# Unterrichtung

Landesbeauftragter für den Datenschutz
Niedersachsen

Hannover, den 30. 12. 1994

An den
Herrn Präsidenten des Niedersächsischen Landtages

Hannover

Betr.: **Zwölfter 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 XII. Tätigkeitsbericht für die Kalenderjahre 1993 und 1994.

Mit vorzüglicher Hochachtung

Dr. Dronsch

# Inhaltsverzeichnis

**Abkürzungen**

| | |
|---|---|
| Abb. | Abbildung |
| Abs. | Absatz |
| ADV | Automatisierte Datenverarbeitung |
| a.F. | alte Fassung |
| AG | Aktiengesellschaft |
| Alt. | Alternative |
| ANIS | Analoganschluß |
| AOK | Allgemeine Ortskrankenkasse |
| AO | Abgabenordnung |
| APC | Arbeitsplatzcomputer |
| APIS | Arbeitsdatei PIOS Innere Sicherheit (PIOS = Personen, Institutionen, Objekte, Sachen) |
| Aufl. | Auflage |
| Art. | Artikel |
| AsylVfG | Asylverfahrensgesetz |
| AuslDÜV | Verordnung über Datenübermittlungen an die Ausländerbehörden |
| AuslG | Ausländergesetz |
| AUT | anonymous unlinked testing |
| AV | Allgemeine Verfügung |
| Az. | Aktenzeichen |
| AZR | Ausländerzentralregister |
| BAFl | Bundesamt für die Anerkennung von Flüchtlingen |
| BBG | Bundesbeamtengesetz |
| BDSG | Bundesdatenschutzgesetz |
| BfD | Bundesbeauftragter für den Datenschutz |
| BGB | Bürgerliches Gesetzbuch |
| BGBl. | Bundesgesetzblatt |
| BGH | Bundesgerichtshof |
| BGS | Bundesgrenzschutz |
| BKA(G) | (Gesetz über das) Bundeskriminalamt |
| BKK | Betriebskrankenkasse |
| BND | Bundesnachrichtendienst |
| BOS | Behörden und Organisationen mit Sicherheitsaufgaben |
| BÜRO-MIN | Bürokommunikation der Ministerien |
| BR-Drs. | Bundesratsdrucksache |
| BRRG | Beamtenrechtsrahmengesetz |
| BSHG | Bundessozialhilfegesetz |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BStatG | Bundesstatistikgesetz |
| BStU | Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes |
| BT-Drs. | Bundestagsdrucksache |
| Btx-StV | Bildschirmtext-Staatsvertrag |
| BVerfG(E) | Bundesverfassungsgericht (Entscheidungssammlung) |
| BVerfGG | Bundesverfassungsgerichtsgesetz |
| bzw. | beziehungsweise |
| ca. | circa |
| CD-ROM | Compact Disc Read Only Memory |
| CR | Computer und Recht |
| DAMAS-KUS | Datei zur Massenauswertung von Kfz-Kennzeichen und sonstigen Daten |
| DBP | Deutsche Bundespost |
| DES | Data Encryption Standard |
| DÖV | Die Öffentliche Verwaltung |
| (MS-) DOS | (ADV-Betriebssystem für Personal Computer) |
| DSG-EKD | Kirchengesetz über den Datenschutz der Evangelischen Kirchen in Deutschland |
| DSV | Datenschutz-Verordnung |
| DV | Datenverarbeitung |
| DVBl. | Deutsches Verwaltungsblatt |
| EC | Eurocheque |
| ED | Erkennungsdienst |
| EDV | Elektronische Datenverarbeitung |
| EG | Europäische Gemeinschaften |
| EIS | Europäisches Informationssystem |
| elvis | Elektronisches Verwaltungs- und Informationssystem |
| EU | Europäische Union |
| FAG | Fernmeldeanlagengesetz |
| FAZ | Frankfurter Allgemeine Zeitung |

| | |
|---|---|
| f(f). | und folgende Seite(n) |
| FGG | Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit |
| FIN | Fahrzeug-Identifizierungsnummer |
| GDG | Gesundheitsdienstgesetz |
| gem. | gemäß |
| Gem. RdErl. | Gemeinsamer Runderlaß |
| GEZ | Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten |
| GG | Grundgesetz |
| ggf. | gegebenenfalls |
| GmbH | Gesellschaft mit beschränkter Haftung |
| GewO | Gewerbeordnung |
| GwG | Geldwäschegesetz |
| HKG | Kammergesetz für die Heilberufe |
| ICD | International Classification of Disease |
| i.d.F. | in der Fassung |
| IHK-G | Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern |
| IMA-IuK | Interministerieller Arbeitskreis Informations- und Kommunikationstechnik |
| INPOL | (bundesweites) Informationssystem der Polizei |
| InVeKos | Integriertes Verwaltungs- und Kontrollsystem |
| ISDN | Integrated Services Digital Network |
| IuK- | Informations- und Kommunikations- |
| IuK-Reg | Pilotprojekt für den Einsatz von IuK-Technik bei den Bezirksregierungen |
| i.V.m. | in Verbindung mit |
| JGG | Jugendgerichtsgesetz |
| JVA | Justizvollzugsanstalt |
| KBA | Kraftfahrtbundesamt |
| Kap. | Kapitel |
| KDO | Anordnung über den kirchlichen Datenschutz |
| Kfz | Kraftfahrzeug |
| KJHG | Kinder- und Jugenhilfegesetz (SGB VIII) |
| KOMNET | Kommunikationsnetz der Niedersächsischen Landesregierung |
| KVN | Kassenärztliche Vereinigung Niedersachsen |
| LAN | Local Area Network/Lokales Netzwerk |
| LfD | Landesbeauftragter für den Datenschutz |
| LIS | Landesinformationssystem |
| LKA | Landeskriminalamt |
| LSG | Landessozialgericht |
| LT-Drs. | Landtagsdrucksache |
| LWL | Lichtwellenleiter |
| MAD | Militärischer Abschirmdienst |
| MAN | Metropolitan Area Network |
| MDK | Medizinischer Dienst der Krankenversicherung |
| MfS | Ministerium für Staatssicherheit |
| MHH | Medizinische Hochschule Hannover |
| MIKADO | Modulares Informations- und Kommunikationssystem Automatisierter Dezentraler Online-Anwendungen |
| NAbfG | Niedersächsisches Abfallgesetz |
| NADIS | Nachrichtendienstliches Informationssystem |
| NArchG | Niedersächsisches Archivgesetz |
| 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 |
| NGefAG | Niedersächsisches Gefahrenabwehrgesetz |
| NGO | Niedersächsische Gemeindeordnung |
| NHG | Niedersächsisches Hochschulgesetz |
| Nieders. | Niedersächsische(r/s) |
| NJW | Neue Juristische Wochenschrift |
| NLfV | Niedersächsisches Landesamt für Verfassungsschutz |
| NLGG | Niedersächsisches Landesgleichberechtigungsgesetz |
| NLO | Niedersächsische Landkreisordnung |
| NLVwA | Niedersächsisches Landesverwaltungsamt |
| NLWG | Niedersächsisches Landeswahlgesetz |
| NLZSA | Niedersächsisches Landesamt für Zentrale Soziale Aufgaben |
| NMG | Niedersächsisches Meldegesetz |
| NöVersG | Gesetz über die öffentlich-rechtlichen Versicherungsunternehmen in Niedersachsen |
| Nr. | Nummer |
| NSchG | Niedersächsisches Schulgesetz |
| NStatG | Niedersächsisches Statistikgesetz |
| NVerf-SchG | Niedersächsisches Verfassungsschutzgesetz |
| o.ä. | oder ähnliches |
| OrgKG | Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität |
| OLG | Oberlandesgericht |
| OVG | Oberverwaltungsgericht |
| OWiG | Ordnungswidrigkeitengesetz |
| PersVG | Personalvertretungsgesetz |
| PC | Personal Computer |
| PKS | Polizeiliche Kriminalstatistik |
| POLAS | Polizeiliches Auskunftssystem (in Niedersachsen) |
| PsychKG | Gesetz über Hilfen für psychisch Kranke und Schutzmaßnahmen |
| PTNeuOG | Gesetz zur Neuordnung des Postwesens und der Telekommunikation |
| RdErl. | Runderlaß |
| RiStBV | Richtlinien für das Straf- und Bußgeldverfahren |
| RSA- | Rivest-Shamir-Adleman- |
| RVO | Reichsversicherungsordnung |
| S. | Seite |
| SCHUFA | Schutzgemeinschaft für allgemeine Kreditsicherung |
| SchwbG | Schwerbehindertengesetz |
| SDÜ | Schengener Durchführungsübereinkommen |
| SIRENE | Supplementary Information Request at the National Entry |
| SIS | Schengener Informationssystem |
| SGB | Sozialgesetzbuch |
| sog. | sogenannt(e/r) |
| StGB | Strafgesetzbuch |
| StPO | Strafprozeßordnung |
| StUG | Stasi-Unterlagen-Gesetz |
| StVollzG | Strafvollzugsgesetz |
| TB | Tätigkeitsbericht |
| TDSV | Telekom-Datenschutzverordnung |
| TKV | Telekommunikationsverordnung |
| TU | Technische Universität |
| u.a. | unter anderem, und andere |
| u.ä. | und ähnliches |
| UDSV | Teledienstunternehmen-Datenschutzverordnung |
| UIG | Umweltinformationsgesetz |
| UNIX | (ADV-Betriebssystem für Mehrplatzsysteme) |
| usw. | und so weiter |
| u.U. | unter Umständen |
| UVollzO | Untersuchungshaftvollzugsordnung |

| | |
|---|---|
| v. | von, vom |
| v.a. | vor allem |
| vgl. | vergleiche |
| VNV | Vorläufige Niedersächsische Verfassung |
| VV | Verwaltungsvorschrift |
| VW | Volkswagen |
| VwGO | Verwaltungsgerichtsordnung |
| VwVfG | Verwaltungsverfahrensgesetz |
| VwZG | Verwaltungszustellungsgesetz |
| WM | Weltmeisterschaft |
| ZASt | Zentrale Anlaufstelle für Asylsuchende |
| z.B. | zum Beispiel |
| ZEVIS | Zentrales Verkehrsinformationssystem |
| Ziff. | Ziffer |
| ZNK | Zentrale Namenskartei der Staatsanwaltschaften |
| ZPO | Zivilprozeßordnung |
| z.Zt. | zur Zeit |

## 1. Vorbemerkung

Mit dem vorliegenden XII. Tätigkeitsbericht, der die Jahre 1993 und 1994 betrifft, ist zum vierten Male ein Zwei-Jahres-Bericht erstellt worden. Redaktionsschluß war Anfang Dezember 1994. Rechtsgrundlage ist jetzt § 22 Abs. 3 Satz 1 des neuen Niedersächsischen Datenschutzgesetzes (NDSG). Dieser Tätigkeitsbericht behält weitgehend die bewährte und vertraute Gliederung bei. Am Ende (Kapitel 34. bis 43.) findet sich wiederum - zum zweiten Male - der Bericht über den Datenschutz im nicht-öffentlichen Bereich. Die Rechtsgrundlage für diesen Berichtsteil ergibt sich jetzt aus § 22 Abs. 6 Satz 3 des neuen NDSG.

## 2. Zur Situation

### 2.1 Bundesrepublik Deutschland

Es besteht kein Zweifel: 1993 und 1994 sind - bundesweit gesehen - schwierige Jahre für den Datenschutz gewesen. Insbesondere unter dem Aspekt Bekämpfung der Kriminalität und des Mißbrauchs sozialer Leistungen ist ein politisches Klima entstanden, das den Erlaß zahlreicher Vorschriften begünstigt hat, die das Instrumentarium zur Kontrolle und Überwachung der Bürgerinnen und Bürger der Bundesrepublik Deutschland ausgeweitet haben.

Es ist höchste Zeit, ein datenschutzrechtlich relevantes Vorhaben nicht für sich allein zu sehen. Mit Blick auf die Gesamtentwicklung sollte - diese Überlegung hat zum ersten Male der Bundesbeauftragte für den Datenschutz in seinem 14. Tätigkeitsbericht entwickelt - bei allen laufenden und noch anstehenden Gesetzesvorhaben vor der Einführung neuer Kontroll- und Überwachungsmaßnahmen die Gesamtsituation der Betroffenen gesehen werden; es ist zu prüfen, ob nicht der Verzicht auf ein Vorhaben die im Interesse des Gemeinwohls insgesamt bessere Lösung darstellt. Sonst kommt schrittweise und gleichsam über Nacht eben doch der "gläserne Bürger". Staat und Gesellschaft müssen, falls sie ihren freiheitlich-demokratischen Charakter nicht aufgeben wollen, auch den Mut zu einem Weniger an Information haben.

Die datenschutzrechtlichen Defizite bei der Bundesgesetzgebung sind noch erheblich. So steht z.B. eine umfassende Überarbeitung der Strafprozeßordnung immer noch aus, und auch eine Regelung des Arbeitnehmerdatenschutzes fehlt.

In den Berichtszeitraum fiel der Tag, an dem vor 10 Jahren das Volkszählungsurteil des Bundesverfassungsgerichts verkündet wurde. Die einzige größere Veranstaltung in der Bundesrepublik aus diesem Anlaß fand am 15. Dezember 1993 in Hannover statt; Einladende waren der Niedersächsi-

sche Innenminister und ich. Nach Eröffnung der Veranstaltung durch mich sprachen Minister Glogowski ("Datenschutz in Niedersachsen - Die Anforderungen an Politik und Verwaltung -") und Spiros Simitis, der Hessische Datenschutzbeauftragte von 1975 bis 1991 ("Die Entscheidung des Bundesverfassungsgerichts zur Volkszählung - 10 Jahre danach"). Das Referat von Simitis, das die positiven und negativen Seiten der Entwicklung des Datenschutzes in der Bundesrepublik Deutschland aufzeigt, ist in der Kritischen Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (1994 S. 121) veröffentlicht und wird als Anlage 23 dieses Tätigkeitsberichts abgedruckt.

10 Jahre Volkszählungsurteil haben selbstverständlich auch der Konferenz der Datenschutzbeauftragten des Bundes und der Länder Veranlassung gegeben, Bilanz zu ziehen. Auf der Sitzung am 9./10 März 1994 in Potsdam ist ein Diskussionspapier (Bestandsaufnahme über die Situation des Datenschutzes "10 Jahre nach dem Volkszählungsurteil") zustimmend zur Kenntnis genommen worden, jedoch bei Stimmenthaltung Bayerns. Das Diskussionspapier ist als Anlage 9 dieses Tätigkeitsberichts abgedruckt.

## 2.2 Niedersachsen

### 2.2.1 Allgemeines

Die Jahre 1993 und 1994 sind in Niedersachsen datenschutzrechtlich insbesondere dadurch gekennzeichnet, daß die gesetzlichen Datenschutzdefizite weiter systematisch abgebaut wurden. Vor allem sind das neue Niedersächsische Datenschutzgesetz (NDSG) vom 17. Juni 1993 (Nds. GVBl. S. 141) und das Niedersächsische Gefahrenabwehrgesetz (NGefAG) vom 13. April 1994 (Nds. GVBl. S. 172) zu nennen. Auf das NDSG wird näher unter 2.2.2 eingegangen, auf das NGefAG unter 12.1. Datenschutzrechtliche Regelungen - allerdings geringeren Ausmaßes - enthalten auch folgende Gesetze: das Niedersächsische Archivgesetz vom 25. Mai 1993 (Nds. GVBl. S. 129), das Zehnte Gesetz zur Änderung der Niedersächsischen Gemeindeordnung und der Niedersächsischen Landkreisordnung vom 14. Juni 1993 (Nds. GVBl. S. 137) - hier: kommunale Frauenbeauftragte -, das Vierte Gesetz zur Änderung des Niedersächsischen Schulgesetzes vom 23. Juni 1993 (Nds. GVBl. S. 178), das Niedersächsische Landesrundfunkgesetz vom 9. November 1993 (Nds. GVBl. S. 523) und das Fünfte Gesetz zur Änderung des Niedersächsischen Hochschulgesetzes vom 8. Dezember 1993 (Nds.GVBl. S. 618). Diese Gesetze werden in späteren Kapiteln behandelt.

Negativ ist zu vermerken, daß die in der Koalitionsvereinbarung vom 19. Juni 1990 angekündigte Verbesserung des Datenschutzes im Gesundheitswesen nicht realisiert wurde. In der neuen Legislaturperiode können Fortschritte in anderen Bundesländern Hilfestellung geben. Die Arbeiten an dem ebenfalls in der Koalitionsvereinbarung genannten Niedersächsischen

Krebsregister sind äußerst langwierig und müssen nun ein Bundesgesetz beachten (21.5.5).

Die Regierungserklärung, die Ministerpräsident Gerhard Schröder am 23. Juni 1994 zu Beginn der Dreizehnten Wahlperiode des Niedersächsischen Landtages abgab, erwähnt den Datenschutz leider nicht. Es besteht derzeit aber kein konkreter Anlaß, dies negativ zu deuten.

Was die Praxis im öffentlichen und nicht-öffentlichen Bereich anbetrifft, so sind auch 1993 und 1994 zahlreiche datenschutzrechtliche Verstöße zu verzeichnen; spätere Kapitel des Tätigkeitsberichts dokumentieren dies. Der Datenschutz in Niedersachsen ist aber grundsätzlich gewährleistet. Die festgestellten Verstöße gehen häufig auf Unkenntnis und mangelndes Problembewußtsein der datenverarbeitenden Stellen zurück. Teilweise mußte ich aber auch mangelnde Bereitschaft feststellen, das gesetzliche Anliegen des Datenschutzes zu berücksichtigen. Aus- und Fortbildung in Fragen des Datenschutzes muß daher, wie auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrem Beschluß vom 9./10. März 1994 (vgl. Anlage 9) gefordert hat, erheblich mehr Gewicht beigemessen werden als bisher.

### 2.2.2 Insbesondere: Das neue Niedersächsische Datenschutzgesetz

Das im letzten Tätigkeitsbericht (2.1) bereits angekündigte neue NDSG wurde nach intensiven Ausschußberatungen vom Landtag in seiner Sitzung am 8. Juni 1993 beschlossen. Leider wiederholte sich die Einstimmigkeit, die beim Gesetz zur Neuregelung der Stellung des Landesbeauftragten für den Datenschutz vom 28. Mai 1991 gegeben war, nicht. Das neue NDSG wurde am 17. Juni 1993 ausgefertigt und am 28. Juni 1993 im Nds. GVBl. verkündet (S. 141). Es ist am 1. Oktober 1993, d.h. nach einer angemessenen Übergangszeit, in Kraft getreten.

Die Aufgabe des neuen NDSG ist in dessen § 1 klar umschrieben: Zum einen (Satz 1 Nr. 1) soll das Recht einer jeden Person gewährleistet werden, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen (Recht auf informationelle Selbstbestimmung); diese Formulierung ist treffender als die in § 1 Abs. 1 des alten NDSG, wo vom Schutz personenbezogener Daten vor Mißbrauch die Rede ist, und auch klarer als die in § 1 Nr. 1 der Regierungsvorlage. Nicht Daten sind zu schützen, sondern Menschen. Zum anderen (Satz 1 Nr. 2) soll einer Beeinträchtigung der Wirkungsmöglichkeiten der Verfassungsorgane des Landes und der Organe der kommunalen Gebietskörperschaften infolge der automatisierten Datenverarbeitung entgegengewirkt werden. An diese Bestimmung wird in den §§ 7 Abs. 3, 22 Abs. 2 NDSG angeknüpft. § 1 Satz 2 NDSG, wonach dieses Gesetz bestimmt, unter welchen Voraussetzungen personenbezogene Daten durch öffentliche Stellen verarbeitet werden dürfen, macht deutlich, daß es auch Aufgabe des NDSG ist, Grundrechtseingriffe zuzulassen.

Die Schwerpunkte der Neuregelung sind folgende:

a) Im Gegensatz zum bisher geltenden NDSG wird auch die Informationsverarbeitung in Akten in den Schutzbereich des Gesetzes einbezogen (§§ 1, 2 Abs. 1). Organisatorisch und datenschutzrechtlich hat die Abgrenzung der Dateien von den Akten längst ihren Sinn verloren.

b) Das neue Gesetz sieht nicht erst die Speicherung personenbezogener Daten, sondern bereits die Erhebung als regelungsbedürftige Verarbeitungsphase an (§§ 3 Abs. 2, 9). Nach § 3 Abs. 2 Satz 1 ist - wie auch in einigen anderen Landesdatenschutzgesetzen - Datenverarbeitung der Oberbegriff für das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen personenbezogener Daten. Demgegenüber spricht das Bundesdatenschutzgesetz vom 20. Dezember 1990 von drei Phasen: Erhebung, Verarbeitung und Nutzung (§ 1 Abs. 2).

c) Grundlegende Bedeutung kommt dem nach dem Volkszählungsurteil des Bundesverfassungsgerichts erforderlichen Zweckbindungsprinzip zu. Dieses ist an etlichen Stellen des neuen NDSG verankert. So ist das Speichern, Verändern und Nutzen personenbezogener Daten grundsätzlich nur zulässig, wenn es zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist und die Daten für diese Zwecke erhoben worden sind (§ 10 Abs. 1 Satz 1). Der Zweckbindungsgrundsatz ist auch für die Übermittlung relevant (§§ 11, 13, 14, 15). Damit wird ein amtshilfefester Schutz gegen Zweckentfremdung erreicht.

d) Erheblich erweitert werden die Rechte der Betroffenen. So sind das Auskunftsrecht den verfassungsrechtlichen Vorgaben angepaßt (§ 16), die Nachberichtspflicht erweitert (§ 17 Abs. 4) sowie der Schadensersatzanspruch (§ 18) und die Möglichkeit der Anrufung des Landesbeauftragten (§ 19) verbessert worden.

e) Durch etliche Vorschriften wird versucht, die Risiken der Informations- und Kommunikationstechniken besser in den Griff zu bekommen. Zu nennen ist z.B. die Einführung von Regelungen über automatisierte Abrufverfahren (§ 12) - in Kraft getreten am 1. Oktober 1994 - und über die Technikfolgenabschätzung (§ 7 Abs. 3). Die Formulierung zurTechnikfolgenabschätzung (Risikoanalyse) ist an das Berliner Informationsverarbeitungsgesetz vom 9. Oktober 1992 angelehnt. Mit ihrer Aufnahme in ein allgemeines Datenschutzgesetz wird aber bundesweit Neuland im Sinne des sogenannten vorgezogenen Datenschutzes betreten.

f) Die Stellung des Landesbeauftragten für den Datenschutz (§§ 21 ff.) ist gegenüber dem NDSG in der Fassung vom 28. Mai 1991 noch in einigen Punkten gestärkt worden. Die Pflicht zur Unterrichtung über Planungen zum Aufbau automatisierter Informationssysteme bezieht jetzt die kommunalen Gebietskörperschaften ein (§ 22 Abs. 2 Satz 3). Neu ist auch die Aktenvorlagepflicht der öffentlichen Stellen (§ 22 Abs. 4 Satz 2).

g) Schließlich sind - erstmalig in Niedersachsen - die besonderen Verarbeitungsregelungen betreffend Dienst- und Arbeitsverhältnisse (§ 24), Forschungsvorhaben (§ 25), Fernmessen und Fernwirken (§ 26) sowie öffentliche Auszeichnungen (§ 27) zu nennen.

Das neue NDSG ist klar formuliert und auch gut gegliedert. Was den Inhalt angeht, kann es sich messen mit den fortschrittlichsten Datenschutzgesetzen der Bundesrepublik Deutschland, z.B. denen von Hessen, Berlin und Brandenburg. Es dürfte kein Zweifel bestehen, daß sich das neue NDSG in der Praxis bewähren wird. Die öffentlichen Stellen sind gut beraten, wenn sie den Leitgedanken "Freiheitssicherung durch Datenschutz" in ihrem Verwaltungshandeln verwirklichen; dann wird auch ein Beitrag zu mehr Bürgerfreundlichkeit der Verwaltung geleistet. Auf die Verwaltungsvorschriften zum NDSG wird unter 6.1 eingegangen.

### 2.3 Verfassung und Datenschutz

Im letzten Tätigkeitsbericht (2.3) wurden die Bemühungen dargestellt, das Recht auf informationelle Selbstbestimmung und die unabhängige Datenschutzkontrolle ausdrücklich im Grundgesetz zu regeln. Auf ihren Konferenzen am 16./17. Februar 1993 und 9./10. März 1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Mein Hamburger Kollege Dr. Schrader hat die Gesamtproblematik in CR 1994, S. 427 ff. näher behandelt. Mit den Beschlüssen des Bundestages und des Bundesrates im Juli und September 1994 sind die Bemühungen vorerst leider gescheitert. Es wäre aber verfehlt, nun das Thema endgültig zu den Akten zu nehmen.

Gerade beim Scheitern der Versuche, den Datenschutz ausdrücklich im Grundgesetz zu verankern, wäre es - wie ich im letzten Tätigkeitsbericht (XI 2.3) ausgeführt habe - angebracht, das Recht auf informationelle Selbstbestimmung überall landesverfassungsrechtlich zu regeln. Leider ist es wegen der erforderlichen Zwei-Drittel-Mehrheit nicht möglich gewesen, das Recht auf informationelle Selbstbestimmung in die neue Niedersächsische Verfassung vom 19. Mai 1993 (Nds. GVBl. S. 107) aufzunehmen. Allerdings ist die Regelung über den Landesbeauftragten für den Datenschutz in Art. 46 a VNV mit unwesentlichen Änderungen als Art. 62 in die neue Landesverfassung übernommen worden (vgl. auch 3.1); es ist bei der Zuordnung zum Abschnitt "Die Verwaltung" geblieben.

## 3. Der Landesbeauftragte

### 3.1 Status

Der Status des Landesbeauftragten ergibt sich jetzt weitgehend aus Art. 62 der neuen Niedersächsischen Verfassung (vgl. 2.3). Auffallend bei den ge-

ringfügigen Änderungen gegenüber Art. 46 a VNV ist allein, daß es früher in Abs. 3 hieß, der Landesbeauftragte sei "nur dem Gesetz unterworfen", während jetzt von der Bindung an Gesetz und Recht die Rede ist. Nach dem Schriftlichen Ausschußbericht zum Entwurf einer Niedersächsischen Verfassung (LT-Drs. 12/5840, S. 38) liegt keine inhaltliche Änderung vor. Auf Anregung des Gesetzgebungs- und Beratungsdienstes des Niedersächsischen Landtags sollte eine Angleichung an die Stellung des Landtagspräsidenten gemäß Art. 18 Abs. 3 Satz 2 der neuen Landesverfassung erfolgen. Ich habe es als befremdlich empfunden, die - wenngleich unwesentliche - Textänderung und ihren Hintergrund erst aus der Niederschrift über die Sitzung des Sonderausschusses "Niedersächsische Verfassung" am 26. Februar 1993 zu erfahren.

Im Berichtszeitraum haben sich Kompetenzerweiterungen durch das neue NDSG (vgl. 2.2.2) und das Niedersächsische Landesrundfunkgesetz vom 9. November 1993 (Nds. GVBl. S. 523) ergeben (vgl. 9.5). Nach § 68 des letztgenannten Gesetzes hat der Landesbeauftragte die Kontrollbefugnis gegenüber den privaten Rundfunkveranstaltern.

## 3.2 Beratung der Landesregierung

Auch 1993 und 1994 gab es Fälle, in denen mich oberste Landesbehörden bei der Vorbereitung allgemeiner Regelungen des Landes und des Bundes nicht oder nicht rechtzeitig beteiligten. Die Ressorts können nicht davon ausgehen, daß der Bundesbeauftragte für den Datenschutz die Landesbeauftragten - schon wegen des oft gegebenen Zeitdrucks - zu allen Gesetzesvorhaben des Bundes beteiligt. Ich begrüße es deshalb, daß die Verwaltungsvorschriften zum NDSG (Nds. MBl. 1994, S. 1147) meine Beteiligung nunmehr ausdrücklich vorsehen (Nr. 17 Satz 1 Nr. 7 zu § 22).

Gemäß § 18 Abs. 2 Satz 2 des alten NDSG habe ich den XI. Tätigkeitsbericht dem Landtag mit Schreiben vom 7. Januar 1993 vorgelegt. Die Stellungnahme der Landesregierung ist erst Anfang Oktober 1994 beim Landtag eingegangen. Diese Verspätung kann nicht akzeptiert werden. Meine Bewertung ist unabhängig von der Frage, ob § 22 Abs. 3 Satz 2 des neuen, seit dem 1. Oktober 1993 geltenden NDSG auf den vorliegenden Fall schon anwendbar war. Das neue Gesetz verlangt eine Stellungnahme innerhalb von sechs Monaten.

## 3.3 Eingaben und Akteneinsicht

Die Eingaben erstreckten sich auf alle Aufgabenbereiche des Landesbeauftragten. Anders als im letzten Berichtszeitraum gingen auch Petitionen aus dem Ausländerbereich bei mir ein; die Initiative hierzu lag jedoch regelmäßig bei Deutschen (vgl. XI 3.4). Eine besonders starke Zunahme von Eingaben ist im nicht-öffentlichen Bereich zu verzeichnen.

Unter Nr. 3.5 des letzten Tätigkeitsberichts habe ich mich zur Frage geäußert, ob ein Petent Einsicht in die zu seiner Eingabe angelegten Akten meiner Geschäftsstelle hat. Seinerzeit bestand ein solcher Anspruch nicht. Mit Inkrafttreten des neuen NDSG hat sich die Rechtslage jedoch geändert. Das in § 16 NDSG festgelegte Recht der Betroffenen auf Auskunft und Akteneinsicht gilt auch für Bürgerinnen und Bürger, die sich mit einer Eingabe an mich wenden. Allerdings können diese Rechte im Einzelfall insoweit beschränkt sein, als personenbezogene Daten wegen berechtigter Interessen Dritter geheimzuhalten sind (§ 16 Abs. 4 Nr. 3 NDSG). Öffentliche Stellen haben einen solchen Anspruch nach dem NDSG nicht.

## 3.4 Geschäftsstelle

Ich danke dem Niedersächsischen Landtag, daß er mir im Haushaltsjahr 1993 eine Stelle der Besoldungsgruppe A 15 und eine Stelle der Besoldungsgruppe A 13 - gehobener Dienst - zur Verfügung stellte.

Ich weiß um die angespannte Haushaltssituation des Landes. Gleichwohl halte ich mich für verpflichtet, darauf hinzuweisen, daß die jetzige Stellenausstattung der Geschäftsstelle nicht ausreichend ist. Die neuen datenschutzrechtlichen Regelungen, die im Berichtszeitraum erfolgten (vgl. oben 2.2.1), haben zu einer erheblichen Mehrbelastung geführt. Nach dem NDSG ist nun z.B. die gesamte Informationsverarbeitung in Akten in meine Kontrolltätigkeit einbezogen. Die Handhabung der Forschungsklausel (§ 25 NDSG) bindet viel Arbeit. Der sprunghaft gestiegene Einsatz der IuK-Technik in der öffentlichen Verwaltung hat meinen Beratungs- und Kontrollaufwand erhöht. Die begonnene Vernetzungstechnik im großen und im kleinen erfordert Kommunikationsspezialisten auch beim Kontrolleur. Die Tätigkeit im nicht-öffentlichen Bereich hat stark zugenommen; es hat sich im Land schnell herumgesprochen, daß es jetzt eine zentralisierte und effektive Aufgabenwahrnehmung durch den Landesbeauftragten gibt.

Die begonnene Automatisierung der Geschäftsstelle mit dem Bürokommunikationssystem Alis konnte zur Vollausstattung ausgebaut werden.

## 3.5 Außenprüfungen und Beratungen

Im öffentlichen Bereich fanden materiell-rechtliche Prüfungen bei der Polizei, beim Landesamt für Verfassungsschutz, beim Justizvollzug und bei mehreren Personalstellen statt. Im Bereich der öffentlichen Verwaltung habe ich ein Finanzamt, ein Finanz-Rechenzentrum, zwei Ministerien, einen Landkreis, eine Stadt, drei Samtgemeinden, ein Katasteramt, eine Industrie- und Handelskammer sowie eine Berufsbildende Schule kontrolliert. Die begonnenen Überprüfungen privater PC von Lehrern wurden von mir an mehreren Schulen im Raum Hannover fortgeführt. Der Prüfungsschwerpunkt meiner Kontrollen des technischen und organisatorischen Datenschutzes und der Datensicherung lag im Bereich der UNIX-Rechnersysteme. Im Bereich der Wirtschaft kam es zu 34 Prüfungen nach § 38 BDSG. Davon wa-

ren vier "Anlaßprüfungen" bei nicht-meldepflichtigen Unternehmen und 30 "Routineprüfungen" bei Registerfirmen (vgl. 35.2). Die Zahl der Prüfungen hätte insgesamt größer sein müssen. Das war aber leider wegen der unter 3.4 angesprochenen hohen Belastung nicht möglich.

1993 und 1994 ist die Zahl der Beratungsgespräche stark gestiegen, insbesondere wegen neuer datenschutzrechtlicher Regelungen (vgl. 2.2.1).

## 3.6 Die neue Dateibeschreibung und das Dateienregister im öffentlichen Bereich

Öffentliche Stellen sind gesetzlich verpflichtet, ihre Verarbeitung personenbezogener Daten transparent zu machen (§ 8 Abs. 1 NDSG). Für jede Sammlung personenbezogener Daten - gleich ob als automatisierte oder nichtautomatiserte Datei betrieben - ist eine Dateibeschreibung zu erstellen. Die Beschreibungen für automatisierte Dateien sind zum Register aller automatisierten Dateien bei mir vorzulegen. Der neue Vordruck für die Dateibeschreibung, der mit mir zusammen entwickelt wurde, ist im Nds. MBl. 1994, S. 1154 als Anlage der Verwaltungsvorschriften zum NDSG veröffentlicht. Erstmals müssen in der Dateibeschreibung auch die technischen und organisatorischen Maßnahmen nach § 7 NDSG für jede Datei angegeben werden. Die bisher für automatisierte Dateien abgegebenen Registermeldungen alter Art gelten bis zu einer Änderung der Dateien, längstens bis zum 31. Dezember 1995. Es ist weiterhin möglich, für gleichartige Dateien eine gemeinsame Beschreibung zu erstellen (z.B. durch die Kommunale Datenzentrale als Auftragnehmer für ihre DV-Anwender). Allerdings ist eine solche "Sammelmeldung" um die spezifischen Festlegungen der datenverarbeitenden Stelle zu ergänzen (z.B. Ansprechpartner, behördlicher Datenschutzbeauftragter, technische und organisatorische Maßnahmen vor Ort).

Teile der Dateibeschreibung werden in meiner Dienststelle in einer Datenbank automatisiert gespeichert, um die Angaben besser als bisher auswerten zu können. Gespeichert werden u.a. die Stammdaten der datenverarbeitenden Stelle, die Bezeichnung der Datei, die Betriebsart des Verfahrens und die Art der Geräte. Ich benötige diese zugriffsfähigen Angaben zur Vorbereitung gezielter Kontrollen und zur gezielten und schnellen Verteilung allgemeiner Informationen über Probleme und Erkenntnisse der Datensicherung.

Leider sind meine ersten Erfahrungen mit der neuen Dateibeschreibung nicht nur positiv. Die bisher eingegangenen Beschreibungen weisen zum großen Teil Mängel auf und erfordern großen Nachbereitungsaufwand in meiner Dienststelle. Diesen Aufwand beabsichtige ich durch verstärkte Aufklärung zu reduzieren.

Die Veröffentlichungspflicht von Dateien ist entfallen. Dies ist aus meiner Sicht keine Verschlechterung des Datenschutzes. Kaum eine Bürgerin oder ein Bürger dürfte im Ministerialblatt bzw. im amtlichen Verkündungsblatt nachgeschaut haben, welche Dateien bei den öffentlichen Stellen geführt werden. Leider nutzen die Bürgerinnen und Bürger nur wenig die Möglich-

keit des kostenlosen Einsichtsrechts und das, Auszüge aus dem Dateienregister fertigen zu lassen (§ 22 Abs. 5 NDSG).

## 3.7 Öffentlichkeitsarbeit

Auf Seminaren, Fortbildungsveranstaltungen, Tagungen und mit Vorträgen haben die Angehörigen der Dienststelle und ich 1993 und 1994 verstärkt Öffentlichkeitsarbeit betrieben. Zu einem erheblichen Teil sind die neuen datenschutzrechtlich relevanten Gesetze des Landes (vgl. 2.2.1) und des Bundes der Anlaß gewesen. Zielgruppen waren beispielsweise: Studierende und Bedienstete der Universitäten Göttingen und Hannover sowie der Medizinischen Hochschule Hannover, Polizeibeamtinnen und -beamte verschiedener Dienststellen, Praktiker im Rahmen der Fortbildung an Kommunalen Studieninstituten, Dozentinnen und Dozenten an der Niedersächsischen Fachhochschule für Verwaltung und Rechtspflege, Hörerinnen und Hörer bei Volkshochschulen, Mitglieder von Gewerkschaften, Angehörige medizinischer Berufsverbände, Bedienstete der Landwirtschaftskammer Hannover und aus dem Justizvollzug, Angehörige der Erfa-Kreise der Gesellschaft für Datenschutz und Datensicherung e.V., Hörerinnen und Hörer der Verwaltungs- und Wirtschaftsakademie Braunschweig, Bedienstete von Städten und Landkreisen.

Zur schriftlichen Öffentlichkeitsarbeit ist folgendes zu bemerken:

- Zum Inkrafttreten des neuen NDSG am 1. Oktober 1993 habe ich eine Broschüre "Datenschutz in Niedersachsen - Das Niedersächsische Datenschutzgesetz vom 17. Juni 1993" herausgegeben, eine Textausgabe mit einführenden Erläuterungen. Die 1. Auflage im Umfang von 12.000 Exemplaren war innerhalb kurzer Zeit vergriffen. Im Frühjahr 1994 erschien eine zweite, unveränderte Auflage mit erneut 12.000 Exemplaren. Die Broschüre erfreut sich weiterhin reger Nachfrage bei Behörden, Gerichten sowie Bürgerinnen und Bürgern. Ich hoffe, daß sie nicht in Bücherregalen verstaubt, sondern rege genutzt wird.

- Im Berichtszeitraum sind ferner als Broschüren oder Merkblätter erschienen: "Tips zum Adressenhandel und gegen die Werbepapierflut im Briefkasten" (gemeinsam mit den Kollegen in Bremen und Hamburg), "Orientierungshilfe Datenschutz und Datensicherung", "Datenschutzprüfkonzept für NOVELL-Fileserver", "Hinweise zum datenschutzgerechten Einsatz von Laptops", "Muster-Dienstanweisung 'Datenschutz' für öffentliche Stellen", "Hinweise zu Stellung und Aufgaben eines behördlichen Datenschutzbeauftragten" und "Vernichtung von Datenträgern mit personenbezogenen Daten".

## 3.8 Zusammenarbeit mit anderen Kontrollorganen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder tagte im Berichtszeitraum viermal. Die Entschließungen sind als Anlagen zu

diesem Bericht abgedruckt. 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 Aufsichtsbehörden für den privaten Bereich, teil. Mit den kirchlichen Datenschutzbeauftragten fand ein häufiger Gedankenaustausch statt.

## 4. Entwicklungen und Probleme der Informations- und Kommunikationstechnik in Verwaltung und Wirtschaft

### 4.1 Stand der automatisierten Datenverarbeitung

#### 4.1.1 Was ist eine Datenautobahn?

In deutschen Medien geistern seit einiger Zeit Schlagworte wie "Datenautobahn", "Home-Banking", "Home-Shopping", "Video on demand", "Multimedia" und viele andere Worthülsen herum, mit denen ein neues Informationszeitalter eingeläutet werden soll. Kein Thema beschäftigt die amerikanische Computer- und Kommunikationsindustrie zur Zeit so intensiv wie der "Information Superhighway". Es geht dabei um den Aufbau eines leistungsfähigen nationalen Datennetzes für multimediale Kommunikation mit riesigen Datenmengen für jedermann. Die Bereiche Datenverarbeitungs-, Telekommunikations- und Medienwirtschaft wachsen weltweit zusammen. Jedes Unternehmen, das etwas auf sich hält, führt voller Überzeugung seine Vision der digitalen Datenautobahn vor und versucht, ein Stück von der Riesentorte zu erwischen. Die Digitalisierung der Medien ist in den Vereinigten Staaten zum nationalen Anliegen erklärt worden. Sie soll die größte Investition der neunziger Jahre werden.

Auch in Deutschland gibt es Modellversuche mit "Datenautobahnen", und das gleich in mehreren deutschen Großstädten (Stuttgart, Nürnberg, Hamburg, Berlin). Der größte Versuch läuft in Stuttgart, an dem 4.000 Haushalte beteiligt sind. Über glasfasergestützte Datenleitungen sind individuell zusammengestellte Zeitungen, Spielfilme, Lernprogramme, Telespiele, Mailboxen und andere Informationsdienste abrufbar. Versandhäuser und Reisebüros laden zum "Interactiv Shopping" ein. Interaktive Beratung, zum Beispiel in rechtlichen und medizinischen Fragen, wird abrufbar sein. Selbst die in Deutschland bisher negativ belegte Heimarbeit soll neu belebt werden - jetzt im modernen Gewand unter dem neudeutschen Begriff "Tele Commuting".

Von der Technik her betrachtet ist die sogenannte Datenautobahn nichts Revolutionäres, sondern lediglich ein attraktiver Transportweg für die weiterhin boomende Informations- und Kommunikationstechnik (IuK-Technik). Die Mikroelektronik bildet auch hierfür die technologische Basis. Damit soll das jüngstes Kind der IuK-Technik, die Multimediatechnik mit integrierter

Verarbeitung von Texten, Graphiken, Bildern, Videos und Klangereignissen, auf komfortable Weise lauffähig werden. Das "Fahrzeug für die Autobahn" kann ein Personal Computer sein, ebenso gut aber auch ein Fernseher mit digitaler Zusatzausstattung. Der Trend in der Mikroelektronik zu immer kleineren, leistungsfähigeren und billigeren Geräten, der unvermindert anhält und nun auch zum verstärkten Einsatz in privaten Haushalten führt, kommt den Utopien dieser neuen Medienwelt entgegen. Trotz vieler propagierter Funktionen und Anwendungsmöglichkeiten fehlt der "Datenautobahn" bisher jedoch eine wirkliche sogenannte "Killer Application", also Anwendungen, die Bürgerinnen und Bürger, Unternehmen sowie Verwaltung wirklich brauchen und die nur über eine solche Datenautobahn zu erreichen sind.

Datenschutzrechtliche Relevanz erhält die "Datenautobahn" dadurch, daß trotz begonnenem "Autobahnbau die notwendigen Verkehrsregeln" weitgehend fehlen (vgl. 4.8.2). Dabei ist regionale, bundes- und weltweite Vernetzung sowohl über selbstverwaltete als auch über öffentliche Kommunikationsnetze längst keine Utopie mehr. Im Bereich der Wirtschaft werden immer stärker wachsende Datenmengen über größte Entfernungen ausgetauscht. Der elektronische Briefkasten - im Fachjargon "Mailbox" genannt - hat enorme Zuwachsraten (vgl. 4.8). Allein im Internet - einem weltumspannenden Computernetz - vermutet man heute über 30 Millionen Teilnehmerinnen und Teilnehmer. Dazu die Frankfurter Rundschau vom 5. November 1994: "Das Internet hat sich fast wie ein Flächenbrand an Universitäten, in wissenschaftlichen Instituten und in der Informationsindustrie ausgebreitet. ... Deutsche wissenschaftliche Fachinformationszentren warnen vor einem Info-Chaos". Auf diesen inzwischen weltweiten Netzen werden zunehmend auch personenbezogene Daten übermittelt und auf externen Rechnern verarbeitet.

Mit der aufgezeigten Vernetzung unterschiedlicher Rechner der öffentlichen Verwaltung wird der traditionelle Entscheidungsprozeß, für eine bestimmte Aufgabe ein dafür geeignetes System zu beschaffen, zugunsten eines Infrastrukturansatzes verlassen. Die Ausstattung mit IuK-Technik erfolgt dabei weitgehend bedarfsunabhängig. Mit jedem angeschlossenen Rechner sollen Nachrichten ausgetauscht werden können, auf jede DV-Anwendung soll zugegriffen werden können, unabhängig davon, auf welchem Rechner die Datenverarbeitung abläuft. Fragen nach Nutzen, Gefahren und Risiken lassen sich jedoch ohne Kenntnis der DV-Anwendungen nur schwer benennen und bewerten; dies erschwert die Steuerung und die Kontrolle solcher vernetzten Systeme. Eine Rechnervernetzung erfordert einen hohen Mindeststandard an Datensicherheit, da nicht vorab feststeht, welche sensiblen Daten zu welcher Zeit mit welchem Rechner verarbeitet werden. Nur durch eine gut durchdachte "Grundsicherung" läßt sich der Schutz der Vertraulichkeit gewährleisten. Doch damit ist nur ein unverhältnismäßig kleiner Teil der mit der IuK-Technik verbundenen Gefahren abgesichert. Zur Gewährleistung des Rechts auf informationelle Selbstbestimmung reichen Ge- und Verbote nicht aus; vielmehr müssen die widerstreitenden öffentlichen und privaten Interessen abgewogen und einer verfassungsverträglichen Regelung zugeführt werden.

