an ein Kreditinstitut

Die Stadtwerke einer niedersächsischen Großstadt wollten die Abrechnung der Dienstreisen ihrer Mitarbeiterinnen und Mitarbeiter vereinfachen und damit erhebliche Verwaltungskosten einsparen. Während bisher ein Reisekostenvorschuss gezahlt und dann mit den tatsächlichen Ausgaben verrechnet wurde, sollten die Beschäftigten künftig eine dienstliche Kreditkarte zur Begleichung ihrer Reisekosten erhalten. Zwar muss jeder Mitarbeiter auch mit der Kreditkarte die Reisekosten zunächst selbst zahlen. Die Stadtwerke sichern ihren Bediensteten aber zu, die Rückerstattung unverzüglich vorzunehmen. Da das Kreditinstitut die Rechnungsbeträge erst nach einigen Wochen vom privaten Konto des Beschäftigten abbucht, hat dieser den Erstattungsbetrag von seinem Arbeitgeber bereits überwiesen bekommen. Neben der dienstlichen Kreditkarte wird den Beschäftigten zugleich eine Kreditkarte für private Ausgaben angeboten. Die Kosten für beide Kreditkarten tragen die Stadtwerke.

Eine vorteilhafte Regelung für die Mitarbeiterinnen und Mitarbeiter. Sie geriet jedoch aus Datenschutzgründen in Misskredit. Dem Kreditinstitut wurden nämlich u. a. Name, Anschrift, Bankverbindung und Personalnummer jedes einzelnen Beschäftigten übermittelt. Aus Servicegründen bereitete es „unterschriftsreife“ Anträge für die angebotenen Kreditkarten vor, in die die genannten Arbeitnehmerdaten bereits aufgenommen worden waren. Die Beschäftigten staunten nicht schlecht, als sie die mit Bankinstitut und Kontonummer versehenen Vordrucke vom Kreditinstitut zugeleitet erhielten. In der Belegschaft kam Unmut auf, der zu zahlreichen Anfragen in meiner Dienststelle und zu kritischen Presseartikeln führte.

Die Stadtwerke rechtfertigten ihr Vorgehen zunächst mit dem Argument, hier liege nichts weiter als eine zulässige Auftragsdatenverarbeitung vor. Diese Einschätzung gaben sie im Zuge der Erörterungen aber bald auf. Im Verlauf der Prüfung stellte sich heraus, dass das Unternehmen die Arbeitnehmerdaten schon vor Abschluss der einschlägigen Verträge dem Kreditinstitut übermittelt hatte. Dieser vorzeitigen – offenbar aus der Hast geborenen – Datenweitergabe an die künftigen Vertragspartner standen schutzwürdige Belange der Bediensteten entgegen (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG).

Auch nach Vertragsschluss wäre eine Übermittlung der Daten ohne Einwilligung der Arbeitnehmer nicht in Betracht gekommen. Ebenso war eine Datenweitergabe an das Kreditinstitut unter dem Gesichtspunkt der Auftragsdatenverarbeitung nach § 11 BDSG unzulässig.

Auftragsdatenverarbeitung liegt vor, wenn ein Unternehmen sich der Unterstützung eines Dritten bei der Verarbeitung seiner personenbezogenen Daten bedient. Der Auftraggeber bleibt dabei weiterhin „Herr“ seiner Daten; das Serviceunternehmen betreibt für ihn gleichsam als verlängerter Arm oder ausgelagerte Organisationseinheit die Datenverarbeitung in voller Abhängigkeit von seinen Weisungen. Das ist zwar der Fall, wenn erforderliche Arbeitnehmerdaten – sofern die Grenze zur Aufgaben(funktions-)übertragung nicht überschritten wird - an einen Auftragnehmer zur Bearbeitung von Dienstreisen weitergegeben werden. Dieser übt dann eine bloße „Hilfsfunktion“ aus. Da im vorliegenden Fall das Kreditinstitut jedoch die Daten auch nutzen wollte, um den Arbeitnehmern eine private Kreditkarte anzubieten, nahm es insofern keine Servicefunktion für die Stadtwerke mehr wahr. Die Bank verfolgte vielmehr eigene Geschäftszwecke. Dafür dürfen die ihr zugänglich gemachten Mitarbeiterdaten im Zuge eines Auftragsverhältnisses nicht genutzt werden.

Nach meinen Hinweisen räumte das Unternehmen Fehler ein und bedauerte gegenüber der Belegschaft die Datenübermittlung. Die Arbeitnehmerdaten wurden vom Kreditinstitut an die Stadtwerke zurückgegeben. Eine weitere Nutzung durch die Bank ist ausgeschlossen. Künftig füllen die Mitarbeiterinnen und Mitarbeiter, die eine Kreditkarte für die Abrechnung ihrer Dienstreisen bzw. für private Zwecke in Anspruch nehmen wollen, einen entsprechenden Antrag aus. Eine Übermittlung ihrer Daten an das Kreditinstitut erfolgt nur mit ihrer Zustimmung. Für den Fall, dass ein Arbeitnehmer nur die dienstliche Kreditkarte nutzen möchte, wird sichergestellt, dass das Kreditinstitut die ihm zu diesem Zweck zulässigerweise übermittelten Daten nicht für Angebote für andere Dienstleistungen nutzt.

38 Telefaxauskunft auf einer CD-ROM

Ein Unternehmen hatte eine CD-ROM mit Angaben zu Telefaxanschlüssen herausgegeben. Als Suchbegriffe waren Vorname und Name des Anschlussinhabers, Straße, Ort, Postleitzahl, Branche und Faxnummer vorgesehen.

Ich habe das Unternehmen darauf hingewiesen, dass es gemäß § 33 Abs. 1 Satz 2 BDSG verpflichtet ist, die Betroffenen von der erstmaligen Übermittlung und der Art der zu übermittelnden Daten zu benachrichtigen. In diesem Zusammenhang ist von Interesse, dass das Telekommunikationsgesetz für Telekommunikationsunternehmen bestimmt, dass neue Telefonkunden nur mit ausdrücklicher Einwilligung auf CD-ROM gespeichert werden dürfen.

Weil es eine solche Benachrichtigungspflicht verneinte, habe ich gemäß § 44 Abs. 1 Nr. 3 BDSG ein Bußgeld verhängt.