### 4.1.2 Die niedersächsischen Datenstraßen

Auch die öffentliche Verwaltung ist dabei, ihre "Datenstraßen" zu konzipieren und auszuprobieren. Ab 1995 erfolgt der Dokumentenaustausch zwischen der Europäischen Union, dem Bund und den Ländern über "Electronic Mail" und ersetzt den herkömmlichen "Postdienst". Auch der "Kooperationsausschuß ADV Bund / Länder / kommunaler Bereich" setzt auf Electronic Mail, um schneller Dokumente auszutauschen und miteinander kommunizieren zu können. Die niedersächsische Landesverwaltung hat die Pilotprojekte MINiNET / X.400, KOMNET und TELENET ins Leben gerufen, um Klarheit über die zu schaffende Infrastruktur und deren Leistungsfähigkeit zu finden. Potentielle Gefahren, ihre Eintrittswahrscheinlichkeit und notwendige Sicherheitsmaßnahmen sollen analysiert und gefunden werden. In 4.6 werden alle im Interministeriellen Arbeitskreis Informations- und Kommunikationstechnik (IMA-IuK-Technik) vorgestellten Projekte der Landesverwaltung, ihre Ziele und ihre Kommunikationsbeziehungen dargestellt.

### 4.1.3 Downsizing - keine Erfolgsstory

"Downsizing" steht für die Umstellung automatisierter Verfahren von Großrechnern auf dezentrale und billigere Arbeitsplatzsysteme. Der mit diesem Begriff gekennzeichnete Trend bestimmt weiterhin den Informationstechnik-Einsatz in der öffentlichen Verwaltung (XI 4.1). Versprechungen, durch Downsizing größere Effektivität, Flexibilität und Kostenersparnisse zu erzielen, sind verstummt und der Ernüchterung gewichen. So heißt es z.B. in einer Verwaltungszeitschrift: "Der Einsatz neuer Informationstechnik ist bislang keine Erfolgsstory gewesen". Mit dieser Feststellung ist die Aufforderung an die Behördenspitzen verbunden, über die Organisation beim Einsatz technikunterstützter Informationsverarbeitung neu nachzudenken. Vergleichbare ernüchternde Erfahrungen über die Einführung von Bürokommunikation ohne begleitende organisatorische Konsequenzen wurden auch in der Wirtschaft gemacht.

Es ist die erklärte Zielsetzung der Landesregierung, eine "schlanke" Verwaltung in Niedersachsens Amtsstuben zu schaffen. Dies soll, angepriesen mit Schlagworten wie "lean management" und "business reengineering", auch durch verstärkten Einsatz von IuK-Technik erreicht werden. Die Begründung zum Technikeinsatz lautet häufig: "Qualitätsverbesserungen der Verwaltungsleistung, Rationalisierung, Verbesserung der Serviceleistungen für den Bürger und verbesserte Arbeitsbedingungen für Mitarbeiter". Die Landesregierung hat die Inanspruchnahme von Investitionsmitteln für einen flächendeckenden Einsatz der Bürokommunikation an die Bedingung geknüpft, daß 8 % der Stellen eingespart werden. Den Zielkonflikt zwischen Qualitätsverbesserung und Rationalisierung will die Landesverwaltung durch einen Strukturwandel auflösen. Mit der Einführung neuer automatisierter Verfahren sollen Arbeitsabläufe überprüft, Aufgaben integriert, verlagert oder neu zugeordnet werden. Managementstrukturen sollen gestrafft und

vereinfacht sowie Kompetenzen und Verantwortung in Frage gestellt werden. Dieser Strukturwandel wirft viele Datenschutzfragen auf und wird sicherlich Änderungen bestehender Rechtsvorschriften erfordern. Die Verwaltungsreform wird daher von mir sehr aufmerksam verfolgt.

### 4.1.4 Kontrolle à la card

Ähnlich großen Medienrummel wie um die Datenautobahn gibt es in letzter Zeit um die Chipkarte. "Kontrolle à la Card", "Revolution im Zahlungsverkehr", "Der gläserne Patient" sind Schlagzeilen, die zwischen Euphorie und Ängsten schwanken. Dabei gehört die Plastikkarte heute längst zum Alltag. Damit werden im In- oder Ausland Hotelkosten beglichen, an der Kaufhauskasse der Einkauf und an der Tankstelle das Benzin bezahlt, oder es wird damit telefoniert. Die Deutsche Bundespost Telekom hat inzwischen 200 Millionen Chipkarten für ihre Kartentelefone verkauft. Von den Krankenversicherungen wurden 70 Millionen Krankenversichertenkarten ausgegeben. 2,2 Millionen Mobilfunk-Teilnehmerinnen und -Teilnehmer telefonieren in den C-, D- und E-Netzen mit der Chipkarte. Es gehört kein Prophetentum dazu, vorherzusagen, daß die Chipkartentechnologie weitere Anwendungsfelder erobern und immer mehr Lebensbereiche aller Bürgerinnen und Bürger berühren wird.

Seit dem 1. Oktober 1994 ersetzt die Chipkarte in Niedersachsen den Krankenschein aus Papier. Die datenschutztechnischen Anforderungen an die Krankenversichertenkarte sehe ich als erfüllt an:

- Es werden nur die gesetzlich zulässigen Daten auf der Chipkarte gespeichert.
- Versuche, darüber hinausgehende Daten (z.B. medizinische Informationen) zu speichern, werden technisch abgesperrt.
- In den Arztpraxen werden Lesegeräte eingesetzt, die durch das Bundesamt für Sicherheit in der Informationstechnik geprüft und zertifiziert worden sind.
- Der Kartenaussteller hat sichergestellt, daß der Betroffene jederzeit vom Inhalt der Chipkarte Kenntnis nehmen kann.

Trotz dieser Sicherungen habe ich Sorge, daß mit dieser Technologie die Automation im Gesundheitswesen vorangetrieben wird mit der Gefahr, den "gläsernen Patienten" zu bekommen. Erhebliche Bedenken habe ich gegenüber den im Schlepptau der Krankenversichertenkarte propagierten, von Interessenverbänden und von der Industrie heftig geforderten Patienten- oder Gesundheitskarten. Die Chipkarte scheint angesichts ihres technischen Potentials erst Sinn zu machen, wenn auch Gesundheitsdaten aufgenommen werden. Gedacht ist an die Speicherung von Diagnosen, Behandlungen, Rezepturen, Impfungen, Allergien, Blutspender- oder Organspendereigenschaften. Die Rahmenbedingungen für diese Chipkarte (Art der gespeicherten Daten, Kreis der Inhaber, Folgen für deren Persönlichkeitsrechte, Lese- und Eingabeberechtigungen, technische Ausgestaltung und Rechtsgrundlagen) sind noch nicht einmal ansatzweise angedacht. Es besteht für die Betroffe-

nen ein starker Druck, die Chipkarte für die Verarbeitung medizinischer Daten zu akzeptieren und interessierten Dritten wie Ärzten, Apotheken, Versicherungen und Arbeitgebern weitgehenden Zugriff auf die so gespeicherten Daten zu gestatten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Entschließung zum Einsatz der Chipkarte im Gesundheitswesen verabschiedet und Forderungen notwendiger rechtlicher, organisatorischer und technischer Bedingungen formuliert (vgl. Anlage 10).

Die Chipkarte wird auch als die Lösung zur automationsgerechten Gebührenerhebung auf Autobahnen und im Nahverkehr propagiert. Ich habe mich über einen Feldversuch auf der Autobahn zwischen Bonn und Köln informiert, bei dem automationsunterstützte Beobachtungs- und Zahlungstechnik erprobt wird. In ihrer Entschließung vom 26./27. Oktober 1993 fordern die Datenschutzbeauftragten des Bundes und der Länder, daß nur Verfahren mit geringstmöglichem Eingriff in das allgemeine Persönlichkeitsrecht eine Chance zur Erprobung erhalten sollten. Bei der Einführung kartengestützter Zahlungssysteme muß sichergestellt sein, daß auch weiterhin eine "datenfreie Fahrt" möglich bleibt und der Gefahr, über die Chipkarte Bewegungsbilder der Autofahrer auswertbar zu machen, begegnet wird (vgl. Anlage 10).

Elektronikindustrie, Kreditwirtschaft, Verkehrsträger und Dienstleister arbeiten fieberhaft an einer Super-Chipkarte, die das Bargeld fast völlig ersetzen soll. Die bekannten Funktionen der Telefonkarte und der Kreditkarte mit und ohne Online-Autorisierung können dann mit Zusatzfunktionen wie der elektronischen Geldbörse (bargeldlose Bezahlung von Kleinbeträgen), Service für Diensteanbieter (z.B. für Bundesbahn, Lufthansa, Reisebüros), Gesundheitskarte, Zugangsausweis für Auto- und Haustüren, Zugriffskontrolle für Rechner, Daten und Dienste kombiniert werden. Gerade bei der Super-Chipkarte besteht die Gefahr, daß durch die Verrechnung unterschiedlicher Dienstleistungen Verhaltens- und Bewegungsprofile über ihre Benutzerinnen und Benutzer entstehen. Die Kombination unterschiedlicher Funktionen potenziert das Mißbrauchsrisiko. Es besteht die Gefahr der Auswertung aller Buchungen auf der Chipkarte, aber auch des Diebstahls und sonstiger Kartenkriminalität .

Ich beobachte aufmerksam Überlegungen und Feldversuche zur Einführung multifunktionaler Chipkarten. Vor der Entscheidung über den Echteinsatz der Chipkarte in einem neuen Anwendungsfeld sind Untersuchungen möglicher Alternativen, Analysen der von ihnen ausgehenden Gefahren für das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger und Darstellungen der technischen und organisatorischen Möglichkeiten zur Gewährleistung des Persönlichkeitsschutzes zu erstellen.

### 4.1.5 Folgerungen für Niedersachsen

Im letzten Tätigkeitsbericht habe ich bereits auf Trends der Informations- und Kommunikationstechnik sowie auf neue Gefahren für die Sicherung des informationellen Selbstbestimmungsrechts und die damit verbundenen Her-

ausforderungen für den Datenschutz aufmerksam gemacht (XI 4.1). Ich habe rechtliche Regelungen zur Steuerung der Informations- und Kommunikationsverarbeitung in der öffentlichen Verwaltung Niedersachsens gefordert und darauf hingewiesen, daß solche Vorschriften mehr als in der Vergangenheit technikbezogen ausgerichtet sein sollten. Das neue NDSG hat einiges davon aufgegriffen. So verpflichtet das Gesetz zur laufenden Überprüfung und Anpassung der Sicherungskonzepte entsprechend "dem Stand der Technik" (§ 7 Abs. 1 NDSG). Die Pflicht zur Technikfolgenabschätzung in § 7 Abs. 3 NDSG, die weitergehenden Dokumentationspflichten in § 8 NDSG und die Abruf-Regelung in § 12 NDSG sind begrüßenswerte Neuerungen.

Trotz der insofern noch fehlenden gesetzlichen Regelung werbe ich vehement für mehr Transparenz bei Planungs- und Entscheidungsprozessen. Grundrechtsrelevante technische Veränderungen dürfen nicht durch die Verwaltung oder durch sonstige Systembetreiber unter Ausschluß der Öffentlichkeit erfolgen. Eine Veröffentlichung der Ergebnisse der Technikfolgenabschätzung könnte ein geeigneter Ansatz zu größerer Transparenz sein. Hierzu gehören auch meine Vorschläge, die betroffenen Bürgerinnen und Bürger, die Mitglieder von Personalvertretungen sowie die Vertretung von gesellschaftlichen Interessenverbänden an Entscheidungen über den Einsatz von Informations- und Kommunikationstechnik in der öffentlichen Verwaltung zu beteiligen.

## 4.2 Technikfolgenabschätzung - wichtiger denn je

### 4.2.1 Der Gesetzgeber fordert Gefahrenanalyse und IuK-Sicherungskonzept

Vor zwei Jahren empfahl ich eine Technikfolgenabschätzung für den Einsatz von automatisierten Verfahren. Der Gesetzgeber griff dieses Anliegen erfreulicherweise auf. Nach der Regelung des § 7 Abs. 3 NDSG haben öffentliche Stellen zukünftig vor der Entscheidung über den Einsatz oder die wesentliche Änderung von automatisierten Verfahren zu prüfen, ob und in welchem Umfang mit der Nutzung der automatisierten Datenverarbeitung Gefahren für die Rechte der Betroffenen oder für die Wirkungsmöglichkeiten der Verfassungsorgane des Landes und der Organe der kommunalen Gebietskörperschaften verbunden sind (Bewertung der Technik). Automatisierte Verfahren dürfen nur eingesetzt oder wesentlich geändert werden, soweit derartige Gefahren durch technische oder organisatorische Maßnahmen wirksam beherrscht werden können (Gestaltung der Technik). Verfahrensalternativen zur angestrebten Lösung sind aufzuzeigen (Abschätzung der Technik). Das Ergebnis der Analyse und Bewertung sowie die Konsequenzen einschließlich Begründung sind aufzuzeichnen.

Mit der Technikfolgenabschätzung nach § 7 Abs. 3 NDSG sind die Gefahren moderner Informations- und Kommunikationstechnik aufzuzeigen, die "Restrisiken" bei einem geplanten Einsatz bestimmbar und die Angemessen-

heit konkreter Sicherungsmaßnahmen beurteilungsfähig zu machen. Beispiele für besondere Verletzlichkeiten und Abhängigkeiten sind Entwicklungen automatisierter Verfahren wie die Mobilkommunikation mit vielfachen Abhör- und Manipulationsmöglichkeiten, die elektronische Autobahnmaut (Electronic Roadpricing) mit der Aufzeichnung von Bewegungsprofilen, die satellitengestützte Kontrolle landwirtschaftlicher Subventionen, die weltweite Vernetzung von Rechnern als ideale Spielwiese für "Hacker" oder der Chipkarteneinsatz für eine bunte Anwendungspalette und Reizen für Neugier, Sicherheit und Kriminalität.

Ich bin überzeugt, daß sich mit der Technikfolgenabschätzung nach § 7 Abs. 3 NDSG neben dem Hauptziel der Gewährleistung der Datenschutzvorschriften als Nebenziele auch Fehlentscheidungen bei der Auswahl von automatisierten Verfahren vermeiden und wirtschaftlich vertretbare Lösungen finden lassen. Natürlich ist die Regelung nicht in der Lage, alle denkbaren Aspekte der Technikfolgen abzudecken, z.B. Fragen der Lebensqualität, der Ökologie, der Arbeit und der Sicherheit. Die Regelung erfaßt aber wohl die gesamte informationstechnische Seite von Folgenabschätzungen und stellt einen wichtigen Beitrag in der gesellschaftspolitischen Debatte über die Gestaltung neuer Techniken und über die Technikfolgen dar.

Ich empfehle, die Technikfolgenabschätzung nicht auf eine Gefahrenanalyse zu beschränken, sondern den Nutzen der angestrebten automatisierten Datenverarbeitung, Verfahrensalternativen und denkbare Gefahren alternativer Lösungen aufzeigen. Sie hat die Gefahren für die Rechte der Betroffenen und für die Wirkungsmöglichkeiten der Organe offenzulegen. Die Bewertung der Technik betrifft damit das gesamte, komplexe Spannungsfeld Individuum - Staat, Mitarbeiter - Behörde, Legislative - Exekutive, Technik - Umwelt. Technische Machbarkeit sowie soziale und ökologische Vertretbarkeit sollten dabei ebenso Kriterien sein wie die Fragen der Wirtschaftlichkeit und Angemessenheit.

Die Verwaltungsvorschriften zum NDSG regeln, daß eine Technikfolgenabschätzung für automatisierte Verfahren dann durchzuführen ist, wenn personenbezogene Daten verarbeitet werden sollen, deren Mißbrauch entweder Existenz, Leben oder Freiheit der Betroffenen gefährden würde, oder wenn personenbezogene Daten verarbeitet werden sollen, deren Mißbrauch die Betroffenen in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen nicht unerheblich beeinträchtigen kann, und wenn dabei der Aufbau eines vernetzten Rechnersystems mit mindestens 20 Rechnereinheiten oder Bildschirmgeräten geplant ist.

Die Regelung des § 7 Abs. 3 Satz 2 NDSG, der die wirksame Beherrschung potentieller Gefahren durch technische oder organisatorische Maßnahmen fordert, bietet die Chance zur aktiven Technikgestaltung. Das Sicherheitskonzept für automatisierte Verfahren sollte unter anderem Vorschläge zur kriteriengerechten Gestaltung der Technik, der Organisation und der rechtlichen Rahmenbedingungen enthalten.

4.2.2 Der niedersächsische Weg: "Learning by doing"

Die niedersächsische Regelung zur Technikfolgenabschätzung ist neu und bislang nahezu einmalig. Lediglich in Berlin und in Schleswig-Holstein sind ähnliche Regelungen vorhanden. Doch auch dort liegen praktisch noch keine Erfahrungen vor. Deshalb gilt es, die Vorschrift zur Technikfolgenabschätzung mit "Leben zu füllen". Klärungsbedürftig sind z.B. die Untersuchungstiefe und die Dokumentationspflichten. Hierbei sollte ein vertretbarer Kompromiß zwischen theoretisch Denkbarem und praktisch Leistbarem gefunden werden. § 7 Abs. 3 NDSG ermöglicht es, interessierte Behörden, Organe und Institutionen in das Verfahren mit einzubeziehen.

Auch wenn gesetzlich geforderte Technikfolgenabschätzung noch sehr jung ist, so gibt es doch zahlreiche Institutionen, die sich bereits mit Technikfolgenabschätzungen und mit Sicherheitskonzepten beschäftigt haben. Um vorhandenes Wissen zu sammeln und aus Erfahrungen zu lernen, habe ich Experten aus Wissenschaft, Wirtschaft und Verwaltung im Herbst 1993 zu einem Geprächskreis "Theorie und Praxis der Technikfolgen-Abschätzung" eingeladen, um Chancen aber auch Probleme bei der Durchführung von Technikfolgenabschätzungen auszuloten. Auf dem Workshop wurden u.a. verschiedene Methoden der Technikfolgenabschätzung dargestellt, die von theoretisch erstellten Abschätzungen bis hin zu Pilotversuchen und Simulationsstudien reichten. Die Expertenrunde war sich einig, daß es nicht ausreicht, die Entwicklung zu einer immer perfekteren Informationsgesellschaft und die wachsenden Herausforderungen und Gefahren für das allgemeine Persönlichkeitsrecht lediglich durch Ge- und Verbote gesetzlich zu regeln. Es bedarf vielmehr der den Datenschutz präventiv sichernden Gestaltung der Technik.

Wegen des Fehlens direkt übernehmbarer Konzepte kann für Niedersachsen die Empfehlung nur lauten: "learning by doing". Ich habe deshalb vorgeschlagen, ein Pilotprojekt auszusuchen und in einem interdisziplinär besetzten Arbeitskreis mit Vertretern aus Verwaltung und Wissenschaft eine erste Technikfolgenabschätzung zu erarbeiten.

Dieser Vorschlag wurde aufgegriffen. Als Pilotfeld ist das Projekt "MINiNET/ X.400 (elektronische Post) in der Landesverwaltung" ausgesucht worden. Es hat sich ein Arbeitskreis gebildet, an dem die beteiligten Ressorts (Innenministerium, Wirtschaftsministerium, Staatskanzlei), eine Vertretung von den Personalräten bzw. vom Hauptpersonalrat der Ressorts, das Niedersächsische Landesverwaltungsamt und ich teilnehmen. Der Arbeitskreis wird von der Zentralen Stelle für Organisationsangelegenheiten im Innenministerium geleitet. Um die Erfahrungen aus wissenschaftlichen Untersuchungen zur Technikfolgenabschätzung nutzen zu können, wurde Prof. Roßnagel von der Gesamthochschule Kassel um Unterstützung gebeten. Der Arbeitskreis soll eine angemessene Methodik der Technikfolgenabschätzung auswählen, die Technikfolgenabschätzung für das Pilotfeld durchführen und konkrete Handlungsempfehlungen für das Projekt sowie für zukünftige Technikfolgenabschätzungen erarbeiten.

Der Arbeitskreis erstellt zur Zeit eine Technikfolgenabschätzung, die im wesentlichen aus den Teilen Gefahrenanalyse, Risikoanalyse, Sicherheitskonzept, Restrisiko-Bewertung und Entscheidungsvorschlag besteht. Diese Gliederung lehnt sich an das Sicherheitshandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an. Ich habe zusätzlich eine Simulation von Angriffsversuchen auf das geplante Verfahren vorgeschlagen.

Da mehrere Projekte in Niedersachsen geplant und zu erwarten sind, bei denen eine Technikfolgenabschätzung notwendig ist, sollte das Pilotprojekt schnell abgeschlossen werden. Die Musterdokumentation soll möglichst konkrete Hilfen für Nachfolgeprojekte bieten. Das Ergebnis der Technikfolgenabschätzung sollte politischen Vertreterinnen und Vertretern und einer interessierten Öffentlichkeit zugänglich gemacht werden.

## 4.3 Wartung und Fernwartung

### 4.3.1 Datenschutzrechtliche Einordnung

Die Voraussetzungen, unter denen die Weitergabe personenbezogener Daten im Rahmen der Wartung und Fernwartung zulässig ist, sind in den meisten Datenschutzgesetzen nicht eindeutig geregelt. Dies führt dazu, daß diese teilweise als Datenübermittlung, überwiegend jedoch als Datenverarbeitung im Auftrag angesehen wird. Die Einstufung als Datenverarbeitung im Auftrag ist am ehesten geeignet, umfassende technische und organisatorische Sicherungsmaßnahmen durchzusetzen (vgl. Anlage 15). Einschränkungen der Zulässigkeit der Verarbeitung personenbezogener Daten im Auftrag können sich insbesondere ergeben

- aus verfassungsrechtlichen Hindernissen (z.B. die Übertragung des Netzwerkmanagements eines Landesverwaltungsnetzes),
- durch entgegenstehende spezialgesetzliche Vorgaben (z.B in einem Landeskrankenhausgesetz) oder
- durch zu wahrende Berufsgeheimnisse (vgl. § 203 Abs. 1 StGB).

Meine Auffassung, die (Fern-)Wartung als besondere Auftragsverarbeitung bzw. -nutzung einzustufen (X 4.4, XI 4.3), wird von der Landesregierung geteilt. Eine von mir angeregte Präzisierung der Regelungen zur Wartung wird jedoch dort nicht für erforderlich gehalten, da dies keinen zusätzlichen Sicherheitsgewinn brächte. Auch wenn mich diese Argumentation nicht überzeugt, bin ich bereit, vor einem erneuten Vorstoß zunächst einmal Erfahrungen mit dem neuen NDSG zu sammeln.

### 4.3.2 Fernwartung bei einer Beratungsstelle für Kinder, Jugendliche und Eltern

Die Beratungsstelle für Kinder, Jugendliche und Eltern eines Landkreises wehrte sich gegen die beabsichtigte Fernwartung ihres eigenen PC-Netzes durch DV-Spezialisten des Hauptamtes. Der Leiter der Beratungsstelle meldete Bedenken gegen diese Lösung an, da die zu speichernden Daten einem besonderen Vertrauensschutz unterliegen. An die Datensicherung seien hohe Anforderungen zu stellen. Diese Bewertung teile ich. Ich mußte aber mitteilen, daß eine solche Wartungslösung nicht etwa grundsätzlich unzulässig sei.

Ich habe für die geplante externe Wartung vorgeschlagen, den Verbindungsaufbau nur durch die Beratungsstelle selbst erfolgen zu lassen und technisch auszuschließen, daß bei dem Fernwartungsvorgang von außen auf personenbezogene Daten der Beratungsstelle zugegriffen werden kann. Die Kreisverwaltung hat salomonisch entschieden und mit der Systemverwaltung einen Mitarbeiter der Beratungsstelle selbst beauftragt. Nur bei auftretenden Systemfehlern, die nicht vom örtlichen Systemverwalter selbst behoben werden können, erfolgen Fehlersuche und -behebung gemeinsam und vor Ort. Nach der Fehlerbehebung wird das Supervisor-Kennwort geändert. Ein Streit um die Zulässigkeit der Fernwartung konnte so vermieden werden.

## 4.4 Personal Computer (PC)

### 4.4.1 PC-Grundschutz

In meinen Tätigkeitsberichten habe ich wiederholt auf die Datensicherungsproblematik bei Personal Computern hingewiesen. In X 4.5 habe ich wichtige Maßnahmen zur Datensicherung aufgeführt. Bei Auswahl und Umsetzung dieser Maßnahmen muß berücksichtigt werden, in welchem Umfang Daten verarbeitet werden und wie sensibel diese Daten sind. Es gibt daneben eine Reihe von Maßnahmen, die ausnahmslos bei jedem PC-Einsatz mit personenbezogenen Daten vorgenommen werden sollten. Dieser "Grundschutz" muß bei Bedarf, z.B. bei erhöhter Sensibilität der Daten, durch zusätzliche Maßnahmen ergänzt werden. So gehören z.B. der Paßwortschutz und die Backup-Datensicherung zu den Grundschutzmaßnahmen, die Verschlüsselung der Daten oder die Protokollierung zu den Zusatzmaßnahmen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt z.Zt. ein IT-Grundschutz-Handbuch, in dem die Grundschutzmaßnahmen zu vielen Bereichen der Informationstechnik, auch für den Einsatz von Personal Computern beschrieben werden. Das BSI-Handbuch enthält wertvolle Hinweise und Hilfen. Mit dem derzeitigen Stand des Maßnahmenkatalogs zum PC-Grundschutz stimme ich in allen wesentlichen Punkten überein.

Zum Grundschutz beim PC-Einsatz gehören bauliche, technische sowie organisatorische Maßnahmen. Hinsichtlich der Sicherheit der Hard- und Software-Ausstattung zeigt sich eine erfreuliche Entwicklung. Waren anfangs überhaupt keine Sicherungsmaßnahmen verfügbar, so ist jetzt ein breites Angebot an Zusatz-Hard- und Software vorhanden. Die Grundschutzforderungen an die Hard- und Software sind:

1. ein sicherer Paßwortschutz,
2. eine Pausenfunktion mit Bildschirmsperre,
3. ein geeignetes Virensuchprogramm.

Bei den meisten neueren PC kann unterhalb der Betriebssystemebene, im Rahmen des "BIOS-Setup", ein Paßwortschutz eingerichtet werden, der eine recht hochwertige Sicherheit bietet. Wird auf dem Personal Computer MS WINDOWS (ab Version 3.1) eingesetzt, besteht die Möglichkeit, eine Pausenfunktion mit Bildschirmsperre einzurichten. Diese kann allerdings nicht per Tastendruck aktiviert werden, sondern schaltet sich automatisch nach einer einstellbaren Zeitspanne ein, wenn keine Tastatur- oder Maus-Aktion erfolgt ist. Auch arbeitet diese nur im Zusammenhang mit Windows-Anwendungen korrekt und nicht bei DOS-Programmen. MS WINDOWS 3.11 bietet zudem ein Virensuchprogramm (im Rahmen des Datei-Managers). Auf die Einrichtung einer Bildschirmsperre kann verzichtet werden, wenn der Rechner bei Verlassen des Raumes regelmäßig ausgeschaltet oder der Raum verschlossen wird. Aber - Hand aufs Herz - wer hält eine solche Forderung schon konsequent durch?

Die baulichen und organisatorischen Grundschutzmaßnahmen sind:

1. geschlossene Erdgeschoßfenster bei Abwesenheit,
2. kontrollierter Zutritt zum PC-Büroraum (z.B. durch Verschluß der Bürotür oder der Haustür),
3. fachgerechte Datenträgerverwaltung (Kennzeichnung und gesicherte Aufbewahrung),
4. festgelegte Regelungen bei Wartungs- und Reparaturarbeiten (nur vertrauenswürdige Personen, Beaufsichtigung),
5. Nutzungsverbot nicht freigegebener Software sowie sporadische Überprüfung des Softwarebestandes,
6. datenschutzgerechte Entsorgung von Datenträgern,
7. gesicherte Hinterlegung von wichtigen Paßwörtern,
8. ausreichende Fachkunde der PC-Nutzer (auch in Datensicherungsfragen, z.B. durch Schulung),
9. regelmäßiges Kopieren der gespeicherten Daten und sichere Lagerung der Backup-Datenträger (z.B. wöchentlich in drei Generationen).

Werden in einer Behörde oder einem Unternehmen mehrere PC eingesetzt, empfiehlt sich die Erstellung einer Dienst- oder Arbeitsanweisung.

### 4.4.2 Der private PC im Dienst - ein Widerspruch in sich

In vielen Bereichen der niedersächsischen Landesverwaltung ist eine Tendenz zum Einsatz privater PC erkennbar. Ich habe frühzeitig gegenüber den

Ministerien und in der Öffentlichkeit auf datenschutzrechtliche Probleme einer derartigen "Privatisierung" öffentlicher Aufgabenerledigung aufmerksam gemacht und Bedenken gegen einen ungenehmigten Einsatz von privaten Rechnern für dienstliche Zwecke geäußert. Die Datenschutzbeauftragten des Bundes und der Länder, der Bundesrechnungshof, das Bundesamt für Sicherheit in der Informationstechnik, das Niedersächsische Innenministerium, der Interministerielle Arbeitskreis Informations- und Kommunikationstechnik (IMA) und der Niedersächsische Landesrechnungshof teilen meine Bedenken. Sie fordern übereinstimmend, die dienstliche Nutzung privater Hard- und Software grundsätzlich zu untersagen und unabweisbare Ausnahmen von einer Prüfung der datenschutzrechtlichen Unbedenklichkeit im Einzelfall abhängig zu machen. Diese Grundsätze wurden in der Stellungnahme der Landesregierung zu meinem XI. TB ausdrücklich bestätigt.

Ich bin stets um einen Ausgleich der verschiedenen Interessen durch praxisgerechte Lösungen bemüht. Sofern die Ministerien bisher Regelungen zur dienstlichen Verwendung privater PC getroffen haben, gehen diese von einer (ausnahmsweisen) Zulassung im Einzelfall aus. So wurden in Abstimmung mit mir für den Bereich der Landespolizei in einem Erlaß restriktive Auflagen und Bedingungen festgeschrieben, nach denen auch die Einhaltung rechtlicher und dienstlicher Vorgaben sichergestellt sowie die datenschutzrechtliche Kontrolle bei diesen privaten Rechnern geregelt werden.

Ein Landesministerium beabsichtigte, die Prüfung und Genehmigung des Einsatzes von Privat-PC durch eine stillschweigende Duldung zu ersetzen. Dies wurde damit begründet, daß die Vorstellungen der Bediensteten nach "zeitgemäßem" Arbeitsumfeld durch Technikeinsatz wegen fehlender Haushaltsmittel nicht erfüllt werden könnten. Das Genehmigungserfordernis sei dienstrechtlich problematisch, da sich der Dienstherr mit einer erklärten Genehmigung einem nicht abschätzbaren Haushaltsrisiko aussetzen würde. Ich habe ebenso wie das Innenministerium erhebliche Bedenken gegen eine solche Duldungsregelung.

Beim Einsatz von privaten Rechnern zur Wahrnehmung dienstlicher Aufgaben ist die Dienststelle datenverarbeitende Stelle im Sinne des § 3 Abs. 3 NDSG. Sie hat die Einhaltung der Datenschutzvorschriften zu gewährleisten und die mit der Datenverarbeitung Beauftragten über die Anforderungen des Datenschutzes zu unterrichten. Zu den besonderen Pflichten der datenverarbeitenden Stelle gehören die Auskunft gegenüber Betroffenen, das Anlegen der Dateibeschreibungen und des Geräteverzeichnisses, die Meldungen zum Register aller automatisierten Dateien und die Gewährleistung der Datensicherheit. Auch beim Einsatz privater Rechner sind gemäß § 7 NDSG die erforderlichen technischen und organisatorischen Maßnahmen zu treffen. Die genehmigende Dienststelle hat zu prüfen und darüber zu entscheiden, ob die beabsichtigten Datensicherungsverfahren des privaten PC den Anforderungen des NDSG entsprechen. Mit der Duldungsregelung wäre die datenverarbeitende Stelle nicht in der Lage, ihren Pflichten aus dem NDSG nachzukommen.

### 4.4.3 Prüfkonzept für PC-Netze am Beispiel von NOVELL NetWare 3.11/3.12

Alleinstehende Personal Computer werden zunehmend miteinander vernetzt. Voraussetzung hierfür ist die Installation eines Netzwerk-Betriebssystems. Außerdem erfolgt im allgemeinen die Einrichtung eines zentralen Rechners im Netz, dem sogenannten Server oder Fileserver. In der Vergangenheit haben sich sehr viele Stellen für den Einsatz von NOVELL NetWare 3.11 oder 3.12 als Netzwerk-Betriebssystem entschieden. NOVELL NetWare 3.11/3.12 bietet diverse Möglichkeiten, um eine datenschutzgerechte Verarbeitung von personenbezogenen Daten sicherzustellen. Ich habe ein Datenschutzprüfkonzept für Fileserver mit dem Netzwerk-Betriebssystem NOVELL NetWare 3.11/3.12 in Form eines Fragenkataloges erstellt. Das Prüfkonzept ist zur Eigenkontrolle datenverarbeitender Stellen geeignet und wird an Interessierte abgegeben. Im folgenden werden einige wichtige Punkte des Prüfkonzeptes und erste Erfahrungen aus der Prüftätigkeit wiedergegeben.

Um zu verhindern, daß sich eine Benutzerin oder ein Benutzer unberechtigt beim Server bzw. im Netz anmeldet, stehen im wesentlichen folgende Systemfunktionen zur Verfügung:

- "Account Balance/Restrictions"
  Im Rahmen dieser Funktionen wird festgelegt, daß sich jeder Benutzer unter seiner Kennung mit einem persönlichen Paßwort anzumelden hat. Außerdem werden die Paßwortoptionen, wie z. B. Paßwort-Mindestlänge, Paßwortwiederholung und Paßwortalterung eingestellt. Es empfiehlt sich, diese Einstellungen standardmäßig für alle Benutzer ("Default Account Balance/Restrictions") und nicht einzeln für jeden Benutzer vorzunehmen.
- "Intruder Detection/Lockout"
  Durch Einstellung dieser Funktion wird ein "Eindringling", der unter einer Kennung eine bestimmte Anzahl erfolgloser Anmeldeversuche mit einem ungültigen Paßwort vornimmt, für diese Kennung eine vorgegebene Zeit lang gesperrt.

Hat sich ein Benutzer berechtigt im Netz angemeldet, sollte er grundsätzlich nur den Zugriff auf Dateien haben, die er zur Erledigung seiner Fachaufgabe benötigt. Unter NOVELL NetWare 3.11/3.12 besteht die Möglichkeit, seinen Zugriff auf Dateien und Verzeichnisse über verschiedene "Rechte" zu beschränken. Dem Benutzer bzw. der Benutzerin kann z.B. eine Lese- oder Schreibberechtigung für Dateien oder ein Recht zum Sichten eines Verzeichnisses erteilt werden. Außerdem können Dateien mit "Attributen" versehen werden, um z.B. ein Kopieren oder Löschen der Datei zu verhindern.

Verantwortlich für die datenschutzgerechte Einstellung der Systemfunktionen ist der Systemadministrator, der sogenannte Supervisor. Hierzu arbeitet dieser unter einer Kennung mit sehr weitreichenden Befugnissen. Es ist deshalb sehr wichtig, daß der Systemadministrator über die notwendige Fachkunde und Zuverlässigkeit verfügt. NOVELL NetWare-Netze sind häufig aus einer Ansammlung einzelner PC heraus aufgebaut worden, weil der

Wunsch nach einem gemeinsamen Zugriff auf Daten von den einzelnen Rechnern aus entstanden ist. Zum Systemadministrator wird in diesen Fällen häufig eine Person bestimmt, die über eine gewisse Erfahrung an ihrem Einzelplatz-PC verfügt. Es ist aber weitaus schwieriger, ein gesamtes Netz zu administrieren als einige Einzelplatz-PC zu betreuen. Meine Prüfungserfahrungen zeigen daher auch, daß die Fachkunde dieser Systemadministratoren oft nicht ausreicht. Daraus resultieren bei PC-Netzen Risiken, die im Großrechnerbereich oder auch im UNIX-Bereich nicht in diesem Maße auftreten. Dem kann durch rechtzeitige und umfassende Schulung der designierten Administratorinnen und Administratoren entgegengewirkt werden. Beim Aufbau und bei der Verwaltung des Netzes ist der Systemadministrator auf eine enge Zusammenarbeit mit dem Fachbereich angewiesen. Maßgeblich für die von ihm vorzunehmenden Systemeinstellungen sind die fachlichen Aufgaben, die die einzelne Benutzerin bzw. der einzelne Benutzer wahrzunehmen hat, sowie die Sensibilität der in dem Aufgabenbereich verarbeiteten Daten. Dies verlangt eine enge Zusammenarbeit zwischen Systemadministrator und Anwendenden.

Die datenverarbeitende Stelle hat regelmäßig die datenschutzgerechte Einrichtung des Netzes sicherzustellen. Die oder der Datenschutzbeauftragte kann dies kontrollieren, indem sie oder er die zum Netzwerk vorhandene Dokumentation über die Benutzerinnen und Benutzer mit den vergebenen Rechten unter Datenschutzgesichtspunkten einsieht. Außerdem sollte sie oder er stichprobenartig einen Ausdruck der Ergebnisse des "SECURITY"-Befehls zusammen mit dem Systemadministrator überprüfen. Hieraus kann man erkennen, ob es Benutzerinnen oder Benutzer gibt, die sich ohne Paßwort anmelden oder mit Supervisor-Rechten ausgestattet sind. Eine standardmäßige Funktion zur Protokollierung von System- und Benutzeraktivitäten gibt es bei NOVELL NetWare 3.11/3.12 bedauerlicherweise nicht. Hierfür muß Zusatzsoftware beschafft werden.

## 4.5 Defizite bei der UNIX-Systemverwaltung

Unter XI 4.5 habe ich darauf hingewiesen, daß durch schlecht verwaltete UNIX-Betriebssysteme hohe Sicherheitsrisiken entstehen. Dabei habe ich meinen UNIX-Prüfkatalog vorgestellt, der auch Systemverwalter und Datenschutzbeauftragte in die Lage versetzt, ihr UNIX-System auf "Herz und Nieren" zu prüfen und so auf einem ausreichend hohen Sicherheitsniveau zu betreiben. Von dem Angebot, den Prüfkatalog anzufordern, wird zahlreich Gebrauch gemacht.

Im Berichtszeitraum habe ich den Bereich der UNIX-Systemverwaltung als einen Schwerpunkt mit der detaillierten Außenprüfung von acht Firmen und Behörden gewählt (vgl. 3.8 und 35.2). Die Prüfungen wurden in Form von Befragungen der Rechenzentrumsleitung, der Systemverwaltung und des Datenschutzbeauftragten vor Ort sowie in Form von Kontrollen an den Rechnern vorgenommen.

Bemerkenswert war die Unterschiedlichkeit der vorgefundenen UNIX-Systeme. Dies bezieht sich nicht nur auf die große Zahl verschiedener UNIX-Versionen und -Derivate (UNIX V.3, UNIX V.4, SINIX, ULTRIX, AIX, SCO-UNIX, HP-UX...) bzw. auf die noch größere Zahl an Herstellerfirmen der Rechner, sondern auch auf die vorgefundenen Rechnerarchitekturen. Neben klassischen Mehrplatzsystemen wurden Client-Server-Systeme und Cluster vorgefunden, z.T. als reine UNIX-Systeme, z.T. in Verbindung mit Großrechnern, DOS-basierenden PC oder Apple MacIntosh-Rechnern.

Auch die geprüften Stellen unterschieden sich deutlich, z.B. in der Größe und der Zielsetzung. So waren sowohl kleinere Stellen mit nur 30 Anwenderinnen und Anwendern als auch wesentlich größere Stellen dabei. Sehr ähnlich war dagegen die Sensibilität der verarbeiteten Daten, die bei allen Stellen zumindest in Teilen der Schutzstufe C (Gefährdung des Ansehens) zugeordnet wurden. In einem Fall mußte auch die Verarbeitung von Daten der Schutzstufe D (Gefährdung der Existenz) angenommen werden. Obwohl das Prüfkonzept nicht sämtliche Besonderheiten der Derivate und der Rechnerarchitekturen berücksichtigen kann, war dennoch eine detaillierte Prüfung aller Systeme möglich.

Die Ergebnisse der Prüfungen geben Anlaß zur Sorge, auch wenn dabei keine "offenen Scheunentore" oder Systemverwalter, die grob fahrlässig oder vorsätzlich Mißbrauch betreiben, vorgefunden wurden (bislang habe ich immer "Systemverwalter" und nicht "Systemverwalterinnen" angetroffen). Wohl aber ist erkennbar, daß Systemverwalter und sonstige Verantwortliche Datensicherungsaufgaben häufig sträflich vernachlässigen (vgl. Tab. 1).

Besonders augenfällig waren Mängel im Bereich der Protokollierung auf Betriebssystemebene. Diese an sich sehr wirkungsvolle gesetzlich explizit geforderte Maßnahme der Datensicherung (siehe "Eingabekontrolle") existiert bei den meisten Stellen schlicht und einfach nicht. Vielen Systemverwaltern war häufig überhaupt nicht bekannt, was in ihrem System protokolliert wurde. Die standardmäßig eingerichteten Systemprotokollierungen wurden vom Rechner durchgeführt und in den entsprechenden Dateien seit Installation des Rechners gespeichert. In solchen Fällen konnte von einer datenschutzgerechten Kontrolle der Protokolle oder einer fristgerechten Löschung der (personenbezogenen) Daten nicht die Rede sein. Auch der Umfang der Protokollierung auf Systemebene war in keinem Fall so eingestellt, daß ich zufrieden sein konnte, In meinem UNIX-Prüfkonzept sind weitgehend Forderungen aufstellt, die mit jedem Standardsystem erfüllt werden können. Nur in wenigen Fällen werden Maßnahmen gefordert, die Zusatzsoftware notwendig machen. Gerade die Protokollierung ist eine solche Ausnahme; hier liegen die Defizite leider bei UNIX selbst. Sie sind vor allem darauf zurückzuführen, daß nur wenige UNIX-Vertreiber bereit sind, ihre Produkte einer Evaluierung nach anerkannten Sicherheitskriterien zu unterziehen. Zur Ehrenrettung von UNIX sei erwähnt, daß in dem wohl gängigsten netzwerkfähigen Konkurrenzprodukt aus dem PC-Bereich, Novell Netware 3.11, im Grunde überhaupt keine Protokollierung vorgesehen ist (vgl. Kap. 4.4.3).

| Prüfaussage | nicht erfüllt bei (Anzahl der Stellen von 8) |
|---|---|
| Das Super-User-Paßwort ist nur den Systemverwaltern bekannt. | 7 |
| Es sind ausreichende schriftliche Dienst- oder Arbeitsanweisungen vorhanden. | 8 |
| Beim Login wird das Datum des letzten Login angezeigt. | 4 |
| Anwender besitzen im Normalfall keinen Betriebssystemzugang. | 2 |
| Der PATH-Befehl in der Startdatei läßt das System zuerst in den Verzeichnissen mit Systembefehlen suchen. | 4 |
| Die Mindestpaßwortlänge beträgt 6 Zeichen. | 3 |
| Die Anzahl der Fehlversuche ist auf maximal 5 begrenzt. | 4 |
| Es ist eine Pausenfunktion installiert, die Rechner oder Terminals bis zur Paßworteingabe sperrt. | 7 |
| Die Paßwortdatei /etc/passwd enthält nur dem Verwalter bekannte und von ihm vorgesehene Einträge. | 1 |
| Systemaktivitäten werden im ausreichendem Maße protokolliert. | 8 |
| Die Systemprotokolle werden regelmäßig kontrolliert. | 6 |
| Die Protokolle werden spätestens nach einem Jahr gelöscht. | 5 |
| Super-User-Paßwörter werden nicht über Fernleitungen übertragen. | 3 |

Tab. 1. Ausgesuchte Punkte des UNIX-Prüfkatalogs und deren Umsetzung bei geprüften Stellen.

Die UNIX-Prüfungen haben auch Defizite beim Umgang mit Paßworten offengelegt. Dies bezieht sich nicht nur auf die Gestaltung des Verfahrens wie die Festlegung einer Paßwort-Mindestlänge oder der Anzahl der zulässigen Fehlversuche. Mißstände wurden auch beim Umgang mit den Paßwörtern der Systemverwalter selbst festgestellt. Wegen der allmächtigen Befugnisse des "Super-Users" unter UNIX halte ich es für wichtig, daß das Super-User-Paßwort nur dem Systemverwalter bekannt ist. Auch Vertreter bzw. Vertreterinnen sollten normalerweise nicht eingeweiht sein. Für den Notfall genügt es, das Super-User-Paßwort gesichert und versiegelt zu hinterlegen, z.B. in einem Tresor. Dieses Verfahren habe ich bei keiner Prüfung vorgefunden. Fast immer kannten zumindest auch die Vertreter oder Vertreterinnen das Super-User-Paßwort, häufig noch weitere Personen. Aber auch für Paßwort-Mängel gilt, daß sie nicht UNIX-spezifisch sind, sondern ebenso in anderen Systemumgebungen anzutreffen sind.

Ich empfehle dringend, wichtige organisatorische Regelungen bei der Nutzung und der Systemverwaltung von UNIX-Systemen in einer Dienst- oder Arbeitsanweisung schriftlich festzuhalten. Eine schriftliche Anweisung hilft nicht nur, Festlegungen für längere Zeiträume aufrechtzuerhalten ("Welche Protokolldateien sollte ich regelmäßig kontrollieren?"), sie hilft z.B. dem Systemverwalter auch, datenschutzrelevante Maßnahmen gegenüber unwilligen Mitarbeiterinnen und Mitarbeitern, dies können auch Vorgesetzte sein, durchzusetzen ("Sie sind ein normaler Anwender des Systems, daher darf ich Ihnen keine Shell-Berechtigung geben"). In Sachen Dienst- oder Arbeitsanweisung zeigen meine Prüfungen ein besonders trauriges Ergebnis. Bei keiner Stelle war eine ausreichende schriftliche Anweisung vorhanden. Es gibt aber Hoffnung, daß sich dies ändert. Mittlerweile sind die ersten Anweisungen für die überprüften UNIX-Systeme in Kraft; weitere werden in Kürze folgen. Regelungsinhalte sind meinem UNIX-Prüfkatalog zu entnehmen.