Das Unternehmen machte im Einspruchsverfahren geltend, die Benachrichtigung sei u. a. deshalb entbehrlich, weil vor der Speicherung durch das Unternehmen zahlreiche Speicherungs- und Übermittlungsvorgänge stattfänden. Die Benachrichtigungspflicht entfalle ebenfalls nach § 33 Abs. 2 Nr. 6 a BDSG. Die auf der CD-ROM gespeicherten Daten seien zu eigenen Zwecken gespeichert. Eine Übermittlung der Daten erfolge nicht mit der Übergabe der CD-ROM, sondern erst durch den Abruf der Daten für eigene Zwecke durch den Käufer. Eine Übermittlung setze eine Kenntnisnahme voraus, die erst bei Abruf der Daten durch den Käufer möglich sei. Wenn man diesen Übermittlungsbegriff nicht teile, greife § 33 Abs. 2 Nr. 7 a BDSG ein. Die Veröffentlichung der Teilnehmerdaten durch die vom Teilnehmer jeweils getroffene Entscheidung bei Abschluss des Anschlussvertrags mit der Telekom AG stehe der Selbstveröffentlichung gleich, weil sie mit Zustimmung des Teilnehmers erfolge.

Ich habe dem Unternehmen entgegengehalten, dass der Begriff „erstmals“ nach § 33 BDSG nur so verstanden werden könne, dass eine erstmalige Speicherung bei der jeweiligen verarbeitenden Stelle gemeint sei. Auch die anderen Argumente habe ich nicht geteilt. Ich habe dem Einspruch daher nicht stattgegeben. Das Verfahren wurde dann allerdings vom Amtsgericht gemäß § 47 Abs. 2 des Ordnungswidrigkeitengesetzes eingestellt.

39 Privates Gesundheitswesen

Weitergabe von Patientendaten an privatärztliche Verrechnungsstellen

Ein großer Teil der niedersächsischen Ärzte und Zahnärzte schaltet bei der Abrechnung mit ihren Patienten die Privatverrechnungsstelle (PVS) der Ärzte und Zahnärzte in Niedersachsen ein.

Die PVS ist eine berufsständische Organisation. Zu ihren Aufgaben gehört insbesondere die Honorarberechnung, das Schreiben von Rechnungen und die Überwachung der Zahlungseingänge. Hingegen tritt der Arzt nicht seine Forderung gegen den Patienten an die PVS ab. Er bleibt also Inhaber der Forderung und muss sie, wenn der Patient nicht zahlt, gerichtlich durchsetzen.

Zwischen der PVS und mir besteht im Grundsatz Einigkeit, dass der Arzt nur mit Einwilligung des Patienten Daten an die PVS weitergeben darf. Dieser Grundsatz wird jedoch nicht von allen Ärzten beachtet.

Auf meine Anregung hat sich der Düsseldorfer Kreis mit der Datenverarbeitung bei den Privatverrechnungsstellen befasst. Weit überwiegend wurde die Auffassung vertreten, dass durch die Privatverrechnungsstellen keine Datenverarbeitung im Auftrag (§ 11 BDSG) erfolgt, sondern eine Funktionsübertragung vorliegt. Einigkeit besteht, dass der Arzt eine schriftliche Einwilligung des Patienten einholen muss.

Die vom Düsseldorfer Kreis gestellten Anforderungen an den Inhalt der Erklärung werden im Wesentlichen durch die Vordrucke der PVS erfüllt. Noch nicht abschließend geklärt ist, in welchen Fällen die Angabe der Diagnose auf der Rechnung, die von der PVS erstellt wird, und damit eine Übermittlung durch den Arzt an die PVS erforderlich ist.

Die PVS hat im Januar 1998 mit einem Rundschreiben den Ärzten und Zahnärzten ein geändertes Einwilligungsformular übersandt und dabei noch einmal auf die Pflicht des Arztes hingewiesen, vor der Weitergabe von Patientendaten die Einwilligung einzuholen.

40 Andere Bereiche

Datenschutzrechtliche Fragen sind nicht nur in den oben dargestellten Branchen wie Adresshandel, Markt- und Meinungsforschung, Schufa, Versicherungen zu lösen, obwohl sie sicherlich den weitaus größten Teil ausmachen, sondern immer wieder auch in manchmal geradezu exotisch anmutenden Bereichen. Zwei Beispiele dafür möchte ich im Folgenden darstellen.

40.1 Mitteilung eines Austritts aus dem Schützenverein an das Ordnungsamt

Ein Schützenverein teilte dem Ordnungsamt den Austritt eines Mitglieds mit. Darüber empörte sich der – ehemalige – Schützenbruder und bat mich um Prüfung, ob dieses Verhalten rechtmäßig sei.

Der von mir um Stellungnahme gebetene Schützenverein berief sich darauf, die Stadt habe ihn verpflichtet, den Austritt aus dem Verein zu melden.

Die Stadt bestätigte, dass sie Vereine, die eine Bescheinigung nach § 32 des Waffengesetzes (WaffG) ausstellen, zur Mitteilung des Vereinsaustritts verpflichte. Zwar bestehe für diese Aufforderung keine Rechtsgrundlage, jedoch ergebe sich die Notwendigkeit aus der Systematik des Waffenrechts, dessen Intention darauf gerichtet sei, möglichst wenig Waffen „ins Volk“ gelangen zu lassen. Durch den Austritt aus dem Verein entfalle möglicherweise das Bedürfnis zum Waffenbesitz, sodass u. U. die Voraussetzungen für einen Widerruf der waffenrechtlichen Erlaubnis (§ 47 Abs. 2 WaffG) vorlägen.

Aufgrund dieser Darstellung erschien mir die Datenerhebung der Stadt bei den Vereinen durchaus sinnvoll. Gegenüber dem Niedersächsischen Innenministerium habe ich jedoch auch auf die fehlende Rechtsgrundlage hingewiesen.

Das Ministerium teilte meine Auffassung, dass eine Rechtsgrundlage für die den Vereinen auferlegte Mitteilungspflicht nicht bestehe. Dennoch sei das Vorgehen der Stadt sinnvoll. Der „Erste vorläufige Entwurf zu einer strukturellen Neuordnung des Waffenrechts“ mache die Anerkennung als schießsportliche Vereinigung davon abhängig, dass durch organisatorische Maßnahmen eine Mitteilung an die zuständige Behörde über einen Vereinsaustritt sichergestellt sei. Die Stadt könne bereits jetzt ihr Ziel, Kenntnis von der Beendigung einer Mitgliedschaft im Schießsportverein zu erlangen, dadurch erreichen, dass sie gemäß § 28 Abs. 1 WaffG die Waffenbesitzkarte des Sportschützen mit einer entsprechenden Auflage verbinde.

Aufgrund einer Umfrage im Jahre 1992 könne ausgeschlossen werden, dass Schützenvereine von den Städten und Gemeinden generell zur Mitteilung von Vereinsaustritten verpflichtet würden. Entweder seien Absprachen mit den Vereinen getroffen worden oder die Kommunen machten von der Möglichkeit einer Auflagenerteilung Gebrauch.

Ich habe der Stadt empfohlen, entsprechend zu verfahren.

40.2 Datenverarbeitung in einer Videothek

Der Kunde einer Videothek teilte mir mit, auf die Frage, ob die Angaben über die von ihm ausgeliehenen Filme gelöscht würden, habe man ihm geantwortet, eine derartige Löschfunktion gebe es nicht. Man könne nur die Kundennummer und damit die Daten über die ausgeliehenen Filme insgesamt löschen; dies jedoch entsprach nicht den Wünschen des Kunden.

Er befürchtete, die Videothek könne aufgrund der über einen längeren Zeitraum ausgeliehenen Videofilme ein teilweises Persönlichkeitsprofil erstellen, und sah die Gefahr, dass die Daten in falsche Hände gerieten, eine Befürchtung, die im Hinblick auf das recht „spezielle“ Angebot mancher Videothek nicht völlig aus der Luft gegriffen ist.

Wegen fehlender Angaben konnte ich nicht beurteilen, ob die Hard- und Software der Videothek eine Datenlöschung nicht zuließen. Ich habe dem Petenten jedoch mitgeteilt, dass gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG die Speicherung und Nutzung der Daten nur im Rahmen der Zweckbestimmung des Vertrags oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen zulässig sind. Die Daten müssen gemäß § 35 Abs. 2 Nr. 3 BDSG gelöscht werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, es sei denn, einer der Ausnahmetatbestände des Abs. 3 greift ein.

Nach meiner Auffassung ist die Speicherung von Angaben über die ausgeliehenen Videofilme nur bis zu ihrer Rückgabe erforderlich. Soweit Kunden an einer längerfristigen Speicherung interessiert sind, müssen sie darin einwilligen.

Anlagen Materialien zum Datenschutz

Anlage 1

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 – **Beratungen zum StVÄG 1996**

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Entwicklung, im Gesetzgebungsverfahren zu einem Strafverfahrensänderungsgesetz 1996, die Gewährleistung der informationellen Selbstbestimmung im Strafverfahren nicht nur nicht zu verbessern, sondern vielmehr bestehende Rechte sogar noch zu beschränken. Dies gilt insbesondere für den Beschluß des Bundesrates, der gravierende datenschutzrechtliche Verschlechterungen vorsieht.

Bereits der Gesetzentwurf der Bundesregierung wird in Teilbereichen den Vorgaben des Bundesverfassungsgerichts nicht gerecht und fällt teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z. B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück.

Kritik erheben die Datenschutzbeauftragten des Bundes und der Länder insbesondere an folgenden Punkten:

- Die Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung sind nicht hinreichend bestimmt. So wird z. B. nicht angemessen zwischen Beschuldigten und Zeugen differenziert.
- Für Privatpersonen und Stellen, die nicht Verfahrensbeteiligte sind, wird als Voraussetzung zur Auskunfts- und Akteneinsicht lediglich ein vages „berechtigtes“ statt eines rechtlichen Interesses gefordert.
- Die Regelungen über Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten bei Staatsanwaltschaften sind unzureichend. Das hat zur Folge, dass nahezu unbeschränkt Zentraldateien oder gemeinsame Dateien eingerichtet und Daten ohne Berücksichtigung der Begehungsweise und Schwere von Straftaten gespeichert werden können. Die Zugriffsmöglichkeiten der Strafverfolgungs- und Strafjustizbehörden auf diese Daten gehen zu weit. Darüber hinaus werden Standardmaßnahmen des technischen und organisatorischen Datenschutzes (z. B. Protokollierung, interne Zugriffsbeschränkungen etc.) weitgehend abgeschwächt.

Die Bedenken und Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder fanden in den ersten Beratungen des Bundesrates zum Gesetzentwurf nahezu keinen Niederschlag.

Darüber hinaus hat der Bundesrat in seiner Stellungnahme weitergehende datenschutzrechtliche Verschlechterungen beschlossen, die vor allem die Entfernung mehrerer im Gesetzentwurf noch vorhandener Beschränkungen und verfahrensrechtlicher Sicherungen zum Schutz des Persönlichkeitsrechts und des Rechtes auf informationelle Selbstbestimmung der Betroffenen zum Inhalt haben.

Beispiele hierfür sind:

- Der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation soll gestrichen werden.
- Die Verwendungsbeschränkungen bei Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht gewonnen wurden, sollen herausgenommen werden.
- Das Auskunfts- und Akteneinsichtsrecht auch für öffentliche Stellen soll erheblich erweitert werden.

- Detaillierte Regelungen für Fälle, in denen personenbezogene Daten von Amts wegen durch Strafverfolgungs- und Strafjustizbehörden an andere Stellen übermittelt werden dürfen, die im weitesten Sinne mit der Strafrechtspflege zu tun haben, sollen gestrichen werden.
- Das Verbot soll gestrichen werden, über die Grunddaten hinausgehende weitere Angaben nach Freispruch, endgültiger Verfahrenseinstellung oder unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens Daten in Dateien zu speichern.
- Speicherungs- und Löschungsfristen für personenbezogene Daten in Dateien sollen ersatzlos gestrichen werden.
- Kontrollverfahren für automatisierte Abrufverfahren sollen aufgehoben werden und die Verwendungsbeschränkungen für Protokolldaten sollen entfallen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Deutschen Bundestag auf, bei den anstehenden weiteren Beratungen des Gesetzentwurfes die vom Bundesrat empfohlenen datenschutzrechtlichen Verschlechterungen nicht zu übernehmen und die noch bestehenden datenschutzrechtlichen Mängel zu beseitigen.

Hingegen sollten Vorschläge des Bundesrates für Regelungen für den Einsatz von Lichtbildvorlagen und für die Datenverarbeitung zur Durchführung des Täter-Opfer-Ausgleichs aufgegriffen werden.

Anlage 2

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 – **Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke**

Immer häufiger wird bei der Verfolgung von Straftaten am Tatort oder beim Opfer festgestelltes, sog. biologisches Material als Spurenmaterial durch die Polizei sichergestellt, mittels DNA-Analyse untersucht und mit anderen DNA-Materialien verglichen. Die DNA-Analyse ist zur Standardmethode geworden, um die Herkunft von Spurenmaterial von bestimmten bekannten Personen (Verdächtigen, Opfern, unbeteiligten Dritten) oder die Identität mit anderem Spurenmaterial unbekannter Personen feststellen zu können.