Meine Prüferfahrungen belegen, daß Defizite in der Datensicherung in vielen Fällen auf eine Überlastung der Systemverwaltung zurückzuführen sind. Bei Systemen mit bis zu 100 Anwenderinnen und Anwendern ist häufig nur ein Systemverwalter vorhanden, der - auf sich allein gestellt - nicht nur die Wartung des Systems durchführen soll, sondern auch den Einkauf neuer Geräte und deren Neuinstallation sowie das Netzmanagement vorzunehmen hat. Außerdem werden ihm häufig noch zusätzliche Aufgaben auferlegt, z.B. die Betreuung des DOS-PC-Bereichs oder die Unterstützung anderer IuK-Projekte. Systemverwalter werden häufig allein gelassen; dabei stellen sie nicht selten einen "Flaschenhals" in der Behörden- oder Unternehmensorganisation dar. Ein DV-System kann nur dann effizient sein sowie Datensicherung und Datenschutz gewährleisten, wenn die Systemverwaltung und -betreuung über ausreichende "manpower" verfügen. Hier haben noch viele Behörden und Unternehmen Nachholbedarf, um die von ihnen selbst geschaffene neue IuK-Welt rationell und gesetzestreu zu nutzen.

Bei keiner der überprüften Stellen war ich restlos zufrieden. Allerdings gab es deutliche Unterschiede des vorgefundenen Sicherheitsniveaus. Dies zeigt sich auch an der unterschiedlich hohen Anzahl der Forderungen und Empfehlungen, die ich aufgrund der einzelnen Prüfungen abgeben mußte (von 5 bis 24 pro Stelle). Die Anzahl meiner Forderungen war im öffentlichen Bereich tendenziell höher als im nicht-öffentlichen. Zu den negativen Fällen zählt leider gerade eine nicht-öffentliche Stelle, bei der von der Verarbeitung besonders sensibler Daten (Schutzstufe D) ausgegangen werden mußte. Hier habe ich vorgeschlagen, auf die Verarbeitung dieser hochsensiblen Daten im vorhandenen UNIX-System gänzlich zu verzichten.

Als Lichtblick sehe ich das Bemühen der meisten Stellen an, die von mir aufgestellten Forderungen und Empfehlungen umzusetzen. Dort, wo noch Defizite bestehen, werde ich nicht locker lassen, bis auch diese behoben sind. Es bleibt zu hoffen, daß sich auch die öffentlichen und nicht-öffentlichen Stellen aus eigenem Interesse um eine sichere UNIX-Systemverwaltung bemühen, die von mir bislang nicht geprüft worden sind. Auch zur Ei-

genkontrolle der datenverarbeitenden Stellen bietet sich mein UNIX- Prüfkonzept besonders an.

## 4.6 Automation in der Landesverwaltung

### 4.6.1 BÜROMIN = Bürokommunikation in den Ministerien

Die Ausstattung der Minsterien mit dem Bürokommunikationssystem Alis hat sich zwar nur langsam, aber dennoch kontinuierlich fortgesetzt. Durch den Beschluß der Landesregierung vom November 1993, in den Ministerien eine flächendeckende Bürokommunikation einzuführen, wurde ein neuer Schub ausgelöst. Es gibt jetzt nicht nur eine klare Vorgabe für die zukünftige IuK-Landschaft in den Ministerien, sondern auch Mittel in Höhe von rund 23,2 Mio. DM, um in den nächsten drei Jahren mit der Erstausstattung aller in Frage kommenden Arbeitsplätze das Werk zu vollenden.

Das Datenschutz- und Datensicherungskonzept für BÜROMIN hat durch enge und gute Zusammenarbeit mit dem Innenministerium klare Konturen bekommen. Der überwiegende Teil meiner nach einer Prüfung im Oktober 1992 erhobenen Forderungen wurde erfüllt. Lediglich in den nachfolgenden Teilbereichen steht noch eine Erledigung aus:

- Es sollte überprüft werden, inwieweit Zusatzsoftware mit abgestuften Systemverwalterbefugnissen, z.B. eine menügesteuerte Benutzerverwaltung, sinnvoll eingesetzt werden kann.
- Die Paßwort-Gestaltung und -Verwendung ist zu verbessern. Allen Benutzerinnen und Benutzern sollte während des Logins das Datum des letzten Logins bzw. des letzten erfolglosen Logins angezeigt werden.
- Es sollte eine automatisierte Sperrung der APC bei längerer Nichtbenutzung der Tastatur oder der Maus (z.B. 10 Minuten) installiert werden, die eine Paßworteingabe vor der Freigabe des APC erzwingt.
- Es wird empfohlen, allen Benutzerinnen und Benutzern eine Verschlüsselungsfunktion zur Datenspeicherung und -übertragung als Option anzubieten.
- Protokolldateien sollten mindestens wöchentlich kontrolliert werden. Der interne Datenschutzbeauftragte sollte gelegentlich an den Kontrollen teilnehmen. Ansonsten müssen ihm Auffälligkeiten angezeigt werden.
- Die unverschlüsselte Übertragung von Daten, insbesondere von Paßworten über das Netz für ein "rlogin" (Anmeldung über fremden Rechner), stellt ein Sicherheitsrisiko dar. Vor allem die generelle Übertragung des Super-User-Paßwortes über Datenfernübertragung (DFÜ) ist nicht hinnehmbar. Auch der alternative Weg der Eintragung in die ".rhosts-Dateien" birgt Gefahren. Es sollte daher insbesondere bei DFÜ generell eine Verschlüsselung vorgenommen werden. Ist dies nicht möglich, sollte das Super-User-login-Verfahren verboten werden.
- Insbesondere solange der vereinfachte "rlogin" vom Systemverwalter-Rechner möglich ist, ist das Systemverwalter-Büro in das Sicherheits-

konzept mit einzuschließen. Die Tür muß mit einem Sicherheitsschloß versehen werden. Das Fenster sollte von der vorhandenen Alarmanlage mitgesichert werden.

4.6.2 IuK-Reg = Einsatz der IuK-Technik bei den Bezirksregierungen

Das Projekt "Konzept und Pilotprojekt für den Einsatz der IuK-Technik bei den Bezirksregierungen (IuK-Reg)" ist zum 30. April 1993 abgeschlossen worden. Die wesentlichen Ergebnisse hat die Projektgruppe in einem Abschlußbericht zusammengefaßt. Der Abschlußbericht wurde im IMA-IuK-Technik erörtert und zustimmend zur Kenntnis genommen. Das Innenministerium hat für seinen nachgeordneten Bereich die Erkenntnisse aus dem Pilotprojekt ausgewertet und durch einen Runderlaß für den zukünftigen Einsatz und Ausbau der IuK-Technik verbindliche Vorgaben gemacht. Danach sind u.a. folgende Standards zu beachten:

- Es ist ein Gesamtkonzept für die Verkabelung aller Diensträume zu erarbeiten, das auch eine abschnittsweise Realisierung ermöglicht.
- Die Netztopologie ist je Gebäude sternförmig mit Multiportrepeatern als aktiven Komponenten auszulegen. Gestufte Konzepte sind wegen der damit verbundenen zusätzlichen Betreuung nicht vorzusehen.
- Als Übertragungsmedium wird grundsätzlich eine durchgehende Kabelinstallation mit Lichtwellenleitern (LWL) bis zum Endgeräteanschluß festgelegt.
- Es ist eine vernetzte Architektur mit UNIX-Servern und Windows-Clients vorzusehen. Sämtliche Programme und Daten sind zentral auf dem Server zu installieren. Einzelplatzsysteme werden nur noch als Ausnahme zugelassen.
- Es sind Vorkehrungen und Regelungen durch den Erlaß von Dienstanweisungen für die Bereiche Datenschutz und Datensicherung zu treffen. Grundlage für die Einschätzung der Sensibilität personenbezogener Daten ist das vom Landesbeauftragten für den Datenschutz empfohlene Schutzstufenkonzept (5 Stufen).

Das seit dem 1. Mai 1993 im Echteinsatz bei der Bezirksregierung Braunschweig praktizierte Datenschutz- und Datensicherungskonzept "IuK-Reg" ist von mir besichtigt und begutachtet worden. Wesentliche Teile meiner Vorschläge und Empfehlungen sind mit dem Abschlußbericht erfüllt worden. Lediglich einige Restforderungen habe ich in meiner Stellungnahme zum Abschlußbericht nochmals zusammengefaßt:

- Verringerung der Diskettenlaufwerke und Schutz der vorhandenen Laufwerke.
- Das im Abschlußbericht dokumentierte Konzept "IuK-Reg" läßt grundsätzlich eine datenschutzgerechte Verarbeitung von Daten bis zur Schutzstufe C ("Gefährdung des Ansehens") unter entsprechender Anwendung der angebotenen Sicherungsfunktionen der verwendeten Betriebssysteme zu. Sollten in Zukunft auch Daten der Schutzstufe D ("Gefährdung der Existenz") verarbeitet werden, sind Zusatzeinrichtungen,

z.B. Verschlüsselungsverfahren, geschlossene Benutzergruppen, notwendig.
- Die Frage, welche Vorgänge, Aktivitäten sowie Eingriffe in das System zu protokollieren und damit kontrollierbar zu machen sind, ist regelungsbedüftig.

Die Umsetzung meiner Forderung hinsichtlich einer umfassenden Protokollierung ist bisher ausgeblieben. Als Gründe wurden unüberwindliche Hindernisse vorgebracht, die sich aus der Kopplung der UNIX- und DOS/WINDOWS-Bereiche mit Hilfe von LAN-Manager ergeben. Diese Begründung überzeugt nicht, zumal von Herstellern bei Ausschreibungen immer wieder behauptet wird, daß mit ihren Systemen umfangreiche Protokollierungen möglich seien. Ich empfehle, die Firmen zum Nachweis ihrer Behauptungen aufzufordern.

Es bleibt zu wünschen, daß durch den Einsatz des Betriebssystems Windows NT, das seit einem halben Jahr bei der Bezirksregierung Braunschweig anstelle des bisherigen UNIX-Betriebssystems testweise eingesetzt wird, das Protokollierungsproblem gelöst wird.

### 4.6.3 MINiNET / X.400 = Einführung von Electronic Mail

Der Electronic Mail-Dienst ermöglicht das Versenden und Empfangen von elektronischer Post von einem Arbeitsplatzrechner zu einem anderen. Auch die in der Verwaltung vorhandenen Arbeitsplatzrechner mit Bürokommunikations-
systemen sind dazu in der Lage, wenn sie Electronic Mail-Komponenten enthalten. Die dabei genutzte Electronic Mail-Software ist jedoch in aller Regel herstellerbezogen und entspricht nicht der internationalen Norm X.400. Deshalb ist gegenwärtig ein Dokumentenaustausch zwischen den verschiedenen Bürokommunikationssystemen nicht möglich.

Es gibt zahlreiche Bestrebungen, über die eigene Behörde hinaus mit anderen Dienststellen innerhalb der Landesverwaltung und auch länderübergreifend über dieses Medium zu kommunizieren. So hat die Innenministerkonferenz beschlossen, ihre Sitzungsvorbereitungen ab 1995 nur noch über Electronic Mail abzuwickeln. Das bedeutet, daß die Bundesländer bis dahin zum Einsatz dieses Dienstes in der Lage sein müssen. Im Kooperationsausschuß ADV Bund, Länder, kommunaler Bereich ist beschlossen worden, ab 1994 in einen Probebetrieb zwischen den IuK-Koordinierungsstellen des Bundes, der Bundesländer und der kommunalen Spitzenverbände einzutreten. Weiterhin existieren im Bereich der Europaminister und -senatoren der Länder Pläne, den Austausch von EU-Dokumenten zwischen EU, Bund und Ländern über Electronic Mail durchzuführen.

Unabhängig von der Notwendigkeit, sich an den bundesweiten Projekten zu beteiligen, hat das Niedersächsische Innenministerium im Einvernehmen mit den anderen Ministerien ein Pilotprojekt zur Einführung von Electronic

Mail auf der Basis von X.400 begonnen. MINiNET stellt hierfür die Infrastruktur zur Verfügung und ist die Übergangslösung bis zur Einführung von KOMNET (vgl. 4.6.4). Die vorhandene lokale Infrastruktur beruht auf Datendirektverbindungen (DDV-Leitungen).

Hierzu wurden ein zentraler sogenannter Message Transfer Agent, MTA ("Hauptpostamt für die Landesverwaltung") im Niedersächsischen Landesverwaltungsamt (NLVwA) sowie weitere Kopfstellen-MTAs ("Poststellen der jeweiligen Ministerien") im Innenministerium (MI), Ministerium für Wirtschaft, Technologie und Verkehr (MW) und der Staatskanzlei installiert. Die Anbindung der bereits vorhandenen Bürokommunikationssysteme (BÜROMIN beim MI und MW, ISAN beim MW und die DOS/WINDOWS-Anwendungen in der Staatskanzlei) erfolgt über sogenannte Gateways. Weiterhin wurde ein Anschluß an das TELEBOX-System der Telekom installiert, so daß ein Dokumentenaustausch auch mit anderen Ländern und dem Bund möglich ist.

Da es sich bei MINiNET / X.400 um ein neues automatisiertes Verfahren mit dem Anschluß von weit über 100 Arbeitsplatzrechnern handelt, ist gemäß § 7 Abs. 3 NDSG eine Technikfolgenabschätzung durchzuführen (vgl. 4.2).

4.6.4 KOMNET = Kommunikationsnetz der Niedersächsischen Landesregierung

KOMNET ist das Kürzel für ein Projekt zur Modernisierung der schon mehr als 30 Jahre alten Telefonnebenstellenanlage aller Ministerien. An die zentrale Fernmeldeanlage der Landesregierung beim Ministerium für Ernährung, Landwirtschaft und Forsten sind inzwischen Telefone von mehr als 3500 Mitarbeiterinnen und Mitarbeitern angeschlossen. In der Projektbegründung wird ausgeführt, daß Ersatzbeschaffungen für die alten Telefonanlagen und Kabel sowohl aus technisch-wirtschaftlichen als auch aus betrieblichen Gründen zwingend erforderlich seien. Ein modernes Telekommunikationsnetz müsse neben der Sprache auch Daten und Bilder sowie langfristig Videokonferenzen übertragen können. Als Grundlage für die moderne Telekommunikation soll ein breitbandiges Metropolitan Area Network (MAN) zwischen den Ministerien über landeseigene Lichtwellenleiter aufgebaut werden. Es wird ein Kernnetz zwischen dem Ministerium für Ernährung, Landwirtschaft und Forsten, dem Finanzministerium und dem Innenministerium (Eckpunkte eines Dreiecks) entstehen, an das die übrigen Ministerien an jeweils einem dieser Eckpunkte angeschlossen werden.

Als Ersatz der betagten elektromechanischen Telefonnebenstellenanlage sollen mehrere verteilte Telekommunikationsanlagen in ISDN-Technik installiert werden. Die ISDN-Telekommunikationsanlagen werden dezentral in den drei Eckpunkten des Kernnetzes bzw. in den jeweiligen Ministerien untergebracht. Zur Übertragung zwischen den Telekommunikationsanlagen wird das MAN genutzt. Die Ministerien werden mit ISDN-fähigen Telefonen ausgestattet, die über die vorhandenen Kabel an die jeweilige Telekommunikationsanlage angeschlossen werden. Auch die in den Ministerien vor-

handenen Bürokommunikationsanlagen sollen ressortübergreifend über KOMNET verbunden werden, so daß ein Dokumentenaustausch auch zwischen unterschiedlichen BK-Systemen möglich wird. Hierzu werden die existierenden lokalen Netze an das MAN angeschlossen.

Mit der Verlegung der Lichtwellenleiter im Stadtgebiet von Hannover ist bereits begonnen worden. Die Ausschreibung der in den Ministerien benötigten Kommunikationskomponenten und der ISDN-Telekommunikationsanlagen ist erfolgt. Nach dem Zuschlag Mitte 1995 sollen die Übertragungstechnik und die ISDN-Telekommunikationsanlagen bis Anfang 1996 installiert und das MAN aufgebaut sein. Nach Anschluß der lokalen Netze der Ministerien soll eine kompatible Bürokommunikation zwischen den Ministerien möglich sein. Der Anschluß weiterer Behörden im Stadtgebiet Hannover ist zu erwarten.

Über die Projektabsicht von KOMNET bin ich frühzeitig unterrichtet worden. Die Verwendung von Lichtwellenleitern für das Basisnetz begrüße ich, da auf diese Weise Abhörmöglichkeiten verringert werden. Die Einrichtung eines zentralen Netzwerkmanagements erscheint plausibel, da so die notwendige Übersicht über die Netzstruktur und die Netzkonfiguration am ehesten gewährleistet ist. Dies gilt insbesondere im Hinblick auf spätere Ausweitungen des Netzes. Mit Hilfe eines Netzwerkmanagements ergeben sich Möglichkeiten, aus Datenschutzsicht fragwürdige Aktivitäten zu erkennen und entsprechend zu reagieren. Bedenken hätte ich allerdings gegen ein nahezu allmächtiges zentrales Netzwerkmanagement, dem eine detaillierte Überwachung jedes Endgerätes möglich ist. Es ist deshalb notwendig, durch technische und organisatorische Maßnahmen eine Kontrolle über das Netzwerkmanagement auszuüben (z.B. Protokollierung, Dienstanweisung). Spätestens bei Ausweitung des Projektes über die Ministerien hinaus ist die zusätzliche Einrichtung dezentraler Netzwerkmanagement-Einheiten notwendig, die an Stelle der Zentrale die Außenbereiche überwachen. Aus Datenschutzsicht bestehen auch keine grundsätzlichen Einwände gegen ISDN-Nebenstellenanlagen. Allerdings sind bei Ausweitung auf den "Non-Voice"-Bereich neue restriktivere Datenschutz- und Datensicherungsmaßnahmen erforderlich (z.B. Verschlüsselung, Versiegelung, elektronische Unterschrift).

Meine Vorstellungen über die Datenschutz-Anforderungen an KOMNET wurden in die Kabinettsvorlage aufgenommen. Für die Einrichtung des MAN als Infrastruktur eines ressortübergreifenden Kommunikations- und Datenverbundes wurde der allgemeine Datenschutz-Grundsatz "Verboten ist, was nicht ausdrücklich erlaubt ist" festgeschrieben. Jeder an das Netz angeschlossene Rechner muß die Datenströme in seinem Teilnetz vollständig kontrollieren und den vorgenannten Grundsatz absichern. Hierfür sind die erforderlichen technischen und organisatorischen Maßnahmen zu treffen. Art und Weise der Sicherheitsmaßnahmen haben sich an den Mißbrauchsgefahren zu orientieren; sie haben sich nach dem jeweiligen Stand der Technik zu richten. Denkbare Mißbrauchsgefahren sind z.B. das Aufschalten auf Übertragungsmedien und das anschließende Abhören, das Mitlesen der übertragenen Daten am Rechner sowie das Eindringen in Vermitt-

lungsrechner und in am Netzbetrieb teilnehmende Rechner. Deshalb genügt es nicht, auf Sicherung der Verfügbarkeit und Zuverlässigkeit des Kommunikationssystems zu achten. Vielmehr umfaßt Informationssicherheit auch den Schutz der Vertraulichkeit, Integrität und Authentizität.

Die Zentrale Stelle wird vor Inbetriebnahme des MAN in Abstimmung mit den Ressorts und mir ein Datenschutz- und Datensicherungskonzept entwickeln. Auch für KOMNET ist eine Technikfolgenabschätzung zu erarbeiten, die die Mißbrauchsgefahren konkretisiert, bewertet und hieraus die zu treffenden Sicherheitsmaßnahmen ableitet. Hierbei kann auf die Erfahrungen der Projektuntersuchung "Technikfolgenabschätzung für das Projekt MINiNET" zurückgegriffen werden.

### 4.6.5 TELENET = Telekommunikationsnetz der Landesverwaltung

Die Landesregierung betreibt seit Jahren flächendeckende Datenfernübertragungsnetze. Hierzu zählen das Netz der Mehrzweckrechenzentren, das Netz der Steuerverwaltung und die Sondernetze der Polizei. Alle diese Netze haben ihre eigene Historie und sind entsprechend den Anforderungen der jeweiligen Fachverwaltung mehr oder weniger organisch gewachsen. Netzübergreifende Kommunikationsbeziehungen bestehen nicht. Die Netze werden auf Mietleitungen der DBP Telekom betrieben. Vielfach bestehen Parallelführungen der Mietleitungen, weil Netzplanungen und -optimierungen nur jeweils für die Einzelnetze vorgenommen worden sind.

Zusammen mit einem Beratungsunternehmen hat das Innenministerium überprüft, inwieweit dieser "Irrgarten" sinnvoll in ein einheitliches, landesweites Telekommunikationsnetz überführt werden kann. Das neue Netz soll gemeinschaftlich genutzt werden, herstellerneutral sein, dem gegenwärtigen Stand der Technik Rechnung tragen und für alle Landesbehörden zweckmäßig und wirtschaftlich sein. Weiterhin sollen eine freizügige Dokumentenübertragung und eine gleichberechtigte Nutzung der Kommunikationsmittel Sprache, Texte, Daten und Bilder möglich sein. Anfang 1992 wurde als Abschlußbericht ein Gutachten vorgelegt, das die Installation eines landesweiten Telekommunikationsnetzes aufzeigt, in dem die unterschiedlichen Anforderungen der Netzbenutzer berücksichtigt werden können (TELENET).

Mit TELENET sollen sowohl die Fachrechenzentren als auch die bestehenden Mehrplatzanlagen, Bürokommunikationssysteme und Einzelplatz-PC der verschiedenen Fachverwaltungen in einer behördlichen und überbehördlichen Netzstruktur integriert werden. Allen Dienststellen soll das Netz für einen Anschluß zur Verfügung stehen. Die übergreifende Vernetzung wird die Einführung neuer automatisierter Verfahren beschleunigen und den Ruf nach IuK-Vollausstattung aller Büroarbeitsplätze auslösen. TELENET stellt eine wesentliche Änderung der bestehenden Kommunikationsmöglichkeiten innerhalb der niedersächsischen Landesverwaltung dar. Der Zugang zu Rechnern der Landesverwaltung über öffentliche Kommunikationsdienste (z.B. Datex-P, Telebox) und die Benutzung privater Dienste (z.B. Mailboxen) stellen neue Gefährdungen des Datenschutzes sowie erhöhte Anforde-

rungen an die Datensicherung dar, weil die vernetzten Rechner anders als bisher auch von außen erreichbar sind.

Die Landesregierung hat dem Netzkonzept im Dezember 1992 zugestimmt und die Zentrale Stelle beauftragt, TELENET stufenweise aufzubauen. In der ersten Stufe soll zunächst ein "Basisnetz" auf der Grundlage des genormten X.25-Protokolls eingerichtet werden, das neben den bestehenden Hauptverbindungen zwischen den Knoten Hannover, Braunschweig, Lüneburg und Oldenburg auch neu einzurichtende Verbindungen für das Umweltressort sowie die Integration des Netzes der Finanzverwaltung vorsieht. Dieses Basisnetz befindet sich derzeit im Aufbau. Parallel zum Netzaufbau ist die Datenübertragung in TELENET durch einen sogenannten TDN-Vertrag (Telekom Designed Network) der DBP Telekom als Dienstleistung übertragen worden. Das heißt, die quasi hinter dem Netz liegende Leitungsführung und die Datenvermittlung zwischen den angeschlossenen Knoten sind Sache der DBP Telekom - eines privaten Unternehmens. Vor der Übertragung des Netzwerkmanagements von TELENET auf die DBP Telekom als "Carrier" ist zwar eine Kostenbetrachtung erfolgt, eine datenschutzrechtliche Bewertung der Übertragung fehlte dagegen. Dies wurde von mir bemängelt.

Ich bin über die Projektabsichten von TELENET frühzeitig unterrichtet worden. In einer ersten Stellungnahme habe ich auf Datenschutz- und Datensicherungsrisiken hingewiesen und ein Datenschutz- und Datensicherungskonzept gefordert. Ich habe meine Forderungen damit begründet, daß TELENET die bestehende Informationslandschaft der niedersächsischen Landesverwaltung völlig verändern wird. Mit einem verstärkten Technikeinsatz wird die Verletzlichkeit der Informationsverarbeitung wachsen. Deshalb muß sich gerade das Projekt TELENET an dem Grundsatz orientieren: "Je komplexer und umfangreicher Informations- und Kommunikationsnetze sind, um so ausgefeilter und erprobter muß die Sicherheitstechnik sein". Das dem Interministeriellen Arbeitskreis (IMA-IuK-Technik) zur Beschlußfassung vorgelegte Konzept zur Einführung von TELENET sichert diesen Grundsatz nicht ausreichend. Es enthält einige Datenschutz-Versprechungen, doch fehlen die notwendigen konkreten Festlegungen. So sind z.B. die getroffenen Aussagen zur Verschlüsselung von Daten, Nachrichten und Dokumenten aus Datenschutzsicht unzureichend. Ich habe deshalb gefordert, daß vor dem Echteinsatz des Landesdatennetzes TELENET die folgenden Grundforderungen zu erfüllen sind:

1. Für das Projekt TELENET muß eine Gefahrenabschätzung entsprechend § 7 Abs. 3 NDSG erfolgen (Mißbrauchsgefahren, Netzausfall, Sabotage, Betriebsbereitschaft). Die Abschätzung sollte auch die Darstellung von Alternativlösungen zu einem einheitlichen Landesnetz (z.B. aufgabenspezifische Subnetze) umfassen. Das vorgeschlagene Konzept ist so zu begründen, daß die in § 7 Abs. 2 genannten Betroffenen, die Abgeordneten des Niedersächsischen Landtages und eine interessierte Öffentlichkeit dies nachvollziehen können.

2. Die technischen und organisatorischen Maßnahmen, mit denen derartige Gefahren wirksam beherrscht werden sollen, sind in einem Datenschutz- und Datensicherungskonzept festzulegen (z.B. Verschlüsselungstechnik, Schlüsselmanagement, Paßwortschutz, elektronische Unterschrift, Schutz der Protokollanalysatoren vor Mißbrauch).

3. In einer für alle Teilnehmerinnen und Teilnehmer verbindlichen Datenschutzrichtlinie sollten datenschutzrechtliche Festlegungen getroffen werden (z.B. zugelassene Anwendungsgebiete, abgeschlossene Benutzergruppen, Datenschutzmaßnahmen bei definierter Sensitivität).

4.6.6 LIS = Landesinformationssystem

LIS will entscheidungsrelevante Verwaltungsinformationen des Landes zusammenfassen und für die Führungsebene erschließen. Das Projekt wird unter der Federführung des Niedersächsischen Innenministeriums betrieben. Mit LIS soll der Zugang zu vorhandenen Informationssystemen verbessert, andere Datenbanken - auch solche außerhalb der Landesverwaltung - angeschlossen, Kommunikationsschwellen insbesondere bei Führungskräften abgebaut und die zentrale Stellung des Mehrzweckrechenzentrums im Landesverwaltungsamt als "Informationsdrehscheibe" gefestigt und ausgebaut werden. LIS soll als "Expertensystem" in jedem Bürokommunikationssystem der Landesverwaltung und darüber hinaus für PC-HOST-Lösungen verfügbar sein.

Nach Vorstellung des Projektbetreibers sollen folgende Informationssysteme angeschlossen werden:

NILAS = Niedersächsisches Landtagsinformationssystem
NILAS wird als Datenbank geführt und enthält die Entscheidungen und Protokolle ab der 10. Legislaturperiode bis hin zu aktuellen Informationen über die Landtagsarbeit.

VORIS = Vorschrifteninformationssystem
Das DV-System ist seit Dezember 1991 freigegeben worden. Allerdings ist die Benutzung auch heute noch - 3 Jahre danach - recht benutzerunfreundlich oder - freundlicher ausgedrückt - verbesserungsfähig.

PRINS = Presseinformationssystem
Das Projekt ist bisher über eine erste Studie nicht hinausgekommen, es scheint fehlenden Haushaltsmitteln und mangelndem Interesse zum Opfer zu fallen.

NIZA = Niedersachsen in Zahlen
Informationen aus der Statistischen Datenbank sollen einem größeren Kreis an Interessierten zur Verfügung gestellt werden. Auch diesem Projekt scheint die personelle und finanzielle Unterstützung zu fehlen. Realisierungsabsicht und -zeitpunkt sind mir unbekannt.

Das LIS scheint sein Leben schon wieder ausgehaucht zu haben, kaum daß der erste Schrei erfolgte. Nur NILAS und VORIS sind verfügbar; andere Datenbanken anzuschließen, scheint inzwischen aus den Augen verloren zu sein.

4.6.7 GENESIS = Gemeinsames neues statistisches Informationssystem

Die Statistikverwaltungen des Bundes und der Länder gehörten zu den Pionieren der automatisierten Datenverabeitung in der öffentlichen Verwaltung. Schon in den 60er Jahren gab es gemeinsame Software-Entwicklungen und den kostenlosen Austausch von Statistikprogrammen. Seit 1990 wird erneut an einer gemeinsamen Lösung eines kompatiblen statistischen Informationssystems gearbeitet. Auch das Niedersächsische Landesamt für Statistik ist im Kernteam mit dabei. Das fachliche Feinkonzept liegt bereits vor und umfaßt 16 dicke Bände. Ernüchternd war für mich, daß in dem dem IMA-IuK-Technik vorgelegten Extrakt die Worte Datenschutz und Datensicherung nicht vorkommen. Das Landesamt für Statistik plant den GENESIS-Einsatz auf einer UNIX-Plattform. Dies wird in einer Technikfolgenabschätzung kritisch zu untersuchen sein.

4.6.8 TRANSEC = Transport Security

TRANSEC ist ein Informationssystem zur Klassifizierung und Kontrolle im Bereich der Beförderung gefährlicher Güter auf der Straße. TRANSEC speichert nationale und europäische Vorschriften sowie geltende Ausnahmeregelungen und Vereinbarungen. Wegen der vielfachen Zuständigkeiten im Gefahrenrecht erwartet das Ministerium für Wirtschaft, Technologie und Verkehr als Projektbetreiber einen starken Informationsbedarf bei den übrigen Ministerien, bei den vier Bezirksregierungen und bei den 54 Straßenverkehrsbehörden. Damit scheint TRANSEC eine interessante Datenbank für das Landesinformationssystem zu sein. Eine Anbindung ist aber bisher nicht geplant.

4.6.9 IGS = Integrierte Gefahrstoff-Datenbank

Das Umweltministerium plant den Aufbau einer Gefahrstoff-Datenbank im Niedersächsischen Landesamt für Ökologie (NLÖ). Hiermit sollen schnell und fundiert Aussagen über Eigenschaften und Wirkungen chemischer Stoffe, über mögliche Risiken und Gefährdungen für die menschliche Gesundheit oder für andere umweltbezogene Schutzgüter abrufbar sein. Das Projekt wird in Bund-Länder-Kooperation erarbeitet. Abrufwünsche werden aus Vollzugsbehörden des Umweltschutzes und des Arbeitsschutzes, insbesondere der Gewerbeaufsichtsverwaltung erwartet. IGS soll Daten zu Stoffeigenschaften und zu Vorkommen von Stoffen in der Umwelt und am Arbeitsplatz allen Interessierten zur Verfügung stellen. Nach Angaben der Projektbetreiber scheidet ein teilweise gewünschter Datenaustausch mit anderen Fachinformationssystemen aus lizenzrechtlichen Gründen aus. Es

würden keine personenbezogenen Daten verarbeitet. Daher verzichte ich auf die Forderung nach einem Datenschutzkonzept. Auch hier liegt der Hinweis auf das Landesinformationssystem nahe.

4.6.10 ISAN = Innovative Seehafentechnologie

Das Ministerium für Wirtschaft, Technologie und Verkehr hat gemeinsam mit Hafenunternehmen der niedersächsischen Seehäfen ein in der Fläche verteiltes Informations- und Kommunikationssystem aufgebaut. ISAN verbindet die dreistufige Organisationsstruktur von Hafenämtern, Bezirksregierungen und Ministerium. Über sog. NKI (Niedersächsisches Kommunikations-Interface) wird ISAN darüber hinaus mit privaten Hafenunternehmen verbunden. Der Datenaustausch erfolgt als Filetransfer unter Verwendung öffentlicher Netze über DATEX-P auf der Basis X.400 und X.500.

Über die Konzeption bin ich bereits 1989 informiert worden. Meine Bedenken gegen eine direkte Anbindung externer Nutzer wurden frühzeitig aufgegriffen und beachtet. Nach § 12 Abs. 4 NDSG ist ein automatisiertes Abrufverfahren unzulässig, soweit dabei personenbezogene Daten betroffen sind. Ob auch meine sonstigen Empfehlungen zum sicheren Betrieb in ISAN umgesetzt worden sind, werde ich in Kürze kontrollieren.

4.6.11 IuK-Technik für die Straßenbauverwaltung

Das Landesamt für Straßenbau hat sein Langzeitkonzept zur technischen Ausstattung der Straßenbauverwaltung dem IMA-IuK-Technik vorgelegt. Selbst in diesem Konzept einer technischen Verwaltung spielen personenbezogene Daten durchaus eine wichtige Rolle; gespeichert werden z.B. Daten über Grundstückseigentümer, Daten über Unfallbeteiligte sowie Daten über Mitarbeiterinnen und Mitarbeiter. Das Konzept geht von einer Verbindung der Mehrzweckrechenzentren mit den lokalen Rechnersystemen vor Ort aus. Bindeglied zu den lokalen Netzwerken (LAN) soll das künftige TELENET werden (4.6.5). Da die notwendigen Festlegungen für TELENET noch fehlen, konnte auch die vorgelegte Konzeption in vielen Bereichen nur grob ausfallen. Die neuentstandene Pflicht zur Technikfolgenabschätzung hat das Landesamt sofort aufgegriffen. Die Entwurfsarbeiten dazu wurden aber im Einvernehmen mit mir zurückgestellt, um Erfahrungen mit der Pilotstudie MINiNET / X.400 abzuwarten (4.6.3).

4.6.12 BASIS = Buchhaltungs- und Abrechnungssystem im Strafvollzug

Aus BASIS ist im Laufe der Jahre ein ausgewachsenes "DV-Gebäude" im Justizvollzug geworden. VG (Vollzug), AV (Arbeitsverwaltung), ZA (Zahlstelle) und WV (Wirtschaftsverwaltung) sind die Namenskürzel für weitere Systemkomponenten. Das BASIS-Grundsystem wurde von der Landesjustizverwaltung Nordrhein-Westfalen für den Einsatz von UNIX-Mehrplatzanlagen entwickelt. Die Verfahrenserweiterungen werden in Abstimmung

mit den übrigen Betreiberländern, die von Brandenburg über das Saarland bis Schleswig-Holstein reichen, von jeweils einem Land entwickelt. Niedersachsen hat den Bereich "Arbeitsverwaltung" übernommen.

BASIS speichert eine Vielzahl recht unterschiedlicher personenbezogener Daten, so z.B. die Stammdaten der Gefangenen, die Vollstreckungsdaten, die Abwesenheitszeiten, den Urlaub und den Ausgang, besondere Sicherungsmaßnahmen, die Entgeltberechnung der Gefangenen, den Nachweis der Arbeitslosenversicherungen, das Gefangenenguthaben mit Entgeltabrechnungen und Auszahlungen für Einkäufe oder Überweisungen, Lieferantendaten und die Abwicklung der Auftragsarbeiten der Anstalten. 21 Justizvollzugsanstalten haben schon auf moderne IuK-Technik gesetzt und BASIS im Einsatz.

Trotz des hohen Automatisierungsgrades und trotz vieler von mir anerkannter Bemühungen des Justizministeriums ist es nicht gelungen, ein scheinbar triviales Problem zu lösen: die Geldüberweisung durch Gefangene ohne einen diskreditierenden Hinweis auf die Anstalt. Die Deutsche Bundespost-Postbank hat sich allen Wünschen und Argumenten widersetzt. Gleich ob Überweisungen auf Papier oder auf Datenträgern erfolgen, in jedem Fall meint die Postbank den Kontoinhaber (die Justizvollzugsanstalt) als Auftraggeber dem an die Empfängerbank übermittelten Datensatz hinzufügen zu müssen.

### 4.6.13 NIFIS = Niedersächsisches Forstliches Informationssystem

Die Landesforstverwaltung beabsichtigt, ihre Informations- und Kommunikationstechnik zu einem integrierten unternehmensweiten Informationssystem auszubauen. NIFIS hat das Ziel, vorhandene Informationen aktueller und schneller bereitzustellen, den Datenzugriff zu erweitern und zu erleichtern, Verknüpfungen von Daten unterschiedlicher Sachgebiete zu ermöglichen und zu standardisieren sowie nichtforstliche Verwaltungen mit planungsrelevanten Daten der Forstwirtschaft und des Naturraumes Wald zu versorgen. Hierbei gilt es, eine Fläche von 340.000 ha darzustellen und zu verwalten, 80 Forstämter mit 450 Revierförstereien sowie Forstplanungsamt, Bezirksregierungen und Ministerium miteinander kommunizieren zu lassen. Dieses Ziel soll in Teilprojekten und in gestuften Phasen erreicht werden. Die Phase 1, "Digitale Basiskarte", die gerade im IMA-IuK-Technik vorgestellt wurde, enthält keine personenbezogenen Daten. Die mir von den Projektbetreibern angebotene Beteiligung an datenschutzrelevanten Teilprojekten werde ich im Rahmen meiner Kapazitäten wahrnehmen.

## 4.7 Automation in der Kommunalverwaltung

"Die Informationsverarbeitung im kommunalen Bereich verändert sich evolutionär". Diese Aussage in XI 4.7 gilt unverändert. Die kommunalen Datenzentralen mit ihren großen Aufgabenbereichen (Finanz-, Personal-, Einwohner- und Sozialwesen) auf den Rechnern der kommunalen Datenzentralen

beherrschen weiterhin die Datenverarbeitungslandschaft der Kommunalverwaltung. Versprechungen, durch Bürokommunikationslösungen größere Effektivität, Flexibilität und Kostenersparnisse zu erzielen, sind in den Kommunalverwaltungen verstummt. Der Einsatz eigener Informations- und Kommunikationstechnik erfordert eine eigene DV-Organisation und damit meist nicht kalkulierte Kosten. Die ernüchternden Erfahrungen und knappe Haushaltsmittel zwingen auch diesen Bereich, über die Organisation beim Einsatz technikunterstützter Informationsverarbeitung nachzudenken.

Die Leiter der kommunalen Datenzentralen arbeiten gegenwärtig an einem Strategiepapier, um vorhandene Gestaltungspotentiale deutlich zu machen und ihre traditionelle Vordenker-Rolle in Fragen der automatisierten Datenverarbeitung für die von ihnen betreuten Verwaltungen erneut unter Beweis zu stellen. Das Papier ist leider "noch so geheim", daß es auch mir nicht gezeigt werden konnte.

Ich begrüße die klare Aussage in der Stellungnahme der Landesregierung zum XI.TB zur frühzeitigen Unterrichtung über datenschutzrelevante kommunale IuK-Projekte. Allein durch die Normierung der Unterrichtungspflicht im § 22 Abs. 2 Satz 3 NDSG hat sich leider für mich noch nichts verbessert. Meine bisherigen Bemühungen, kompetente Gesprächspartner aus der kommunalen Informationsverarbeitung zu finden, die umfassendes Wissen über die eingesetzte Datenverarbeitung und über den Aufbau neuer Informationssysteme haben, sind bisher ohne Erfolg geblieben. Selbst der Leiter des EDV-Amtes einer großen niedersächsischen Stadt bekannte erst kürzlich offen, daß auch er nicht über den Einsatz der IuK-Technik in seiner Behörde umfassend informiert sei. Da es eine Institution zur Koordinierung der kommunalen Informationsverarbeitung nicht gibt, werde ich auch weiterhin auf Einzelmeldungen der jeweils datenverarbeitenden Stelle angewiesen sein. Die Regelungsabsicht des § 22 Abs. 2 NDSG, die Auswirkungen der automatisierten Datenverarbeitung zu beobachten und insbesondere aufzuzeigen, wie sich die Wirkungsmöglichkeiten der Organe der kommunalen Gebietskörperschaften verändern, war bisher nicht leistbar.

Auf den richtigen Weg zur Gewährleistung der Datenschutzvorschriften führt die Initiative der Kommunalen Gemeinschaftsstelle für Verwaltungsvereinfachung mit ihrem Rundbrief "Datenschutz ist Chefsache" vom 10. März 1994; ihren Empfehlungen schließe ich mich in vollem Umfange an:

"1. Verschaffen Sie sich mit Unterstützung Ihrer Organisations- und Automationsstelle einen Überblick über die Verankerung des Datenschutzes in Ihrer Verwaltung.
2. Überzeugen Sie die Führungsebene Ihrer Verwaltung von der Notwendigkeit eines modernen, konzeptionellen Datenschutzes.
3. Informieren Sie Ihre Mitarbeiter und Mitarbeiterinnen. Dies sollten Sie schriftlich und persönlich tun, etwa anläßlich einer Personalversammlung.
4. Bilden Sie eine Projektgruppe und geben Sie ihr einen klaren Arbeitsauftrag.

5. Stimmen Sie Arbeitsergebnisse mit den Führungskräften ab und verabschieden Sie die Ergebnisse.
6. Lassen Sie sich regelmäßig über die Umsetzung berichten.
7. Sie sind Vorbild. Wenn es Ihnen ernst ist mit einem modernen Datenschutz, werden auch Ihre Mitarbeiter und Mitarbeiterinnen 'mitziehen'."

## 4.8 Mailboxen in Wirtschaft und Verwaltung

### 4.8.1 Was ist eine Mailbox?

Unter einer Mailbox versteht man im Computerjargon einen elektronischen Briefkasten in einem Rechner mit Zugang zu einem Datennetz, z.B. über das Telefon. In einer Mailbox geschieht das gleiche wie in einem herkömmlichen Postfach, es werden Nachrichten abgelegt und abgerufen - nur auf elektronischem Wege. Die Mailbox kann in Minutenschnelle beschickt und entleert werden, rund um die Uhr und oftmals weltweit.

Eine funktionierende Mailbox setzt einen ständig betriebsbereiten Rechner, eine eindeutige Adressierung sowie kompatible Kommunikationsprogramme voraus. Üblicherweise wird eine Vielzahl von Mailboxen auf dem Rechner eines Mailbox-Betreibers installiert - ähnlich den vielen Postfächern in einem Postamt. Die Mailbox-Nutzenden können Nachrichten von ihrem Arbeitsplatzrechner oder über ihren privaten PC zuhause abrufen. Der Mailbox-Betreiber sorgt für die ständige Betriebsbereitschaft des Mailbox-Rechners, für eine geeignete Organisation der Speicherung der Nachrichten und für einen kontrollierten Zugriff auf die Mailboxen.

Die Palette der Mailbox-Betreiber ist sehr bunt. Sie umfaßt die weltweit arbeitende kommerzielle Firma Compuserve, das riesige, vor allem im Hochschulbereich populäre System Internet, die national tätigen Anbieter wie die Telekom mit Telebox, Mailbox-Systeme von Behörden und Firmen sowie zahlreiche private Betreiber regionaler Systeme, die oft von Computerfreaks nach Feierabend betreut werden. Die Akzeptanz dieses Mediums wächst. Weltweit gibt es bereits mehr als 50 Millionen Nutzerinnen und -Nutzer.

### 4.8.2 Datenschutzrechtliche Einordnung von Mailbox-Diensten

Zur datenschutzrechtlichen Einordnung von Mailbox-Diensten muß sowohl die fernmelderechtliche als auch die medienrechtliche Seite beleuchtet werden. Aus der Sicht des Fernmelderechts sind das Fernmeldeanlagengesetz (FAG) und die aufgrund des § 14a FAG ergangene "Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen, (UDSV)" zu beachten. Die UDSV ist dann anzuwenden, wenn eine Telekommunikationsdienstleistung nur gegen Entgelt zu erlangen ist. Auch wenn bei vielen privaten oder halbkommerziellen Mailboxen Zweifel an der Geschäftsmäßigkeit bestehen, sollte der Begriff des Entgelts weit

ausgelegt werden. Auch die Pflicht, regelmäßig selbst Mailboxbeiträge zu schreiben, kann z.B. als Entgelt in diesem Sinne gewertet werden. Die UDSV regelt das Verhältnis zwischen Kunde und Netzbetreiber. § 12 UDSV beschränkt die Datenverarbeitung des Netzbetreibers auf das, was zur Durchführung des Vertragsverhältnisses erforderlich ist. Nachrichteninhalte darf der Netzbetreiber nur speichern, soweit dies technisch zur jeweiligen Telekommunikationsdienstleistung gehört.

Medienrecht ist Landesrecht. In Niedersachsen bestehen für Mailboxen keine bereichsspezifischen Regelungen. Allenfalls wäre der Bildschirmtext-Staatsvertrag (Btx-StV) heranzuziehen. Auf den Btx-StV verweist z.B. das Hamburgische Mediengesetz, das auch "rundfunkähnliche Kommunikationsdienste" umfaßt. Ich habe mich der Empfehlung des Hamburgischen Datenschutzbeauftragten angeschlossen, entsprechende medienrechtliche Vorschriften ländereinheitlich festzuschreiben - etwa durch Staatsvertrag.

Btx-StV und UDSV weisen Unterschiede auf, z.B. beim Umgang mit Verbindungs- und Abrechnungsdaten. Nach Btx-StV dürfen Verbindungsdaten nur zur Herstellung der Verbindung erhoben werden, sie sind grundsätzlich nach Ende der Verbindung zu löschen. Abrechnungsdaten sind unmittelbar nach Abrechnung zu löschen. Nach UDSV sind sie nach spätestens 6 Monaten zu löschen. Wenn die Nutzerin oder der Nutzer nach Mahnung nicht zahlt, darf der Netzbetreiber nach UDSV Verbindungs- und Abrechnungsdaten an den Anbieter übermitteln; nach Btx-StV dagegen nur die Abrechnungsdaten. Die folgenden Regelungen der UDSV sind auch für Mailboxen relevant:

- Das Unternehmen muß Maßnahmen treffen, um Fehlübermittlungen und das unbefugte Offenbaren von Nachrichteninhalten auszuschließen. Bei Gefährdungen der Netzsicherheit müssen die Beteiligten unterrichtet werden.
- Personenbezogene Daten über die Nutzerinnen und Nutzer dürfen nur verarbeitet werden, soweit dies erforderlich ist.
- Das Unternehmen muß die Nutzenden über die Verarbeitung personenbezogener Daten unterrichten.
- Es muß gewährleistet sein, daß personenbezogene Daten von Nutzenden nur bewußt und gewollt übermittelt werden können.
- Nutzerinnen und Nutzer haben ein Widerspruchsrecht gegen die Veröffentlichung ihrer Daten z.B. in elektronischen Verzeichnissen; sie müssen auf dieses Recht hingewiesen werden.

Da in Niedersachsen keine bereichsspezifischen Regelungen bestehen, gelten die Bestimmungen der Datenschutzgesetze, also insbesondere die des BDSG für den nicht-öffentlichen Bereich. Voraussetzung ist hier, daß der Mailbox-Anbieter personenbezogene Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeitet oder nutzt. Die Anwendbarkeit des BDSG wird weiter eingeschränkt, wenn der Betrieb einer solchen Mailbox inhaltlich als Pressetätigkeit ausgestaltet ist. Das Presseprivileg des § 41 Abs. 1 Satz 1 BDSG befreit von den allgemeinen Datenschutzregeln der kommerziellen Datenverarbeitung und schränkt diese auf

das Datengeheimnis und die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes ein (§§ 5 und 9 BDSG).

Mailbox-Anbieter, die ihre Tätigkeit geschäftsmäßig als Dienstleistungsunternehmen betreiben und damit Datenverarbeitung im Auftrag durchführen, haben ihre Tätigkeit zum Dateienregister nach § 32 BDSG bei mir anzuzeigen. Eine geschäftsmäßige Tätigkeit ist grundsätzlich dann anzunehmen, wenn für die Nutzung des Mailbox-Systems ein Entgelt eingenommen wird. Öffentlich-rechtlich organisierte Mailboxen haben diese besondere Form der personenbezogenen Datenverarbeitung in einer Dateibeschreibung gemäß § 8 Abs. 1 NDSG zu dokumentieren und mir zu melden.

### 4.8.3 Mailboxen in der öffentlichen Verwaltung

Ich habe einige Mailbox-Anbieter über ihre Tätigkeit befragt, um ihre datenschutzrechtliche Einordnung vorzunehmen und den Stand von Datenschutz- und Datensicherungsmaßnahmen in diesem Bereich beurteilen zu können.

Zu den von mir besuchten Unternehmen gehörte die TELEHAUS NORDHORN GmbH, die stolz ist über die ca. 500 Mailbox-Teilnehmer, überwiegend aus der Kommunalverwaltung, aber auch von Banken, Rechtsanwälten, Bauunternehmen, Speditionen und anderen Wirtschaftsunternehmen der Ems-Dollart-Region sowie deren Mitgliedskörperschaften. Auch der Niedersächsische Städtetag benutzt die Technik des TELEHAUSES für einen schnellen Informationsaustausch mit mehr als 150 Verwaltungen. Die Liste der Mailbox-Anwendungen im kommunalen Bereich enthält den Informationsaustausch mit Aufsichtsbehörden, Kommunikation mit Gemeinden, anderen Behörden und Institutionen, Korrespondenz mit beauftragten Notaren und Anwälten, Kreditaufnahmen und Abfragen der Konditionen bei Kreditinstitutionen bundesweit, Sitzungsdienst sowie Datenbankrecherchen.

Die TELEHAUS NORDHORN GmbH ist eine Vereinigung zweier öffentlicher Stellen. Für diesen Mailbox-Betreiber findet das NDSG Anwendung, soweit nicht die UDSV bereichsspezifische Regelungen trifft. Dies gilt, obwohl das TELEHAUS privatrechtlich als GmbH organisiert ist (vgl. 6.2). Allerdings sind vom NDSG nur § 8 Abs. 1 und 2 mit seinen Dokumentationspflichten, die §§ 19 und 26 über die Anrufung des Landesbeauftragten für den Datenschutz und über Fernmessen und Fernwirken sowie die Regelungen des vierten Abschnitts mit der Kontrollkompetenz des Landesbeauftragten für den Datenschutz zu beachten. Im übrigen finden die für nicht-öffentliche Stellen geltenden Vorschriften des BDSG Anwendung, da es sich bei der TELEHAUS NORDHORN GmbH um ein am Wettbewerb teilnehmendes Unternehmen handelt.

Die TELEHAUS NORDHORN GmbH führt ganz überwiegend Nachrichtenübermittlung (elektronische Post) für seine Benutzer aus Verwaltung und Wirtschaft durch. Diese Tätigkeit ist datenschutzrechtlich als Datenverarbeitung im Auftrag anzusehen. Aufträge, Weisungen zu technischen und organisatorischen Maßnahmen und die Zulassung von Unterauftragsverhält-

nissen sind schriftlich festgehalten. Vertraulichkeit und Datenschutz werden durch ein ausgefeiltes Sicherheitsangebot mit Paßwort-Vergabe, "Challenge-Response"-Methode zur Authentizitätsprüfung, Verschlüsselung nach dem DES-Algorithmus und Schlüssel-Management mit "Public-Key-System" nach dem RSA-Verfahren gewährleistet. Hack-Versuche werden beim dritten Versuch abgebrochen, protokolliert und dem legitimen Benutzer beim nächsten Einwählen als erstes angezeigt. Mittels Challenge-Response-Verfahren wird eine Authentizitätskontrolle möglich, bei der durch Kreieren immer neuer Sicherungsnummern, die mit Zufallszahlengeneratoren erzeugt werden, auch ein Mitschneiden von einmal verwendeten Nummern zu keinem Erfolg führt. Ein zweites Paßwort ("secondary password") schützt besonders vertrauliche Nachrichten. Die angebotenen Verschlüsselungsverfahren erlauben es nicht nur, Nachrichten in kryptographischer Form abzuspeichern, sondern auch Nachrichten verschlüsselt zu übertragen.

Auch die Stadt Diepholz ist von Anfang an Teilnehmerin des Mailbox-Systems des Niedersächsischen Städtetages. Inzwischen betreibt sie zusätzlich ein eigenes Mailbox-System mit den Zielsetzungen Datenaustausch im Rahmen des Schreibdienstes der Stadt, elektronische Post im eigenen Haus, papierlose Post zu den Ratsmitgliedern, digitaler Aktenschrank aller Ratsdrucksachen einer Legislaturperiode, Depot für Shareware-Programme zum kostenlosen Zugriff aller berechtigten Teilnehmer und als Medium zur Übermittlung von Bild-, Ton- und Filmdokumenten. Das Mailbox-System wird von der Stadtverwaltung Diepholz genutzt, auch Ratsmitglieder können sich anschließen lassen. Eine Mailbox für Bürgerinnen und Bürger mit Stadtinformationen (z.B. Fremdenverkehr, Veranstaltungen, Behördenwegweiser) ist geplant.

### 4.8.4 Mailbox-Anbieter in der Privatwirtschaft

Zur Zeit findet ein enormer Boom im Bereich der privat genutzten Mailboxen statt. Überall schießen regionale Mailbox-Systeme wie Pilze aus dem Boden, die von Computerfreaks am heimischen PC oder von kleinen EDV-Unternehmen betrieben werden. Allein in der Region Hannover soll es über 100 Mailbox-Betreiber mit über 5000 Teilnehmerinnen und Teilnehmern geben. In den privaten Mailbox-Systemen spielt die vertrauliche Individualkommunikation nur eine untergeordnete Rolle. Sie werden vielmehr von Schwarzen Brettern geprägt, die als Diskussionsforen eingerichtet sind, zu denen alle Nutzerinnen und Nutzer Beiträge liefern können. Auch wird "chatting" angeboten, eine Möglichkeit zum elektronischen Plaudern durch die Weitergabe von elektronischen Notizen. Ferner werden in Mailbox-Systemen Shareware-Programme und Fachinformationen angeboten. Häufig sind Systeme untereinander mit Gateways verbunden.

Die vorwiegend öffentliche Kommunikation hat zur Folge, daß die Systeme auch entsprechend offen betrieben werden. Doch auch bei diesen Systemen gibt es Bereiche, in denen das informationelle Selbstbestimmungsrecht berührt wird. Dies bezieht sich nicht nur auf den Austausch persönlicher Nachrichten, bei denen die Notwendigkeit von Vertraulichkeit offensichtlich

ist. Bedenklich ist vielmehr auch, wenn z.B. die Nutzenden im Mailbox-System über alle anderen Nutzenden nachlesen können, wann diese das letzte Mal das Mailbox-System verwendet haben. Auch eine bedenkenlose Weitergabe sämtlicher Nutzerdaten etwa an einen Adreßhändler wäre sicherlich nicht im Sinne der Betroffenen.

Solche Datenschutzbelange werden mit dem weiteren Anwachsen der Teilnehmerzahlen und mit zunehmender Kommerzialisierung der Mailbox-Systeme an Bedeutung zunehmen. Es ist daher wichtig, daß auch Mailbox-Betreiber für den privaten Bereich auf die Einhaltung von Datenschutzregelungen achten. Die Datensicherheit muß gewährleistet sein; Erforderlichkeitsprinzip, Unterrichtungspflichten, Widerspruchsrechte usw. müssen berücksichtigt werden.

## 4.9 Datenschutzgerechte Aktenvernichtung

### 4.9.1 Was ist "Vernichtung nach Datenschutz"?

Bei der Aktenvernichtung werden Daten "gelöscht". Sie gelten als gelöscht, wenn sie "unkenntlich" gemacht wurden (§ 3 Abs. 5 BDSG bzw. § 3 Abs. 2 NDSG). In Zeitungsanzeigen und auf firmeneigenen Lkw werben zahlreiche Unternehmen mit dem Slogan: "Aktenvernichtung nach Datenschutz". Die Erfahrung zeigt, daß viele Kunden und vielleicht auch das eine oder andere Aktenvernichtungsunternehmen selbst gar nicht so genau wissen, was damit eigentlich gemeint ist.

Konkrete Aussagen über eine gesicherte Vernichtung von Informationsträgern enthält die DIN 32 757, die im Oktober 1985 verabschiedet worden ist und demnächst durch eine modifizierte Version ersetzt werden soll. Diese Norm unterscheidet fünf Sicherheitsstufen bei der Vernichtung und berücksichtigt bei der Festlegung den Grad der Schutzwürdigkeit von Informationen, die physikalischen Eigenschaften von Informationsträgern und die zur Anwendung kommenden technischen Verfahren. Als Mindestanforderung einer datenschutzgerechten Vernichtung sehe ich die Sicherheitsstufe 3 der DIN 32 757 an. Bei Daten, deren Mißbrauch Existenz, Gesundheit, Leben oder Freiheit der Betroffenen gefährden würde, ist die Vernichtung nach einer höheren Sicherheitsstufe der DIN 32 757 durchzuführen, d.h. nach der Sicherheitsstufe 4 oder gar nach der Sicherheitsstufe 5. Zusatzmaßnahmen wie das Verwirbeln oder Pressen erhöhen die Vernichtungsgüte und gestatten, die Sicherheitsstufe bei der Zerkleinerung um eine, in besonderen Einzelfällen auch um zwei Stufen abzusenken. Die noch aktuelle DIN 32 757 fordert bei der Stufe 3 eine Streifenbreite unter 2 mm bei beliebiger Länge oder unter 4 mm bei maximal 60 mm Länge. Diese Werte werden sich mit der neuen Norm nur geringfügig ändern.

Die Stufe 3 ist mit fast keinem Schredder der geprüften Betriebe erreichbar. Lediglich ein geprüftes Unternehmen kann tatsächlich mit einer Streifenbreite unter 2 mm vernichten. Die meisten Schredder ermöglichen allenfalls eine Vernichtung nach Stufe 1 der DIN 32 757 (Streifenbreite maximal 12 mm oder Fläche maximal 1000 $mm^2$ bzw. 2000 $mm^2$ bei der neuen Norm). Von einer datenschutzgerechten Vernichtung kann in diesen Fällen nur dann ausgegangen werden, wenn umfangreiche Zusatzmaßnahmen wie Verwirbeln, Pressen, Vernichten in großen Mengen usw. durchgeführt werden. Dies erfordert eine Prüfung im Einzelfall.

Die Maßnahmen der Firmen zur Realisierung datenschutzgerechter Aktenvernichtung variieren sehr stark. So habe ich in einem Fall einen "Aktenvernichtungs-Container" für jedermann auf dem Gelände des Vernichters vorgefunden, dessen Inhalt erst durch den Schredder geschickt wird, wenn sich genug Material angesammelt hat. In einem anderen Fall war ein Gebäude mit mehreren Sicherheitsbereichen hergerichtet worden, in das die fest verschlossenen Lkw mit Vernichtungsmaterial einfahren und dessen zweiter Sicherheitsbereich erst zugänglich wird, wenn das Tor zum ersten Bereich verschlossen worden ist. Dabei wird der ganze Entladungs- und Vernichtungsvorgang mit Videokameras genauestens beobachtet. Derartige Maßnahmen sind den "zehn Geboten" des Datenschutzrechts zuzuordnen (v.a. Datenträgerkontrolle, Auftragskontrolle und Transportkontrolle). Die zu treffenden technischen und organisatorischen Maßnahmen sollten entsprechend dem Schutzzweck angemessen sein.

BDSG und NDSG legen fest, daß die Auftraggeber für die datenschutzgerechte Verarbeitung von Daten im Auftrag verantwortlich bleiben. Als Kunde eines Vernichtungsunternehmens darf man sich deshalb nicht mit dem Hinweis "Vernichtung nach Datenschutz" zufrieden geben. Vielmehr empfehle ich, sich die technischen und organisatorischen Maßnahmen persönlich vor Ort anzusehen. Wichtige Punkte sind vertraglich festzulegen. In dem Vertrag sollte aufgeführt werden, nach welcher Sicherheitsstufe der DIN 32 757 zerkleinert wird und welche zusätzlichen Maßnahmen wie Verwirbelung oder Ballenpressen getroffen werden. Hierbei sollte die oben aufgeführte Bewertung einer datenschutzgerechten Vernichtung beachtet werden. Hilfreich hierfür ist der "Mustervertrag über die Vernichtung von Schriftgut", der als Anhang zu den Verwaltungsvorschriften des NDSG im Niedersächsischen Ministerialblatt veröffentlicht worden ist (Nds. MBl. 1994, S. 1147). In meinem Merkblatt "Vernichtung von Datenträgern mit personenbezogenen Daten" wird auf die notwendigen technischen und organisatorischen Maßnahmen bei der Vernichtung eingegangen.

### 4.9.2 Aktenvernichtung: Kleine und große Pannen

Leider macht die nachlässige Vernichtung von Akten und sonstigen Datenträgern immer wieder Schlagzeilen. Es kommt vor, daß Schriftgut mit sensiblen personenbezogenen Daten einfach weggeworfen wird, ohne daß es unleserlich gemacht worden ist.

Ein besonders krasser Fall ist aus Stadthagen gemeldet geworden, bei dem große Mengen gut erhaltener Krankenscheine mit ärztlichen Diagnosen auf der Papierhalde eines Altpapierhändlers gefunden wurden. Verursacht wurde dieser Skandal durch ein Transportunternehmen, das die Unterlagen nicht zu einem Aktenvernichtungsbetrieb, sondern zum "gewöhnlichen" Altpapierhändler geliefert hat. Dieses Unternehmen war offensichtlich nicht darüber informiert, daß es sich bei dem Material um Schriftgut mit sensiblen medizinischen Daten handelt. Eine große Krankenkasse als Auftraggeber hatte es versäumt, einen schriftlichen Vertrag über den Transport und die Vernichtung der Altunterlagen abzuschließen. Ich mußte dieses Versäumnis des Auftraggebers beanstanden. Der Fall macht die hohe Verantwortung des Auftraggebers deutlich und unterstreicht die Notwendigkeit eines schriftlichen Vertrages, um Klarheit über Aufgaben, Pflichten und Verantwortlichkeiten zu schaffen.

## 4.10 Der behördliche Datenschutzbeauftragte - richtig ausgewählt

### 4.10.1 Das Ziel heißt "Sicherstellung des Datenschutzes"

An die Stelle jahrelangen Werbens um die freiwillige Bestellung behördlicher Datenschutzbeauftragter ist eine gesetzliche Pflicht getreten. Nach § 8 Abs. 3 NDSG haben alle öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten und hierbei mindestens fünf Bedienstete ständig beschäftigen, eine Beauftragte oder einen Beauftragten zu bestellen. Diese haben ihre Behörden bei der Durchführung der technischen und organisatorischen Maßnahmen nach § 7 NDSG zu beraten und auf die Durchführung der Maßnahmen hinzuwirken. Weiter wirken sie bei der Erstellung der Dateibeschreibungen und der Geräteverzeichnisse mit. Einen Mindestkatalog an Kontrollaufgaben enthalten die Verwaltungsvorschriften zum NDSG. Für wünschenswerte Erweiterungen des Aufgabenkatalogs einer oder eines "NDSG-Datenschutzbeauftragten" werbe ich in meinem Informationsblatt "Hinweise zu Stellung und Aufgaben eines behördlichen Datenschutzbeauftragten".

Im Bereich der Datenverarbeitung nicht-öffentlicher Stellen gibt es diese Pflicht der Berufung einer oder eines Datenschutzbeauftragten schon seit 1978. Bestellung und Aufgaben des BDSG-Beauftragten sind in den §§ 36 und 37 BDSG geregelt. Die Pflicht zur Bestellung kann neben Stellen der Wirtschaft auch öffentliche Stellen treffen, so z.B. die öffentlich-rechtlichen Wettbewerbsunternehmen von Kommunen, v.a. auch öffentlich-rechtliche Krankenhäuser. Die Verweisung des § 2 NDSG führt nämlich auf entsprechende Bestimmungen des BDSG. Die Verpflichtung zur Bestellung eines besonderen SGB-Beauftragten - wie in der Vergangenheit - wurde dagegen durch das Zweite Gesetz zur Änderung des Sozialgesetzbuchs (2. SGBÄndG) wieder aufgehoben. Die NDSG-Bestimmungen über behördliche Datenschutzbeauftragte sind in diesem Bereich nun allein anzuwenden.

Ich wage die Aussage, daß bei der Umsetzung der neuen Pflicht nach dem NDSG zur Bestellung eines behördlichen Datenschutzbeauftragten in der öffentlichen Verwaltung Niedersachsens ein erhebliches Vollzugsdefizit besteht. Dies wird durch meine Kontrollerfahrungen und auch durch die langsam bei mir eintreffenden Dateibeschreibungen nach § 8 Abs. 1 NDSG deutlich. Die Formularfrage nach dem behördlichen Datenschutzbeauftragten bleibt häufig unausgefüllt. Einem solchen Versäumnis werde ich zukünftig nachgehen und die Bestellung in jedem Falle überprüfen. Verstöße gegen § 8 Abs. 1 NDSG können von mir förmlich beanstandet werden. Bei der "richtigen" Auswahl und der Aufgabenzuweisung bin ich gern beratend tätig.

### 4.10.2 Organisatorische Stellung eines behördlichen Datenschutzbeauftragten

Die Behördenleitung kann weitgehend frei entscheiden, wie die oder der behördliche Datenschutzbeauftragte in die Behördenstruktur eingebunden wird. Die Bedeutung des Datenschutzes, das Verständnis in der Öffentlichkeit sowie die Akzeptanz bei betroffenen Bürgerinnen und Bürgern sprechen dafür, den behördlichen Datenschutzbeauftragten der Behördenleitung direkt zuzuordnen. Zu beachten ist, daß § 66 Nr. 9 Nds. PersVG bei der Bestellung und Abberufung der oder des Beauftragten für den Datenschutz eine Mitbestimmung des Personalrates vorschreibt.

Ich werde häufig gefragt, welchen zeitlichen Umfang die Tätigkeit der oder des behördlichen Datenschutzbeauftragten ausfüllt und ab welchem Punkt eine Behörde einen hauptamtlichen Datenschutzbeauftragten zu bestellen hat. Die Verwaltungsvorschriften zum NDSG lassen diese Frage offen. Es ist möglich, behördliche Datenschutzbeauftragte zusätzlich mit anderen Verwaltungsaufgaben zu betrauen. Es muß aber ausreichend Zeit für Schulung, Weiterbildung und für regelmäßige Datenschutzkontrollen zur Verfügung stehen. Die Kontrollbefugnisse und die Pflichten für Beauftragte für den Datenschutz sollten schriftlich festgelegt werden, um Klarheit für alle Beteiligte zu schaffen und Konflikte mit den Kontrollierten zu vermeiden.

Bei entsprechender Verwaltungsgröße kann es in Betracht kommen, neben der oder dem behördlichen Datenschutzbeauftragten fachspezifisch weitere Personen zur Sicherstellung des Datenschutzes einzusetzen.

### 4.10.3 Persönliche Voraussetzungen der Ausgewählten

Die Beauftragten sollen die erforderliche Fachkunde und Zuverlässigkeit besitzen. Diese Voraussetzungen gelten für NDSG- und BDSG-Beauftragte in gleicher Weise. Fachkunde ist notwendig auf dem Gebiet der automatisierten Datenverarbeitung, der Organisation der Behörde oder des Unternehmens, des Datenschutzrechts und sonstiger relevanter Rechtsvorschriften. Auch pädagogisch-didaktische Befähigungen sollten vorhanden sein, um Mitarbeiterinnen und Mitarbeiter in Datenschutzfragen zu schulen.

Schwerer als die Definition der Fachkunde ist es, die Zuverlässigkeitsvoraussetzungen zu beschreiben und deren Erfüllung im Einzelfall zu bewerten. Dabei ist es noch einfach, den Begriff der persönlichen Zuverlässigkeit zu erklären. Kriterien wie sorgfältige Arbeitsweise, Gewissenhaftigkeit, Charakterfestigkeit, Loyalität und Belastbarkeit erscheinen selbstverständlich; sie bei Kontrollen zu erfragen, wird nicht selten als "Majestätsbeleidigung" empfunden. Zur persönlichen Zuverlässigkeit gehört aber auch Verantwortungsbewußtsein, Engagement und Mut zur eigenen Meinung.

In der Literatur wird der Begriff der Zuverlässigkeit überwiegend mit der Frage des Interessenkonflikts zu anderen - hauptamtlichen - Aufgaben in Zusammenhang gebracht. Interessenkonflikte sind offenkundig bei der Leitung der Datenverarbeitung oder von Organisationseinheiten mit intensiver Anwendung personenbezogener Daten und bei der Behördenleitung selbst. In jedem dieser Fälle würde sich die Person selbst kontrollieren. Vergleichbare Interessenkonflikte entstehen aber auch bei der Systemverwaltung von IuK-Systemen. Mit diesen Aufgaben Betraute haben umfassende Zugangsrechte zu allen Geräten. Sie haben Zugriffsrechte auf sämtliche Ressourcen; sie können zumeist Dateien lesen und verändern; sie können Zugriffsrechte auf sie und die Eigentumsrechte an ihnen verändern; sie können die Systeminformationen über Dateien manipulieren, die Paßwort-Datei bearbeiten, Benutzerinnen und Benutzer hinzufügen oder sperren sowie deren Berechtigungen verändern. Die Möglichkeiten der Systemverwaltung sind praktisch unbegrenzt; diese ist kaum kontrollierbar, denn selbst die Systemprotokolle können unbemerkt verändert oder gelöscht werden (vgl. XI 4.3). Diese offenkundigen Interessenkonflikte zur Haupttätigkeit lassen Mitarbeitende der beschriebenen Bereiche als Beauftragte für den Datenschutz ungeeignet erscheinen.

Ein Interessenkonflikt kann sich aber auch aus fehlender "Präsenz" der bzw. des Datenschutzbeauftragten ergeben. Wer nicht genügend Zeit für seine Kontrollaufgabe hat, wer nicht stets von Kolleginnen und Kollegen oder als Bürgeranwalt seiner Behörde ansprechbar ist, gerät ebenfalls in Konflikte zu seiner Kontrollaufgabe und wird nicht akzeptiert. Gerade im Zeitmangel sehen die meisten behördlichen Datenschutzbeauftragten ihr Hauptproblem. Sie klagen darüber, daß sie mit anderen Aufgaben überlastet sind und Datenschutz in ihren Behörden nur als "Nebentätigkeit" oder gar als Restriktion abgetan wird. Anders als in der Wirtschaft sind in der öffentlichen Verwaltung bisher nur selten "hauptamtliche" Datenschutzbeauftragte ernannt worden, die kein weiteres Amt ausüben müssen und deshalb genügend Zeit für ihre Kontrollaufgaben, für Schulung von Kolleginnen und Kollegen, für eigene Weiterbildung und für Literaturstudien haben. Mangelnde Qualifikation der Beauftragten, Bestellungen als "Feigenblatt" und Frust bei Betroffenen können vermieden werden.

### 4.10.4 Externe Datenschutzbeauftragte

Ich bin mehrfach aus dem Kommunalbereich gefragt worden, ob die gesetzliche Pflicht durch einen externen Beauftragten für den Datenschutz erfüllt

werden könne, z.B. angesiedelt bei einem Landkreis für seine kreisangehörigen Gemeinden oder bei einer Datenzentrale für mehrere kleinere Mitgliedsgemeinden. Die Bestellung eines externen Datenschutzbeauftragten ist weder durch das NDSG noch durch das BDSG ausgeschlossen, wenngleich diese Lösung nicht der Intention des Gesetzgebers nach Eigenkontrolle der datenverarbeitenden Stellen entspricht. Ich vertrete wie schon in der Vergangenheit auch jetzt die Ansicht, daß die oder der behördliche Datenschutzbeauftragte die gesetzlichen Kontrollaufgaben nur dann voll erfüllen kann, wenn er sich möglichst nahe am Ort des Geschehens befindet und nicht nur nachträglich vom fernen Schreibtisch aus prüft. Die oder der Beauftragte soll die Behördenleitung und die zuständigen Mitarbeiter kontinuierlich beraten, sie sollen bereits bei der Planung und Vorbereitung von IuK-Vorhaben mitarbeiten und so präventiven Datenschutz ermöglichen.

## 4.11 Der betriebliche Datenschutzbeauftragte

### 4.11.1 Welche persönlichen Voraussetzungen müssen erfüllt sein?

Die interne Kontrolle des betrieblichen Datenschutzbeauftragten hat sich bewährt; sie scheint sich auch bei der anstehenden europarechtlichen Regelung durchzusetzen. Bestellung und Aufgabenzuweisung sind in den §§ 36 und 37 BDSG geregelt. Viele Datenschutzbeauftragte sind schon seit Jahren im Amt; sie entstammen oft der Generation der DV-Pioniere und -Praktiker. Gegenwärtig vollzieht sich ein Generationswechsel. Zunehmend tauchen jüngere Leute bei Prüfungen und beim Erfahrungsaustausch auf. Leider erfüllt nicht jede Person auf Anhieb die "persönlichen Voraussetzungen", so wie dies das BDSG mit dem Ziel einer qualifizierten Eigenkontrolle für die Wirtschaft erwartet.

§ 36 Abs. 2 BDSG bestimmt, daß zum Beauftragten für den Datenschutz nur bestellt werden darf, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Für die Auswahl des BDSG-Beauftragten gelten die gleichen Kriterien wie für den behördlichen Datenschutzbeauftragten (4.10.3). Deutlich häufiger als in der öffentlichen Verwaltung sind in der Wirtschaft hauptamtliche Datenschutzbeauftragte anzutreffen. Damit entfällt das Problem der Kompatiblität mit der Hauptaufgabe. Kritik mußte ich bei mehreren Prüfungen an mangelhaften Fachkenntnissen der bestellten Beauftragten üben; mal fehlten ausreichende DV-Kenntnisse, mal waren mangelhafte Kenntnisse über das Datenschutzrecht zu beanstanden. Insgesamt gesehen funktioniert aber die Eigenkontrolle in der Wirtschaft.

### 4.11.2 Welche Konflikte sind hinnehmbar?

Es gibt leider Unternehmen, bei denen das Bundesdatenschutzgesetz noch "ein Buch mit sieben Siegeln" ist. Auch zu diesen dringt von irgendwo die

Nachricht vor, daß ein Datenschutzbeauftragter bestellt werden muß, wenn eine gewisse Zahl von Beschäftigten mit der Verarbeitung von personenbezogenen Daten in Dateien zu tun hat. Welche Voraussetzungen dieser erfüllen muß, ist aber unbekannt, denn hierfür müßte ein BDSG-Kommentar zur Hand sein. Also wird jemand bestellt, bei dem man das Gefühl hat, daß er oder sie diese Aufgabe noch "mitmachen" kann. Wenn man es sich besonders leicht machen möchte, bestellt man den Geschäftsführer selbst. Oder es wird die EDV-Leiterin bzw. der EDV-Leiter ausgesucht, denn die oder der weiß ja am besten, was mit den automatisierten Daten passiert, und hat sich ohnehin um die Datensicherheit zu kümmern. So geht es natürlich nicht. Es wird dabei außer Acht gelassen, daß die oder der Datenschutzbeauftragte eine möglichst unabhängige Kontrollinstanz sein sollte, die ähnlich einer Aufsichtsbehörde die Einhaltung von Datenschutzvorschriften überprüft. EDV-Leiter, Systemverwalter, Geschäftsführer und Prokuristen können eine solche Kontrolle aber nur sehr bedingt wahrnehmen, weil sie sich selbst kontrollieren müßten. Sie unterliegen einem massiven Interessenkonflikt, der ihre Zuverlässigkeit als Datenschutzbeauftragter von vornherein in Frage stellt.

Nach § 38 Abs. 5 BDSG kann ich bei gravierenden Interessenkonflikten die Abberufung des Datenschutzbeauftragten verlangen. Entsprechende Empfehlungen habe ich mehrfach ausgesprochen. Diesen wurde regelmäßig auch entsprochen. Vor der Entscheidung über eine Abberufung prüfe ich, ob trotz eines bestehenden Interessenkonfliktes gewichtige Gründe gegen die Abberufung sprechen. Dies könnte z.B. der Fall sein, wenn es keine andere Person im Unternehmen gibt, die zum Datenschutzbeauftragten geeignet ist. Ein geringer Interessenkonflikt ist dann hinnehmbar, wenn die oder der Bestellte die Kontrollaufgaben korrekt und engagiert wahrnimmt.

In einem Fall wurde von mir die Abberufung eines Datenschutzbeauftragten verlangt, der gleichzeitig DV-Leiter war. Maßnahmen zur Sicherung der Daten selbst waren in diesem Unternehmen vom DV-Leiter in begrüßenswerter Weise durchgeführt worden. Hier verbanden sich Unternehmens- und Datenschutzinteressen. Mängel ergaben sich aber bei der rechtlichen Fachkunde des Datenschutzbeauftragten. Außerdem wurden von ihm keine Überprüfungen der Datenschutzmaßnahmen in den Filialen des Unternehmens vorgenommen. Eine Beibehaltung des Datenschutzbeauftragten kam daher nicht in Frage.

In einem anderen Fall war der Datenschutzbeauftragte gleichzeitig Prokurist und Leiter der Abteilung, in der die Bereiche EDV, Organisation und Recht angesiedelt waren. Außerdem nahm er die Aufgabe das Datenschutzbeauftragten für weitere in der ganzen Bundesrepublik verteilte Stellen wahr. Auch hier lagen massive Interessenkonflikte vor. Zudem gab es signifikante Hinweise auf mangelhafte Erfüllung der Datenschutzaufgaben, so daß ich eine Abberufung verlangen mußte.

### 4.11.3 Abberufung des Datenschutzbeauftragten eines Landeskrankenhauses

Ein Landeskrankenhaus stand vor der Frage, ob und wie ein ordnungsgemäß bestellter Datenschutzbeauftragter auch gegen seinen Willen abberufen werden kann. Da das Krankenhaus nicht nur hoheitliche Aufgaben wahrnimmt, sondern auch Wettbewerbsunternehmen ist, waren bei der Beantwortung der an mich herangetragenen Fragen auch die Bestimmungen des BDSG zu beachten. Das BDSG bestimmt in § 36 Abs. 3 Satz 4, daß die Bestellung zum Datenschutzbeauftragten "nur auf Verlangen der Aufsichtsbehörde oder in entsprechender Anwendung von § 626 BGB widerrufen werden" kann. Eine BDSG-Aufsichtsbehörde gibt es in der vorliegenden Fallgestaltung des öffentlich-rechtlichen Krankenhauses aber gar nicht. Ich selbst werde in diesen Fällen nach dem NDSG tätig. Die Frage nach meiner Kontrollkompetenz wird dort im vierten Abschnitt beantwortet. Da die NDSG-Regelung über meine Kontrollpflichten als Landesbeauftragter für den Datenschutz die BDSG-Regelung zur Aufsichtsbehörde ersetzt, tritt mein Abberufungsverlangen als öffentlicher Datenschutzbeauftragten an die Stelle des Verlangens der Aufsichtsbehörde. Jedoch steht mir kein Anordnungsrecht nach § 38 Abs. 5 BDSG zu, sondern allenfalls das Beanstandungsrecht nach § 23 Abs. 1 NDSG. Ich habe das anfragende Krankenhaus aufgefordert, den Beauftragten für den Datenschutz von seinen Pflichten zu entbinden, da seine Hauptaufgabe als Systemverwalter einen nicht hinnehmbaren Interessenkonflikt zu den Aufgaben eines Beauftragten für den Datenschutz darstellten. Mit meiner Aufforderung vor einer "angedrohten" Beanstandung wollte ich dem Krankenhaus Gelegenheit geben, die Abberufung einvernehmlich vorzunehmen. Der Aufforderung wurde gefolgt, eine arbeitsgerichtliche Auseinandersetzung konnte vermieden werden.

Der Widerruf der Bestellung eines BDSG-Beauftragten durch die datenverarbeitende Stelle selbst ist jedoch auch in entsprechender Anwendung von § 626 BGB denkbar. Notwendig für den Widerruf ist ein wichtiger Grund wie z.B. beharrliches Untätigsein des Beauftragten, ein schwerwiegender Verstoß gegen Verschwiegenheitspflichten, ein Vergehen gegen persönlichkeitsschützende Normen (z.B. §§ 201 StGB, § 43 BDSG) oder auch Tatsachen, auf Grund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalles und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnisses nicht zugemutet werden kann. Auch die Empfehlung der Aufsichtsbehörde zum Widerruf der Bestellung kann ein solcher wichtiger Grund sein.

## 5. Ausland, Europa

### 5.1 Kein grenzenloser Datenschutz

Die grenzüberschreitende Datenverarbeitung gewinnt immer mehr an Bedeutung. Dies zeigt sich daran, daß bei mir auch Eingaben eingehen, die die Datenverarbeitung ausländischer Stellen betreffen. So passiert es offenbar in

zunehmendem Maße, daß Direktwerbemaßnahmen aus dem Ausland erfolgen. Nicht selten handelt es sich dabei um offensichtlich unseriöse Aktivitäten. Was Unternehmen dazu bringt, für derartige Aktionen ins Ausland zu gehen, kann ich nur vermuten. Ich kann nicht ausschließen, daß dabei auch der geringere Datenschutzstandard des jeweiligen Landes eine Rolle spielt. Erfolgt die Datenverarbeitung vom Ausland aus, so sind mir zumeist die Hände gebunden. Oft bin ich auch mangels genauerer Kenntnis des dortigen Datenschutzrechts nicht in der Lage, eine rechtliche Beurteilung abzugeben. In meiner Dienststelle verfüge ich aber über eine Liste ausländischer Datenschutz-Kontrollinstanzen. Auf Anfrage bin ich gerne bereit, die jeweils einschlägige Adresse betroffenen Bürgerinnen und Bürger mitzuteilen.

Vom Zusammenschluß der für die Privatwirtschaft zuständigen Datenschutzaufsichtsbehörden, dem sog. "Düsseldorfer Kreis", wurde eine Checkliste zur Verbesserung des Datenschutzes beim grenzüberschreitenden Verkehr mit Personendaten erarbeitet, die insbesondere Wirtschaftsbetrieben eine Handhabe bei internationalen Aktivitäten gibt (abgedruckt in DSB 1/1994 , 9 ff.).

## 5.2 EU-Datenschutzrichtlinie

Während der deutschen Präsidentschaft im Rat der Europäischen Union (EU) in der zweiten Hälfte des Jahres 1994 versuchte die Bundesregierung, die Arbeiten an der EU-Datenschutzrichtlinie voranzutreiben (vgl. XI 6.2). Grundlage der Verhandlungen war eine "konsolidierte Fassung" des Richtlinientextes vom 20. Juni 1994. Es zeichnet sich ab, daß die Richtlinie keine umfassenden Änderungen des deutschen Datenschutzrechts erforderlich machen wird. Auch die Befürchtung, die Selbstkontrolle durch die betrieblichen Datenschutzbeauftragten nach den §§ 36 f. BDSG könnte nach Erlaß der Richtlinie unzulässig werden, dürfte unberechtigt sein. Der Richtlinienvorschlag läßt für derartige nationale Besonderheiten genügend Raum. Von seiten der Datenschutzbeauftragten wurde immer wieder darauf hingewiesen, daß es auch auf EU-Ebene einer handlungsfähigen unabhängigen Datenschutzkontroll-Instanz bedarf (vgl. Anlage 17 Nr. 10). Ich rechne damit, daß die EU-Richtlinie nach Abschluß der Abstimmung zwischen den EU-Mitgliedern im Schnellgang das Europäische Parlament passieren wird. Sollte sich die Verabschiedung über den Zeitraum des Beitritts weiterer europäischer Länder zur EU hinauszögern, so hätte dies zwangsläufig neuen Abstimmungsbedarf und starke Verzögerungen zur Folge.

## 5.3 Was hat das VW-Haustelefonbuch in den USA verloren?

Nicht wenig verblüfft war ich, als in meiner Dienststelle ein Fax der Volkswagen AG einging, in dem mich die dortige "Abteilung Datenschutz" darum bat, eine eidesstattliche Versicherung im Rahmen eines vor einem US-Gericht anhängigen Streitverfahren abzugeben. US-amerikanische Bürgerinnen und Bürger hatten offensichtlich gegen die Volkswagen AG ein Pro-

dukthaftungsverfahren eingeleitet wegen behaupteter Konstruktionsmängel eines Kraftfahrzeugs dieser Firma aus dem Baujahr 1970.

Nach der Darstellung der VW AG wurde sie im Rahmen dieses Verfahrens aufgefordert, ihr gültiges Haustelefonbuch von 1993 herauszugeben. Dieses Telefonbuch der VW AG enthält die Namen von mehr als tausend Firmenangehörigen des Hauptwerkes Wolfsburg als auch der Zweigwerke Braunschweig, Emden, Kassel und Salzgitter sowie einer Anzahl von Tochtergesellschaften, einschließlich der Wohnungsgesellschaften, des Leasing und der Audi AG. Enthalten sind weiterhin die Dienstbezeichnung der Personen und die Dienststellung innerhalb der Firmen sowie die Angabe ihres hierarchischen Status, woraus wiederum auf den sozialen und finanziellen Status geschlossen werden kann. Die im Haustelefonbuch genannten Telefonnummern sind einmalige, international direkt anwählbare Nummern am Arbeitsplatz. Außerdem enthält das Haustelefonbuch persönliche private Heim-Telefonnummern von Personen in Führungspositionen.

Mit der Bitte um Abgabe einer eidesstaatlichen Versicherung verfolgte die VW AG offensichtlich das Ziel, dem Klägerersuchen entgegenzutreten. Ich mußte der VW AG mitteilen, daß es mir rechtlich verwehrt ist, im Rahmen von Gerichtsverfahren für eine Partei "eidesstattliche Versicherungen" über eine datenschutzrechtliche Bewertung abzugeben. Derartige Erklärungen sieht das Datenschutzrecht nicht vor. Nach § 38 BDSG überprüfe und überwache ich als Aufsichtsbehörde die Ausführung des Gesetzes sowie anderer Vorschriften über den Datenschutz. Eine rechtsverbindliche Bestätigung der Rechtmäßigkeit oder Rechtswidrigkeit bestimmter Maßnahmen oder die Erteilung von Genehmigungen fällt nicht in meine Kompetenz. Ich teilte jedoch der VW AG mit, daß die Übermittlung des Haustelefonbuchs an das US-Gericht gegen deutsches Datenschutzrecht verstoßen würde.

Das Zurverfügungstellen des Haustelefonbuches im Rahmen des genannten Gerichtsverfahrens ist datenschutzrechtlich als "Übermittlung" zu bewerten. Die Zulässigkeit der Datenübermittlung ins Ausland beurteilt sich nach § 28 BDSG. Im konkreten Fall kam als Übermittlungstatbestand nur § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Die Erforderlichkeit der Angaben aus dem Haustelefonbuch der VW AG von 1993 für ein Gerichtsverfahren, in dem es um Entwicklung, Tests und Konstruktion von VW-Käfern aus dem Jahr 1970 geht, war für mich nicht ersichtlich. Es war ausgeschlossen, daß die Angaben über alle im Hausbuch aufgeführten Personen erforderlich sind, d.h. daß die Angaben im Rahmen des vor dem Gericht geführten Verfahrens benötigt werden.

Außerdem war davon auszugehen, daß schutzwürdige Interessen der im Telefonbuch aufgeführten VW-Bediensteten der Datenübermittlung entgegenstehen. Der Umstand, bei VW in einer bestimmten Position beschäftigt und über ein bestimmtes Telefon erreichbar zu sein, ist eine grundsätzlich schutzwürdige Information. Ein einer Übermittlung entgegenstehendes schutzwürdiges Interesse kann sich zudem schon aus dem Umstand ergibt, daß eine Datenübermittlung ins Ausland erfolgen soll, wo kein dem deutschen Recht vergleichbares Datenschutzrecht gilt.

Nachdem meine datenschutzrechtliche Bewertung vom Bundesministerium für Arbeit und Sozialordnung bestätigt worden ist und diese dem US-Gericht vorgelegt wurde, wirkte das amerikanische Gericht auf die Kläger ein, nicht mehr auf der Herausgabe des Telefonbuches zu bestehen.

## 6. Datenschutzrecht - allgemein

### 6.1 Verwaltungsvorschriften zum NDSG

Zum neuen NDSG hat das Niedersächsische Innenministerium nach Abstimmung mit den übrigen Ressorts Verwaltungsvorschriften erlassen (Gem.RdErl. v. 23. Juni 1994, Nds. MBl. S. 1147). Sie enthalten knappe Hinweise zur Gesetzesauslegung, z.T. auch Regelungen zu dessen Durchführung. An der Erarbeitung der Verwaltungsvorschriften habe ich mich intensiv beteiligt. In vielen Fällen habe ich auf eine datenschutzfreundlichere Fassung hinwirken können.

Aus den Verwaltungsvorschriften möchte ich folgende Punkte hervorheben:

1. Anwendung des NDSG bei Wettbewerbsunternehmen (VV-Nr. 1.2)

Bei wirtschaftlichen Unternehmen und sonstigen Einrichtungen, die überwiegend wirtschaftliche Aufgaben wahrnehmen bzw. am Wettbewerb teilnehmen, richtet sich die Verarbeitung personenbezogener Daten grundsätzlich nach den Vorschriften des BDSG (Dritter Abschnitt) für nicht-öffentliche Stellen. Der Grund dafür liegt darin, daß diese Wettbewerbsunternehmen der öffentlichen Hand privaten Mitbewerbern gleichgestellt werden und keine Wettbewerbsnachteile durch die strengeren Vorschriften des NDSG erleiden sollen. Dies gilt aber nur, soweit personenbezogene Daten in Ausübung der wirtschaftlichen Tätigkeit verarbeitet werden. Hierzu zählt die Verarbeitung von Daten der in solchen Unternehmen beschäftigten Personen nicht. Für sie sind die Vorschriften des NDSG, insbesondere § 24, anzuwenden.

Im übrigen gelten für derartige Wettbewerbsunternehmen die Bestimmungen über die Fertigung einer Dateibeschreibung und eines Dateiverzeichnisses (§ 8 Abs. 1 und 2) sowie die Regelungen zur Anrufung des Landesbeauftragten für den Datenschutz und seiner Kontrolle. Die Verpflichtung für diese Unternehmen zur Bestellung eines internen Datenschutzbeauftragten ergibt sich aus § 36 BDSG.

2. Grundsatz der Zweckbindung (VV-Nr. 8.1)

Entscheidende Bedeutung für die Datenverarbeitung hat das Prinzip der Zweckbindung (§ 10 NDSG). Es besagt, daß personenbezogene Daten nur für den ursprünglich beabsichtigten Zweck und - von den gesetzlich zugelassenen Ausnahmen abgesehen - nicht für andere Zwecke verarbei-

tet werden dürfen. Damit wird eine multifunktionale Datennutzung im Grundsatz ausgeschlossen.