Der Gesetzgeber hat zwar vor kurzem im Strafverfahrensänderungsgesetz -DNA-Analyse ("Genetischer Fingerabdruck")- die Voraussetzungen und Grenzen genetischer Untersuchungen im Strafverfahren geregelt. Eine Festlegung, ob und in welchen Grenzen die Speicherung und Nutzung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken zulässig ist, enthält dieses Gesetz jedoch nicht.

Bezüglich des Aussagegehalts der gespeicherten Daten der Analyseergebnisse ist ein grundsätzlich neuer Aspekt zu berücksichtigen:

Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen derzeit tatsächlich zwar keine über die Identifizierung hinausgehenden Aussagen zur jeweiligen Person oder deren Erbgut. In Einzelfällen können die analysierten nicht codierenden persönlichkeitsneutralen DNA-Merkmale jedoch mit codierenden Merkmalen korrespondieren. In Anbetracht der weltweiten intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, dass künftig auch auf der Basis der Untersuchung von bisher als nicht codierend angesehenen Merkmalen konkrete Aussagen über genetische Dispositionen der betroffenen Personen mit inhaltlichem Informationswert getroffen werden können. Dieses Risiko ist deshalb nicht zu vernachlässigen, weil gegenwärtig weltweit mit erheblichem Aufwand die Entschlüsselung des gesamten menschlichen Genoms vorangetrieben wird.

Dieser Gefährdung kann dadurch begegnet werden, daß bei Bekanntwerden von Überschussinformationen durch die bisherigen Untersuchungsmethoden andere Untersuchungmethoden (Analyse eines anderen Genomabschnitts) verwendet werden, die keine Informationen über die genetische Disposition liefern. Derartige Ausweichstrategien können jedoch zur Folge haben, dass die mit anderen Methoden erlangten Untersuchungsergebnisse nicht mit bereits vorliegenden vergleichbar sind. Datenspeicherungen über verformelte Untersuchungsergebnisse könnten daher dazu führen, dass einmal verwendete Untersuchungsformen im Interesse der Vergleichbarkeit beibehalten werden, obwohl sie sich als problematisch herausgestellt haben und unproblematische Alternativen zur Verfügung stehen, z. B. durch Verschlüsselung problematischer Informationen.

In Anbetracht dieser Situation und angesichts der Tendenz, mittels der DNA-Analyse gewonnene Daten nicht nur in einem bestimmten Strafverfahren zu verwenden, sondern diese Daten in abrufbaren Datenbanken auch für andere Strafverfahren zugänglich zu machen, fordern die Datenschutzbeauftragten des Bundes und der Länder ergänzend zu §§ 81 e und f StPO für die automatisierte Speicherung und Nutzung von DNA-Identitätsdaten eine spezielle gesetzliche Regelung in der Strafprozessordnung, um das Persönlichkeitsrecht der Betroffenen zu schützen:

1. Es muss ein grundsätzliches Verbot der Verformelung und Speicherung solcher Analyseergebnisse statuiert werden, die inhaltliche Aussagen über Erbanlagen ermöglichen.

Im Hinblick auf die nicht auszuschließende Möglichkeit künftiger Rückschlüsse auf genetische Dispositionen ist bereits jetzt ein striktes Nutzungsverbot für persönlichkeitsrelevante Erkenntnisse zu statuieren, die aus den gespeicherten Verformelungen der DNA resultieren.

2. Wenn zum Zweck des Abgleichs mit Daten aus anderen Verfahren (also zu erkennungsdienstlichen Zwecken) DNA-Informationen automatisiert gespeichert werden sollen (DNA-Datenbank mit der Funktion, die bei Fingerabdrücken die AFIS-Datenbank des BKA besitzt), müssen darüber hinaus folgende Regelungen geschaffen werden:

   – Nicht jede DNA-Analyse, die zum Zweck der Aufklärung einer konkreten Straftat erfolgt ist, darf in diese Datei aufgenommen werden. Die Speicherung von Verformelungen der DNA-Struktur in eine Datenbank darf nur dann erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte künftig strafrechtlich in Erscheinung treten wird und dass die Speicherung aufgrund einer Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafverfolgung fördern kann.

   – Eine Speicherung kommt insbesondere dann nicht in Betracht, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt wurde. Bereits erfolgte Speicherungen sind zu löschen. Gleiches gilt für den Fall, dass die Anordnung der DNA-Untersuchung oder die Art und Weise ihrer Durchführung unzulässig war.

   – Die Aufbewahrungsdauer von Verformelungen der DNA-Struktur ist konkret festzulegen (z. B. gestaffelt nach der Schwere des Tatvorwurfs).

3. Voraussetzung für Gen-Analysen muss in jedem Fall mindestens die richterliche Anordnung sein, unabhängig davon, ob die Daten in einem anhängigen Strafverfahren zum Zweck der Straftatenaufklärung, wie in § 81 f Absatz 1 Satz 1 StPO normiert, oder ob sie zum Zweck der künftigen Strafverfolgung (also zu Zwecken des Erkennungsdienstes) benötigt werden.

4. Ein DNA-Screening von Personengruppen, deren Zusammensetzung nach abstrakt festgelegten Kriterien ohne konkreten Tatverdacht gegenüber Einzelnen erfolgt, führt im Regelfall zur Erhebung von DNA-Daten zahlreicher völlig unbeteiligter und unschuldiger Bürger. Die Daten dieser Personen sind unmittelbar dann zu löschen, wenn sie für das Anlassstrafverfahren nicht mehr erforderlich sind. Sie dürfen nicht in verfahrensübergreifenden DNA-Dateien gespeichert werden und auch nicht mit solchen Datenbeständen abgeglichen werden.