Im Falle der Einwilligung von Betroffenen in die Verarbeitung ihrer Daten ergibt sich der Verarbeitungszweck aus der Einwilligungserklärung, die deshalb eindeutig abgefaßt sein muß. Aus ihr muß z.B. klar hervorgehen, ob und inwieweit die oder der Betroffene auch in eine Weiterverarbeitung der Daten, z.B. eine Übermittlung an Dritte, einwilligt. Im Zweifelsfall darf die Behörde eine Einwilligung nicht ohne weiteres im Sinne ihrer Interessen großzügig auslegen.

Erfolgt die Datenverarbeitung auf gesetzlicher Grundlage, so ist der Verarbeitungszweck durch Rechtsvorschrift festgelegt oder jedenfalls unter Anknüpfung an die behördliche Aufgabe aus der gesetzlichen Regelung abzuleiten. Nach VV-Nr. 8.1 soll in den Fällen, in denen eine ausdrückliche Regelung zur Datenverarbeitung fehlt, regelmäßig angenommen werden können, daß es sich bei der Ausführung einer Rechtsvorschrift insgesamt um einen Zweck und nicht um verschiedene Zwecke handelt. Eine solche generalisierende Aussage kann aus meiner Sicht nicht getroffen werden. Zwar ist es durchaus denkbar, daß innerhalb eines Gesetzes nur ein relativ weiter Verarbeitungszweck verfolgt wird (wie etwa im Bereich der Steuerverwaltung der einheitliche Zweck der Steuererhebung); einen Grundsatz, daß alle von einem Gesetz verfolgten "Einzelzwecke" unter einer "Zweckglocke" zusammenzufassen sind und damit nur einen Verarbeitungszweck im Sinne des Datenschutzes darstellen, gibt es jedoch nicht. Er würde den Bürgerinnen und Bürgern einen Überblick über die Verarbeitung ihrer Daten erheblich erschweren. Deshalb muß jeweils im Einzelfall geprüft werden, ob innerhalb eines Gesetzes unterschiedliche Zwecke oder tatsächlich ein gemeinsamer Verarbeitungszweck verfolgt werden. Für einen gemeinsamen Zweck reicht es nicht aus, daß zwischen verschiedenen Aufgaben eine bloße Ähnlichkeit besteht oder sie in einem zeitlichen, räumlichen oder sachlichen Zusammenhang stehen.

3. Einführung automatisierter Abrufverfahren und regelmäßiger Datenübermittlungen (VV-Nr. 10.2)

§ 12 NDSG läßt automatisierte Abrufverfahren und regelmäßige Datenübermittlungen wegen ihrer spezifischen Risiken für den Datenschutz nur durch besondere Rechtsvorschrift zu. Für den einzelnen Abruf bzw. die Übermittlung muß jedoch bereits ein Erlaubnistatbestand nach § 4 Abs. 1 NDSG vorliegen. § 12 NDSG enthält keine Ermächtigung, über die Einrichtung der genannten Verfahren hinaus materielle Grundlagen für eine sonst nicht zulässige Datenübermittlung zu schaffen. Die Voraussetzungen der verfahrensrechtlichen Vorschrift des § 12 NDSG können auch nicht durch Einwilligungen der Betroffenen zum automatisierten Abrufverfahren oder zu regelmäßigen Datenübermittlungen ersetzt werden.

Ermächtigt zum Erlaß von Verordnungen für die genannten Verfahren sind nach § 12 Abs. 2 NDSG die Landesregierung bzw. die Fachministerien für ihren Geschäftsbereich. Eine Verordnungsermächtigung für die Kommunen und die sonstigen der Aufsicht des Landes unterstehenden öffentlichen Stellen enthält das Gesetz nicht. Dennoch gehen die VV (Nr. 10.2) davon aus, daß diese Stellen im Bereich ihres eigenen Wirkungskreises entsprechende Rechtsvorschriften erlassen können. Die Rechtsgrundlage hierfür wird im Satzungsrecht der Körperschaften, Anstalten und Stiftungen (z.B. § 6 NGO, § 5 NLO für die Kommunen) gesehen.

Ich halte dies für zweifelhaft. Nach der Rechtsprechung des Verwaltungsgerichtshofs Baden-Württemberg (Beschluß v. 15. Dezember 1992, DVBl. 1993, 778) stellt die allgemeine Satzungsautonomie keine ausreichende Ermächtigungsgrundlage für Grundrechtseingriffe - z.B. in das informationelle Selbstbestimmungsrecht - dar. Hätte der Gesetzgeber auch die Kommunen und die übrigen seiner Aufsicht unterliegenden Stellen zum Erlaß der nach § 12 NDSG erforderlichen Rechtsvorschriften ermächtigen wollen, hätte er dies ausdrücklich regeln können. Gerade wegen der Gefährdungsmöglichkeiten, die von automatisierten Abrufverfahren und regelmäßigen Datenübermittlungen ausgehen können, hat das Gesetz besondere Voraussetzungen für deren Einrichtung aufgestellt. So muß ein solches Verfahren nach einer Interessenabwägung zwischen den Belangen der Betroffenen und den Aufgaben der beteiligten Stellen angemessen sein, für den Verordnungsinhalt werden bestimmte Vorgaben gemacht, u.a. müssen die wesentlichen Maßnahmen zur Kontrolle der Datenverarbeitung festgelegt werden. Schließlich ist der Landesbeauftragte für den Datenschutz vor Erlaß einer solchen Verordnung zu hören. Da der Gesetzgeber diese sachlich gebotenen Regelungen nicht auf die Kommunen und die übrigen in Betracht kommenden öffentlichen Stellen erstreckt hat, wurde offensichtlich nicht an eine Rechtsetzungsmöglichkeit für diese Stellen gedacht.

Dieses Ergebnis versuchen die Verwaltungsvorschriften zu korrigieren, indem sie die Voraussetzungen zum Erlaß entsprechender Landesverordnungen für die Kommunen und für andere öffentliche Stellen für verbindlich erklären. Der Wille des Gesetzgebers, wie er im Wortlaut des § 12 NDSG seinen Niederschlag gefunden hat, wird damit allerdings unterlaufen.

4. Datenübermittlungen ins Ausland (VV-Nr. 12.1)

Ins Ausland dürfen personenbezogene Daten übermittelt werden, wenn die Voraussetzungen erfüllt sind, die bei einer Datenübermittlung im Inland vorliegen müssen, und wenn darüber hinaus im Empfängerland gleichwertige Datenschutzregelungen gelten. Die Verwaltungsvorschriften gehen davon aus, daß die zuletzt genannte Voraussetzung erfüllt ist, wenn die Grundsätze des Übereinkommens des Europarates über den Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28. Januar 1981 (BGBl. 1985 II S. 538) verwirk-

licht worden sind. Für die Mitgliedsstaaten der Europäischen Union - mit Ausnahme Griechenlands - wird dies unterstellt.

Eine solche pauschale Annahme gleichwertiger Datenschutzregelungen ist nicht gerechtfertigt. Die Europäische Datenschutzkonvention verpflichtet die Vertragsstaaten, die dort niedergelegten Grundsätze als gemeinsames datenschutzrechtliches Minimum zu verwirklichen, trifft aber keine entsprechende selbständige Anordnung. Ob und inwieweit die Umsetzung in innerstaatliches Recht tatsächlich erfolgt, ist nicht sichergestellt. Deshalb ist es nicht gerechtfertigt, bei den Unterzeichnerstaaten ohne weiteres davon auszugehen, daß gleichwertige Datenschutzregelungen bestehen. Ebensowenig kann unterstellt werden, daß dies bei den Mitgliedsstaaten der Europäischen Union der Fall ist. Anstelle der pauschalen Feststellung der Gleichwertigkeit bedarf es eines Vergleichs des national geltenden Rechts mit den Regelungen des NDSG. Dabei ist u.a. von Bedeutung, ob der für das niedersächsische Recht zentrale Grundsatz der Zweckbindung gilt. Erst eine solche nähere inhaltliche Überprüfung kann zur entsprechenden Feststellung der Gleichwertigkeit der ausländischen Regelungen führen.

5. Löschung personenbezogener Daten in Akten (VV-Nr. 15.2)

Personenbezogene Daten in Akten, die zur Aufgabenerfüllung insgesamt nicht mehr erforderlich sind und die das zuständige Archiv nicht übernommen hat, sind zu löschen. Wie lange Akten zur Aufgabenerfüllung benötigt werden, kann in Rechts- oder Verwaltungsvorschriften (für die niedersächsische Landesverwaltung z.B. in der Niedersächsischen Aktenordnung oder im Niedersächsischen Aktenplan) geregelt sein. Fehlt es an solchen generellen Festlegungen, muß jeweils im Einzelfall entschieden werden, ob eine Akte zur Aufgabenerfüllung noch weiter aufbewahrt werden darf. Um diese verwaltungsaufwendige Einzelfallprüfung zu vermeiden, sollten Kommunen und andere öffentliche Stellen mit dem Recht der Selbstverwaltung regelmäßig eigene Verwaltungsvorschriften zur Aktenaufbewahrung erlassen. Dies ist z.B. für Personalakten erforderlich, sofern die VV zum NBG (Nds. MBl. 1993, 93) nicht für anwendbar erklärt worden sind.

## 6.2 Was ist privat - was öffentlich?

Es ist oft unklar, wann eine datenverarbeitende Stelle als öffentliche, wann als nicht-öffentliche (private) Stelle anzusehen ist. Davon ist nämlich abhängig, ob das NDSG oder, bei Privaten, das BDSG anzuwenden ist. So bat mich z.B. das "Forschungsinstitut Frau und Gesellschaft" um Bewertung ihres datenschutzrechtlichen Status'. Das Institut ist eine gemeinnützige GmbH, deren einziger Gesellschafter und hauptsächlicher Zuwendungsgeber das Land Niedersachsen ist. Die Mitglieder des Aufsichtsrates werden vor allem durch niedersächsische Ministerien gestellt. Trotz der Vielzahl öffentlich-rechtlicher Bezüge handelt es sich bei dieser Forschungsgesell-

schaft aber um eine nicht-öffentliche Stelle im Sinne des Datenschutzrechts.

Nach § 2 Abs. 1 Satz 1 NDSG ist das Gesetz auf öffentliche Stellen des Landes, der Kommunen, der sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts und deren Vereinigungen anzuwenden. Auch privatrechtlich organisierte Vereinigungen können öffentliche Stellen im Sinne des Datenschutzrechts sein. Allerdings muß es sich bei den Vereinigungen, wie mit dem Wort "deren" im Gesetzestext zum Ausdruck gebracht wurde, um solche handeln, die die in den Nrn. 1 bis 3 genannten Stellen untereinander gebildet haben. Nicht mit erfaßt sind also Vereinigungen z.B. allein des Landes, wie etwa eine vom Land gegründete Gesellschaft mit beschränkter Haftung. Diese fällt in der Anwendungsbereich des BDSG. Nr. 1.1. der VV zum NDSG sieht deshalb vor, daß eine nur vom Land oder einer Gemeinde gegründete Gesellschaft als private Stelle anzusehen ist, für die das BDSG, nicht das NDSG gilt.

## 6.3 Abgabe von Eingaben an die zuständige Behörde; Einholung behördlicher Stellungnahmen

Ein häufiger Fall in der Verwaltungspraxis: Eine Bürgerin oder ein Bürger, die bei der örtlichen Verwaltungsbehörde kein offenes Ohr für ihr Anliegen gefunden haben, wenden sich an die Ministerien und erbitten deren Hilfe, oft in der Erwartung, die Ministerin oder der Minister persönlich werde sich ihrer Belange annehmen.

Eine solche Erwartung aber wird zumeist enttäuscht: Das Ministerium gibt die Eingabe in der Regel an die zuständige nachgeordnete Behörde ab. So erhält der Bürger Mitteilung von einer Stelle, an die er bei seiner Eingabe möglicherweise nicht gedacht oder von der er sich vielfach keine wirksame Hilfe versprochen hat. In mehreren Fällen haben Bürgerinnen und Bürger diese behördliche Verfahrensweise kritisiert.

Unter Datenschutzgesichtspunkten ist gegen die geschilderte Praxis im Grundsatz jedoch nichts einzuwenden. Die Ministerien haben sich im Verwaltungsvollzug im wesentlichen auf allgemeine ressortlenkende Aufgaben, die Richtliniensetzung, landesweite Planungsaufgaben sowie die zentrale Dienst- und Fachaufsicht zu beschränken. Die Prüfung von Einzelfällen ist dagegen Aufgabe der nachgeordneten Behörden. Die Weiterleitung einer Eingabe stellt eine Datenübermittlung an eine andere öffentliche Stelle dar. Sie ist nach § 11 Abs. 1 NDSG zulässig, da sie zur Aufgabenerledigung der zuständigen nachgeordneten Stelle erforderlich ist. Denn nach der Zuständigkeitsordnung ist es Aufgabe der Ortsbehörde, sich der Angelegenheit anzunehmen. Im Falle einer Beschwerde ist die nächsthöhere Aufsichtsbehörde einzuschalten. Die Abgabe an die zuständige Behörde hält sich auch im Rahmen der gesetzlich geforderten Zweckbindung. Mit der Weiterleitung des Schreibens werden die Daten zu dem Zweck verwandt - nämlich der Prüfung der Angelegenheit, um die es dem Bürger geht -, zu dem sie erstmals gespeichert worden sind.

Bearbeitet die Aufsichtsbehörde eine Eingabe selbst, so wird sie regelmäßig die Ortsinstanz zur Aufklärung des Sachverhaltes einschalten. Dabei ist es üblich, im Rahmen der Anforderung einer Stellungnahme eine Ablichtung des Beschwerdeschreibens zu übersenden. Auch hiergegen bestehen nach § 11 Abs. 1 NDSG grundsätzlich keine Bedenken. Im Regelfall kann die Behörde davon ausgehen, daß die Weitergabe für die ihr obliegende Prüfung erforderlich ist. Wie die Verwaltungspraxis zeigt, ist eine gründliche und zuverlässige Prüfung regelmäßig nur möglich, wenn der Wortlaut des Schreibens des Betroffenen der um Stellungnahme angegangenen Verwaltungsbehörde bekannt ist.

Allerdings kann diese Verfahrensweise in Einzelfällen Probleme aufwerfen. Sofern aus einer Eingabe deutlich erkennbar wird, daß der Betroffene die Abgabe an eine andere Behörde oder deren Einschaltung nicht wünscht, sollte eine entsprechende Datenübermittlung ohne sein Einverständnis nicht erfolgen. In dieser Weise sollte z.B. auch dann verfahren werden, wenn der Bürger durch eine Weiterleitung seines Schreibens möglicherweise Nachteile befürchten muß, etwa weil er sich in der Erregung über eine aus seiner Sicht unverständliche Behördenentscheidung bei seiner Kritik im Ton vergriffen hat.

Von den mir vorgetragenen Fällen will ich hier beispielhaft folgenden nennen: Ein Ratsherr hatte schon mehrfach die Vorgehensweise seiner Gemeinde bei Grundstücksverkäufen kritisiert. Er wandte sich schließlich an den zuständigen Minister. In seinem Schreiben erbat er im wesentlichen eine Beantwortung von einschlägigen Rechtsfragen. Das Ministerium gab sein Schreiben an die zuständige Bezirksregierung ab. Diese wiederum leitete es der Gemeinde mit der Bitte um Stellungnahme zu. Der Hauptverwaltungsbeamte gab den Ratsmitgliedern eine Ablichtung (zu dieser Problematik vgl. 16.2). So hatte schließlich jedes Ratsmitglied das aus Sicht des Betroffenen nur für den Minister bestimmte Schreiben in der Hand. Hier hätte die Bezirksregierung von der Weiterleitung der vollständigen Eingabe an die Gemeinde absehen sollen, da die in Rede stehenden Fragen auch ohne die persönlichen Bemerkungen des Petenten und seine Namensangabe hätten beantwortet werden können.

## 6.4 Datenschutzrecht geht alle an!

Ich bin nach Kräften bemüht, Bürgerinnen und Bürgern, aber auch öffentlichen und privaten Stellen, in Datenschutzangelegenheiten zu unterstützen und ihnen bei der Problemlösung zu helfen. Diese Aufgabe sehe ich als einen Schwerpunkt meiner Tätigkeit an.

Mehrfach habe ich allerdings feststellen müssen, daß meine Beratungsfunktion von öffentlichen Stellen auch mißverstanden wird. So haben nach Inkrafttreten des NDSG die Fälle zugenommen, in denen Behörden, ohne sich offenbar selbst mit den von ihnen aufgeworfenen Fragen näher auseinanderzusetzen, die direkte Lösung von mir erwarteten.

Stellvertretend hierfür sei das Beispiel einer Bezirksregierung genannt: Sie wurde im Rahmen einer Landtagseingabe vom zuständigen Fachministerium um Stellungnahme zu dem vom Petenten geschilderten Sachverhalt in tatsächlicher und rechtlicher Hinsicht gebeten. Dabei sollte sich die rechtliche Prüfung nach dem Wunsch des Ministeriums ausdrücklich auch auf eine datenschutzrechtliche Bewertung erstrecken. Hiermit hielt sich die Bezirksregierung jedoch nicht lange auf. Offenbar nach dem Motto: "Wozu haben wir einen Datenschutzbeauftragten im Lande?" schickte sie mir mit Kurzmitteilung ohne jedes erläuternde Wort den Vorgang zur Stellungnahme. Diesem Wunsch habe ich mich in diesem Fall aus grundsätzlichen Erwägungen entziehen müssen.

Datenschutz ist eine Aufgabe, mit der sich jede Stelle eigenverantwortlich zu befassen hat. Denn neben der Beachtung fachspezifischer Vorschriften gehört auch die Einhaltung datenschutzrechtlicher Bestimmungen zur rechtmäßigen Aufgabenerfüllung der öffentlichen Verwaltung. Jede öffentliche Stelle ist deshalb selbst zur Prüfung verpflichtet, ob die Verarbeitung personenbezogener Daten mit den Datenschutzvorschriften im Einklang steht (vgl. VV-NDSG Nr. 17). Die Beratungsfunktion des Landesbeauftragten für den Datenschutz kann nur ergänzende Hilfestellung geben, nicht aber an die Stelle eigenverantwortlicher Aufgabenwahrnehmung treten.

## 7. Statistik

### 7.1 Mikrozensus: aus der Vergangenheit nichts gelernt

Vom Bundesministerium des Innern wurde ein Arbeitsentwurf (Stand April 1994) für ein novelliertes Mikrozensusgesetz vorgelegt. Dieser Arbeitsentwurf sieht eine Ausweitung der Auskunftspflicht auch auf solche Erhebungsmerkmale vor, deren Beantwortung bisher freiwillig war. Außerdem sollen ab 1996 neue Erhebungsmerkmale aufgenommen werden, die ebenfalls der Beantwortungspflicht unterfallen sollen. Schließlich soll eine Reihe von Merkmalen in kürzeren Abständen (nach einem Jahr statt drei Jahren) wieder erhoben werden.

Die Ausweitung der Auskunftspflicht steht im Gegensatz zu den im Volkszählungsurteil des BVerfG genannten Grundsätzen, wonach Statistikdaten soweit wie möglich auf freiwilliger Basis zu erheben sind. Durch die geplante Erweiterung des Erhebungsprogramms wächst die Gefahr einer detaillierten Registrierung der Persönlichkeit der Betroffenen und damit der Wunsch nach Persönlichkeitsprofilen. Ich trete weiterhin dafür ein, der Freiwilligkeit der Beantwortung von Fragen den eindeutigen Vorrang einzuräumen und den Umfang der Datenerhebung auf die strikte Notwendigkeit der Statistik zu beschränken.

Das Niedersächsische Innenministerium hat mir mitgeteilt, daß der Vorentwurf auf einer gemeinsamen Sitzung der Dienstaufsichtsbehörden der Statistischen Ämter der Länder und des Interministeriellen Ausschusses für Koordinierung und Rationalisierung der Statistik erörtert wurde. Hierbei wurde der Vorentwurf von den Vertretern aller Länder aus inhaltlichen und aus Kostengründen abgelehnt. Da das z.Zt. geltende Mikrozensusgesetz bis zum 31. Dezember 1995 befristet wurde, ist im nächsten Jahr mit einer Verabschiedung des neuen Gesetzes zu rechnen. Das Innenministerium hat mir meine Beteiligung im Rahmen des Statistischen Landesausschusses zugesichert. Ich werde dort die bereits schriftlich mitgeteilten Bedenken nochmals vortragen.

## 7.2 Strafverfolgungsstatistik - noch immer ohne Rechtsgrundlage

Die Landesregierung teilt meine Auffassung, daß die Verabschiedung eines Strafverfolgungsstatistikgesetzes dringend erforderlich ist. Meines Erachtens wäre es problematisch, wenn hierbei die Verknüpfung unterschiedlichen Statistiken auf dem Gebiet der Strafrechtspflege zugelassen würde.

Wie berechtigt meine Forderung nach einer klaren gesetzlichen Grundlage für Strafverfolgungsstatistiken ist, mag folgender praktische Fall verdeutlichen: Vom Niedersächsischen Justizministerium wurde ich darüber unterrichtet, daß ein süddeutscher Kriminologe alljährlich die Magnetbänder mit den Landessummen der Strafverfolgungsstatistik vom Statistischen Bundesamt übermittelt bekommen möchte. Der Professor wertet die Statistik aus und hätte gern "zwecks technischer Vereinfachung" die Angaben auf elektronischen Datenträgern verfügbar. Dies ist problematisch, da sich aus den auf Landesebene aggregierten Daten des Bundesamtes in Einzelfällen (z.B. bei spektakulären Straftaten) Einzelpersonen eindeutig identifizieren lassen.

Da keine bereichsspezifischen Regelungen bestehen, mußte ich bei der Beurteilung des Anliegens auf allgemeine Datenschutzregelungen zurückgreifen. Die Forschungsklausel des NDSG war auf diesen Fall nicht anwendbar; vielmehr war hier allgemeines Statistikrecht heranzuziehen. Nach § 16 Abs. 6 BStatG dürfen für die Durchführung wissenschaftlicher Vorhaben Einzelangaben übermittelt werden, wenn "die Einzelangaben nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können" und die Empfänger Amtsträger oder sonstwie zur Geheimhaltung verpflichtet sind. Eine entsprechende Regelung besteht für Landesstatistiken in § 8 Abs. 3 NStatG. Die beabsichtigte Übermittlung an den Kriminologen erfüllt diese Voraussetzungen nicht. Der Forscher will die Daten allgemein zu wissenschaftlichen Zwecken nutzen, ohne daß die Forschungsvorhaben zuvor eindeutig bestimmt wurden. Aus § 16 Abs. 8 BStatG, der davon ausgeht, daß die wissenschaftliche Arbeit inhaltlich und zeitlich begrenzt ist, ergibt sich, daß nur einzelne konkrete Forschungsvorhaben eine Übermittlung begründen können. Die Landesdienststellen haben sich gegenüber dem Statistischen Bundesamt entprechend meiner Empfehlung gegen die geplante Datenübermittlung ausgesprochen.

7.3 Finanz- und Personalstatistik im öffentlichen Dienst - Statistikgeheimnis ade?

Am 21. Dezember 1992 wurde das Gesetz über die Statistiken der öffentlichen Finanzen und des Personals im öffentlichen Dienst (Finanz- und Personalstatistikgesetz - FPStatG -) verkündet (BGBl. I S. 2119). Gegenüber dem alten Finanzstatistikverfahren werden mehr und differenziertere Merkmale erhoben. Damit wird das Reidentifizierungsrisiko erheblich erhöht. Unbefriedigend ist auch, daß die auskunftspflichtigen Stellen, deren Daten nicht in automatisierter Form verfügbar sind, nur bis 1997 geschätzte Summensätze angeben dürfen. Durch diese Regelung wird ein mittelbarer Druck ausgeübt, die Personaldatenverarbeitung auch dort zu automatisieren, wo ansonsten keine Notwendigkeit für einen EDV-Einsatz besteht. Zu kritisieren ist schließlich, daß Tabellen an oberste Bundes- oder Landesbehörden für die Verwendung gegenüber den gesetzgebenden Körperschaften und für Zwecke der Planung übermittelt werden dürfen, auch insoweit Tabellenfelder nur einen einzigen Fall ausweisen. All diese Bedenken konnte ich nicht rechtzeitig vorbringen, da ich an diesem Gesetzesvorhaben nicht beteiligt worden bin.

7.4 Sozialhilfestatistik

Aus anderen Bundesländern wurde ich darüber unterrichtet, daß dort zusätzlich zu den amtlichen Vordrucken des Statistischen Landesamtes Ergänzungsbogen eingeführt wurden, in denen von Sozialhilfeempfängern weitere Fragen beantwortet werden sollen. Diese Datenerhebung stützt sich auf die durch das Gesetz zur Umsetzung des föderalen Konsolidierungsprogramms vom 23. Juni 1993 (BGBl. I S. 944 ff.) geänderten §§ 127 ff. BSHG. Hiernach werden u.a. folgende Daten für Statistikzwecke verlangt: Angaben zur Staatsangehörigkeit, Angaben zur besonderen sozialen Situation bei der Hilfegewährung wie Freiheitsentzug, Haftentlassung und Suchtabhängigkeit, Angaben zur Einstellung der Sozialhilfe, bei Beendigung der Sozialhilfegewährung durch Aufnahme einer Erwerbstätigkeit, Angaben zur Art dieser Tätigkeit und Angaben zum höchsten allgemeinbildenden Schulabschluß und zum höchsten Berufsbildungsabschluß. Diese Daten sind - jedenfalls im Regelfall - für die Zwecke der Sozialhilfegewährung nicht erforderlich. Insofern stellt sich die Frage, auf welcher Rechtsgrundlage diese Daten erhoben werden. § 60 SGB I findet keine Anwendung, wenn die Daten für die Leistung nicht erheblich sind. Eine Erhebung auf freiwilliger Basis würde voraussetzen, daß nach den statistikrechtlichen Vorschriften im Rahmen einer Sekundärstatistik eine eigenständige Erhebung für statistische Zwecke (Primärstatistik) durchgeführt werden darf. Zur Klärung dieser Frage habe ich Kontakt mit dem Niedersächsischen Innenministerium und dem Niedersächsischen Sozialministerium aufgenommen.

Für den Fall der Zulässigkeit einer solchen Primärstatistik halte ich es für eine datenschutzgerechte Lösung, wenn den Antragstellern/Hilfeempfängern ein statistischer Erhebungsbogen vorgelegt wird, in dem die ausschließlich für die Bundessozialhilfestatistik erforderlichen Daten erfragt werden. Die-

ser Bogen ist unter Hinweis auf die gesetzlichen Grundlagen eindeutig als freiwillig zu kennzeichnen. Die Betroffenen sind darüber zu informieren, daß ein Nichtausfüllen keinerlei Nachteile hinsichtlich ihres Antrages auf Sozialhilfe mit sich bringt. Überdies muß für die Betroffenen ersichtlich sein, daß die Angaben einzig zum Zwecke der Sozialhilfestatistik erhoben werden und nicht anderweitig durch das Sozialamt genutzt werden dürfen. Sie sind im Sozialamt vom übrigen Sozialhilfevorgang abgeschottet abzulegen und nur für die Zusammenführung im statistischen Erhebungsbogen zu nutzen. Eine solche Handhabung ergibt sich zwangsläufig aus dem im Zusammenhang mit dem Volkszählungsurteil des Bundesverfassungsgerichts aufgestellten Abschottungsgebot für statistische Erhebungen.

### 7.5 Agrarstatistik - zukünftig per Satellit?

Vom Niedersächsischen Ministerium für Ernährung, Landwirtschaft und Forsten wurde ich frühzeitig um eine datenschutzrechtliche Bewertung des EG-Beschlußentwurfes zum Einsatz der Fernerkundung in der Agrarstatistik gebeten. Da hierin Festlegungen und Aussagen über Umfang und Durchführung der Datenerhebung, über die gespeicherten Daten, deren konkrete Zweckbestimmung und über technische und organisatorische Maßnahmen zur Datensicherung fehlen, konnte ich noch keine abschließende datenschutzrechtliche Bewertung vornehmen.

Unabhängig davon habe ich gegen eine flächendeckende Erfassung aller landwirtschaftlichen Flächen erhebliche grundsätzliche Bedenken, die in die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 1993 zum Integrierten Verwaltungs- und Kontrollsystem (InVeKos) Eingang gefunden haben (Anlage 8). Der EG-Beschlußvorschlag erfüllt nicht die vom Bundesverfassungsgericht im sog. Volkszählungsurteil festgestellten Voraussetzungen der Normenklarheit und der Verhältnismäßigkeit. Aus dem Entwurf kann kein Betroffener erkennen, welche Daten über ihn erhoben werden und ob diese Daten zur Aufgabenerfüllung erforderlich sind. Das Volkszählungsurteil verlangt aber ausdrücklich, daß der Betroffene das Recht hat, zu erfahren, "wer was wann und bei welcher Gelegenheit über ihn weiß." Hinzu kommt, daß der Beschlußvorschlag eindeutig unverhältnismäßig wäre, da durch eine flächendeckende Erfassung aller landwirtschaftlichen Flächen nicht nur diese Flächen, sondern komplette Regionen einschließlich aller Wohnsiedlungen erfaßt würden. Das würde bedeuten, daß nicht nur die Daten der Landwirte, sondern auch die Daten einer Vielzahl Nichtbetroffener gespeichert würden. Ich habe daher dem Ministerium empfohlen, den Beschlußvorschlag abzulehnen.

## 8. Archivwesen: Das neue Niedersächsische Archivgesetz

Das in meinem letzten Tätigkeitsbericht (vgl. XI 8) angesprochene Gesetz über die Sicherung und Nutzung von Archivgut in Niedersachsen (Nieder-

sächsisches Archivgesetz - NArchG), zu dessen Entwurf ich mehrfach Stellung genommen hatte, ist 1993 vom Parlament verabschiedet worden (Nds. GVBl. S. 129); die Verwaltungsvorschriften hierzu werden im Nds. MBl. Anfang 1995 veröffentlicht.

Das Gesetz bestimmt, daß Schriftgut der Behörden, Gerichte und sonstigen Stellen des Landes, dessen Aufbewahrungsfrist abgelaufen ist, den Staatsarchiven anzubieten ist. Diese prüfen, ob das Schriftgut von bleibendem Wert für die Erfüllung öffentlicher Aufgaben, für die Sicherung berechtigter privater Interessen oder für die Forschung und somit als Archivgut aufzubewahren ist. Der Begriff des Schriftguts ist weit gefaßt; dazu gehören nicht nur Akten im traditionellen Sinne, sondern alle Informationen, die in einer bestimmten Form verkörpert (z.B. Film- oder Videoaufnahmen) oder maschinenlesbar gespeichert sind. Die Archivierung erstreckt sich damit auch auf Informationsträger im Rahmen neuer Bürokommunikationsformen.

Kommunen und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts können ihr Schriftgut zwar auch den Staatsarchiven anbieten; in der Regel aber dürften sie eigene oder gemeinsame Archive unterhalten. Soweit sie ihr Archivgut selbst verwalten, gelten für sie dieselben Vorschriften zur Sicherung und Nutzung des Schriftguts und zur Gewährleistung des informationellen Selbstbestimmungsrechts wie für die Staatsarchive.

Zur Wahrung der schutzwürdigen Belange der Betroffenen sieht das Gesetz erst nach Ablauf von relativ langen Schutzfristen eine archivalische Nutzung durch die Allgemeinheit zu wissenschaftlichen Zwecken oder bei sonstigem berechtigten Interesse vor:

- 30 Jahre nach der letzten inhaltlichen Bearbeitung oder
- bei Unterlagen zu einer bestimmten Person 10 Jahre nach deren Tod.

Betroffene haben neben einem Auskunftsanspruch über die sie betreffenden Daten ein Akteneinsichtsrecht.

## 9. Neue Medien

### 9.1 Telekommunikation

#### 9.1.1 Rechtsgrundlagen in Bewegung

Mehr als 100 Jahre lang war die Telekommunikation rund um den Globus eine Staatsaufgabe. Das Telefon- und Postgeheimnis nach Art. 10 GG ist eine verfassungsrechtliche Datenschutznorm, deren Wirksamkeit gesichert schien. Am 1. Januar 1995 wird die Deutsche Bundespost Telekom Aktiengesellschaft (AG) und damit die Telekommunikation in der Bundesrepublik Deutschland privatisiert. 1998 fällt schließlich das letzte Monopol im Telefondienst. Auf die mit der Privatisierung öffentlicher Aufgaben verbundenen

datenschutzrechtlichen Probleme hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in zwei Entschließungen hingewiesen (Anlagen 4 und 13). Sie hat gefordert, daß durch die Privatisierung der Schutz der Bürgerinnen und Bürger nicht verringert werden darf und daß für die künftige Telekom-AG und ihre Tochterunternehmen eine einheitliche Datenschutzkontrolle zu gewährleisten ist, bei der, wie bisher, eine Kontrolle von Amts wegen möglich ist. Dies ist erforderlich, weil gerade im Bereich der Telekommunikation nur noch wenige durchschauen können, welche personenbezogenen Daten über sie gespeichert und ausgewertet werden.

Auch wenn das Gesetz zur Neuordnung des Postwesens und der Telekommunikation (PTNeuOG) gerade noch vor Ende der 12. Legislaturperiode des Deutschen Bundestages beschlossen wurde, um damit die Voraussetzungen für die Privatisierung der Telekommunikation zu schaffen, sind doch viele Fragen offen geblieben (BGBl. I 1994 S. 2325). Mit dem Inkrafttreten des PTNeuOG zum 1. Januar 1995 wird nämlich die notwendige Rechtsverordnung zur Regelung des Datenschutzes in der Telekommunikation fehlen. Ungeklärt und strittig ist, ob die bestehenden Regelungen der Telekom-Datenschutz-Verordnung (TDSV) und Teledienstunternehmen-Datenschutz-Verordnung (UDSV) über den 1. Januar 1995 hinaus rechtsverbindlich bleiben. Weiterhin unklar ist, ob die Kontrolle über die Telekom und ihre Töchter weiterhin dem Bundesbeauftragten für den Datenschutz obliegt oder ob sie auf die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich übergeht. Die notwendige Klarheit sollte umgehend geschaffen und die Datenschutzverordnung beschlossen werden.

Auf der Ebene der Europäischen Union ist die Absicht bekräftigt worden, europaweit bereichsspezifische Regelungen zum Datenschutz in Telekommunikationsnetzen zu schaffen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung zum geänderten Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994 einige Verbesserungsvorschläge gemacht, um so einen einheitlichen Datenschutzstandard zu sichern. Sie hat die Bundesregierung aufgefordert, in ihrer Ratspräsidentschaft im zweiten Halbjahr 1994 den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen (Anlage 22).

Der Ministerrat der Europäischen Gemeinschaften hat am 22. Juni 1993 beschlossen, daß die Monopole im öffentlichen Sprachtelefondienst europaweit bis zum 1. Januar 1998 beseitigt werden müssen. Dies wird zu einem massiven Wettbewerb zwischen zahlreichen europäischen Netzanbietern führen. Spätestens zu diesem Zeitpunkt muß dann auch das Problem eines einheitlichen Datenschutzstandards in der Europäischen Union gelöst und die Richtlinie für das ISDN verabschiedet sein. Dieser Regelungsbedarf gilt schon heute für die Mobilkommunikation, die ja längst grenzüberschreitend betrieben wird. Es müssen wirksame Vorkehrungen gegen das Erstellen von Bewegungsbildern getroffen werden. Auch müssen die Daten der Mobilfunkteilnehmer auf der Funkstrecke wirksam verschlüsselt werden, um die Vertraulichkeit der Kommunikationsinhalte besser als bisher zu sichern. Eine bloße Digitalisierung der Signale reicht nicht aus. Den Benutzerinnen

und Benutzern sollte eine kostenlose Ende-Zu-Ende-Verschlüsselung auf Unionsebene garantiert werden.

9.1.2 Wie lange dürfen Telefondaten gespeichert werden?

Obwohl die TDSV eine Speicherung der Abrechnungsdaten bis zu achtzig Tagen nach Versenden der Entgeltrechnung zuläßt, hat das Oberverwaltungsgericht Bremen (CR 1994, 700) entschieden, daß die Telekom die vollständigen Telefondaten von Anrufern mit ISDN-Anschluß nicht so lange speichern darf. Danach sind die letzten drei Ziffern der Rufnummern bei technisch störungsfreiem Ablauf spätestens ab dem Ende des vierten Arbeitstages nach Verbindungsende zu löschen. Das Gericht sah das Grundrecht auf informationelle Selbstbestimmung verletzt, da die Telekom ohne Wissen der Betroffenen Datum, Uhrzeit und die volle Rufnummer aller Anrufe aus dem ISDN-Netz erfaßt und für eine zu lange Zeit speichert. Darüber hinaus verletze es das Fernmeldegeheimnis, daß die Telekom auf einer detaillierten Fernmelderechnung diese Daten ohne Einwilligung der Angerufenen herausgibt. Auch wenn die Telekom gegen das Urteil Revision eingelegt hat, so hält sie sich in der Praxis an die Vorgaben des Urteils. Auf den Entgeltabrechnungen mit detailliertem Einzelnachweis werden mittlerweile die drei letzten Ziffern der Zielnummern nicht mehr ausgewiesen.

9.1.3 Anzeige der Rufnummer beim Angerufenen

Seit dem 1. Januar 1994 haben Telefonkundinnen und -kunden das Recht, fallweise - also bei jedem Telefongespräch - darüber zu entscheiden, ob sie die bei ISDN-fähigen Telefonapparaten mögliche Anzeige ihrer Rufnummern bei den Angerufenen unterdrücken wollen oder nicht.

Diese Wahlmöglichkeit wird durch die Gebührenpolitik der Deutschen Bundespost Telekom jedoch gefährdet. Die fallweise Unterdrückung der Rufnummer ist nämlich kostenpflichtig, gebührenfrei ist dagegen nur die ständige Unterdrückung. Da aber zahlreiche Personen und Institutionen die Annahme eines Anrufs von der Anzeige der Rufnummer der Anrufenden abhängig machen werden, werden die Nutzenden der ständigen Rufnummernunterdrückung in ihren Kommunikationsmöglichkeiten eingeschränkt. Ich habe datenschutzrechtliche Bedenken gegen diese Verfahrensweise, zumal auch der Vorschlag für die ISDN-Richtlinie der Europäischen Union ein gebührenfreies Angebot dieser Funktion vorsieht. Den Kundinnen und Kunden, die sich grundsätzlich für die Unterdrückung entschieden haben, muß die technische Möglichkeit eröffnet werden, auch im Einzelfall die Nummernanzeige freizugeben, und zwar kostenfrei.

Es ist mehrfach beobachtet worden, daß auch die Rufnummer von Analoganschlüssen (sog. ANIS-Anschlüsse) ungewollt und unbemerkt bei den Angerufenen mit ISDN-fähigen Apparaten angezeigt worden ist. Die Anzeige der Rufnummer von ANIS-Anschlüssen ist nach den Bestimmungen der TDSV nicht zulässig. Die Telekom hat diese Fehler zugegeben und zugleich

bestätigt, daß die Übermittlung der Rufnummer von ANIS-Anschlüssen auch zukünftig nicht vorgesehen sei.

9.1.4 Vertrauensschutz für Beratungsstellen

Unter XI 9.1.4 habe ich auf Beeinträchtigungen telefonischer Beratungstätigkeiten durch einen vollständigen Ausdruck aller geführten Telefongespräche in Einzelentgeltnachweisen aufmerksam gemacht. Meinen Handlungsempfehlungen sind viele Beratungsstellen gefolgt, leider nicht immer mit dem erhofften Erfolg. Die Anerkennung als Beratungsstelle hat sich häufig als "Glückspiel" erwiesen, da äußerst restriktiv entschieden wurde. Auch ist vielfach unklar geblieben, wer zu entscheiden hat. Einmal war es die Telekom, dann der Diensteanbieter. Die Telekom verweist jetzt in Formbriefen an Beratungsstellen generell auf die gegenwärtige Verkürzung der Zielnummern in Einzelentgeltnachweisen um die letzten drei Stellen. Das reicht für viele Beratungsstellen nicht aus, da deren Rufnummer auch nach der Verkürzung durch ihre Eigenart erkennbar bleibt. Ich empfehle diesen Stellen, sich erneut an die Telekom zu wenden, um zu erreichen, daß die betreffenden Anrufe in den Einzelentgeltnachweisen überhaupt nicht ausgewiesen, sondern in einer Summenzeile unter "Sonstige Verbindungen" aufsummiert werden. Diesem Begehren wird auch in aller Regel entsprochen.

Schwierigkeiten bereitet auch die Unterdrückung der Rufnummernanzeige bei Beratungsstellen, wenn dort Telefonnebenstellenanlagen betrieben werden. Zum einen ist die Kennzeichnung in den Kundenverzeichnissen der Telekom unvollständig, zum anderen ist es zweifelhaft, ob die Unterdrückung bei allen Telefonnebenstellenanlagen technisch gelingt.

9.1.5 Suchmöglichkeiten bei elektronischen Telefonverzeichnissen

Seit langem geben private Unternehmen elektronische Telefonverzeichnisse auf CD-ROM heraus. Neu sind Suchhilfen, die neben den traditionellen Kriterien "Ort und Name" auch die Suche nach der "Rufnummer" zulassen, um so alle weiteren Einträge über die Telefonkundin bzw. den Telefonkunden zu ermitteln. Teilweise erhält man bei der Suche unter dem Namen auch alle Einträge des betreffenden Namens in allen Orten oder bei der Eingabe von einzelnen Eintragungsbestandteilen alle Einträge, die entsprechende Eintragungsbestandteile enthalten ("Sternchensuche"). Die elektronischen Verzeichnisse und die sog. "Invertierte Suche" nach dem Namen der Telefonkundin oder des Telefonkunden sind in der parlamentarischen Diskussion zur TDSV und UDSV kritisch diskutiert worden. § 10 Abs. 1 TDSV/UDSV enthält eine Erlaubnis, auch elektronische Verzeichnisse herauszugeben, jedoch keine Vorgaben für deren Gestaltung. Da die Kundinnen und Kunden selbst bestimmen können, ob und in welcher Weise sie ins Telefonbuch eingetragen werden möchten und die Telekom sie darauf ausdrücklich hinweist, wird von der Einwilligung in Speicherung und Verwendung der Telefonbuchdaten ausgegangen. Sicherzustellen sind allerdings die unverzügliche Realisierung eines Widerspruchs und das Recht auf Be-

schränkung des Eintrages (§ 10 Abs. 3 TDSV). Dem Persönlichkeitsrecht der Kundin bzw. des Kunden sollte darüber hinaus dadurch Rechnung getragen werden, daß bei Abonnements von CD-ROM die Rücknahme der jeweils nicht mehr aktuellen CD-ROM erfolgt.

## 9.2 Telefax

Meine Empfehlungen zum datenschutzgerechten Einsatz von Telefax-Geräten sind auf große Resonanz gestoßen. Meine Orientierungshilfe "Datenschutz bei Telefax" wurde in großer Auflage verteilt. Die organisatorischen Empfehlungen wurden weitgehend umgesetzt. Auch das besondere Problem der schnellen Übermittlung ärztlicher Gutachten als Grundlage einstweiliger Unterbringungen nach dem PsychKG im Raum der Landeshauptstadt Hannover wurde gelöst. In einem Arbeitskreis aller an der Einweisung beteiligter Stellen - mitgearbeitet haben Vertreter aller Krankenanstalten, der Amtsgerichte und der Verwaltungsbehörden - wurde ein einheitliches Verschlüsselungssystem ausgewählt, um so die erforderliche Kommunikationssicherheit gewährleisten zu können. Der Arbeitskreis hat ein Verschlüsselungsgerät mit Chipkarte als Zusatz für alle Telefaxgeräte der Gruppe 3 ausgewählt, so daß beliebige Geräte-Kombinationen möglich sind. Es handelt sich um ein separates Gerät, das nur mit eingesteckter Chipkarte verschlüsselte Informationen senden und empfangen kann. Nachteilig erscheint, daß bei eingesteckter Chipkarte keine unverschlüsselten Informationen empfangen werden können. Dies macht eine kurze telefonische Verständigung erforderlich. Doch die sollte ohnehin erfolgen, um den berechtigten Empfang sicherzustellen. Da Sender und Empfänger mit demselben System ausgestattet sein müssen, ist die verschlüsselte Übermittlung von Daten auf diese Standorte beschränkt. Erfreulich war, daß der Gerätepreis durch die koordinierte Beschaffung aller Beteiligten auf die Hälfte gesenkt werden konnte.

## 9.3 Risiken beim Mobilfunk

Mobile Sprach- und Datenübertragungsdienste boomen zur Zeit. Die Zahl der Nutzerinnen und Nutzer der Funktelefonnetze C und D hat sich zwischen 1990 und heute in Deutschland von 20.000 auf 2,2 Millionen erhöht. Neu auf diesen Markt drängen Diensteanbieter im E-Netz. Der Zuwachs im Mobilfunk geht exponentiell weiter, bis zum Jahr 2000 werden 40 Millionen Mobilfunkteilnehmer in der Europäischen Union erwartet. 80 Millionen sollen es bis zum Jahr 2010 sein. Das mobile Telefon scheint als Statussymbol für Fortschritt und Erfolg angesehen zu werden, das öffentlich zur Schau getragen wird. Keine öffentliche Veranstaltung bleibt ungestört, selbst in Straßenbahn und Bus wird telefoniert. Im italienischen Parlament wurde ein Benutzungsverbot ausgesprochen, um Störungen der Sitzungen zu reduzieren.

Den meisten Teilnehmerinnen und Teilnehmern ist nicht bekannt, daß die Mobilfunkdienste besondere Gefährdungen für den Datenschutz auslösen.