Anlage 3

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 – **Geplante Verpflichtung von Telediensteanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln**

Der Entwurf der Bundesregierung für ein Teledienstedatenschutzgesetz (Artikel 2 (§ 5 Absatz 3) des Informations- und Kommunikationsdienste-Gesetzes vom 20.12.1996 - BR-Drs. 966/96) sieht vor, dass die Anbieter von Telediensten (z. B. Home-Banking, Home-Shopping) dazu verpflichtet werden sollen, insbesondere der Polizei und den Nachrichtendiensten Auskunft über Daten zur Begründung, inhaltlichen Ausgestaltung oder Änderung der Vertragsverhältnisse mit ihren Kunden (sog. Bestandsdaten) zu erteilen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Aufnahme einer solchen Übermittlungsvorschrift in das Teledienstedatenschutzgesetz des Bundes. Eine Folge dieser Vorschrift wäre, dass Anbieter von elektronischen Informationsdiensten (z. B. Diskussionsforen) offenlegen müssten, welche ihrer Kunden welche Dienste z. B. mit einer bestimmten politischen Tendenz in Anspruch nehmen. Darin läge ein massiver Eingriff nicht nur in das Recht auf informationelle Selbstbestimmung, sondern auch in die Informations- und Meinungsfreiheit des Einzelnen. Das geltende Recht, insbesondere die Strafprozeßordnung und das Polizeirecht enthalten hinreichende Möglichkeiten, um strafbaren und gefährlichen Handlungen auch im Bereich der Teledienste zu begegnen. Über die bisherige Rechtslage hinaus würde bei Verabschiedung der geplanten Regelung zudem den Nachrichtendiensten ein nichtöffentlicher Datenbestand offenstehen. In keinem anderen Wirtschaftsbereich sind vergleichbare Übermittlungspflichten der Anbieter von Gütern und Dienstleistungen hinsichtlich ihrer Kunden bekannt.

Mit guten Gründen haben deshalb die Länder davon abgesehen, in den inzwischen von den Ministerpräsidenten unterzeichneten Staatsvertrag über Mediendienste eine vergleichbare Vorschrift aufzunehmen. In der Praxis werden sich aber für Bürger und Online-Dienstanbieter schwierige Fragen der Abgrenzung zwischen den Geltungsbereichen des Mediendienste-Staatsvertrags und des Teledienstedatenschutzgesetzes ergeben. Auch aus diesem Grund halten die Datenschutzbeauftragten eine Streichung der Vorschrift des § 5 Absatz 3 aus dem Entwurf für ein Teledienstedatenschutzgesetz für geboten.

Anlage 4

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 – **Achtung der Menschenrechte in der Europäischen Union**

Die DSB-Konferenz ist gemeinsam der Überzeugung, daß hinsichtlich nicht Verdächtiger und hinsichtlich nicht kriminalitätsbezogener Daten die Forderung des Europäischen Parlaments vom 17.09.1996 zu den Dateien von Europol unterstützt werden soll.

Das Europäische Parlament hat in seiner Entschließung zur Achtung der Menschenrechte gefordert, „alle Informationen persönlichen Charakters, wie Angaben zur Religionszugehörigkeit, zu philosophischen oder religiösen Überzeugungen, Rasse, Gesundheit und sexuellen Gewohnheiten, von der Erfassung in Datenbanken von EUROPOL auszuschließen."

Anlage 5

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 – **Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen**

Die Datenschutzbeauftragten des Bundes und der Länder halten es für sehr problematisch, dass in Folge technischer und gesellschaftlicher Veränderungen in einer zunehmenden Anzahl von Konstellationen personenbezogene medizinische Patientendaten außerhalb des ärztlichen Bereiches verarbeitet werden. Sie fordern, dass zunehmend die Möglichkeiten einer anonymen oder pseudonymen Datenverarbeitung mit Verschlüsselung genutzt werden. Soweit dennoch Patientendaten personenbezogen weitergegeben werden, ist ein wesentliches Problem, dass außerhalb des ärztlichen Gewahrsams der von der Strafprozeßordnung vorgesehene Schutz personenbezogener Patientendaten vor Inanspruchnahme als Beweismittel durch Zeugeneinvernahme oder Beschlagnahme nicht mehr zweifelsfrei sichergestellt ist bzw. überhaupt nicht existiert.

Die folgenden Beispiele machen dies deutlich:

1. Ärzte bzw. Krankenhäuser haben z. B. keinen Gewahrsam an den personenbezogenen Patientendaten, die der Patient auf einer (freiwilligen) Patientenchipkarte bei sich trägt/besitzt oder die von einer dritten Stelle außerhalb des ärztlichen Bereichs im Auftrag verarbeitet werden, wie z. B. bei Mailbox-Systemen, externer Archivierung oder der Vergabe von Schreibarbeiten an selbständige Schreibbüros.

   Fraglich ist auch die Aufrechterhaltung des ärztlichen Gewahrsams, wenn Hilfspersonal des Arztes oder Krankenhauses Patientendaten in der Privatwohnung bearbeitet.

2. Zunehmend werden einzelne Unternehmensfunktionen bzw. fachliche Aufgaben ausgelagert und einer externen Stelle - in der Regel einem Privatunternehmen - übertragen (sog. Outsourcing), - z. B. bei Einschaltung eines externen Inkassounternehmens, bei externem Catering für stationäre Patienten, bei externer Archivierung oder bei Vergabe von Organisationsanalysen an externe Beratergesellschaften.

3. Medizinische Daten mit Patientenbezug sollen an Forscher oder Forschungsinstitute zu Zwecken wissenschaftlicher Forschung übermittelt werden. Je umfassender und komplizierter der Einsatz automatisierter Datenverarbeitung für Forschungszwecke vorgesehen wird, desto weniger werden die personenbezogenen Patientendaten ausschließlich durch ärztliches Personal verarbeitet. Hier setzt sich vielmehr die Verarbeitung durch Informatiker und Statistiker immer mehr durch. Aber auch bei Verarbeitung durch Ärzte, die in der Forschung tätig sind, ist keineswegs sichergestellt, dass die personenbezogenen Patientendaten diesen Ärzten „in ihrer Eigenschaft als Arzt“ bekannt geworden sind, wie dies durch die Strafprozeßordnung für den Beschlagnahmeschutz als Voraussetzung festgelegt ist.

Die zunehmende Verlagerung personenbezogener Patientendaten aus dem Schutzbereich des Arztgeheimnisses nach außen verstößt nach Ansicht der Datenschutzbeauftragten massiv gegen Interessen der betroffenen Patienten, solange nicht ein gleichwertiger Schutz gewährleistet ist.

Die Datenschutzbeauftragten des Bundes und der Länder bitten daher den Bundesgesetzgeber - unabhängig von weiteren Fragen des Datenschutzes, die mit der Verarbeitung medizinischer Daten im Rahmen der Telemedizin verbunden sein können - für die sich zunehmend entwickelnden modernen Formen der Auslagerung medizinischer Patientendaten sowie für die Weitergabe medizinischer Patientendaten für Zwecke wissenschaftlicher medizinischer Forschung einen dem Arztgeheimnis entsprechenden Schutz der Patientendaten zu schaffen.