So wird neben den üblichen und zur Abrechnung notwendigen Verbindungsdaten auch erhoben und gespeichert, wo sich der mobile Telefonierer jeweils aufhält. Das ist notwendig, um überall und zu jeder Zeit erreicht werden zu können. Diese Standortinformationen bieten ideale Voraussetzungen, um sog. "Bewegungsprofile" über die Nutzenden zu erstellen. Da im Regelfall alle Informationen unverschlüsselt per Funk übertragen werden, ist darüber hinaus die Vertraulichkeit der Kommunikation gefährdet. Bei satellitengestützten Diensten ist es zudem möglich, die übertragenen Daten im gesamten, teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich der Satelliten unbemerkt abzuhören und aufzuzeichnen.

Viele Nutzenden wissen auch nicht, daß bei der internationalen Mobilkommunikation die Kommunikationsdaten vielfach in solchen Staaten gespeichert und ausgewertet werden, in denen keine gleichwertigen Datenschutzregelungen wie in der Bundesrepublik Deutschland gelten.

In einer Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder werden die Hersteller und Betreiber der Mobilkommunikation aufgefordert, diesen Gefahren für das Fernmeldegeheimnis und für den Persönlichkeitsschutz durch technische Vorkehrungen und organisatorische Gestaltung entgegenzuwirken (Anlage 5). Darüber hinaus sollten sie die Benutzerinnen und Benutzer von mobilen Diensten besser als bisher über die mit der Nutzung verbundenen Risiken und den erreichten Sicherheitsstandard aufklären.

## 9.4 Abhörsicherheit des Funkverkehrs

Von Behörden und Organisationen mit Sicherheitsaufgaben - dazu gehören Polizei, Katastrophenschutz, Zoll, Feuerwehren, Technisches Hilfswerk, Deutsches Rotes Kreuz, Arbeiter-Samariter-Bund, Johanniter-Unfall-Hilfe, Malteser-Hilfsdienst - werden gegenwärtig für den Sprechfunk analoge Geräte mit einem technischen Stand der 70er Jahre eingesetzt, die bekanntlich seit jeher abhörbar sind. So genügte eine kleine Skalenverschiebung am Radioempfänger, um den Polizeifunk mithören zu können. Daß dies strafbar war, hielt die Neugierigen nicht ab, zumal das Entdeckungsrisiko gering war. Nach der Freigabe der Frequenzbereichsgrenzen Mitte 1992 ist der Funkverkehr mit handelsüblichen Radioempfängern ohne jegliche Manipulation abhörbar.

Die Technische Kommission der Konferenz der Innenminister wurde zum Schutz des Funkverkehrs mit der Erarbeitung eines Sicherheitskonzepts beauftragt. Das Land Niedersachsen übernahm es, geeignete Sprachverschleierungs-Systeme zu erproben. Die Technische Kommission kam zu dem Ergebnis, daß die erprobten Geräte die gestellten Sicherheitsanforderungen nicht erfüllen konnten. Das Innenministerium des Landes hat sich trotz dieser Erkenntnisse 1989 für eine "niedersächsische Lösung" entschieden und die vorhandenen Analogfunkgeräte der Polizei mit einer Inverterschaltung nachgerüstet. Bis Ende 1993 wurden alle Geräte mit Sprachverschleierungsmodulen flächendeckend ausgestattet. Diese Lösung bezeichnet das Nie-

dersächsische Innenministerium als eine "erste Stufe der Erschwerung des Abhörens, Mithörens und Auswertens des polizeilichen Sprechfunkverkehrs durch Dritte". Übereinstimmend mit den Datenschutzbeauftragten des Bundes und der Länder halte ich die Inverterschaltung keineswegs für geeignet, die gewünschte Vertraulichkeit des Sprechfunkverkehrs zu erreichen. Es ist heute legal und für einen geringen Preis möglich, Funkempfänger mit Invertern zu beschaffen, um das Mithören "verschleierter" Funkgespräche zu erreichen. Nach Experten-Meinung werden durch den Einsatz von Invertern sogar die Selektionsmöglichkeiten zum Ausforschen sensitiver Informationen "verbessert". Damit ist nicht nur das informationelle Selbstbestimmungsrecht von Betroffenen, sondern auch die Funktionsfähigkeit der jeweiligen Stellen beinträchtigt.

Wie es gemacht wird, zeigt die "Szene", die sich der D-Autotelefonnetze und damit der Digitaltechnik bedient, auf denen sie - hochwertig verschlüsselt und damit nicht abhörbar - ihre "geschäftlichen Absprachen" treffen kann. Die Versuche, die Einsatzfunknetze abhörsicher zu machen, scheitern bisher an fehlender Normung. Zwar haben sich die im Schengener Abkommen zusammengeschlossenen Staaten auf einen Anforderungskatalog für die zukünftigen Funknetze ihrer Sicherheitsbehörden geeinigt, doch die europäische Norm liegt immer noch nicht vor. Damit kann die mehrere Jahre dauernde Entwicklung und Erprobung durch die Hersteller nicht gestartet werden. Allen Beteiligten am Entscheidungsprozeß ist klar, daß an der digitalen Funktechnik kein Weg vorbeiführt. Dieser Weg sollte so schnell als möglich betreten werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf die Gefährdung der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten hingewiesen und die frühestmögliche Absicherung gefordert (Anlage 6).

Als problematisch sehe ich die Aussage des Niedersächsischen Innenministeriums an, daß hier noch weit über das Jahr 2000 hinaus analoge Technik im Sprechfunkverkehr eingesetzt werden soll. Ich habe daran erinnert, daß § 7 des neuen NDSG dazu verpflichtet, die Art und Weise der Sicherungsmaßnahmen nach dem jeweiligen Stand der Technik auszurichten.

## 9.5 Novellierung des Landesrundfunkgesetzes

Ich bin frühzeitig über die Novellierungsabsicht des Landesrundfunkgesetzes unterrichtet und in die Beratung eingebunden worden. Meine Vorschläge wurden bei der Novellierung berücksichtigt. Das neue Niedersächsische Landesrundfunkgesetz vom 9. November 1993 (Nds. GVBl. S. 523) entspricht neueren Entwicklungen, z.B. den Regelungen der Länder Bayern, Berlin und Hamburg. Die erweiterten Datenschutzvorschriften sind in einem eigenständigen Teil des Gesetzes zusammengefaßt worden.

Nicht ausreichend vorbereitet ist das Medienrecht auf "rundfunkähnliche Kommunikationsdienste" wie "pay TV", "pay per view", "video on demand" und andere Formen des interaktiven Fernsehens. Zwar sind Verteildienste im Sinne des Rundfunkstaatsvertrages erfaßt, reine Abruf- und Zugriffs-

dienste jedoch nicht. Insoweit bedarf der Rundfunkstaatsvertrag zumindest einer Klarstellung, in welcher Weise rundfunkähnliche Kommunikationsdienste einbezogen werden. Für den öffentlich-rechtlichen Rundfunk fehlt bisher eine Regelung entsprechend § 28 Rundfunkstaatsvertrag. Klare Regelungen über Abrechnungs- und Verbindungsdaten sind erst noch zu schaffen. Dies setzt eine Entscheidung voraus, daß der öffentlich-rechtliche Rundfunk zumindest für sein eigenes Programmangebot auch die Möglichkeit z.B. zum interaktiven Fernsehen haben soll. Der NDR veranstaltet dies in seinem Dritten Programm seit kurzem versuchsweise. Weiter wäre zu entscheiden, ob dem öffentlich-rechtlichen Rundfunk auch die Möglichkeit offen stehen soll, sein eigenes Programmangebot im Wege von Abruf- und Zugriffsverfahren nutzen zu können.

In jedem Falle setzen Rundfunkdienste und rundfunkähnliche Kommunikationsdienste, bei denen Abrechnungs- und Verbindungsdaten entstehen, datenschutzrechtliche Regelungen im Sinne des § 28 Rundfunkstaatsvertrag voraus. Soweit Telekommunikationsdienste einschließlich ISDN in Anspruch genommen werden, reichen die einschlägigen Datenschutzvorschriften des Bundes nicht. Ihr Adressat sind die Telekommunikationsunternehmen, nicht aber die Veranstalter von Rundfunk oder rundfunkähnlichen Diensten. Notwendig sind für diesen Bereich - wie bei Bildschirmtext - möglichst einheitliche Länderregelungen für die Nutzungsseite. Auf diese Problematik habe ich die Niedersächsische Staatskanzlei aufmerksam gemacht.

## 10. Veröffentlichungen durch die öffentliche Hand

Der Datenschutz ist kein Hinderungsgrund für eine umfassende Information der Öffentlichkeit, auch wenn es um sensible Dinge geht. Dies zeigte sich exemplarisch am folgenden Fall: Die Landeszentrale für politische Bildung erarbeite Unterrichtsmaterial zum Thema "Rechtsextremismus in Deutschland", das kostenlos für Schule und Unterricht abgegeben werden sollte. Ein Arbeitsheft sollte unter anderem eine Reihe von "Portraits" (Darstellung in Bild und Text) von Jugendlichen enthalten, die dem "rechten" und z.T. auch gewaltbereiten Spektrum zugerechnet werden. Alle Texte und Fotos dieser Beiträge waren bereits zu einem früheren Zeitpunkt im Druck öffentlich erschienen, z.B. im "Stern" oder im "Spiegel".

Ich mußte der Landeszentrale mitteilen, daß ich die Herausgabe der Schrift durch sie nur dann für zulässig halte, wenn

- von allen Betroffenen eine Einwilligung eingeholt wird oder
- die namentliche Bezeichnung der Personen für die Erreichung des Zwecks der Broschüre erforderlich ist.

Anders als eine private Person kann sich die öffentliche Hand nicht auf das Grundrecht der Meinungsäußerungsfreiheit (Art. 5 Abs. 1 GG) und das daraus abgeleitete Medienprivileg berufen. Das neue NDSG erfaßt, anders als das alte Recht, neben der Verarbeitung in Dateien auch die Datenverarbeitung in Akten, wozu auch von öffentlichen Stellen herausgegebene Publika-

tionen gehören. Das Bild- und Textmaterial der Landeszentrale war personenbezogen. Auf den Fotos waren die abgebildeten Personen zunächst eindeutig wiederzuerkennen. In den Texten wurden teilweise sehr sensible Aussagen über die abgebildeten Personen gemacht, z.B. über deren politische Anschauung, über begangene Straftaten, über persönliche Verhältnisse usw.

Veröffentlichungen sind aus datenschutzrechtlicher Sicht Datenübermittlungen an einen unbestimmten Empfängerkreis von Personen oder Stellen außerhalb des öffentlichen Bereichs (§ 13 NDSG). Ich äußerte Zweifel, ob die personenbezogene Veröffentlichung in dieser Form "erforderlich" sei. Der Zweck der Publikation konnte auch dadurch erreicht werden, daß die Bilder hinreichend anonymisiert und die Texte so abgewandelt werden, daß eine Identifizierung einzelner beschriebener Personen nicht mehr möglich ist. Zu berücksichtigen war auch, daß durch die personenbezogene Darstellung eine Abstempelung der Betroffenen als gewalttätige, rechtsextremistische Menschen auch für die Zukunft bewirkt werden konnte, was ein besonders massiver Eingriff in deren Persönlichkeitsrechte gewesen wäre. Für unproblematisch hielt ich es, Text und Bilder so zu verändern, daß die Einzelangaben nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (Anonymisierung).

Auch wenn für die Erstveröffentlichung der Bilder und Texte Einwilligungen vorlagen, so wäre die Publikation durch die Landeszentrale doch eine erneute Beeinträchtigung des Persönlichkeitsrechts gewesen. Die Erstveröffentlichung erfolgte durch eine nicht-öffentliche Stelle in einer Zeitschrift, die regelmäßig nur ein Woche lang gelesen wird. Die Zweitveröffentlichung durch eine öffentliche Stelle sollte dagegen über Jahre hinweg genutzt werden. Einem Text einer Landeszentrale für politische Bildung dürfte von der Leserschaft eine größere Autorität zugestanden werden als einer reinen Zeitschriftenveröffentlichung. Angesprochen würde zudem ein anderer Adressatenkreis (Schülerinnen und Schüler). Der mit der Neuveröffentlichung einhergehende Eingriff hätte daher einer neuen gesonderten Einwilligung bedurft.

Die Landeszentrale berücksichtigte meine Bedenken und achtete darauf, daß Bilder und Texte anonymisiert wurden. Als mir Anfang 1994 die fertige Publikation von der Landeszentrale vorgelegt wurde, konnte ich mit Freude feststellen, daß sie nicht nur hervorragend gelungen ist, sondern auch, daß die Anonymisierung der Personenangaben dem Informationsgehalt der Schrift in keinster Weise schadete. Ich meine sogar, daß die offensichtliche Berücksichtigung des Persönlichkeitsrechts auch bei Rechtsextremisten die Seriosität der Publikation eher erhöhte.

## 11. Ausweis- und Meldewesen

### 11.1 Personalausweis im Postamt

Unter XI 11.1 habe ich darauf hingewiesen, daß die Deutsche Bundespost auf der Grundlage von Verwaltungsvereinbarungen vermehrt die Aufgabe übernommen hat, Anträge auf Reisepässe und Personalausweise entgegenzunehmen und ausgestellte Ausweispapiere auszuhändigen. Diese Praxis begegnet rechtlichen Bedenken, solange die Deutsche Bundespost als unzuständige Stelle Daten der antragstellenden Person verarbeitet. Diese Problematik hat der Landesgesetzgeber, soweit er hierfür die Regelungskompetenz hat, durch eine Änderung des Niedersächsischen Gesetzes zur Ausführung des Gesetzes über Personalausweise ausgeräumt (Nds. GVBl. 1993 S. 360). Die Ausweisbehörden können nach der neuen Regelung andere öffentliche oder private Stellen in ihrem Bezirk mit der Entgegennahme von Anträgen auf Ausstellung von Ausweisen und mit der Aushändigung der Ausweise beauftragen. Aus datenschutzrechtlicher Sicht ist wichtig, daß die Vorschriften des Niedersächsischen Datenschutzgesetzes über die Verarbeitung personenbezogener Daten im Auftrag gelten. Damit ist ein Vorgang abgeschlossen, den ich 1990 aufgegriffen hatte. Für die ggf. erforderliche Bearbeitung von Personalausweisanträgen im Postamt bestehen jedenfalls nunmehr ausreichende Rechtsgrundlagen.

### 11.2 Einsichtnahme der Polizei in das Personalausweis- bzw. Paßregister

Mit der Einsichtnahme der Polizei in das Personalausweis- bzw. Paßregister wird in das Recht auf informationelle Selbstbestimmung der Betroffenen eingegriffen (vgl. XI 11.2). Im Berichtszeitraum sind zahlreiche Anfragen von Ausweisbehörden zur Nutzung des Registers für Zwecke der Verfolgung von Straßenverkehrsordnungswidrigkeiten (Abgleich des Lichtbildes mit Frontfotos) an mich gerichtet worden. Das scheint mir auf eine gewisse Unsicherheit im Umgang mit den einschlägigen Vorschriften hinzudeuten. Ich habe gegenüber dem Niedersächsischen Innenministerium angeregt, in den Verwaltungsvorschriften zum Personalausweisgesetz auf diese Problematik einzugehen.

Aus datenschutzrechtlicher Sicht sind - auch nach Auffassung des Niedersächsischen Innenministeriums - folgende Grundsätze zu beachten:

Die Nutzung des Paß- bzw. Personalausweisregisters ist im Zusammenhang mit der Verfolgung von Verkehrsordnungswidrigkeiten prinzipiell zulässig. Der Grundsatz der Verhältnismäßigkeit gebietet es allerdings, einen Abgleich des Registers mit Frontfotos nur bei nicht geringfügigen Verkehrsordnungswidrigkeiten vorzunehmen.

Grundsätzlich gilt auch hier das allgemeine datenschutzrechtliche Prinzip, die Daten bei dem Betroffenen zu erheben. Ausnahmen sind nur zugelassen, wenn die Datenerhebung bei dem Betroffenen nicht oder nur mit unverhält-

nismäßigem Aufwand möglich ist. Unverhältnismäßig ist der Aufwand dann, wenn er in keinem vernünftigen Verhältnis zum angestrebten Erfolg steht. Diese Feststellung verlangt eine gewissenhafte Abwägung von notwendigen finanziellen Aufwendungen sowie administrativen und/oder organisatorischen Schwierigkeiten. Das Aufsuchen des Halters und dessen Vorladung müssen deshalb ergebnislos geblieben sein, bevor die Einsichtnahme der Polizei bzw. der Bußgeldbehörde in das Personalausweisregister erfolgt.

## 11.3 Melderegisterauskünfte an Privatpersonen

Meldebehörden dürfen Daten aus dem Melderegister an Privatpersonen weitergeben, wenn dadurch schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Je nach Umfang der gewünschten Auskunft schreibt das Niedersächsische Meldegesetz (NMG) zusätzlich bestimmte Voraussetzungen vor:

- Für die einfache Melderegisterauskunft über einzelne Einwohnerinnen und Einwohner (Vor- und Familienname, Doktorgrad und Anschriften) gibt es keine besonderen Voraussetzungen.
- Erweiterte Melderegisterauskünfte (z.B. mit Angaben zum Familienstand oder Geburtstag) dürfen nur erteilt werden, soweit ein berechtigtes (also z.B. ein wirtschaftliches) Interesse glaubhaft gemacht worden ist. Der Betroffene ist von der Meldebehörde über die Datenweitergabe unter Angabe des Empfängers unverzüglich zu unterrichten. Diese Verpflichtung entfällt nur, wenn der Datenempfänger ein rechtliches Interesse an der Auskunft glaubhaft gemacht hat.
- Die Gruppenauskunft ist eine Übermittlung von im Gesetz abschließend aufgezählten Daten über eine Vielzahl nicht namentlich bezeichneter Einwohner. Sie ist nur zulässig, wenn ein öffentliches Interesse vorliegt. Für die Zusammensetzung der Personengruppe dürfen nur bestimmte Kriterien herangezogen werden (z.B. Tag der Geburt, Geschlecht).
- Außerdem sind vom Datenumfang begrenzte Melderegisterauskünfte in besonderen Fällen möglich, und zwar im Zusammenhang mit Wahlen an Träger von Wahlvorschlägen, bei Alters- und Ehejubiläen an Presse, Rundfunk sowié Ratsmitglieder oder Abgeordnete. Auskünfte an Adreßbuchverlage hatte ich unter XI 11.6 behandelt (vgl. auch 11.5). Der Betroffene hat das Recht, diesen Übermittlungen zu widersprechen.

Über die dargestellten Auskunftsarten hinausgehende Übermittlungen an Privatpersonen darf die Meldebehörde nicht vornehmen. Einen weitergehenden Auskunftsanspruch haben nur die Betroffenen selbst. Um so erstaunter war ein Petent, als eine sogenannte Aufenthaltsbescheinigung, die wegen ihres Inhaltes nur ihm selbst hätte ausgestellt werden dürfen, in einem Privatrechtsstreit vom gegnerischen Anwalt vorgelegt wurde. Im Prozeß kam der Aufenthaltsbescheinigung nahezu existentielle Bedeutung zu. Die Bescheinigung enthielt Daten, die selbst an andere Behörden nicht ohne weiteres hätten weitergegeben werden dürfen. Mit den Mitteln des Datenschutzrechts war es mir nicht möglich, diesen Sachverhalt aufzuklären. Das lag

zum einen daran, daß unterschiedliche Darstellungen zum "Weg" der Bescheinigung vorlagen. Zum anderen konnte die beteiligte Meldebehörde nicht belegen, an wen sie die Daten weitergegeben hat. Die Ausstellung der Aufenthaltsbescheinigung wurde weder in Verwaltungsvorgängen noch im automatisierten Meldeprogramm protokolliert. Das Niedersächsische Meldegesetz schreibt eine entsprechende Dokumentation nicht vor. Aus von mir durchgeführten Fortbildungsveranstaltungen weiß ich, wie datenschutzbewußt sehr viele Mitarbeiter in den Meldeämtern sind. So werden z.B. Aufenthaltsbescheinigungen, die von einer vertretungsberechtigten Person beantragt werden, häufig per Post an den betreffenden Einwohner direkt verschickt. Der geschilderte Fall legt aus meiner Sicht die Überlegung nahe, ob nicht - auch ohne Rechtsverpflichtung - derart umfangreiche Datenweitergaben in den Meldeämtern festgehalten werden sollten. Jedenfalls könnte dann bei Bedarf jeglicher Anschein einer unzulässigen Datenweitergabe an Private vermieden werden.

## 11.4 Keine Ausforschung bei der Bestimmung der Hauptwohnung

Mehrere Eingaben von betroffenen Bürgerinnen und Bürgern geben mir Veranlassung, auf die Problematik der Datenerhebung durch die Meldebehörde bei der Bestimmung der Hauptwohnung einzugehen.

Die Meldebehörden sind nach § 40 NMG befugt, die Hauptwohnung eines Einwohners, der mehrere Wohnungen bewohnt, festzulegen. Es steht den Einwohnern also nicht frei, unabhängig von der Nutzung eine Wohnung als ihre Hauptwohnung auszuwählen. Die Hauptwohnung bestimmt sich nach den im Gesetz genannten Kriterien: Die vorwiegend benutzte Wohnung ist die Hauptwohnung. Dem Schwerpunkt der Lebensbeziehungen, der nicht zwingend am Ort der vorwiegend benutzten Wohnung liegen muß, kommt nach § 8 Abs.1 Satz 3 NMG nur in Zweifelsfällen Bedeutung zu.

Die Meldepflichtigen haben nach dem Meldegesetz der Meldebehörde die zur Führung des Melderegisters erforderlichen Auskünfte zu erteilen. Dazu gehören auch Angaben über Haupt- und Nebenwohnungen. Nach den Verwaltungsvorschriften zum NMG (Nds. MBl. 1992 S. 1380) sind die Meldebehörden nicht verpflichtet, im Einzelfall Nachforschungen über die Wohnverhältnisse anzustellen. Sie sollen sich vielmehr auf die Prüfung beschränken, ob die Angaben der Einwohnerin bzw. des Einwohners plausibel erscheinen, d.h. in sich schlüssig und glaubhaft sind. Anlaß zur Nachprüfung besteht m.E. nur dann, wenn im Einzelfall konkrete Anhaltspunkte dafür bestehen, daß die Angaben des Meldepflichtigen nicht mit § 8 NMG zu vereinbaren sind, z.B. weil er von einem eigenen Recht zur Bestimmung der Hauptwohnung ausgeht. In diesen Fällen können von den Betroffenen nähere Angaben über die Wohnverhältnisse, ggf. auch die Vorlage von Unterlagen (vgl. § 13 Abs. 1 NMG) verlangt werden. Bei eigenen Ermittlungen der Meldebehörde ist im Hinblick auf den verfassungsrechtlichen Schutz der Privatsphäre Zurückhaltung geboten.

In Zweifelsfällen, also wenn die vorwiegend benutzte Wohnung nicht oder nicht eindeutig festgestellt werden kann, ist die Hauptwohnung dort anzunehmen, wo der Schwerpunkt der Lebensbeziehungen liegt. Die Entscheidung über den Schwerpunkt der Lebensbeziehungen muß den Betroffenen überlassen werden. Das Gesetz räumt der Meldebehörde nicht die Befugnis ein, die zur Bestimmung des Schwerpunktes der Lebensbeziehungen erforderlichen Daten zu erheben. Dazu wäre eine weitgehende Ausforschung des persönlichen Lebensbereiches der Einwohnerinnen und Einwohner erforderlich, die im Hinblick auf den Schutz der Privatsphäre unzulässig wäre (vgl. BVerfG, DVBl. 1993, 601). § 8 Abs. 1 Satz 3 NMG stellt deshalb lediglich für den Zweifelsfall eine Entscheidungsregel bereit.

## 11.5 Adreßbücher unter der schützenden Hand des Innenministeriums

Unter XI 11.6 habe ich gefordert, im Niedersächsischen Meldegesetz Datenübermittlungen an Adreßbuchverlage nur noch mit vorheriger Einwilligung der Betroffenen zuzulassen. Nach der zur Zeit im Gesetz verankerten Regelung dürfen die Daten der volljährigen Einwohnerinnen und Einwohner an Adreßbuchverlage übermittelt werden, wenn die Betroffenen dem nicht widersprochen haben. Diese vom Melderecht erlaubte Widerspruchslösung ist merkwürdig: Warum sollen sich eigentlich die Einwohner ihr Recht erst durch einen Widerspruch zurückholen, wo es ihnen doch schon zusteht? Zum Verfahren: Die Einwohner sind auf ihr Widerspruchsrecht bei der Anmeldung sowie einmal jährlich durch öffentliche Bekanntmachung hinzuweisen. Wie an mich gerichtete Eingaben zeigen, werden diese Hinweise von den Betroffenen kaum wahrgenommen.

Das Niedersächsische Innenministerium hat Meldebehörden des Landes um eine Stellungnahme zu meinem Änderungsvorschlag gebeten. Einige Behörden haben meine Initiative unterstützt. Mehrere Gemeinden haben wie ich zudem ein Defizit bei der Unterrichtung der Betroffenen über ihr Widerspruchsrecht gesehen. Bedauerlicherweise sieht das Innenministerium trotz dieser Aussagen keine Veranlassung, das Niedersächsische Meldegesetz in diesem Punkt zu ändern. Nach wie vor wird die Widerspruchsmöglichkeit für ausreichend gehalten, schutzwürdige Belange der Einwohner zu gewährleisten. Verfahrensmäßig soll aber eine bessere Information der Betroffenen über ihr Widerspruchsrecht erfolgen. So wurden die Meldebehörden gebeten, darum bemüht zu sein, daß über das Widerspruchsrecht im redaktionellen Teil der Zeitungen berichtet wird. Ich sehe nicht, wie die Meldebehörden entsprechende Bitten gegenüber den Zeitungen durchsetzen könnten. Sie sind insoweit auf den "goodwill" der Redakteure angewiesen. Mit der Weitergabe der Daten an Adreßbuchverlage nimmt man den Betroffenen ohne Not ihr Recht, selbst zu entscheiden, wann und inwieweit persönliche Angaben offenbart werden sollen. Die vom Innenministerium an die Meldebehörden weitergegebene Bitte scheint mir im Verhältnis dazu kein ausgewogenes Mittel zu sein.

Der vorgeschlagenen Gesetzesänderung kann nicht das Argument eines unangemessenen Verwaltungsaufwandes entgegengehalten werden. Da das In-

nenministerium sowieso beabsichtigt, die Meldescheine zu überarbeiten, kann bei dieser Gelegenheit die Einwilligungserklärung eingefügt werden. Damit würde man die Einwohnerinnen und Einwohner erreichen, die sich an- oder ummelden. Die anderen Betroffenen kann die Meldebehörde im Rahmen von Verwaltungstätigkeiten ansprechen, die sich auf einen Großteil der Bevölkerung auswirken, beispielsweise bei der jährlichen Versendung der Lohnsteuerkarten.

Es ist wohl richtig: Niemand hat bisher belegen können, daß Adreßbücher Wohnungsdieben bei der Vorbereitung ihrer Straftaten behilflich gewesen sind. Ich meine aber, daß staatliche Stellen ohne ausdrückliche Einwilligung der Betroffenen neue Quellen der Informationsgewinnung nicht fördern sollten, da hierin in jedem Fall für die Betroffenen ein Risikopotential steckt. Sind persönliche Daten erst einmal "öffentlich", weiß niemand mehr, wer dann was mit den Angaben macht. Es ist schon verwunderlich, daß es im Melderecht insofern mit der staatlichen Fürsorge nicht weit her ist. Auf der anderen Seite gibt es hinsichtlich der "Fürsorge" keine Grenzen, wenn die Polizei mit dem Ziel der Prävention umfassend sensible Daten, auch über unverdächtige Personen, sammeln möchte (vgl. 12.1).

Die Meldebehörden können mit der Weitergabe der Daten ihrer Einwohnerinnen und Einwohner an Adreßbuchverlage Geld verdienen. Nach der Allgemeinen Gebührenordnung besteht die Möglichkeit, pro Einwohnerdatensatz bis zu 30 Pfennig zu verlangen. Es mag spekuliert werden, ob in der finanziellen Seite der Angelegenheit der eigentliche Grund für die ablehnende Haltung gegenüber einer Einwilligungslösung zu suchen ist.

## 11.6 Rundfundgebühreneinzug: Beim Geld hört der Datenschutz auf

Regelmäßige Datenübermittlungen von den niedersächsischen Meldebehörden an den Norddeutschen Rundfunk (NDR) bzw. an die Gebühreneinzugszentrale (GEZ) sind z.Zt. nicht erlaubt. Ob eine erlaubende Rechtsgrundlage geschaffen wird, bleibt abzuwarten.

Die Konferenz der Innenminister des Bundes und der Länder hat in ihrer Sitzung am 26. November 1993 den Ländern empfohlen, in ihre Datenübermittlungsverordnungen den freien Zugang der Rundfunkanstalten auf die Meldedaten zu verankern. Die Meldebehörden sollen der jeweiligen Rundfunkanstalt bzw. der GEZ zum Zwecke der Erhebung und des Einzuges der Rundfunkgebühren von sich aus im Fall der Anmeldung, der Abmeldung oder des Todes eines volljährigen Einwohners folgende Daten übermitteln: Familienname (jetziger und früherer Name mit Namensbestandteilen), Vorname, Doktorgrad, Geburtstag, gegenwärtige und frühere Anschriften, Tag des Ein- und Auszuges, Familienstand und ggf. Sterbetag. Niedersächsische Vertreter hatten gegen den Beschlußentwurf zunächst Bedenken geäußert, sich dann der Stimme enthalten und schließlich in der Konferenz zugestimmt. Der Beschluß geht auf eine bereits seit längerer Zeit bestehende Forderung der Rundfunkanstalten zurück, die sich durch den ständigen Abgleich ihrer Datenbestände mit den Meldedaten letztendlich die Erhöhung

des Gebührenaufkommens versprechen. Welche Veränderungen bei der Höhe des Gebührenaufkommens die in den Ländern Hessen und Nordrhein-Westfalen bereits praktizierten Regelungen gebracht haben, konnte mir gegenüber allerdings nicht beziffert werden.

Unabhängig davon, ob eine erlaubende Rechtsgrundlage im Melde- oder im Rundfunkrecht geschaffen wird, sind regelmäßige Datenübermittlungen der beschriebenen Art rechtlich bedenklich. Sie lassen sich nicht auf die eigentliche Zielgruppe beschränken. Es werden nicht diejenigen herausgefiltert, die sich ihrer Zahlungspflicht entziehen, vielmehr sind alle betroffen, die in einem ganz anderen Zusammenhang beim Einwohnermeldeamt vorstellig werden. Die GEZ erhält damit unzählige Daten, die sie überhaupt nicht benötigt, und zwar von den Kunden, die nach einem Umzug ihre Gebühren von sich aus weiterbezahlen. Beim restlichen Datenbestand kann sie keinesfalls von "schwarzen Schafen" ausgehen. Darin enthalten sind Daten von Personen, die gar nicht zahlungspflichtig sind, weil sie Haushaltsangehörige sind, von der Gebühr befreit wurden bzw. kein Rundfunkgerät besitzen. Nach den Angaben des Statistischen Bundesamtes sind 4 % der privaten Haushalte in der Bundesrepublik nicht mit einem Fernsehgerät, immerhin noch 1 % nicht mit einem Hörfunkgerät ausgestattet.

Welche Maßnahmen werden nun in den Ländern, in denen das Melderegister bereits für Zwecke des Rundfunkgebühreneinzuges ausgewertet wird, ergriffen? In Nordrhein-Westfalen erhält der Personenkreis, der nicht beim WDR gespeichert ist, ein Anschreiben, mit dem um eine freiwillige Anmeldung etwa bereitgehaltener Rundfunkgeräte gebeten wird. Erfolgt hierauf keine Antwort, wird ein Erinnerungsbrief verschickt. An weiteren Aktionen sieht man sich man sich dort rechtlich gehindert. Im Ergebnis finden damit massenhaft Datenübermittlungen statt, um der GEZ Direktwerbemaßnahmen zu ermöglichen. Hartnäckige Schwarzhörer und -seher werden bei dieser Verfahrensweise letztendlich nicht zur Zahlung herangezogen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung gegen die Änderung der Meldedatenübermittlungsverordnungen gewandt (vgl. Anlage 3). Ich empfehle, es in Niedersachsen bei der bislang praktizierten Verfahrensweise zu belassen: Die GEZ fragt wegen der neuen Anschrift von säumigen Rundfunkteilnehmern bei den Meldebehörden an und erhält von dort (im Datenträgeraustauschverfahren) die angeforderte Auskunft (vgl. XI 11.7).

## 11.7 Die Tücken der Technik - Beachtung von Widersprüchen

Das Niedersächsische Meldegesetz gestattet den Meldebehörden, in bestimmten Fällen Daten aus dem Melderegister an Dritte zu übermitteln. Es handelt sich dabei um die Erteilung von Melderegisterauskünften an Träger von Wahlvorschlägen im Zusammenhang mit Wahlen, an Presse und Rundfunk sowie Mitgliedern parlamentarischer und kommunaler Vertretungskörperschaften über Alters- oder Ehejubiläen von Einwohnern sowie um Übermittlungen von Daten aller volljährigen Einwohner an Adreßbuchverlage.

Wollen die Betroffenen die Weitergabe ihrer Daten verhindern, müssen sie bei der Meldebehörde Widerspruch einlegen. Die Widersprüche führen zur Speicherung einer Übermittlungssperre im Melderegister.

Ich hatte mich mit einem Fall zu befassen, bei dem die Daten von 66 Einwohnerinnen und Einwohnern an Adreßbuchverlage übermittelt worden sind, obwohl die Betroffenen dagegen Widerspruch erhoben hatten. Die Meldebehörde hat bei diesem Sachverhalt in unzulässiger Weise - weil ohne Rechtsgrundlage - in das Recht auf informationelle Selbstbestimmung der Betroffenen eingegriffen.

Bei der Aufklärung der Angelegenheit ergab sich, daß die unerlaubten Datenweitergaben zwar auf einen Fehler in der Anwendung des in der Meldebehörde eingesetzten automatisierten Verfahrens zurückzuführen waren, dieser Fehler allerdings durch den Ablauf des ADV-Programms begünstigt wurde. Das Programm arbeitete wie folgt: Wollte die Meldebehörde aus ihrem Melderegister Daten zur Übermittlung an einen Adreßbuchverlag selektieren, fragte das System, ob Übermittlungssperren berücksichtigt werden sollen oder nicht. Wurde die Auswahl "N" für nein getroffen, kopierte das Programm die Datensätze sämtlicher volljährigen Einwohner auf eine Diskette, die dem Adreßbuchverlag zur Verfügung gestellt wurde. Eine Kontrolle des Arbeitsschrittes war durch die Sachbearbeiterin bzw. den Sachbearbeiter anschließend nicht mehr möglich, weil aus dem Anwenderprogramm heraus der Inhalt der Diskette nicht gelesen werden konnte. So führte die falsche Eingabe eines Buchstabens zu einer Offenbarung von Daten, die die Betroffenen nicht wollten. Meine Beanstandung führte zu einer Änderung des ADV-Programms. Bei der Selektion von Daten zur Übermittlung an einen Adreßbuchverlag wird die im Register gespeicherte Übermittlungssperre nunmehr automatisch berücksichtigt.

Der von mir geschilderte Einzelfall zeigt einmal mehr, welche Gefahren mit der Einführung der automatisierten Datenverarbeitung für die Rechte der Betroffenen entstehen können. Um so wichtiger ist es, daß ADV-Programme vor ihrem Einsatz nicht nur darauf untersucht werden, ob sie die verwaltungsmäßige Abwicklung eines Aufgabenbereichs reibungslos sicherstellen, sondern auch, ob die Rechte der Betroffenen durch das automatisierte Verfahren gewährleistet werden.

## 11.8 Keine Kennzeichnung von Aussiedlern im Melderegister

Bei der Bearbeitung einer Eingabe bin ich darauf gestoßen, daß eine Meldebehörde die in ihrem Gebiet wohnhaften Aussiedler im Melderegister besonders kennzeichnete. Die Gemeinde hielt das für erforderlich, um die Kommunalpolitiker über den jeweiligen Aussiedleranteil unterrichten sowie im schulischen Bereich besonderen Förderunterricht für Aussiedler planen zu können. Ich habe die Gemeinde darauf hingewiesen, daß es für die Kennzeichnung von Aussiedlern im Melderegister keine Rechtsgrundlage gibt. Der zulässige Inhalt des Melderegisters wird durch § 22 NMG abschließend geregelt. Das Datum "Aussiedler" ist dort nicht aufgeführt. Mir ist auch kei-

ne Rechtsgrundlage bekannt, die die Speicherung von personenbezogenen Daten über Aussiedler außerhalb des Melderegisters rechtfertigen könnte. Ihre Registrierung wäre deshalb allenfalls mit Einwilligung der Betroffenen zulässig. Die Gemeinde hat ihr Melderegister inzwischen bereinigt.

### 11.9 Datenschutz als Ausrede

Immer wieder muß der Datenschutz als Ausrede herhalten, wenn eine Behörde einem ihr unliebsamen Anliegen nicht nachkommen will und sonst eine ausreichende Begründung dafür nicht zur Verfügung steht. Über ein besonders krasses Beispiel unterrichtete mich ein Ortsbeauftragter der Bundesanstalt Technisches Hilfswerk. Er hatte die umliegenden Gemeinden gebeten, bei der Unterrichtung der Wehrpflichtigen über ihre Wehrerfassung nicht nur wie bisher Informationsmaterial der Bundeswehr und des Bundesgrenzschutzes, sondern auch ein Informationsblatt des Technischen Hilfswerkes beizufügen. Bekanntlich besteht die Möglichkeit, statt der Ableistung des Wehrdienstes für die Dauer von acht Jahren bei einer Katastrophenschutzorganisation wie dem Technischen Hilfswerk mitzuarbeiten. Einige Kommunen lehnten die Übersendung des Informationsmaterials aus Gründen des Datenschutzes ab. Dabei ging es doch bei der Beilegung des Merkblattes gar nicht um die Nutzung irgendwelcher persönlicher Daten. Solche Erfahrungen tragen wohl kaum dazu bei, bei den Beteiligten das Verständnis für datenschutzrechtliche Belange zu wecken.

## 12. Polizei

### 12.1 Die präventive Wende - das neue Niedersächsische Gefahrenabwehrgesetz

Der Niedersächsische Landtag hat am 19. Januar 1994 das Niedersächsische Gefahrenabwehrgesetz (NGefAG) beschlossen. Es löst das frühere Niedersächsische Gesetz über die öffentliche Sicherheit und Ordnung ab. Das NGefAG ist seit dem 1. Juni 1994 in Kraft (Nds. GVBl. S. 172).

Das neue Gefahrenabwehrgesetz ist aus meiner Sicht grundsätzlich positiv zu beurteilen. Positiv deshalb, weil die handelnden Bediensteten erstmalig die für ihren Umgang mit persönlichen Daten notwendigen gesetzlichen Grundlagen erhalten haben. Ein Ruhmesblatt ist die Geschichte dieses Gesetzes für das Land Niedersachsen jedoch nicht gewesen. Das Land war schon seit dem Volkszählungsurteil des Bundesverfassungsgerichts 1983 aufgefordert, für Rechtsgrundlagen zur Datenverarbeitung zu sorgen. Es hat diese Materie als letztes der alten Bundesländer geregelt. Nunmehr ist die früher bestehende Rechtsunsicherheit, was überhaupt erlaubt ist beim Umgang mit persönlichen Daten, beendet. Hierin liegt ein nicht zu unterschätzender Gewinn an Rechtsstaatlichkeit. Positiv sehe ich das Gefahrenabwehrgesetz auch, weil das Gesetz an mehreren Stellen Regelungen enthält, die den Bürgerinnen und Bürgern eher als bisher verdeutlichen, wer was

über sie weiß - und was gegebenenfalls von ihnen unternommen werden kann.

Diese für die Betroffenen wichtigen Vorschriften haben ihren Ausgangspunkt in der vom BVerfG geforderten verfahrensrechtlichen Gewährleistung des Persönlichkeitsschutzes. Einige Beispiele: Die Gefahrenabwehrbehörden haben die Verpflichtung, bei Befragungen auf eventuelle Rechte hinzuweisen. Auf Verlangen der Befragten müssen Hinweise nicht nur zur Freiwilligkeit von Aussagen gegeben werden, sondern auch dazu, daß über den späteren Umgang mit den Angaben eine Auskunft eingeholt werden kann. Datenerhebungen ohne Kenntnis der Betroffenen wiederum müssen diesen nicht unbekannt bleiben. Das Gesetz sieht hier die Verpflichtung vor, nach der jedenfalls grundsätzlich eine nachträgliche Information der Betroffenen über die Speicherung und die Übermittlung ihrer persönlichen Angaben zu erfolgen hat. Jede Person hat auch das gesetzlich verbriefte Recht, Auskunft über die zu ihr gespeicherten Daten, deren Herkunft und Übermittlungsempfänger zu erhalten bzw. Einsicht in die entsprechenden Akten zu nehmen. Angaben über unbeteiligte Dritte, wie z.B. Zeugen, Hinweisgeber, Kontakt- und Begleitpersonen dürfen grundsätzlich nur befristet, nämlich drei Jahre lang vorgehalten und damit genutzt werden. Bei späteren Auseinandersetzungen mit den Sicherheitsinstanzen können eventuell auch behördeninterne Dokumentationspflichten eine Bedeutung erlangen. So sind z.B. bestimmte Datenweitergaben an Private besonders aufzuzeichnen. Bei all diesen Beispielen handelt es sich um Grundregeln. Leider sieht das Gesetz hiervon häufig auch Ausnahmen vor.

Auch die von der Verwaltung erlassenen Ausführungsbestimmungen zum NGefAG enthalten einige zum Teil ergänzende Verfahrensvorschriften zu Gunsten der Betroffenen. Diese internen Bestimmungen steuern ganz wesentlich das Verhalten "vor Ort". Vor Datenweitergaben an Private ist hiernach z.B. zu prüfen, ob nicht andere Stellen entsprechende Anfragen zu beantworten haben. Diese Vorgabe berücksichtigt u.a. die spezifische Situation bei Polizeidienststellen, die häufig im Wege des ersten Zugriffs zwar über erste, aber nicht immer gesicherte Informationen verfügen. Ein umfassenderes Bild ergibt sich erst bei der Verwaltungsbehörde, die den Vorgang später erhält. Die Polizei ist eben keine allgemeine Auskunftei.

Es gibt aber aus Sicht der Betroffenen auch weniger erbauliche interne Vorgaben. So wurde im Gesetzgebungsverfahren und dann im Gesetz davon ausgegangen, daß z.B. Begleitperson nur derjenige sein kann, der in einer polizeirelevanten Bindung zum Tatverdächtigen steht. Die Ausführungsbestimmungen erwecken nun den Eindruck, daß schon bei flüchtigem Kontakt mit einem Tatverdächtigen (Autofahrer; Anhalter; Kioskbesitzer; Nachbar) diese Einordnung erfolgen kann, mit der Folge einer gegebenenfalls umfassenden Datenverarbeitung bei der Polizei. Datenübermittlungen ins Ausland dürfen nach dem Gefahrenabwehrgesetz u.a. nur aufgrund von "internationalen Verträgen" erfolgen. Diese Voraussetzung schützt niedersächsische Bürgerinnen und Bürger in der Weise, daß nur das Parlament entscheidet, ob Datenweitergaben ermöglicht werden sollen oder nicht. Ein erster Entwurf der Ausführungsbestimmungen "interpretierte" den Parlamentsvorbe-

halt weg und ließ Übermittlungen schon aufgrund von einfachen Verwaltungsabkommen zu. Die veröffentlichte Fassung der Ausführungsbestimmungen schweigt jetzt zu diesem Punkt. Die Landesregierung bleibt aufgerufen, sich für den Abschluß der nötigen internationalen Verträge einzusetzen. Nur so können die handelnden Stellen die für ihre Arbeit erforderlichen Rechtsgrundlagen erhalten.

Das NGefAG erlaubt auch die von mir im letzten Tätigkeitsbericht als problematisch dargestellten Handlungsmöglichkeiten des Staates im "Vorfeld" von Gefahren (XI 12.4 und 12.5). Unter dem Strich erhält die Polizei mehr gesetzliche Eingriffsmöglichkeiten als sie früher hatte. Dabei handelt es sich insbesondere um Befugnisse, die ohne Kenntnis der betroffenen Bürgerinnen und Bürger eingesetzt werden können. Gerade diese "verdeckten" Maßnahmen werden viele unbeteiligte Personen treffen. Eine solche Konzeption muß verwundern, wenn man bedenkt, daß das von der Landesregierung zur Notwendigkeit des Gesetzes herangezogene Volkszählungsurteil dem Staat aufgibt, auf eine Minimierung des als unerläßlich erkannten Umgangs mit persönlichen Daten hinzuwirken. Augenscheinlich wurde der sicherlich nicht einfach zu lösende Konflikt zwischen Sicherheits- und Individualinteressen häufig zugunsten staatlicher Sicherheitsphilosophie entschieden.

Ein wesentlicher Bestandteil dieser Sicherheitsphilosophie ist der Aspekt der Prävention. Vorsorge ist gut. Wir alle betreiben sie in irgendeiner Form, um uns gegen eventuelle zukünftige, nicht immer ganz klare, Risiken zu wappnen. Private Vorsorge ist allerdings gekennzeichnet durch Freiwilligkeit. Jeder weiß auch, welche persönlichen Daten er gegebenenfalls wem gibt. Etwas völlig anderes kann herauskommen, wenn sich der Staat den Präventionsgedanken zu eigen macht. Im Bereich der Sicherheitsgesetze, und dazu zählt das NGefAG, hat die Prävention einen hohen Preis. Bezahlt wird er von den Bürgerinnen und Bürgern. Im Gegensatz zur privaten Vorsorge kann und wird hier der Staat agieren, ohne daß die Betroffenen es merken. Dies führt zu einem schleichenden Abbau von Bürgerrechten. In einem demokratischen Gemeinwesen sollte der Staat nämlich stets mit "offenem Visier" den Bürgerinnen und Bürgern gegenübertreten. Die vom BVerfG betonte Datenerhebung beim informierten Betroffenen gerät ins Hintertreffen.