Anlage 6

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 20. Oktober 1997 zu den Vorschlägen der Arbeitsgruppe des ASMK **„Verbesserter Datenaustausch bei Sozialleistungen“**

Mit dem von der ASMK-Arbeitsgruppe vorgeschlagenen erweiterten Datenaustausch bei Sozialleistungen wird die Bekämpfung von Leistungsmissbräuchen angestrebt. Soweit dieses Ziel der Arbeitsgruppe mit einer Veränderung der Strukturen der Verarbeitung personenbezogener Daten im Sozialleistungsbereich – insbesondere mit veränderten Verfahren der Datenerhebung – erreicht werden soll, muss der verfassungsrechtlich gewährleistete Grundsatz der Verhältnismäßigkeit beachtet werden.

Die gegenwärtigen Regelungen der Datenerhebung im Sozialleistungsbereich sehen unterschiedliche Verfahren der Datenerhebung vor, vor allem

– Datenerhebungen beim Betroffenen selbst

– Datenerhebungen bei Dritten mit Mitwirkung des Betroffenen

– Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen aus konkretem Anlass

– Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen ohne konkreten Anlass (Stichproben / Datenabgleich).

Diese Verfahren der Datenerhebung sind mit jeweils unterschiedlich schwerwiegenden Eingriffen in das Persönlichkeitsrecht der Betroffenen verbunden. So weiß z. B. bei einer Datenerhebung beim Betroffenen dieser, wer wann welche Daten zu welchem Zweck über ihn erhebt, und Dritte erhalten keine Kenntnis von diesen Datenerhebungen. Im Gegensatz dazu wird bei einer Datenerhebung bei Dritten ohne Mitwirkung des Betroffenen dieser darüber im Unklaren gelassen, wer wann welche Daten zu welchem Zweck über ihn erhebt, und Dritten werden Daten über den Betroffenen zur Kenntnis gegeben (z. B. der Bank die Tatsache, dass der Betroffene Sozialhilfeempfänger ist).

Dieses System der Differenzierung des Verfahrens der Datenerhebung entspricht dem Grundsatz der Verhältnismäßigkeit. Ferner ist zu differenzieren, ob Daten aus dem Bereich der Sozialleistungsträger oder Daten außerhalb dieses Bereichs erhoben werden.

In dem Bericht der Arbeitsgruppe wird dieses System zum Teil aufgegeben. Es werden Verfahren zur Datenerhebung vorgesehen, die schwerwiegend in die Rechte der Betroffenen eingreifen, ohne dass hinreichend geprüft und dargelegt wird, ob minder schwere Eingriffe in das Persönlichkeitsrecht zum Erfolg führen können. Die Datenschutzbeauftragten wenden sich nicht um jeden Preis gegen Erweiterungen des Datenaustauschs, gehen aber davon aus, dass pauschale und undifferenzierte Änderungen des gegenwärtigen Systems unterbleiben.

Datenabgleichsverfahren sollen nur in Frage kommen bei Anhaltspunkten für Missbrauchsfälle in nennenswertem Umfang. Deshalb müssen etwaige neue Datenabgleichsverfahren hinsichtlich ihrer Wirkungen bewertet werden. Daher ist parallel zu ihrer Einführung die Implementierung einer Erfolgskontrolle für das jeweilige Abgleichsverfahren vorzusehen, die auch präventive Wirkungen erfasst. Dies ermöglicht, Aufwand und Nutzen zueinander in das verfassungsmäßig gebotene Verhältnis zu setzen.

Soweit unter Beachtung dieser Prinzipien neue Kontrollinstrumente gegen den Leistungsmissbrauch tatsächlich erforderlich sind, muss für den Bürger die Transparenz der Datenflüsse sichergestellt werden. Diese Transparenz soll gewährleisten, dass der Bürger nicht zum bloßen Objekt von Datenerhebungen wird.

Bezug nehmend auf die bisherigen Äußerungen des BfD und von LfD bestehen gegen folgende Vorschläge im Bericht gravierende Bedenken:

1. Mitwirkung bei der Ahndung des Missbrauchs (für alle Leistungsträger) und Verbesserungen für die Leistungsempfänger (zu D.II.10.1 und B.I) (S. 30 u. S. 2)

   Die vorgeschlagenen Möglichkeiten von anlassunabhängigen Missbrauchskontrollen beinhalten keine Klarstellung der gegebenen Rechtslage, sondern stellen erhebliche Änderungen des bisherigen abgestuften Systems der Datenerhebung dar.

   Die mit der Datenerhebung verbundene Offenlegung des Kontaktes bzw. einer Leistungsbeziehung zu einem Sozialleistungsträger stellt einen erheblichen Eingriff für den Betroffenen dar, u. a. da sie geeignet ist, seine Stellung in der Öffentlichkeit, z. B. seine Kreditwürdigkeit, wesentlich zu beeinträchtigen. Anfragen bei Dritten ohne Kenntnis des Betroffenen lassen diesen im Unklaren, welche Daten wann an wen übermittelt wurden.

   Derartige Datenerhebungen werden vom geltenden Recht deshalb mit Rücksicht auf das verfassungsrechtliche Verhältnismäßigkeitsprinzip nur in begrenzten und konkretisierten Ausnahmefällen zugelassen. Von dieser verfassungsrechtlich gebotenen Systematik würde die vorgeschlagene Neuregelung grundlegend abweichen. Die Datenschutzbeauftragten betonen bei dieser Gelegenheit den allgemeinen Grundsatz, dass Datenerhebungen, die sowohl pauschal und undifferenziert sind, als auch ohne Anlass erfolgen, abzulehnen sind.

   Die Datenschutzbeauftragten weisen schließlich darauf hin, dass gegen eine Ausnutzung der technischen Datenverarbeitungsmöglichkeiten zugunsten des Betroffenen (B.I des Berichts) nichts spricht, solange die Betroffenen davon informiert sind und soweit sie dem Verfahren zugestimmt haben.

2. Nachfrage beim Wohnsitzfinanzamt des Hilfesuchenden und Schenkungen und Erbschaften (zu D.I.1.1) (S. 6)

   Die Datenschutzbeauftragten teilen nicht die Auffassung, dass Stichproben nach der geltenden Rechtslage zu § 21 Abs. 4 SGB X möglich sind. § 21 Abs. 4 SGB X ist eine Auskunftsvorschrift für die Finanzbehörden, die über die Datenerhebungsbefugnis der Sozialleistungsträger nichts aussagt. Die Leistungsträger dürfen diese Auskünfte bei den Finanzbehörden als Dritten nur nach Maßgabe des § 67 a SGB X einholen, soweit das erforderlich ist: Diese Erforderlichkeit setzt Anhaltspunkte für Leistungsmissbrauch im Einzelfall voraus.