Das von allen gewünschte und unterstützte Ziel der Bekämpfung zukünftiger Gefahren muß wegen der einer Vorsorgetätigkeit innewohnenden Komplexität logischerweise schwammig bleiben. Risiken, auf die es sich vorzubereiten gilt, können eben nicht schon von vornherein klar bestimmt sein. Dies hat die im NGefAG nachzulesende fatale Folge, daß präzise Aussagen zur Zielrichtung möglicher Maßnahmen mehr als unbestimmt bleiben. Die für Niedersachsen geltende Formulierung lautet: Die Polizei hat "insbesondere auch für die Verfolgung von Straftaten vorzusorgen und Straftaten zu verhüten". Was damit eigentlich gemeint ist, bleibt offen. Entgegen der sonst üblichen Technik, grundlegende Bestimmungen im Interesse der politischen Steuerung im Gesetz näher zu erläutern, fehlen entsprechende parlamentarische Festlegungen und Begrenzungen in den Begriffsbestimmungen des § 2. Damit erhält die Exekutive einen großen Spielraum bei der Anwendung des

Gesetzes. Aus Sicht der grundrechtsbetroffenen Bürgerinnen und Bürger (und dies ist die Sicht des Datenschutzes) führt diese Situation zu einer Vernachlässigung der vom BVerfG besonders herausgestellten Notwendigkeit von präzisen Zweckbestimmungen bei staatlichen Eingriffen.

Schließlich fordert die so beschriebene allgemeine Vorsorgetätigkeit geradezu heraus, eine nicht mehr begrenzbare Sammlung von Kenntnissen über Personen anzulegen. Die Prävention erhöht damit ganz wesentlich den Informationsbedarf des Staates. Dies ist der Grund für die eingangs genannte gesetzliche Neueinführung einer Vielzahl von Befugnissen. Bereits heute hat - statistisch gesehen - etwa jeder 14. erwachsene Niedersachse eine Kriminalakte mit persönlichen Angaben, die gegebenenfalls auch an andere Behörden, private Dritte und ins Ausland weitergegeben werden können.

Ein Blick in die Zukunft: Eine staatliche Sicherheitsphilosophie, nach der mehr staatliche Eingriffsmöglichkeiten unter präventiven Vorzeichen zu einem "mehr" an innerer Sicherheit verhelfen sollen, führt fast zwangsläufig zu weiteren Grundrechtseinschränkungen. Neue "Szenarien" werden kommen und jede behauptete neue Qualität von "Bedrohung" bedarf selbstverständlich neuer Gegenmittel. Eine Schraube ohne Ende. Ich meine, daß präventive Arbeit nicht repressiv im Sinne eines Abbaus von Bürgerrechten angelegt sein muß. Andere Formen der Prävention sind denkbar. Wesentliche Ursachen der Massenkriminalität wie der organisierten Kriminalität sind bekannt. Massenkriminalität z.B. hat etwas zu tun mit der sozialen Situation, dem Alter und evtl. bestehender Arbeitslosigkeit. Organisierte Kriminalität wirft nicht selten die unangenehme Frage nach der Korrumpierbarkeit von Organen des Staates und von Unternehmen auf. Möglicherweise wäre es hilfreich, Sicherheitspolitik wieder zur Gesellschaftspolitik zu machen.

## 12.2 Controlling - ein Fremdwort?

In Niedersachsen wird viel davon gesprochen, im Interesse einer Effizienz (-steigerung) der Verwaltung Modelle und Verfahren aus der privaten Wirtschaft zu übernehmen. Nun muß nicht alles gut sein, was andere machen. Einen Punkt allerdings halte ich für bedenkenswert: die Durchführung einer Effizienzkontrolle. Es geht um die Erforderlichkeit polizeilicher Befugnisse. Hier sind intelligente Konfliktlösungen gefragt.

Aus Sicht der Grundrechtsbetroffenen ist immer zu fragen, ob gesetzlich eingeräumte staatliche Eingriffsmöglichkeiten in Bürgerrechte im überwiegenden Allgemeininteresse unerläßlich sind. Das "überwiegende Allgemeininteresse" ist die Grenze, an der der Datenschutz zu Recht zurücktreten muß, weil anders ein gedeihliches Zusammenleben in einer Gemeinschaft nicht funktionieren kann. Für mich steht außer Frage, daß Kriminalität nachhaltig bekämpft werden muß. Auf der anderen Seite ist ein unnötiger Grundrechtsabbau, der ja auch schleichend vonstatten gehen kann, zu vermeiden.

Im Sicherheitsbereich genügen oft einzelne handfeste Beispiele, um die Verankerung "flächendeckender" Regelungen im Gesetz - im Interesse des überwiegenden Allgemeinwohls - zu rechtfertigen. Das Niedersächsische Gefahrenabwehrgesetz wie auch die Strafprozeßordnung räumen der Polizei zahlreiche weitreichende Eingriffsmöglichkeiten ein, insbesondere zur heimlichen Informationsbeschaffung. Dabei handelt es sich um Maßnahmen, die unter Einsatz von modernster Technik viele unbeteiligte Bürgerinnen und Bürger treffen werden. Es liegt auf der Hand, daß dieses Befugnispotential besondere Aufmerksamkeit verdient. Hinzu kommt, daß zumindest bei den zentralen Einrichtungen der Polizei in den letzten 10 bis 15 Jahren die elektronische Datenverarbeitung immens ausgebaut wurde, allenfalls gebremst durch die verfügbaren Haushaltsmittel. Der rasante Ausbau der polizeilichen Datenverarbeitung durch immer mehr "technische" Befugnisse erfolgt, wie mir scheint, eher unter dem Gesichtspunkt der Nützlichkeit. Wer die Frage nach der Effizienz stellte, geriet womöglich in den Verdacht, ein Gegner von Sicherheit zu sein.

Eine informierte Auseinandersetzung mit dem "überwiegenden Allgemeininteresse" setzt das Wissen um die Ist-Situation voraus. Dazu sind Informationen nötig, z.B. über die tatsächliche Inanspruchnahme "technischer" Befugnisse, damit verbundene Eingriffe in das Recht auf informationelle Selbstbestimmung unbeteiligter Dritter, und den Anteil dieser Maßnahmen am Erfolg polizeilicher Arbeit (Erfolgskontrolle, vgl. XI 12.1). Natürlich spielen auch die Kosten eine Rolle. Untersuchungen zur Effizienz polizeilicher Instrumente gab es bisher leider nur vereinzelt. Eine Auswertung von Kriminalakten der Hamburger Polizei hat u.a. gezeigt, daß Kriminalakten viel zu schnell angelegt und durch eigene Arbeitsstrategien selbst produziert werden.

Ich habe ebenso wie andere Kollegen gegenüber dem Niedersächsischen Innenministerium angeregt, sich mit der Thematik zu befassen und um die Beantwortung folgender Fragen gebeten:

1. Welche praktischen Möglichkeiten bestehen, um gesetzlich vorgesehene Befugnisse und einzelne Instrumente der Strafverfolgung, Gefahrenabwehr und vorbeugenden Verbrechensbekämpfung - vor allem im technischen Bereich - auf ihre Geeignetheit und Wirksamkeit zu untersuchen? Welche Feststellungen sind insoweit bereits getroffen worden? Sind diese Maßnahmen nach den bisherigen Erfahrungen tatsächlich unabdingbar, oder könnten einzelne wenigstens zeitweise oder gebietsweise ausgesetzt werden, ohne daß sich Nachteile für die Aufgabenerfüllung zum Schutz der inneren Sicherheit ergeben?
2. Wie wird durch vorhandene und künftige Regelungen sichergestellt, daß Unbeteiligte von den Maßnahmen zur Verbrechensbekämpfung so wenig wie möglich betroffen werden, damit schwerwiegende Eingriffe in ihre Grundrechte vermieden werden? Welche rechtlichen und praktischen Schritte kommen insoweit in Betracht? Könnten diese Schritte zeitweise oder gebietsweise erprobt werden, um eine realistische Überprüfung der Notwendigkeit zu erreichen?

Das Innenministerium lehnte eine Befassung mit dem Thema ab: "Mangels einer erkennbaren oder zu erwartenden allgemeinen Fehlentwicklung bei der Ausübung vorhandener oder zukünftig zur Verfügung stehender Befugnisse der Polizei sehe ich jedenfalls gegenwärtig keinen begründeten Anlaß, die Geeignetheit und Wirksamkeit entsprechender Maßnahmen großflächig verwaltungspraktisch zu untersuchen." Diese Reaktion verblüfft. Im Umkehrschluß muß angenommen werden, daß Forderungen nach neuen Befugnissen sachlich nicht begründet werden können und müssen. Im übrigen steht die Antwort des Niedersächsischen Innenministeriums auch im Gegensatz zur Meinung anderer Innenministerien, die die Notwendigkeit einer Erfolgskontrolle bejahen. Man sei auch schon auf dem richtigen Weg. So wurde z.B. auf eine bundesweite Absprache verwiesen, nach der die Effizienz des bundesweiten polizeilichen Informationssystems INPOL untersucht werden soll. Weitere Überlegungen gingen in Richtung der Einrichtung einer Rechtstatsachen-Sammelstelle.

Die Bereitschaft vieler Innenministerien in Bund und Ländern zur "Innenrevision" liegt vor. Die Datenschutzbeauftragten des Bundes und der Länder haben daher Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen erarbeitet (vgl. Anlage 18). Mein Appell geht an das Niedersächsische Innenministerium, sich dem allseitigen Anliegen anzuschließen.

## 12.3 Entwicklungen auf der Bundesebene

### 12.3.1 Bundeskriminalamt

Die polizeiliche Datenverarbeitung in Niedersachsen ist auf vielfältige Weise mit dem Bundeskriminalamt (BKA) verknüpft. Zwar könnte man nach einer Durchsicht des Niedersächsischen Gefahrenabwehrgesetzes den Eindruck haben, als ob es nur eine Datenverarbeitung innerhalb Niedersachsens gibt. Nur ein kleiner Absatz deutet - fast schon versteckt - auf einen Datenverbund u.a. mit dem Bund hin (§ 42 Abs. 5). Real sieht es aber anders aus. Die polizeiliche Praxis ist geprägt von dem INPOL-Verbundsystem des Bundes und der Länder. Die zentralen Dateien beim BKA arbeiten im wesentlichen mit von den Länderpolizeien eingegebenen Daten. Die Weitergabe niedersächsischer Daten an das BKA unterliegt den Regeln des NGefAG, so wie es der Niedersächsische Landtag entschieden hat.

Sind nun die persönlichen Angaben beim Verbund im BKA angekommen, so geschieht eine wundersame Wandlung. Aus niedersächsischen Daten, für die natürlich das niedersächsische Recht maßgeblich sein müßte, werden faktisch Bundesdaten bzw. Daten der anderen Länder. Alle Verbundteilnehmer können grundsätzlich auf die gespeicherten Angaben zugreifen. Diese, Bund und Länder, können von Niedersachsen vorgegebene Speicherfristen verlängern und teilweise sogar von Niedersachsen eingegebene Datensätze verändern. Von der ursprünglichen Verantwortlichkeit des Landes für

"seine" Daten bleibt nicht mehr viel übrig. Daher äußerte ein Kollege von mir, die Polizeien der Länder verhielten sich im Rahmen ihrer Teilnahme am INPOL-Verbund gelegentlich wie bessere Abteilungen einer einheitlichen Bundespolizei. Die Folgen für Betroffene sind klar: Sie müssen damit rechnen, daß ihre Angaben bundesweit zum Abruf bereitstehen.

Die Datenverarbeitung beim BKA bedarf seit dem Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahre 1983 erlaubender gesetzlicher Grundlagen. Diese liegen unverständlicherweise immer noch nicht vor. Ende 1993 erhielt ich einen überarbeiteten Referentenentwurf für ein Gesetz über das Bundeskriminalamt. Der Entwurf stieß jedoch in wesentlichen Punkten auf den Widerstand der Länder und der Datenschutzbeauftragten. Die Begründung des Entwurfs rechtfertigte die vorgesehenen Bestimmungen mit datenschutzrechtlichen Erfordernissen. Das war - ähnlich wie bei anderen Vorhaben - eher ein Deckmantel. Es ging - kurz gefaßt - darum, eine allwissende Bundes-Super-Exekutivbehörde gesetzlich abzusichern. Damit wäre die in Art. 87, 73 Nr. 10 des Grundgesetzes angelegte Zentralstellenkonzeption des BKA als Service-Einrichtung mit Koordinierungsbefugnissen verlassen worden, mit der Folge eines erheblichen Abbaus von Länderkompetenzen im Polizeibereich. Datenschutzrechtliche Entscheidungen des Niedersächsischen Landtages über den Umgang mit persönlichen Daten niedersächsischer Bürgerinnen und Bürger in Gestalt des Gefahrenabwehrgesetzes und des Datenschutzgesetzes drohten leerzulaufen.

Das Niedersächsische Innenministerium stimmte mir in vielen meiner Bewertungen und Empfehlungen zu. Es ist wohl davon auszugehen, daß der Entwurf in dieser Legislaturperiode im Bundestag wieder auf den Tisch kommt. Ich hoffe, dann wieder zu einer überwiegend gemeinsamen Position mit dem Fachressort zu gelangen. Es besteht also für das Land Niedersachsen noch die Möglichkeit, seine Interessen einzubringen.

### 12.3.2 Bundesgrenzschutz

Die "Polizei des Bundes" verfügt bei ihren Maßnahmen seit kurzem über ein Gesetz, das (umfassende) Datenverarbeitungen erlaubt, das Bundesgrenzschutzgesetz (BGBl. I 1994, S. 2978).

Aufgrund bestimmter Vorschriften erfuhr die Öffentlichkeit erstmalig, daß der Bundesgrenzschutz (BGS) eine funktechnische Abhörstelle hat, die als "Vollzugshand" des Verfassungsschutzes agiert. 50 % bis 90 % (genauere Zahlen sind nicht bekannt) der gewonnenen Daten werden an den Verfassungsschutz weitergegeben. Angesichts der engen Beziehungen zwischen dem Bundesamt für Verfassungsschutz und den Landesämtern für Verfassungsschutz ist eine Weitergabe der Angaben auch an die Landesämter nicht auszuschließen. Die Aktivitäten der "Lauscheinheit" sollten mit dem BGS-Gesetz nach 40 Jahren Tätigkeit legalisiert werden.

Die Zusammenarbeit zwischen Polizei und Nachrichtendiensten war ein wichtiges Thema bei den Beratungen zum Niedersächsischen Verfassungs-

schutzgesetz. Der Niedersächsische Landtag hat - anders als der Bund - entschieden, daß Ersuchen des Niedersächsischen Landesamtes für Verfassungsschutz an die Polizei keine polizeilichen Datenerhebungen auslösen dürfen. In meiner Stellungnahme zum Entwurfstext habe ich gegenüber dem Niedersächsischen Innenministerium auf diesen Aspekt hingewiesen. Ich halte die "funktechnische Unterstützung" des Verfassungsschutzes für sehr problematisch angesichts des Trennungsgebotes zur Arbeit von Polizei und Geheimdiensten. Das Innenministerium teilt meine Auffassung. Im Bundesrat hatte sich zunächst die Mehrheit der Länder, einschließlich Niedersachsen, mit Blick auf das Trennungsgebot ebenfalls gegen diese Zusammenarbeit zwischen Polizei und Nachrichtendiensten ausgesprochen. In der Folgezeit - im Sommer 1994 - lag den Parteien dann wohl doch einiges daran, sich im "Vorwahlkampf" als besonders gute Sicherheitsschützer darzustellen. Das Gesetz ist noch im September 1994 zustande gekommen.

## 12.4 Entwicklungen auf der europäischen Ebene

### 12.4.1 Schengener Informationssystem

Bei dem Schengener Informationssystem (SIS) handelt es sich um eine gemeinsame Fahndungsdatei von derzeit neun Staaten: Belgien, Deutschland, Frankreich, Griechenland, Italien, Luxemburg, Niederlande, Portugal und Spanien. Mit der gemeinsamen Fahndungsdatei sollen die Folgen, die mit dem Wegfall der Grenzkontrollen an den Binnengrenzen verbunden sind, ausgeglichen werden (vgl. XI 6.3; X 12.3). Völkerrechtliche Grundlage ist das Schengener Durchführungsübereinkommen (SDÜ). Dieses Abkommen enthält Bestimmungen zu den Bereichen Einreise von Drittausländern bzw. Visaerteilung, Behandlung von Asylanträgen, Zusammenarbeit der Polizeibehörden bei der Vorbeugung und Bekämpfung von Verbrechen, Regelungen zur Rechtshilfe und zu Maßnahmen im Betäubungsmittel- und Waffenrecht. Ein weiterer Teil des SDÜ behandelt die Einrichtung des Schengener Informationssystems.

Das SIS dient der Ausschreibung (Speicherung) von Personen und Sachen zur Fahndung. Gründe können sein: die Festnahme mit dem Ziel der Auslieferung - der Verdächtige wird z.B. per Haftbefehl gesucht -; Einreiseverweigerung gegenüber Drittausländerinnen und Drittausländern; Aufenthaltsermittlung von Zeugen, vermißten oder angeklagten Personen; verdeckte Registrierung (Polizeiliche Beobachtung) von Personen und Fahrzeugen, soweit konkrete Anhaltspunkte dafür vorliegen, daß z.B. außergewöhnlich schwere Straftaten geplant werden; bestimmte Sachen, die zur Sicherstellung oder Beweissicherung in einem Strafverfahren benötigt werden. Abschließend vorgegeben ist auch der nutzbare Umfang personenbezogener Daten. Es handelt sich im wesentlichen um Identifikationsdaten, eventuelle Hinweise auf Bewaffnung oder Gewalttätigkeit, Ausschreibungsgrund und die zu ergreifenden Maßnahmen. Die Dauer der Speicherung beträgt im Regelfall drei Jahre.

Die angeschlossenen Staaten verfügen mit dem SIS über einen gemeinsamen Fahndungsdatenbestand. Schätzungen zufolge wird Deutschland ca. 600.000 Datensätze über Personen in das System eingeben. Ein Zentralcomputer in Straßburg sorgt dafür, daß alle Staaten identische und aktuelle Datenbestände haben. Diese Systemstruktur ist vergleichbar mit dem bundesdeutschen Verbundsystem INPOL. Derzeit wird der Zentralcomputer mit echten Fahndungsdaten "geladen". Die Inbetriebnahme des SIS soll bald erfolgen. Zusätzlich werden fahndungsbegleitende Daten zwischen den jeweiligen Zentralstellen (sog. "SIRENEN") ausgetauscht. Die deutsche SIRENE ist beim Bundeskriminalamt angesiedelt. Zugriff auf den Datenbestand haben in Deutschland das Bundeskriminalamt, die Polizeidienststellen der Länder, Grenzschutzdienststellen, der Bundesgrenzschutz, der Polizei- und Sicherheitsdienst des Deutschen Bundestages, Zolldienststellen und - im Fall der Ausschreibung zur Einreiseverweigerung - die Ausländerbehörden der Länder und die deutschen Auslandsvertretungen. In Deutschland werden die Zugriffe durch ca. 13.000 Terminals ermöglicht.

Eine Ausschreibung zur verdeckten Registrierung durch Geheimdienste ist nach dem Abkommen zulässig. Die Möglichkeit soll aber in Deutschland nicht realisiert werden, weil man darin einen Verstoß gegen das Trennungsgebot zwischen Polizei und Nachrichtendiensten sieht. Dies darf allerdings nicht darüber hinwegtäuschen, daß von Geheimdiensten anderer Staaten eingegebene Daten von deutschen Polizeidienststellen genutzt werden können und dieses gegebenenfalls auch umgekehrt funktioniert.

Zum Ausgleich für die verstärkten Eingriffsmöglichkeiten im internationalen Bereich sind zum Schutz der Persönlichkeitsrechte der Bürgerinnen und Bürger datenschutzrechtliche Bestimmungen vorgesehen. Das SDÜ regelt den Gesamtkomplex der Datenverarbeitung im Rahmen der Ausschreibungen aber nur ausschnittsweise. Die datenschutzrechtlichen Bestimmungen betreffen ausschließlich die Verarbeitung im SIS und - so die deutsche Interpretation - bei den SIRENEN. Unberührt bleibt jedoch das jeweilige nationale Recht der Staaten für die Anlieferung (Datenerhebung) und für die Weiterverwendung der Angaben nach einem Zugriff auf das System. Diese Struktur führt auf der internationalen Ebene zu einer Einebnung vorhandener Datenschutzstandards. Im Inland geltende Weiterverarbeitungsregelungen laufen bei einer Abgabe ins Ausland leer, unterschiedliche Datenerhebungsregeln spielen nach einer Eingabe in das Informationssystem keine Rolle mehr. Hinzukommt, daß die angeschlossenen Staaten generell nur über Datenschutzbestimmungen verfügen müssen, die auf dem Niveau der Datenschutzkonvention des Europarates von 1981 liegen und sich damit jedenfalls unterhalb der modernen deutschen Standards bewegen.

Die für das SIS selbst getroffenen datenschutzrechtlichen Regelungen halte ich für akzeptabel. Vorgesehen sind Ansprüche der Betroffenen auf Auskunft, Berichtigung, Löschung oder Schadensersatz. Bemerkenswert ist, daß Betroffene ihre Rechte in jedem Vertragsstaat geltend machen können. Dies ermöglicht eine freie Wahl des anzuwendenden Rechts. Auch die weiteren Bestimmungen über die Verantwortung für die Richtigkeit und Aktua-

lität der im SIS gespeicherten Daten, Zweckbindung, Protokollierung der Abrufe und Datensicherung sind grundsätzlich den bei uns geltenden Vorschriften vergleichbar. Eine Kontrolle der Datenverarbeitung durch unabhängige Instanzen (bei uns: BfD/LfD) ist gewährleistet.

Mit dem Niedersächsischen Innenministerium habe ich vereinbart, die notwendigen Umsetzungen im Land gemeinsam anzugehen. Dazu gehört auch eine eventuelle Änderung der schon bestehenden niedersächsischen Richtlinien über die internationale Fahndung nach Personen im SIS. Art. 94 Abs. 1 Satz 2 SDÜ fordert, vor einer Einspeicherung in das System zu prüfen, ob im Einzelfall eine internationale Ausschreibung erforderlich ist. Im Gegensatz hierzu sehen die Richtlinien generell die Eingabe in das SIS vor. Gleichsam im Sinne einer Ausnahme wird nur geprüft, ob nicht schon eine nationale Fahndungsausschreibung ausreicht. Die Erörterungen insbesondere mit dem Landeskriminalamt zur Aufbereitung der auf das Land zukommenden Fragen waren sehr konstruktiv.

### 12.4.2 Europäisches Informationssystem

Als nächster bzw. ergänzender Schritt zu einem größeren Fahndungsraum wird der Aufbau eines Europäischen Informationssystems (EIS) geplant. Möglicherweise wird das EIS zunächst begrenzt auf Ausschreibungen zur Einreiseverweigerung. Als Vertragsstaaten kommen in Betracht die unter 12.4.1 genannten Schengen-Staaten und Dänemark, Irland sowie Großbritannien.

### 12.4.3 EUROPOL

Hierunter ist zum einen die Errichtung eines europäischen Polizeiamtes mit Sitz in Den Haag zu verstehen. Im Februar 1994 wurde das Amt offiziell eröffnet. EUROPOL als Einrichtung der Europäischen Union (EU) soll vor allem folgende Aufgaben erhalten: Verhütung und Bekämpfung des Terrorismus, des illegalen Drogenhandels, der Nuklearkriminalität, der illegalen Einschleusung, der Kraftfahrzeugkriminalität sowie die damit verbundenen Geldwäschehandlungen. Da EUROPOL zur Erfüllung seiner Aufgaben eigenständige Befugnisse erhalten soll, muß eine völkerrechtliche Grundlage in Form eines Übereinkommens (Konvention) geschaffen werden.

Zur Durchführung der Aufgaben wird ein gemeinschaftsweites Informationssystem eingerichtet. Das ist die zweite Bedeutung von EUROPOL. Dieses System ist nicht nur als ein reines Fahndungssystem wie das Schengener Informationssystem (vgl. 12.4.1) ausgelegt. Der Entwurf der Konvention läßt erkennen, daß es bei EUROPOL um ein aktives Recherche-, Analyse- und Nachweissystem geht. Vorgesehen ist eine Datenanlieferungspflicht der polizeilichen Zentralinstanzen der Mitgliedsstaaten, bei uns voraussichtlich das BKA. Zugriffsmöglicheiten auf das System sollen die bei EUROPOL beschäftigten Verbindungsbeamten und die Zentralinstanz der Polizei erhalten. Die Mitgliedsstaaten dürfen die von EUROPOL erhaltenen Daten nur

zur Verhütung oder Bekämpfung von Straftaten mit erheblicher Bedeutung verwenden. Sie dürfen die Daten aber auch für andere, insbesondere geheimdienstliche Zwecke nutzen. Geplant ist weiter die Befugnis von EUROPOL, in eigener Kompetenz über die ggf. weltweite Weitergabe von Daten zu entscheiden.

Für mich steht außer Frage, daß die Polizeien der EU bei der Bekämpfung des internationalen Verbrechens gut zusammenarbeiten müssen. Aus datenschutzrechtlicher Sicht habe ich besonders auf die Einhaltung unserer Datenschutzstandards zu achten. In meiner Stellungnahme gegenüber dem Niedersächsischen Innenministerium mußte ich gravierende datenschutzrechtliche Mängel im Konventionsentwurf feststellen. So wird z.B. das Auskunftsrecht der Betroffenen erheblich schlechter als in Niedersachsen ausgestaltet. Es fehlt zudem das Recht auf Akteneinsicht. Unklar ist weiter, ob die geplante unabhängige Datenschutzkontrollinstanz auch von sich aus die Datenverarbeitung bei EUROPOL überprüfen kann.

Es geht vor allem um zwei Aspekte der vorliegenden Konventionsarchitektur: 1. die Ausgestaltung von EUROPOL als eine Stelle mit eigener Rechtspersönlichkeit und 2. die Länderkompetenzen opfernden Regelungen über die Zusammenarbeit zwischen EUROPOL und dem BKA. Konsequenz der "eigenen Rechtspersönlichkeit" ist, daß Betroffene ihre Rechte ausschließlich gegenüber EUROPOL geltend machen können. Auch wenn die Daten aus Niedersachsen stammen, wäre der Weg versperrt, niedersächsische Polizeibehörden vor einem örtlichen Gericht zu verklagen. Konsequenz der Beschneidung von Länderkompetenzen ist z.B. die Monopolisierung der polizeilichen Kontakte mit EUROPOL beim Bundeskriminalamt und die Datenanlieferungspflicht des BKA ohne Rücksicht auf länderspezifische Zweckbindungsregelungen.

Dies alles würde zu einem merklichen Verlust der Polizei- und Datenhoheit bei den bundesdeutschen Ländern führen. Es gäbe keine "Länderverantwortlichkeit" mehr für Daten, die auch in die Dateien des BKA eingegeben sind. Nicht die Regelungen des NGefAG zur Datenverarbeitung wären zukünftig maßgeblich, sondern das EUROPOL-Übereinkommen. Der Konventionsentwurf wurde nicht - wie man vermuten könnte - von einem eher zentralistisch geprägten Mitgliedsstaat der EU vorgelegt. Er stammt von der föderalen Bundesrepublik Deutschland. Ich kann mir nicht vorstellen, daß der vorliegende Entwurf die Zustimmung des Landes Niedersachsen finden kann. Die vom Niedersächsischen Landtag getroffenen Entscheidungen zum verantwortlichen Umgang mit persönlichen Daten im Polizeibereich müssen respektiert werden. Alle Datenschutzbeauftragten des Bundes und der Länder haben in einer gemeinsamen Entschließung noch einmal eindringlich auf die verfassungsrechtliche Kompetenzverteilung im Polizeibereich zwischen dem Bund und den Ländern und auf die materielle Verantwortung der Länder für "ihre" Daten hingewiesen (vgl.Anlage 20). Ich empfehle, die Landesinteressen bei den weiteren Beratungen offensiv zu vertreten. Hat dies keinen Erfolg, so wird es zu einem Abbau förderaler Strukturen kommen. Ich begrüße es sehr, daß sich der Niedersächsische Landtag - Ausschuß für innere Verwaltung - der Thematik angenommen hat.

Seit dem Sommer 1994 haben die deutschen Verbindungsbeamten bei EUROPOL zur Bekämpfung der Drogenkriminalität auch einen Online-Zugriff auf Dateien beim Bundeskriminalamt. Für den praktizierten Datenaustausch EUROPOL/BKA gibt es keine durch einen internationalen Vertrag begründeten erlaubende Rechtsgrundlagen. Daten niedersächsischer Bürgerinnen und Bürger können schon bei EUROPOL vorliegen und ggf. an andere Mitgliedsstaaten der EU weitergegeben worden sein. Auch an diesem Beispiel läßt sich leider zeigen, daß wieder einmal das Recht der Praxis folgt.

## 12.5 Polizeiliche Beobachtung: Jeder ist verdächtig

Die "Polizeiliche Beobachtung" von Personen (früher: Beobachtende Fahndung) gehört zu den verdeckten Datenerhebungsmaßnahmen der Polizei. Dabei werden die Personalien der Betroffenen in der INPOL-Fahndungsdatei ausgeschrieben. Zweck dieser Maßnahme ist es, bei jedem Kontakt der ausgeschriebenen Personen mit der Polizei unauffällig Informationen zu sammeln, um Anhaltspunkte für Ermittlungen zu erhalten. Bei einem Kontakt werden beispielsweise Ort und Zeit, Begleitpersonen, mitgeführte Sachen und Verhalten gemeldet (Kontrollmeldungen). Weder die ausgeschriebene Person noch deren Begleiter ahnen, daß sie ins Blickfeld der Polizei gerückt sind. Das Instrument wird u.a. bei Rauschgift- und Eigentumsdelikten, gegen Terroristen, Schleuser und gefährliche Intensivtäter eingesetzt.

Ich habe im Landeskriminalamt Niedersachsen (LKA) eine datenschutzrechtliche Prüfung der Verarbeitung von personenbezogenen Daten im Zusammenhang mit der Polizeilichen Beobachtung durchgeführt. Dabei habe ich mich auf den Bereich Terrorismus, den Hauptanwendungsfall der Polizeilichen Beobachtung, beschränkt. Von allen zum Zeitpunkt der Prüfung ausgeschriebenen Personen waren mehr als die Hälfte als "Terroristen" oder deren Unterstützende betroffen. Bei meiner Prüfung habe ich u.a. folgendes festgestellt:

- Rechtsgrundlagen der Polizeilichen Beobachtung

  Das Instrument der Polizeilichen Beobachtung wird sowohl zur Strafverfolgung als auch zur Gefahrenabwehr eingesetzt. Für die Polizeiliche Beobachtung zu Zwecken der Strafverfolgung wurde mit dem Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) vom 15. Juli 1992 eine Rechtsgrundlage geschaffen, die grundsätzlich die Anordnung durch den Richter, bei Gefahr im Verzug durch die Staatsanwaltschaft vorsieht (BGBl. I S. 1302). Im Bereich der Gefahrenabwehr gab es zum Prüfungszeitraum dagegen keine gesetzliche Grundlage für die Polizeiliche Beobachtung. Durch Erlaß des Niedersächsischen Innenministeriums wurde die Polizei ermächtigt, selbst die entsprechende Anordnung zu treffen. Lag es aus polizeilicher Sicht bei dieser Konstellation nicht nahe, Polizeiliche Beobachtungen auf die Füße der Gefahrenabwehr zu stellen? Alle im Prüfungszeitraum erfolgten Personenausschreibungen

wurden seitens des LKA als gefahrenabwehrende Maßnahmen angesehen. An dieser Zuordnung sind Zweifel angebracht. Gegen alle ausgeschriebenen Personen war ein strafrechtliches Ermittlungsverfahren wegen Bildung einer terroristischen Vereinigung (§ 129a StGB) anhängig. Zuständig für die Durchführung von Ermittlungsverfahren nach § 129a StGB ist das LKA. Die Verfahren werden dort in der Organisationseinheit geführt, die auch die Ausschreibung beantragt und schließlich die Kontrollmeldungen erhält. Auch aus der Stellungnahme des Innenministeriums zu meinem Prüfungsbericht wird deutlich, daß der Schwerpunkt der Ausschreibungen tatsächlich nicht im Bereich der Gefahrenabwehr lag. So wird dort die Polizeilichen Beobachtung als strafprozessuale Ermittlungsart bezeichnet.

In der Zukunft ergibt sich die dargestellte Problematik nicht mehr. Nach dem NGefAG bedarf die Polizeiliche Beobachtung der richterlichen Anordnung. Die Verlagerung der Anordnung auf eine externe Instanz bewirkt offensichtlich, daß mit einem solchen Ermittlungsinstrument zurückhaltender umgegangen wird. Mit der Einführung der richterlichen Anordnung im Bereich der Strafverfolgung ist die Gesamtzahl der Polizeilichen Beobachtungen in Niedersachsen etwa auf die Hälfte zurückgegangen.

- Polizeiliche Beobachtung von Jugendlichen

Zu den im Prüfungszeitraum als "Terroristen" ausgeschriebenen Personen gehörte ein Jugendlicher. Das Niedersächsische Innenministerium ist mit mir der Auffassung, daß bei der Ausschreibung von Jugendlichen dem Grundsatz der Verhältnismäßigkeit eine besondere Bedeutung zukommen muß. Es folgt meinem Vorschlag, zukünftig bei der Polizeilichen Beobachtung von Jugendlichen den Beauftragten für Jugendsachen in das Verfahren einzubeziehen.

- Erfassung von Kontakt- und Begleitpersonen

Ziel meiner Prüfung war es insbesondere festzustellen, auf welche Weise die Polizei die Daten, die sie mit den Kontrollmeldungen über Kontakt- und Begleitpersonen erhält, weiterverarbeitet. Aus den von mir geprüften Akten ergab sich eine hohe Zahl von Speicherungen innerhalb eines Jahres. Betroffene wurden allein deshalb in der bundesweiten Staatsschutzdatei APIS gespeichert, weil sie bei einer polizeilichen Kontrolle in der Nähe einer ausgeschriebenen Person angetroffen wurden.

Bezüglich der Frage, unter welchen Bedingungen die Speicherung von Daten über Kontakt- und Begleitpersonen im Bereich der Terrorismusbekämpfung zulässig ist, gibt es zwischen dem Niedersächsischen Innenministerium und mir unterschiedliche Auffassungen. Mit datenschutzrechtlichen Grundsätzen wäre es nicht zu vereinbaren, wenn jede Art von Kontakt zum Anlaß für die Registrierung von Begleitpersonen genommen würde. Die Erfassung von Kontakt- oder Begleitpersonen kann nur gerechtfertigt sein, wenn Anhaltspunkte dafür bestehen, daß diese Perso-

nen ebenfalls in die Szene verstrickt sind und deshalb die sie betreffenden Informationen zur Gefahrenabwehr oder vorbeugenden Straftatenbekämpfung erforderlich sind. Das Niedersächsische Innenministerium vertritt dagegen die Auffassung, zunächst einmal müsse jeder Kontakt der ausgeschriebenen Person zu anderen Personen übermittelt und ausgewertet werden. Erst wenn im Rahmen einer auch längerfristigen Auswertung festgestellt wird, daß die Daten erkennbar ohne Relevanz für den Ausschreibungsgrund sind, könnten sie gelöscht werden.

Sicherlich ist die Verfolgung des Terrorismus eine wichtige Aufgabe der Polizei. Damit verbundene erforderliche Eingriffe in das Recht auf informationelle Selbstbestimmung müssen aus Gründen des überwiegenden öffentlichen Interesses hingenommen werden. Wie weit darf jedoch die Befugnis bei Personen gehen, die nicht zu den "Terroristen" zählen? Aus den von mir geprüften Akten konnte ich bei einem Drittel aller gespeicherten Kontakt- und Begleitpersonen keine Hinweise darauf finden, daß sie als Kuriere, Wohnungsbeschaffer, Teilnehmerinnen oder Teilnehmer an Treffen der terroristischen Szene oder in sonstiger Funktion unterstützend tätig geworden sind.

Meine Zweifel an der Zulässigkeit der Speicherungen sind durch die Stellungnahme des Niedersächsischen Innenministeriums nicht ausgeräumt worden. Die den Ausschreibungen zugrunde liegenden Sachverhalte finden offensichtlich auch bei anderen Instanzen eine von der Polizei abweichende Bewertung. Zeitungsberichten konnte ich entnehmen, daß Strafverfahren, die aus Sicht der Polizei Grundlage für die Ausschreibung der betroffenen Personen und für die Speicherung der mit ihnen bei Polizeikontrollen angetroffenen Begleitpersonen waren, wegen geringer Schuld eingestellt worden sind.

## 12.6 Kriminalakten

Ich habe wiederholt (zuletzt unter XI 12.17) auf die weitreichenden Folgen hingewiesen, die die Existenz einer Kriminalakte für die Betroffenen haben kann. Daraus ergibt sich für die Polizeidienststellen die Verpflichtung, bei der Führung von Kriminalakten äußerst sorgfältig vorzugehen.

- Ewiges Ärgernis: Keine Information über den Ausgang des Strafverfahrens

Die Polizei legt in der Regel Kriminalakten nach Abgabe ihrer Ermittlungsvorgänge an die Staatsanwaltschaft an. Immer wieder treffe ich auf Kriminalakten, in denen zwar das Ergebnis der polizeilichen Ermittlungen, nicht jedoch der Ausgang des gegen den Beschuldigten geführten Strafverfahrens festgehalten ist. Dabei handelt es sich um ein altbekanntes Problem. Ich habe die lückenhaften Meldungen über den Ausgang von Strafverfahren seit 1982 wiederholt bei Justiz und Polizei angesprochen. Es ist zu bedauern, daß das Abstellen dieses Mißstandes in der Praxis offensichtlich zu erheblichen Schwierigkeiten führt.

Aus datenschutzrechtlicher Sicht kann es nicht akzeptiert werden, daß diese Schwierigkeiten zu Lasten der Betroffenen gehen. Der Ausgang des Strafverfahrens kann - nicht nur im Fall des Freispruches - durchaus dazu führen, daß der von der Polizei ermittelte Sachverhalt neu beurteilt werden muß. Da der Inhalt von Kriminalakten nicht nur für polizeiinterne Zwecke genutzt wird, kann in diesen Fällen die fehlende Berücksichtigung des Verfahrensausganges erhebliche Nachteile für die Betroffenen mit sich bringen. So werden aus Kriminalakten vielfältige Auskünfte an andere Stellen erteilt, z.B. im Rahmen von Sicherheitsüberprüfungen, bei der Zulassung zu bestimmten Berufen oder bei der Erteilung von Konzessionen. Aber auch für Bewertungen, die polizeiintern verwendet werden, ist der Abschluß des Strafverfahrens von Bedeutung. So wurde z.B. ein Petent im Auskunftssystem der niedersächsischen Polizei (POLAS) über mehrere Jahre als "gewalttätig" und "Schläger" bezeichnet, obwohl der sachbearbeitenden Polizeidienststelle in keinem Fall bekannt war, welches Ergebnis die gegen den Betroffenen geführten Strafverfahren erbracht haben.

Ich gehe davon aus, daß das Niedersächsische Gefahrenabwehrgesetz zur Bewältigung des aufgezeigten Problems beiträgt. Nach § 39 Abs. 3 Satz 3 NGefAG hat die speichernde Polizeidienststelle bis zum Abschluß des strafrechtlichen Ermittlungsverfahrens jeweils nach einem Jahr zu prüfen, ob die Voraussetzungen für die Speicherung noch vorliegen. In meiner Stellungnahme zum Erlaßentwurf "Führung polizeilicher Dateien und Akten mit personenbezogenen Daten" habe ich vorgeschlagen, den Polizeibehörden in den Ausführungshinweisen vorzugeben, daß Erkundigungen bei der zuständigen Staatsanwaltschaft einzuholen sind, wenn der Verfahrensausgang innerhalb der einjährigen Speicherungsdauer nicht mitgeteilt wird.

- Berücksichtigung des Verfahrensausganges

  Erhält die Polizei die Mitteilung über den Ausgang des Strafverfahrens, so hat sie unter Berücksichtigung dieses Ergebnisses zu prüfen, ob die Kriminalakte über die oder den Betroffenen weitergeführt werden darf. Das NGefAG enthält das Gebot, gespeicherte Daten zu löschen, wenn der dem Ermittlungsverfahren zugrundeliegende Verdacht entfallen ist. Wird der Betroffene im Strafverfahren freigesprochen, so darf nach meiner Auffassung eine weitere Speicherung aufgrund dieses Verfahrens nicht erfolgen. Ich bedauere, daß sich das Niedersächsische Innenministerium dieser Auffassung nicht angeschlossen hat. In den Ausführungsbestimmungen zum NGefAG hat es den Polizeibehörden die Möglichkeit eröffnet, auch im Fall des Freispruchs Daten über den Betroffenen weiter zu behalten. Das Ministerium macht insoweit keinen Unterschied zur Einstellung des Verfahrens nach § 170 Abs. 2 StPO: In beiden Situationen entfällt zwar nach der Ausführungsbestimmung in der Regel der Verdacht mit der Folge der Löschung. Bestehen allerdings auf der Grundlage der hierfür maßgeblichen Entscheidungen nach polizeilicher Bewertung nach wie vor gewichtige Gründe für die Annahme, die ver-

dächtige Person habe die Tat dennoch begangen, soll die weitere Speicherung in der Kriminalakte möglich sein. Dies soll - wohlgemerkt - auch bei einem Freispruch gelten. Ich habe Zweifel, ob Speicherungen aus "freisprechenden" Urteilen zulässig sind. Immerhin gibt es keinen Freispruch 1. oder 2. Klasse. Die Urteilsformel bei Freispruch lautet nach § 260 StPO: "Der Angeklagte wird freigesprochen". Zusätze sind nach dem Gesetz unzulässig. Die polizeiliche Speicherung führt zu einem staatlichen Eingriff in das Recht auf informationelle Selbstbestimmung, obwohl das Gericht den behaupteten Tatvorwurf nicht dem Betroffenen zugeordnet hat.

Aber auch im Fall der Einstellung des Verfahrens hat die Polizei die hierfür maßgebenden Gründe bei ihrer Entscheidung über die weitere Aufbewahrung der Kriminalakte zu beachten. Der folgende Fall zeigt beispielhaft, daß dem in der Praxis nicht immer entsprochen wird:

Der Petent schrieb mir, daß die Polizei gegen ihn, so seine Worte, eine "ungeheuerliche Anschuldigung" erhoben hat: Verdacht auf sexuellen Mißbrauch von Kindern. Die Polizei hatte ihn erkennungsdienstlich behandelt und eine Kriminalakte über ihn angelegt. Seine Daten waren in das polizeiliche Informationssystem INPOL eingegeben worden, so daß der gegen ihn bestehende Verdacht bundesweit durch die Polizei abrufbar war. Was war passiert?

Vier Schülerinnen waren von einem Mann verbal belästigt worden und hatten deshalb Anzeige bei der Polizei erstattet. Die dabei abgegebenen Personenbeschreibungen widersprachen sich beim Äußeren und beim Alter des Täters. Der Petent geriet in Verdacht, weil er sich genau eine Woche nach der Belästigung zur Tatzeit im Tatortbereich (Fußgängerüberweg) aufhielt. Zur Identifizierung des Täters wurden den Schülerinnen sechs Lichtbilder vorgelegt, u.a. auch das des Petenten. Dabei erkannte ein Kind Ähnlichkeiten mit dem Täter, konnte sich allerdings nicht genau erinnern; zwei Kinder zeigten auf das Bild des Petenten, nannten allerdings zusätzliche Tätermerkmale, die er nicht aufwies; ein Kind stellte Ähnlichkeiten des Täters mit einem anderen Mann fest. Die Staatsanwaltschaft hat das Strafverfahren gegen den Petenten eingestellt, weil eine zweifelsfreie Identifizierung nicht möglich war und der Petent für die Tatzeit ein Alibi nachweisen konnte. Die Polizei hielt die Aufbewahrung der Kriminalakte weiterhin für erforderlich. Für sie war der Tatverdacht nicht vollständig ausgeräumt worden. Bei der Bewertung des Sachverhalts kam sie zu der Prognose, der Petent (im Rentenalter, bisher vollkommen unbescholten) könnte erneut straffällig werden.

Auf meine Bitte, die Entscheidung über die Weiterführung der Kriminalakte des Petenten nochmals zu überprüfen, verfügte die zuständige Bezirksregierung die Vernichtung aller über den Petenten angelegten Unterlagen.