3. Auskunftspflicht der Banken und Lebensversicherungen (zu D.II.1.6) (S.13)

   Die Datenerhebung im Sozialbereich ist von einer möglichst weitgehenden Einbeziehung des Betroffenen gekennzeichnet. Der Vorschlag zur Einführung einer Auskunftspflicht geht auf dieses differenzierte System der Datenerhebungen im Sozialbereich überhaupt nicht ein.

   Die Annahme in der Begründung des Vorschlags, ohne eine derartige Auskunftspflicht bestünden keine sachgerechten Ermittlungsmöglichkeiten, trifft nicht zu. Der Betroffene ist verpflichtet, Nachweise zu erbringen; dazu können auch Bankauskünfte gehören. Allerdings ist dem Betroffenen vorrangig Gelegenheit zu geben, solche Auskünfte selbst und ohne Angabe ihres Verwendungszwecks beizubringen. Nur soweit dennoch erforderlich, ist der Betroffene im Rahmen seiner Mitwirkungspflicht gehalten, sein Einverständnis in die Erteilung von Bankauskünften zu geben. Die vorgeschlagene pauschale Auskunftsverpflichtung birgt deshalb die Gefahr in sich, dass dann generell ohne Mitwirkung des Betroffenen und ohne sein Einverständnis sofort an die Bank/Lebensversicherung herangetreten wird mit der Wirkung, dass der Betroffene desavouiert wird.

   Die Datenschutzbeauftragten halten deshalb eine Klarstellung für dringend erforderlich, dass derartige unmittelbare Anfragen und Auskünfte erst in Betracht kommen, wenn die Ermittlungen unter Mitwirkung des Betroffenen zu keinem ausreichenden

Ergebnis führen und Anhaltspunkte dafür bestehen, dass bei der fraglichen Bank/Lebensversicherung nicht angegebenes Vermögen vorhanden ist.

4. Akzeptanz des Datenaustausches (zu E.IV) (S. 36)

   Datenabgleiche beinhalten eine Verarbeitung personenbezogener Daten, die nicht beliebig durchgeführt werden darf und anerkanntermaßen einer gesetzlichen Grundlage bedarf. Die im Papier der Arbeitsgruppe unter E.IV vertretene These, dass anlassunabhängige Datenabgleiche keiner speziellen gesetzlichen Grundlage bedürften, trifft deshalb nicht zu.

   Die Datenschutzbeauftragten wenden sich nicht gegen einzelne Veränderungen der Datenverarbeitung im Sozialleistungsbereich, soweit sie tatsächlich erforderlich und verhältnismäßig sind und die zuvor aufgezeigten Grundsätze beachtet werden. Die Datenschutzbeauftragten sind dazu gesprächsbereit.

Anlage 7

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 – **Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts**

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Oktober 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.

Noch immer gibt es keinen Kabinettsbeschluss; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

– Verbesserungen des Datenschutzes der Bürger, z. B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;

– dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

Zur Harmonisierung des europäischen Datenschutzrechts empfehlen die Datenschutzbeauftragten der Bundesregierung und dem Gesetzgeber folgende Grundsatzentscheidungen:

– weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlassunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;

– Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;

– Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG, z. B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;

– Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen, die der EU-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen;

– Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Als ebenso vordringlich betrachten die Datenschutzbeauftragten eine Anpassung der noch von der Großrechnertechnologie der siebziger Jahre bestimmten gesetzlichen Regelungen an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft. Dazu gehören insbesondere folgende Punkte:

– Verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystemen und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;

- mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutzaudits;
- Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Video-Überwachung;
- Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren;
- Einführung einer Vorabkontrolle für besonders risikoreiche Datenverarbeitung, namentlich bei Verarbeitung sensitiver Daten;
- Regelungen für Chipkarten-Anwendungen;
- Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing, unter anderem auch mindestens durch die Festlegung von Hinweispflichten hinsichtlich der Möglichkeit des Widerspruchs; vorzuziehen ist in jedem Fall eine Einwilligungsregelung;
- –- Verstärkung des Schutzes gegenüber der Einholung von Selbstauskünften vor Abschluß von Miet-, Arbeits- und ähnlich existenzwichtigen Verträgen;
- Datenexport nach Inlandsgrundsätzen nur bei angemessenem Schutzniveau im Empfängerstaat; Festlegung, unter welchen Voraussetzungen ein Mitgliedstaat Daten, die er im Anwendungsbereich der Richtlinie (also nach Inlandsgrundsätzen) erhalten hat, außerhalb ihres Anwendungsbereichs verwenden darf;
- möglichst weitgehende Ersetzung der Anmeldung von Dateien bei der Aufsichtsbehörde durch Bestellung weisungsfreier Datenschutzbeauftragter; Beibehaltung des internen Datenschutzbeauftragten auch bei Sicherheitsbehörden;
- Stärkung der Kontrollrechte des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz durch uneingeschränkte Kontrollbefugnis bei der Verarbeitung personenbezogener Daten in Akten einschließlich solcher über Sicherheitsüberprüfungen.

Die Konferenz weist ferner auf die Rechtspflicht der Länder hin, ihr Datenschutzrecht ebenfalls der EU-Richtlinie fristgerecht anzupassen.

Anlage 8

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 – **Informationelle Selbstbestimmung bei Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren**

Überlegungen des Gesetzgebers und eine beginnende öffentliche Diskussion, moderne Dokumentationstechnik der Wahrheitsfindung und dem Zeugenschutz in gerichtlichen Verfahren nutzbar zu machen, liegen auch im Interesse des Datenschutzes. Dabei ist allerdings zu beachten, dass Bild-Ton-Aufzeichnungen von Vernehmungen im Strafverfahren einen erheblichen Eingriff in das Persönlichkeitsrecht darstellen. Sie spiegeln die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend wider. Zweck und Erforderlichkeit dieses Eingriffs bedürfen einer sorgfältigen Begründung durch den Gesetzgeber. Sie bildet den Maßstab, der über Möglichkeiten, Grenzen und Verfahren der Videotechnologie im Strafprozess entscheidet. Erkennbar und nachvollziehbar sollte sein, dass der Gesetzgeber die Risiken des Einsatzes dieser Technologie, insbesondere die Verfügbarkeit der Aufzeichnungen nach den allgemeinen Vorschriften über die Beweisaufnahme bedacht und bewertet hat. Ferner sollte erkennbar und nachvollziehbar sein, dass Alternativen zur Videotechnologie, namentlich die Verwendung von Tonaufzeichnungen, in die Erwägungen des Gesetzgebers aufgenommen wurden.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sollten die vorliegenden Gesetzentwürfe des Bundesrates (BT-Drs. 13/4983 vom 19.06.1996) sowie der Fraktionen der CDU/CSU und F.D.P. (BT-Drs. 13/7165 vom 11.03.1997) in einem umfassenderen Bedeutungs- und Funktionszusammenhang diskutiert werden. Zunehmend tritt das Anliegen der Praxis hervor, Bild-Ton-Aufzeichnungen auch mit anderer Zielsetzung zu verwerten:

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einmalige Vernehmung, die möglichst zeitnah zum Tatgeschehen durchgeführt und aufgezeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten („Vermeidung kognitiver Dissonanzen“). Ausgehend von diesen Überlegungen, hat der Gesetzgeber unter Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Videotechnologie sogar überlegen ist.

Für Videoaufzeichnungen des Betroffenen, die zu seinem Schutz gefertigt werden sollen, ist dessen Einwilligung unverzichtbare Voraussetzung für die Zulässigkeit einer Bild-Ton-Aufzeichnung im Strafverfahren. Sofern der Betroffene nicht in der Lage ist, die Bedeutung und Tragweite einer Bild-Ton-Aufzeichnung und ihrer Verwendungsmöglichkeiten hinreichend zu beurteilen, hat der Gesetzgeber festzulegen, wer anstelle des Betroffenen die Einwilligung erteilen darf. Vor Abgabe der Einwilligungserklärung ist der Betroffene umfassend aufzuklären, insbesondere auch über alle zulässigen Arten der weiteren Verwertung und über die Möglichkeit des Widerrufs der Einwilligung für die Zukunft. Die Aufklärung ist zuverlässig zu dokumentieren. Entsprechendes gilt für die Herausgabe von Videoaufzeichnungen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts bei Verwendung von Bild-Ton-Aufzeichnungen im Strafverfahren. Unabhängig von der Frage, welche Zielsetzung mit Bild-Ton-Aufzeichnungen im Strafverfahren verfolgt werden soll, sind hierbei insbesondere folgende Gesichtspunkte von Bedeutung:

1. Es ist sicherzustellen, daß der Eindruck des Aussagegeschehens z. B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild und Zoom nicht gezielt verfremdet oder verzerrt wird.
2. Einsatz und Verwertung von Bild-Ton-Aufzeichnungen sind so zu regeln, dass gesetzliche Zeugnisverweigerungsrechte gewahrt bleiben. Insbesondere ist eine weitere Nutzung der Aufnahme, auch zum Zwecke des Vorhalts, ausgeschlossen, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft.
3. Vorbehaltlich des o. g. Einwilligungserfordernisses darf eine Übermittlung von Videoaufzeichnungen an Stellen außerhalb der Justiz, wenn überhaupt, nur in Ausnahmefällen erlaubt sein, da nur so ein wirksamer Schutz vor Missbrauch, etwa durch kommerzielle Verwertung, gewährleistet werden kann. Soweit der Gesetzgeber aus Gründen eines fairen, rechtsstaatlichen Strafverfahrens die Weitergabe von Videokopien an Verfahrensbeteiligte zulässt, müssen jedenfalls wirksame Vorkehrungen gegen Missbrauch gewährleistet sein, z. B. sichtbare Signierung und strafbewehrte Regelungen über Zweckbindungen und Löschungsfristen.
4. Eine Verwertung der Aufzeichnungen im Rahmen eines anderen Strafverfahrens ist nur zulässig, soweit sie auch für die Zwecke dieses anderen Verfahrens hätten angefertigt werden dürfen.
5. Soweit eine Verwertung in einem anderen gerichtlichen Verfahren - etwa zur Vermeidung erneuter Anhörung kindlicher Zeugen vor dem Familien- oder Vormundschaftsgericht - zugelassen werden sollte, sind in entsprechenden Ausnahmeregelungen präzise Voraussetzungen hierfür abschließend zu bestimmen und enge Verwendungsregelungen zu treffen.
6. Spätestens mit dem rechtskräftigen Abschluß des Strafverfahrens sind grundsätzlich die Aufzeichnungen unter Aufsicht der Staatsanwaltschaft zu vernichten. Der Betroffene ist davon zu benachrichtigen. Soweit der Gesetzgeber ausnahmsweise zur Wahrung vorrangiger Rechtsgüter eine längere Aufbewahrung der Aufzeichnungen zulässt, müssen Voraussetzungen, Umfang und Fristen der weiteren Aufbewahrung klar und eng geregelt werden.

Anlage 9

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 – **Erforderlichkeit datenschutzfreundlicher Technologien**

Moderne Informations- und Telekommunikationstechnik (IuK-Technik) gewinnt in allen Lebensbereichen zunehmende Bedeutung. Die Nutzer wenden diese Technik z. B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des Einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z. B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der IuK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie lässt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflusst wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptographische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne dass die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff „Privacy enhancing technology (PET)“ eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfasst, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, dass er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, dass sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit lässt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, dass die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm „Forschung und Entwicklung“ aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von IuK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

Anlage 10

Entschließung der 55.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20.März 1998 – **Datenschutz beim digitalenFernsehen**

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

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

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

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

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

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

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

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

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

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

Anlage 11

Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20.März 1998 – **Datenschutzprobleme der Geldkarte**

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

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

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

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

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

Anlage 12

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 – **Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten**

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

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

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

Anlage 13

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 – **Fehlenden bereichsspezifische Regelungen bei der Justiz**

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

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

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

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

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

- weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien

  namentlich die

  - Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen,
  - Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in Bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden.
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;
- Datenübermittlung zu wissenschaftlichen Zwecken;
- Datenverarbeitung in der Zwangsvollstreckung;
- Datenverarbeitung im Jugendstrafvollzug;
- Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeiten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muss vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Da-

tenerhebung und –verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitung Privaten übertragen werden dürfen.

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

– Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung

– Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte

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

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

Anlage 14

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 – **Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge**

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

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

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

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

Anlage 15

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober1998 – **Weitergabe von Meldedaten an Adressbuchverlage und Parteien**

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

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

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

Anlage 16

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 – **Entwicklungen im Sicherheitsbereich**

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

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

Anlage 17

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 – **Dringlichkeit der Datenschutzmodernisierung**

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

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.
- Die anlassfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muss in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.
- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.
- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.
- Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.