- Prognose zur Wiederholungsgefahr

Kriminalakten sollen der Polizei helfen, zukünftige Straftaten des Betroffenen aufzuklären. Sie richten sich damit gegen solche Personen, von denen aufgrund polizeilicher Prognose angenommen werden muß, daß sie erneut straffällig werden. Diesem Grundsatz trägt nunmehr § 39 Abs. 3 Satz 1 NGefAG Rechnung. Danach kann die Polizei im Strafverfahren erlangte personenbezogene Daten speichern, also Kriminalakten anlegen, wenn wegen der Art, Ausführung oder Schwere der Tat sowie der Persönlichkeit der oder des Verdächtigen die Gefahr der Begehung weiterer vergleichbarer Straftaten besteht und wenn die Speicherung zur Vorsorge für die Verfolgung oder zur Verhütung einer künftigen Straftat erforderlich ist. Die Wiederholungsgefahr muß sich danach aus den tatsächlichen Umständen des Einzelfalles ergeben. Die Polizei muß sich mit der einzelnen Tat und der Persönlichkeit des Täters bzw. der Täterin auseinandersetzen. Kriminalistisch anerkannte Erfahrungsgrundsätze sowie die Tatsache des strafrechtlichen Ermittlungsverfahrens können für sich allein kein Anlaß zum Führen einer Kriminalakte sein. Stereotype Begründungen, wie sie mir teilweise bei Prüfungen bekannt geworden sind ("insbesondere bei Brandstiftungsdelikten" oder "insbesondere bei einem Sittendelikt ist aus kriminalpolizeilicher Erfahrung grundsätzlich die Wiederholungsgefahr nicht auszuschließen"), reichen als Rechtfertigung für die Kriminalakte nicht aus. Ich habe gegenüber dem Niedersächsischen Innenministerium angeregt, in den Erlaß "Führung polizeilicher Dateien und Akten mit personenbezogenen Daten" entsprechende steuernde Vorgaben aufzunehmen.

## 12.7 Hinweise auf Aids im Polizeicomputer

Die Speicherung von Aids-Daten im Polizeicomputer führt zu einem erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung. Es gibt wohl keine andere Krankheit, bei der die Gefahr so groß ist, daß die Betroffenen ins gesellschaftliche Abseits gedrängt werden. Das Niedersächsische Innenministerium hatte nach einer Diskussion im Landtag über die Speicherung von HIV-infizierten Personen im polizeilichen Informationssystem 1988 entschieden, daß auf entsprechende Hinweise zukünftig verzichtet werden sollte. Die Polizei des Landes wurde mit Erlaß vom 7. Dezember 1988 angewiesen, die niedersächsischen Datensätze im POLAS zu überprüfen und zu bereinigen (vgl. IX 12.4). Ausschlaggebend für diese Entscheidung war die Einschätzung, daß in Anbetracht der erfolgten Sensibilisierung der Polizeibeamten und der generell zu treffenden Vorsichtsmaßnahmen die Speicherung von Hinweisen auf eine HIV-Infektion keinen wesentlichen zusätzlichen Schutz bietet.

Bei einer Prüfung habe ich festgestellt, daß sich eine Kriminalpolizeiinspektion nicht an den Erlaß gehalten hat. Sie hatte bei drei Personen in den entsprechenden POLAS-Datensätzen den personengebundenen Hinweis "Ansteckungsgefahr" zugespeichert, nachdem sie von der Aids-Erkrankung erfahren hatte. In zwei Fällen hatte sie zusätzlich im Freitextfeld Informatio-

nen erfaßt, die den Rückschluß auf die HIV-Infizierung zuließen. Die Speicherungen sind umgehend gelöscht worden. Ich habe diese Praxis zum Anlaß genommen, alle von niedersächsischen Polizeidienststellen vergebenen personenbezogenen Hinweise "Ansteckungsgefahr" zu überprüfen. Das Ergebnis lag bei Redaktionsschluß noch nicht vor. Es steht allerdings bereits fest, daß mehrere niedersächsische Polizeidienststellen Hinweise auf eine Aidserkrankung in POLAS gespeichert und damit die Vorgabe des Innenministeriums mißachtet haben.

12.8 Die niedersächsische Polizei interessiert sich weiterhin für Suizidversuche

Ich habe in meinem letzten Tätigkeitsbericht (XI 12.11) über die Speicherung von Suizidversuchen bei der niedersächsischen Polizei berichtet. Meine Prüfung von Kriminalakten führte zur Beanstandung von zahlreichen Einzelfällen. Außerdem habe ich empfohlen, in Niedersachsen vorhandene Suizidspeicherungen zu löschen und zukünftig auf die Erfassung von Vorfällen dieser Art zu verzichten.

Eine inhaltliche Auseinandersetzung des Niedersächsischen Innenministeriums mit den Gründen meiner Beanstandung liegt bis heute noch nicht vor. Die Landesregierung hat in ihrer Stellungnahme zu meinem XI.Tätigkeitsbericht ausgeführt, in Zukunft würden von der Polizei keine Daten über Personen allein deshalb gespeichert, weil sie einen Suizidversuch wiederholen könnten. Aus diesem Grund gespeicherte Daten würden gelöscht. Eine Umsetzung dieser Ankündigung ist allerdings meines Wissens bislang nicht erfolgt. Ich muß daher davon ausgehen, daß die Polizei nach wie vor Kriminalakten anlegt, wenn sie von einem Suizidversuch erfährt. Für mindestens zwei Jahre wird der Hinweis "Freitodgefahr" im polizeilichen Auskunftssystem gespeichert. Bei polizeilich bereits bekannten Personen wird der Suizidversuch dazugespeichert. Damit werden Informationen zusammengeführt, die nicht zusammengehören. Der Suizidversuch ist zumeist ein psychiatrisches, jedenfalls kein polizeiliches Problem. Die Polizei argumentiert, sie müsse die Information über zurückliegende Suizidversuche speichern, damit sie entsprechend reagieren kann, wenn Suizidenten Kontakt mit der Polizei haben. Ich habe hierzu in meinem letzten Tätigkeitsbericht Stellung genommen.

Weiterungen wären denkbar. Es könnte die Frage aufkommen, warum die Speicherung auf behandlungsbedürftige psychisch Kranke beschränkt wird. Müßten nicht auch Menschen mit Herzschrittmachern, Bluter, Diabetiker und Infarktgefährdete - weil sie ebenso mit der Polizei in Berührung kommen können - erfaßt werden? Das Niedersächsische Sozialministerium als für den Bereich Gesundheitsprävention zuständiges Fachressort bezweifelt im übrigen, daß eine Datensammlung bei der Polizei einen Menschen, der den Entschluß zum Suizid gefaßt hat, davon abhalten kann.

Das Land Baden-Württemberg hat sich inzwischen entschieden, den Hinweis "Freitodgefahr" im polizeilichen Informationssystem nicht mehr zu verwenden. Nach der Stellungnahme der dortigen Landesregierung zum

13. Tätigkeitsbericht meiner Kollegin war hierfür entscheidend, daß nach den bisherigen Erfahrungen der Speicherung von "Freitodgefahr" für die Strafverfolgung und die Gefahrenabwehr nicht dieselbe Bedeutung zukommt wie anderen personengebundenen Hinweisen.

### 12.9 Elvis lebt!

Unter XI 12.8 wies ich auf die datenschutzrechtlichen Probleme bei der Anwendung des "Elektronischen Vorgangsverwaltungs- und Informationssystems (elvis)" hin. Dort werden personenbezogene Daten gespeichert, die nach den verbindlichen Richtlinien der Polizei längst hätten gelöscht werden müssen. Weil elvis zunächst als Pilotprojekt deklariert worden ist, hatte man davon abgesehen, verbindliche Löschungsvorgaben festzulegen.

Für Personen mit einer Kriminalakte im Zuständigkeitsbereich der Kriminalpolizeiinspektionen Hildesheim und Osnabrück, wo das Projekt betrieben wird, bedeutet dies, daß ihre Daten in dem Informationssystem bisher nicht gelöscht wurden, obwohl diese Stellen hierzu schon längst verpflichtet waren. Betroffen hiervon sind u.a. auch Minderjährige, über die Kriminalakten angelegt worden sind, und Personen, die Straftaten von geringer Bedeutung begangen haben. Bei Kindern hätte die Löschung beispielsweise nach zwei Jahren erfolgen müssen.

Bis zum Redaktionsschluß lag mir das endgültige Konzept zur datenschutzgerechten Löschung von Daten in elvis noch nicht vor. Nach Meinung der Fachleute bedeutet es einen immensen Aufwand, den Betroffenen nachträglich zu ihrem Recht zu verhelfen. Ich stelle fest, daß mit elvis eine Technik eingeführt worden ist, bei der das Recht der Betroffenen auf informationelle Selbstbestimmung nicht gewährleistet ist.

Diese Erfahrungen zeigen, daß vor der Einführung automatisierter Systeme - auch wenn sie als Pilotprojekt bezeichnet werden - eingehend geprüft werden muß, ob ihre Anwendung die Rechte der Betroffenen gewährleistet. Das gilt beispielsweise auch für MIKADO (vgl. XI 12.7), da nach der mir bekannten Fassung der Errichtungsanordnung für dieses System Fragen im Zusammenhang mit der Löschung von Daten noch nicht geklärt sind. Ich habe die Lösung dieses Problems beim Niedersächsischen Innenministerium angemahnt.

### 12.10 Die Kehrseite der Protokollierung

Die Protokollierung von Anfragen in automatisierten Datensammlungen erfüllt eine wichtige datenschutzrechtliche Funktion: Es wird nachprüfbar, welche Stelle sich wann für welche Daten interessiert hat. Allerdings wird mit der Protokollierung ein neuer Datenbestand geschaffen, der schnell die Begehrlichkeit weckt, die vorhandenen Informationen auch zu anderen als den ursprünglichen Zwecken zu nutzen. In den allgemeinen Datenschutzgesetzen (§ 14 Abs. 4 BDSG, § 10 Abs. 4 NDSG) wurde die ausschließliche

Zweckbindung von Protokolldaten (zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage) festgeschrieben. In Spezialgesetzen wird jedoch von dieser Linie abgewichen. So hat der niedersächsische Gesetzgeber der Polizei im NGefAG den Zugriff auf die Protokolldaten sowohl aus Gründen der Gefahrenabwehr als auch aus Gründen der Strafverfolgung unter bestimmten Voraussetzungen erlaubt. Fremdnutzungen sind aus datenschutzrechtlicher Sicht problematisch, weil in der Protokolldatei Daten gespeichert sind, die die Polizei - gäbe es die aus datenschutzrechtlichen Überlegungen erforderliche Protokollierung nicht - gar nicht vorhalten dürfte. Es handelt sich hier um Informationssammlungen, die in großem Umfang Daten unbescholtener Bürgerinnen und Bürger enthalten. Alle können betroffen sein. In einer polizeilichen Protokolldatei sind beispielsweise Autofahrerinnen und Autofahrer gespeichert, deren Daten bei einer allgemeinen Verkehrskontrolle im polizeilichen Auskunftssystem ohne Ergebnis abgefragt worden sind.

Ich habe im Berichtszeitraum die im Jahr 1992 vorgenommenen Fremdnutzungen der polizeilichen Protokolldatei überprüft. Auffällig waren dabei folgende Punkte:

- Die Polizei hat die Befugnis zur Nutzung der Protokolldaten sowohl zu Zwecken der Strafverfolgung als auch der Gefahrenabwehr gefordert. 1992 - und, wie sich herausgestellt hat, auch 1993 - ergab sich in Niedersachsen kein Sachverhalt, bei dem aus Gründen der Gefahrenabwehr auf die Protokolldatei zurückgegriffen werden mußte. Diese Feststellung legte für mich die Überlegung nahe, ob eine die Zweckdurchbrechung erlaubende Regelung im NGefAG wirklich erforderlich ist oder ob sie nicht eigentlich in die Strafprozeßordnung gehört. Der niedersächsische Gesetzgeber hat sich dafür entschieden, die Fremdnutzung im NGefAG auch für einen zwar noch nicht eingetretenen, jedoch theoretisch denkbaren Fall zu erlauben.
- Abgesehen von einem besonders gelagerten Fall hat die Selektion der Protokolldaten keine Ermittlungserfolge in den jeweiligen Strafverfahren gebracht. In dem besonderen Fall hatte die Polizei ein nicht zugelassenes Fahrzeug mit Hilfe der Identifizierungsnummer (FIN) in der Kfz-Fahndungsdatei abgefragt. Da der Sachbearbeiter die FIN nicht notiert hatte, mußte sie später über die Protokolldatei festgestellt werden.
- Die Selektion der Protokolldatei erfolgt im Landeskriminalamt. Das Ergebnis der Auswertung wird von dort in Listenform an die antragstellende Polizeidienststelle weitergegeben. Die Listen sind zum Teil sehr umfangreich. In einem Fall waren Daten über 826 Betroffene aufgeführt. Aus datenschutzrechtlicher Sicht war der Frage nachzugehen, wie die Polizei mit diesen Listen weiter umgeht. Meine Prüfung ergab, daß diese Unterlagen von einigen Dienststellen auch dann zu den Akten genommen und damit im weiteren Verfahren mitgeführt werden, wenn sie für die Ermittlungen keinerlei Bedeutung haben. Ich habe gefordert, daß die Selektionsergebnisse in diesen Fällen zu vernichten sind. Das Landeskriminalamt prüft, ob eine entsprechende Verpflichtung in die neue Dateibeschreibung für die Protokolldatei aufgenommen wird.

## 12.11 Die Polizei ist keine Auskunftei

Die Polizei wird häufig von Bürgerinnen und Bürgern gebeten, Daten von Privatpersonen herauszugeben. Ein Beispiel: Auf der Straße wird durch ein Fahrzeug ein Stein hochgeschleudert; dieser beschädigt die Windschutzscheibe des nachfahrenden Fahrzeuges. Der Geschädigte geht zur Polizei in der Erwartung, dort Name und Anschrift des Halters zu erhalten. Selbstverständlich muß der Geschädigte in diesem Fall die Möglichkeit haben, an die Daten des Schadensverursachers zu kommen. Nur: Bei diesem Sachverhalt handelt sich nicht um eine Angelegenheit, die den Aufgabenbereich der Polizei berührt. Das Straßenverkehrsgesetz hat in diesen Fällen die Befugnis zur Übermittlung von Halterdaten der Zulassungsstelle und dem Kraftfahrt-Bundesamt zugewiesen. Die Polizei darf ihre vielfältigen Informationsmöglichkeiten nicht einsetzen, um auskunftssuchenden Personen in Fällen dieser Art bei der Geltendmachung von Rechtsansprüchen zu unterstützen. Das Niedersächsische Innenministerium teilt meine Auffassung und wird die Polizeidienststellen auf die Rechtslage hinweisen.

## 12.12 Fußball-WM und Datenschutz

Im Vorfeld der Fußball-WM in den Vereinigten Staaten hatten amerikanische Stellen deutsche Behörden gebeten, Erkenntnisse über Personen zu übermitteln, die bei der Sportveranstaltung zu einem Sicherheitsrisiko werden könnten. Gewünscht wurden detaillierte Informationen über diejenigen, die für eine Anstiftung zu fußballbezogenen Gewaltdelikten bekannt waren oder über die Erkenntnisse aus dem Bereich der allgemeinen Kriminalität vorlagen und die wahrscheinlich anläßlich der WM in die USA reisen wollten. Nach niedersächsischem Recht kam die Weitergabe solcher Daten nur in Betracht, wenn sie zur Abwehr einer erheblichen Gefahr erforderlich war. Diese Voraussetzung hätte - auch nach Auffassung des Innenministeriums - nur vorgelegen, wenn über einzelne Personen bekannt gewesen wäre, daß sie mit Störungsabsicht in die USA reisen wollten. Eine pauschale Übermittlung aller bekannten deutschen Hooligans wäre nicht zulässig gewesen. Die deutschen Behörden brauchten letztendlich über das Ermittlungsersuchen nicht entscheiden, weil die amerikanischen Stellen fachliche Rückfragen unbeantwortet ließen. Eine ähnliche Problematik wird sich im Zusammenhang mit der nächsten Fußball-Europameisterschaft 1996 in England stellen.

## 12.13 Geplant: VW liefert Informationen an die Polizei

In meinem letzten Tätigkeitsbericht hatte ich Datenübermittlungen der niedersächsischen Polizei an private Dritte (HUK-Verband) angesprochen (vgl. XI 12.23). Im Ergebnis hatte ich mich den Datenweitergaben nicht entgegengestellt. Problematisiert habe ich die elektronische Vernetzung zwischen staatlichen und privaten Stellen.

Handelte es sich damals noch um die Weitergabe von Daten, die bei der Polizei vorhanden sind, so geht es neuerdings um die Anlieferung von Informationen an die niedersächsische Polizei durch private Dritte. Über entsprechende Planungen bin ich von dritter Seite informiert worden. Danach sollen - so die erste Darstellung der Fachleute - vom Kfz-Hersteller vorgehaltene "Produktionsdaten", wie z.B. Modell, Fahrgestell-Nummer, Motor-Nummer, Farbe, Zusatzausstattung usw. von polizeilichen Stellen direkt abgefragt werden. Insgesamt ginge es um Sachdaten ohne Personenbezug. Technisch soll die Datenübertragung über eine Online-Verbindung realisiert werden. Das neue Verfahren soll zu einer Intensivierung der Fahndungshilfe im Bereich der Kfz-Kriminalität führen. Hintergrund hierfür sind Erkenntnisse, nach denen gestohlene Fahrzeuge vollständig umgebaut werden, um so die Herkunft zu verschleiern. Das bisher praktizierte Einzelabfrageverfahren (z.B. Grenzdienststelle - Polizei Wolfsburg - VW und zurück) - wird als zu aufwendig und zu zeitraubend angesehen.

Was ist gegen diese sinnvoll erscheinende Planung datenschutzrechtlich einzuwenden? Zunächst einmal stellte sich auf Nachfrage heraus, daß zu den Produktionsdaten auch - leicht entschlüsselbar - Namen und Anschriften von VW-Einzelhändlern gehören, an die ein bestimmtes Fahrzeug ausgeliefert wurde. Die Polizei könnte die erhaltenen Händlerdaten für alle polizeilichen Zwecke nutzen, aber gegebenenfalls auch an Dritte weitergeben. Diese Nutzungsmöglichkeiten haben mit der beabsichtigten Fahndungshilfe nichts mehr zu tun. Das Innenministerium hat in Aussicht gestellt, die Technik so zu gestalten, daß Angaben über Händler nicht mehr auf dem Bildschirm der Polizei lesbar sind.

Im Kern geht es aber um etwas anderes. Nämlich um die aufgrund des Technikeinsatzes neue Qualität von Ermittlungsmaßnahmen, d.h. auch Datenerhebungen, der Polizei. Die Strafprozeßordnung beschreibt in den §§ 161, 163 allgemeine Ermittlungsbefugnisse zur Strafverfolgung im konkreten Einzelfall. An Online-Verbindungen hatte bei Schaffung der StPO niemand gedacht. Online-Verbindungen ermöglichen immer einen Zugriff auf Datenbestände, ohne daß es noch einer Entscheidung im Einzelfall bedarf, ob die Daten übermittelt werden sollen oder nicht. Wird eine solche Verbindung eingesetzt, so erfolgt ein unkontrollierter Datentransfer. Gerade auch deswegen enthalten neuere Rechtsvorschriften hierzu die Verpflichtung, vorher die Angemessenheit eines solchen Verfahrens zu prüfen bzw. eine Technikfolgenabschätzung durchzuführen. Meine Erfahrung hinsichtlich eingesetzter technischer Systeme kann ich auf einen kurzen Nenner bringen: Wenn erst einmal eine Technik installiert wurde, dann wird es immer auch praktische Gründe geben, die technischen Möglichkeiten extensiv zu nutzen und voll auszuschöpfen.

Aus Sicht des Datenschutzes habe ich zudem der Frage nachzugehen, ob eine Maßnahme oder ein Verfahren unerläßlich (erforderlich) ist. Unerläßlich kann ein Verfahren nicht sein, wenn schon vorhandene Kapazitäten das Gewünschte ermöglichen. Genau dies scheint hier der Fall zu sein. Das bestehende Recht läßt eine Erweiterung der Möglichkeiten für die nötigen

Zugriffe beim Kraftfahrt-Bundesamt zu. Eine Online-Verbindung in den privaten Bereich erübrigte sich dann.

## 13. Ausländerangelegenheiten

### 13.1 Datenschutz zweiter Klasse - das Ausländerzentralregister

Was lange währt, wird noch lange nicht gut! Diese Feststellung mußte ich hinsichtlich der Verabschiedung des Gesetzes über das Ausländerzentralregister (AZR) machen. Kurz vor Ende der 12. Legislaturperiode verabschiedete der Deutsche Bundestag dieses Gesetz, das auch gleich am 1.10.1994 in Kraft trat (BGBl. I S. 2265). Dem war eine datenschutzrechtliche Leidensgeschichte vorangegangen, während der sich zu dem Thema zwölf dicke Bände in meiner Registratur angesammelt haben: Schon für das Jahr 1979 stellte der Bundesbeauftragte für den Datenschutz in seinem zweiten Tätigkeitsbericht heraus, daß der Zugriff auf diese elektronische Großdatei ohne Rechtsgrundlage erfolge. Nach dem Volkszählungsurteil des BVerfG wurde die Notwendigkeit einer gesetzlichen Grundlage für diese einstmals größte Verwaltungs-Personendatei jedem gewahr. Anfang 1987 kündigte dann die Bundesregierung für die 11. Legislaturperiode die Vorlage eines AZR-Gesetzes an. Tatsächlich wurde Mitte 1988 ein erster Entwurf für ein solches Gesetz vorgelegt. Diesem folgten eine Vielzahl weiterer Entwürfe, die aus datenschutzrechtlicher Sicht kritikwürdig waren und daher von mir und meinen Kollegen auch kritisiert wurden. Nachdem sich abzeichnete, daß die vielen schriftlichen Stellungnahmen der Datenschutzbeauftragten weitgehend unbeachtet bleiben sollten, wandte sich die Konferenz der Datenschutzbeauftragten im März 1994 nochmals mit einigen zentralen Datenschutzforderungen an die Öffentlichkeit (Anlage 14). Vergebens: Das nunmehr verabschiedete Gesetz enthält mehrere Regelungen, die ich für mehr als problematisch halte.

Das AZR soll nicht nur als bundesweites Melderegister über alle nichtdeutschen Staatsangehörige genutzt werden, sondern als bundesweite Informationszentrale für praktisch alle Verwaltungsbereiche. Damit verabschiedete sich der Bundesgesetzgeber vom Prinzip der "informationellen Gewaltenteilung" des Bundesverfassungsgerichtes und kehrte zum obrigkeitsstaatlichen Grundsatz der "Einheit staatlicher Verwaltung" zurück. Insbesondere die Einbindung des gesamten Sicherheitsapparates von Bund und Länder per automatisierte Übermittlungsverfahren in das AZR ist mir ein Dorn im Auge. Mit der Aufnahme aller Ausländerinnen und Ausländer in eine "Sicherheitsdatei" wird eine gesamte Bevölkerungsgruppe indirekt zum abstrakten Sicherheitsrisiko und zu potentiellen Rechtsbrechern deklariert. Das BVerfG hat klargestellt, daß mit einer Datensammlung nicht Zwecke verfolgt werden dürfen, die sich gegenseitig ausschließen. Mir ist nicht ersichtlich, wie die polizeiliche und nachrichtendienstliche Nutzung des AZR mit ausländerrechtlichen Zwecken in Einklang gebracht werden können, zumal im Ausländerrecht soziale Aspekte wie z.B. die Integration oder die Famili-

enzusammenführung eine große Rolle spielen sollen. Es dürfte kaum bestreitbar sein, daß ein entsprechendes Register über Deutsche verfassungswidrig wäre. Ebenso unbestreitbar ist, daß das Grundrecht auf Datenschutz auch für Nichtdeutsche gilt. Dessenungeachtet bestand beim Gesetzgeber hinsichtlich der Registrierung von Ausländerinnen und Ausländern keine verfassungsrechtliche Scham. Folgende Einzel-Kritikpunkte möchte ich herausheben:

- Viele Regelungen sind derart unbestimmt, daß die Betroffenen die Verarbeitung Ihrer Daten nicht absehen können.
- Der Speicherung von "Einreisebedenken" erfolgt aufgrund wenig präzisierter Hypothesen ohne formalisiertes rechtsstaatliches Verfahren.
- Die Erforderlichkeit von Doppelspeicherungen im AZR und im polizeilichen INPOL-System ist mir nicht einsichtig.
- Es werden Personen gespeichert, die durch das Bundesgebiet "durchgeliefert" werden, ohne daß dabei deutsche Belange tangiert werden müßten.
- Die AZR-Nummer läuft Gefahr, als Personenkennzeichen verwendet zu werden.
- In Ausnahmefällen sollen trotz eingetragener Übermittlungssperre Datenübermittlungen, z.B. auch ans Ausland, ohne Anhörung der Betroffenen möglich sein. Dadurch geht die Sicherungsfunktion der Übermittlungssperre verloren.
- Bei der Speicherung von Suchvermerken wird keine Einschränkung der beteiligten Behörden vorgenommen.
- Die On-Line-Verknüpfung von Geheimdiensten und AZR verstößt gegen das Gebot der Trennung von Ordnungsverwaltung und Nachrichtendiensten.
- Durch die Verwendung der vom AZR übermittelten Begründungstexte sollen für die Betroffenen nachteilige Eilentscheidungen ohne Anhörung getroffen werden können.
- Es wird mit der Gruppenauskunft die Rasterfahndung mit Ausländerdaten erlaubt, ohne daß präzise Verwendungsregelungen bestehen.
- Die Zugriffsmöglichkeiten insbesondere von Sicherheits- und Justizbehörden gehen weit über das hinaus, was für deren Aufgabenerfüllung erforderlich ist.
- Für die Regelung der für die Betroffenen äußerst gefährlichen Datenübermittlung vom AZR ins Ausland (z.B. in den Herkunftsstaat) kann ich keine Erforderlichkeit erkennen.
- Eine Auskunftsverweigerung gegenüber den Betroffenen aus Gründen der öffentlichen Ordnung ist in jedem Fall unverhältnismäßig. Die Sicherheitsklauseln bei der Auskunftsverweigerung, die im Einzelfall sogar zur Verweigerung der Kontrollmöglichkeit durch den Bundesbeauftragten für den Datenschutz führen kann, macht unter Umständen eine Rechtskontrolle unmöglich.

In einzelnen Regelungen wurde die datenschutzrechtliche Kritik aufgegriffen. Insofern ist positiv zu vermerken, daß das Niedersächsische Innenministerium sich über die Beteiligung des Bundesrates für eine Verbesserung des Entwurfes eingesetzt hat und daß diese Bestrebungen von der Ausländ-

derkommission des Niedersächsischen Landtags aktiv unterstützt wurden. Dies ändert nichts daran, daß das jetzt geltende AZR-Gesetz das verfassungsrechtlich geforderte Mindestdatenschutzniveau unterschreitet. Es ist nun Aufgabe der praktischen Umsetzung, dem Gesetz die gefährlichsten Zähne zu ziehen.

Inzwischen ist mir der Text einer Verordnung zur Durchführung des AZR-Gesetzes zugegangen. Diese Verordnung enthält leider keine Eingrenzung der zu weiten gesetzlichen Befugnisse. Sie sieht auch nicht vor, daß Rechtsmittel, die von den Betroffenen gegen gespeicherte Entscheidungen eingelegt worden sind, mitgespeichert werden. Dies führt dazu, daß die tatsächliche und rechtliche Richtigkeit von Eintragungen bestritten wird, ohne daß dies aus dem Register erkennbar ist. Hier muß meines Erachtens nachgebessert werden.

13.2 Ausnahmslose ED-Behandlung von Bürgerkriegsflüchtlingen?

Auf der Innenministerkonferenz am 6./7. Mai 1994 wurde der Beschluß gefaßt, die Bundesregierung zu bitten, durch eine entsprechende Änderung des Ausländergesetzes die generelle erkennungsdienstliche (ED-) Behandlung auch von Bürgerkriegsflüchtlingen zu ermöglichen. Bis zu der erforderlichen Rechtsänderung sollten die vorhandenen Möglichkeiten zur ED-Behandlung nach § 41 AuslG konsequent ausgeschöpft werden. Nur das Land Hessen sah die generelle Erfassung der Fingerabdrucke von Bürgerkriegsflüchtlingen nicht als sinnvoll und nicht als rechtmäßig an. Dieser Bewertung kann ich mich anschließen:

In § 16 AsylVfG ist geregelt, daß die Identität von Ausländerinnen und Ausländern, die um Asyl nachsuchen, durch erkennungsdienstliche Maßnahmen zu sichern sei, es sei denn, daß eine unbefristete Aufenthaltsgenehmigung vorliegt oder das 14. Lebensjahr noch nicht vollendet wurde. Es dürfen Lichtbilder und Abdrucke aller zehn Finger erstellt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten die Regelung für verfassungsrechtlich problematisch, weil auch Personen betroffen sind, über deren Identität keine Zweifel bestehen (XI Anlage 7). Dies gilt natürlich auch in Bezug auf Bürgerkriegsflüchtlinge. In XI 13.1 wies ich darauf hin, daß es auch bei umfangreichsten Überwachungsmaßnahmen keinen hundertprozentigen Schutz vor Rechtsmißbrauch geben kann. Es darf keine totale Erfassung geben, die Menschen miterfaßt, die sich gesetzeskonform verhalten. Erst bei Anhaltspunkten für den Mißbrauch von staatlichen Leistungen kommt die Anfertigung von ED-Unterlagen in Frage. Unverhältnismäßig ist zudem, daß ebenso wie von Asylsuchenden auch bei Bürgerkriegsflüchtlingen die Fingerabdruckdaten aller 10 Finger erhoben werden sollen. Für eine eindeutige Identifizierung reicht der Abdruck eines Fingers aus. Bei der Erhebung, Speicherung und Nutzung von ED-Unterlagen handelt es sich zudem um eine äußerst sensible Anwendung, da die Verwendung für Strafverfolgungs- und Gefahrenabwehrzwecke möglich ist und auch stattfindet. Meine Aufforderung an das Niedersächsische Innenministerium, seine Position zu revidieren, fand dort leider bisher kein Gehör.

13.3 Folgenreicher Streit im Sozialamt

Welche Konsequenzen unzulässige Datenübermittlungen für Asylsuchende haben können zeigt ein Fall, der mir von einer Flüchtlingsinitiative vorgetragen wurde: Ein Asylbewerber wurde vom einem Sozialamt beschuldigt, einen tätlichen Angriff auf eine Angestellte vorgenommen zu haben. Wie mir mitgeteilt wurde, bestritt der Flüchtling den ihm zur Last gelegten Vorwurf und gab nur an, aufgrund des schikanösen Verhaltens des Sozialamtes etwas lauter geworden zu sein. Hinterher habe er sich hierfür entschuldigt. Inzwischen hat er wegen dieses Vorgangs jedoch einen Strafbefehl mit einer geringen Strafe wegen Körperverletzung und Nötigung erhalten und auch akzeptiert.

Nach Ansicht der Stadt, zu der das Sozialamt gehört, handelte es sich bei dem tätlichen Angriff um einen Straftatbestand, der einen Ausweisungsgrund im Sinne von § 46 AuslG darstellt, weshalb diese Information an die zuständige Ausländerbehörde des Landkreises gemäß § 76 Abs. 2 AuslG weitergegeben werden durfte. Die Ausländerbehörde gab diese Information an das Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) weiter und berief sich auf die neue Regelung des § 8 AsylVfG. In einem Erlaß des Niedersächsischen Innenministeriums vom 14. Dezember 1992 (Az.: 56.31-12231/3-9) ist vorgesehen, daß die Ausländerbehörden das BAFl um beschleunigte Bearbeitung von Asylanträgen zu bitten haben, wenn ein Kapitalverbrechen vorliegt. Der Landkreis meinte, dies sei hier der Fall gewesen. Das BAFl verwendete die Information im Rahmen des Anerkennungsverfahrens und zog aus dem tätlichen Angriff in der Begründung der Asylablehnung den Schluß, daß der Antragsteller nicht ausschließlich an seiner Anerkennung als Asylbewerber interessiert sei.

Die Nutzung der Informationen durch die Bundesbehörde BAFl entzieht sich meiner Überprüfungszuständigkeit. Zuständig bin ich aber für die erfolgten Datenübermittlungen vom Sozialamt zur Ausländerbehörde und von dort zum BAFl. Diese hielt ich für rechtswidrig, so daß ich zwei Beanstandungen aussprechen mußte.

Die Datenübermittlung des Sozialamtes an die Ausländerbehörde war nicht durch § 76 Abs. 2 AuslG gedeckt. Nach § 76 Abs. 2 AuslG haben öffentliche Stellen unverzüglich die zuständige Ausländerbehörde zu unterrichten, wenn sie von einem Ausweisungsgrund Kenntnis erlangen. Nach § 46 Nr. 2 AuslG kann ausgewiesen werden, wer einen nicht nur vereinzelten oder geringfügigen Verstoß gegen Rechtsvorschriften begangen hat. Unter diesen Voraussetzungen kann auch eine Datenübermittlung ans Ausländeramt erfolgen. Davon konnte aber bei einem einmaligen Verstoß, der mit einem Strafbefehl und einer relativ niedrigen Strafe geahndet wurde, keine Rede sein. Da der Betroffene einen Asylantrag gestellt hatte, der noch nicht beschieden war, besaß er nach § 55 Abs. 1 AsylVfG unabhängig von § 46 AuslG eine Aufenthaltsgestattung. Die Information war daher in diesem Verfahrensstadium nicht erforderlich. Wegen der Weite des § 76 Abs. 2

AuslG sah sich der Bundesminister des Innern veranlaßt, in vorläufigen Anwendungshinweisen Konkretisierungen vorzunehmen. Mitteilen darf danach nur die sachnächste öffentliche Stelle. Zur Übermittlung von Straftaten und Ordnungswidrigkeiten sind die zuständigen Stellen befugt. Dies sind im konkreten Fall die Polizei- und Ordnungsbehörden sowie die Staatsanwaltschaft (vgl. § 76 Abs. 4 AuslG), nicht jedoch das Sozialamt.

Unzulässig war auch die Datenübermittlung von der Ausländerbehörde an das BAFl. Nach § 8 Abs. 1 AsylVfG bedarf es für eine Datenübermittlung durch öffentliche Stellen prinzipiell eines Ersuchens. Daran fehlte es hier. Die Voraussetzungen für eine Spontanübermittlung nach § 8 Abs. 2 AsylVfG lagen nicht vor. Die Unzulässigkeit der Datenübermittlung dürfte sich auch aus dem Umstand ergeben, daß die Datenspeicherung bei der Ausländerbehörde wegen der vorausgegangenen unzulässigen Übermittlung des Sozialamtes rechtswidrig war. Der Verweis des Landkreises auf den Erlaß des Niedersächsischen Innenministeriums ging fehl. Erhebliche Straftaten sind nach dem Erlaß "schwere Straftaten (z.B. Kapitalverbrechen, Sexualdelikte, Raub)" sowie Betäubungsmittelkriminalität und Wiederholungstaten. Die dem Betroffenen vorgeworfene Tat gehörte hierzu gewiß nicht. Der betreffende Erlaß regelt zudem nur die Bitte um um beschleunigte Bearbeitung, räumte aber keine Befugnis ein, den der Bitte zugrundeliegenden Sachverhalt zu übermitteln. Ich muß in diesem Zusammenhang darauf hinweisen, daß ein Erlaß als rechtliche Grundlage für eine Datenübermittlung generell nicht ausreicht.

## 13.4 Asylwohnheime

Der Umstand, daß Wohnheime für Asylsuchende und sonstige Flüchtlinge oft von privaten Betreibern geführt werden, kann zu datenschutzrechtlichen Problemen führen. Die Kommunen bedienen sich der Privaten nicht nur für die Unterbringung und Versorgung, sondern auch, was naheliegt, um sich Daten über die Flüchtlinge zu beschaffen. Dabei werden die Privaten im Auftrage der unterbringungspflichtigen Kommunen tätig. Ich mußte eine Kommune darauf hinweisen, daß eine derartige Datenverarbeitung im Auftrag nach § 6 NDSG schriftlich erfolgen und ausreichend konkret sein muß. Mitgeteilt werden dürfen nur die Daten, die zur Aufgabenerfüllung der Kommune erforderlich sind. So hält die Landeshauptstadt für ihre Aufgabenerfüllung Name, Vorname, Geburtsdatum, Nationalität, Aufenthaltsstatus, Asylantragsdatum und evtl. Angaben zur Erwerbstätigkeit der Flüchtlinge für notwendig. Der Betreiber darf die Daten nur für die Gewährung der entsprechenden Unterkunft und die damit zusammenhängenden Aufgaben nutzen. Die teilweise sehr intimen Angaben, die im Rahmen der sozialen Beratung durch einen Betreiber erlangt werden, werden nicht im Auftrag erhoben und dürfen daher den Kommunen grundsätzlich nicht mitgeteilt werden.

Aus Datenschutzsicht wenig erfreulich war ein Vorgang, bei dem ein privater Betreiber per Formblatt gegenüber Flüchtlingen schriftliche Verweise aussprach, z.B. wegen Nichteinhaltens der Nachtruhe oder wiederholten starken Alkoholkonsums. Er verband dies mit der Androhung, daß weitere

Verstöße der Bezirksregierung und der Ausländerbehörde gemeldet würden. Außerdem behauptete er, eine derartige Meldung würde beim Asylverfahren schwerwiegende Folgen haben. Das Ministerium für Bundes- und Europaangelegenheiten teilte mir mit, daß es sich bei dem konkreten Vorgang um einen Einzelfall gehandelt habe. Zu den angedrohten Übermittlungen sei es nicht gekommen. Es teilte meine Bewertung, daß ein entsprechendes Vorgehen rechtswidrig wäre.

## 13.5 Fürsorgliche Meldung für Flüchtlinge

Asylverfahren werden heute von der Verwaltung weitgehend als Massenverfahren behandelt. Hierbei wird ADV zur effektiven Aufgabenerfüllung eingesetzt. Auch wenn mit derartigen automatisierten Verfahren Geld und Personal eingespart werden kann, so muß dabei die Beachtung der Menschenwürde und der Grundrechte der Flüchtlinge nicht auf der Strecke bleiben. Gesetze sind gegenüber ausländischen Flüchtlingen ebenso einzuhalten wie bei Deutschen.

Seit dem 1. April 1994 unterliegen ausländische Flüchtlinge und Asylsuchende in den Aufnahmeeinrichtungen des Landes der allgemeinen Meldepflicht. Es zeigte sich, daß die Flüchtlinge ohne amtliche Unterstützung dieser Pflicht oft nicht nachkommen. Aus Fürsorge für die Flüchtlinge suchte die Verwaltung ein Verfahren, bei welchem den Meldepflichtigen behördliche Hilfestellung gegeben werden kann. Außerdem sollte verhindert werden, daß durch verschiedene Stellen mehrfache Befragungen durchgeführt werden müssen. Übersetzungsprobleme und Kommunikationsschwierigkeiten, z.B. wegen verschiedener Namensschreibweise, sollten bei den regelmäßig verwaltungsunerfahrenen Betroffenen auf ein Minimum begrenzt werden.

Um diese Probleme zu lösen, können nicht einfach die Tagesaufnahmelisten der Aufnahmeeinrichtungen an die Meldebehörden übermittelt werden. Nach § 9 NMG liegt die Meldepflicht bei der Person, die eine Wohnung bezieht, nicht beim Wohnungsgeber. Dies ist Folge des in § 11 NMG niedergelegten Grundsatzes der Datenerhebung bei den betroffenen Meldepflichtigen. Eine Ausnahme für Flüchtlinge ist im Gesetz nicht vorgesehen. Eine solche Ausnahme enthält auch nicht § 12 NMG, wonach sich der Wohnungsgeber oder sein Beauftragter davon überzeugen muß, daß die bei ihm Wohnenden der Meldepflicht nachgekommen sind. Damit wird kein eigenständiges Melderecht begründet. § 12 Abs. 2 NMG sieht lediglich eine Anzeigepflicht gegenüber der Meldebehörde vor, die die Meldepflicht bei Ab- und Anmeldung durch die Umziehenden nicht verdrängt.

Aus diesem Grund halte ich das sog. "Braunschweiger Modell" für problematisch, bei dem eine teilweise abgedeckte Kopie der "Niederschrift zu einem Asylantrag" zu Meldezwecken an die Meldebehörde weitergegeben wird. Auch hier erfolgt nämlich die Meldung durch die Aufnahmeeinrichtung und nicht durch die betroffenen Flüchtlinge. Die Bezirksregierung Braunschweig versicherte mir, daß künftig durch das Abdecken beim Kopie-

ren des Asylantrags alle nicht erforderlichen Angaben unterdrückt werden. Für eine Übermittlung dieser Daten gibt aber keine rechtliche Grundlage.

Keine Einwände habe ich dagegen gegen das vom damaligen Niedersächsischen Ministerium für Bundes- und Europaangelegenheiten vorgeschlagene sog. "Melde-Modul". Dabei werden die meldepflichtigen Flüchtlinge auf ihre Meldepflicht hingewiesen. Es wird ihnen freigestellt, selbst der Meldepflicht nachzukommen. Zugleich wird ihnen aber das Angebot gemacht, daß die im Rahmen des "ZASt-Verfahrens" (vgl. XI 13.2) erhobenen Daten der Aufnahmeeinrichtung der Meldebehörde mitgeteilt werden. Die hierzu erteilte Einwilligung, die durch das Unterschreiben des per EDV-Verfahren ausgefüllten Anmeldeformulars erfolgen kann, muß freiwillig sein. Ich teilte daher dem Ministerium mit, daß es wünschenswert ist, wenn die Flüchtlinge in ihrer Landessprache prägnant über den Sinn der Anmeldung und Ablauf und Zweck des "Melde-Modul"-Verfahrens unterrichtet werden. Verweigert eine meldepflichtige Person das angebotene Verfahren, so ist ensprechend den Regelungen nach dem NMG zu verfahren.

Da das "Melde-Modul"-Verfahren zugleich eine regelmäßige Datenübermittlung im Sinne von § 12 Abs. 6 NDSG darstellt, ist für das Verfahren außerdem eine Rechtsverordnung erforderlich. Nach Nr. 10.3 der Verwaltungsvorschriften zum NDSG ist eine regelmäßige Datenübermittlung immer dann gegeben, wenn Datenübermittlungen ohne Ersuchen einer anderen Behörde in allgemein bestimmten Fällen wiederkehrend durchgeführt werden. Daran ändert auch der Umstand nichts, daß die Flüchtlinge durch ihre Unterschrift eine Einwilligung zur Datenübermittlung geben.

## 13.6 Der direkte Draht zur Meldebehörde

Von einer Ausländerbehörde wurde ich darauf hingewiesen, daß offensichtlich bei einer Vielzahl von Ausländerbehörden die Möglichkeit des automatisierten Abrufs von Meldedaten besteht. Dies wirft meines Erachtens datenschutzrechtliche Probleme auf.

In § 2 der bundesweiten "Verordnung über Datenübermittlungen an Ausländerbehörden" (AuslDÜV) vom 18. Dezember 1990 (BGBl. I S. 2997) ist vorgesehen, daß die Meldebehörden den Ausländerbehörden aus Anlaß von Anmeldung, Abmeldung, Scheidung, Nichtigerklärung oder Aufhebung der Ehe, Namensänderung, Staatsangehörigkeitsänderungen, Geburt und Tod bestimmte Daten von Ausländerinnen und Ausländern regelmäßig übermitteln. Als Rechtsgrundlage für die Verordnung wird § 76 Abs. 5 AuslG angegeben. Eine Regelung zum automatisierten Abrufverfahren enthält aber weder das AuslG noch die AuslDÜV. Seit dem 1. Oktober 1994 ist nunmehr § 12 NDSG anzuwenden (§ 34 Abs. 2 NDSG), der für On-Line-Verfahren eine Rechtsverordnung fordert. Eine entsprechende Verordnung liegt bisher nur im Entwurf vor. Aus § 12 Abs. 6 NDSG, der die entsprechende Anwendung der Abrufregelungen auf regelmäßige Übermittlungen vorsieht, kann nicht geschlossen werden, daß bei Zulassung regelmäßiger Datenübermitt-

lungen auch automatisierte Abrufverfahren zugelassen sein sollen. Die Rechtsvorschrift soll Anfang 1995 veröffentlicht werden.

13.7 Flüchtlinge als Telefongebühren-Risiko?

Ein Fernmeldeamt der Deutschen Bundespost Telekom fragte per Telefax regelmäßig bei der räumlich zuständigen Ausländerbehörde nach dem Aufenthaltsstatus von Ausländerinnen und Ausländern, insbesondere ob es sich um Asylsuchende handelt. Begründet wurde dies damit, daß die DBP Telekom Aufgaben der Daseinsvorsorge wahrnehme. Um Einnahmeverluste im Interesse aller Kundinnen und Kunden zu minimieren, müsse sie wissen, ob eine einen Telefonanschluß beantragende Person einen Asylantrag gestellt habe. Bei Asylsuchenden wird offensichtlich ein Risiko teurer Auslandsgespräche, die nicht bezahlt werden können, gesehen, als auch das Risiko unerwarteter Abschiebungen, was das Eintreiben unerledigter Forderungen unmöglich macht. Um diese wirtschaftlichen Risiken zu minimieren, kann die DBP Telekom nach § 8 Abs. 1 Satz 1 TKV bei der Einrichtung eines Telefonanschlusses oder bei entsprechenden Monopoldienstleistungen im Einzelfall Sicherheitsleistungen oder Vorauszahlung in angemessener Höhe verlangen, aber nur, "wenn zu besorgen ist, daß der Kunde seinen vertraglichen Verpflichtungen nicht oder nicht rechtzeitig nachkommt". Die Anfragen verfolgten den Zweck festzustellen, ob Sicherheitsleistung verlangt werden soll. Eine Umfrage im Land ergab, daß 12 der 55 Ausländerbehörden einmal oder mehrfach entsprechende Auskünfte gegeben haben.

Die DBP Telekom ist, trotz der Teilprivatisierung im Rahmen des Poststrukturreform, eine öffentliche Stelle, die bei der Meldebehörde - nicht aber beim Ausländeramt - nach § 29 Abs. 1 NMG über Vor- und Familiennamen sowie Anschrift Auskunft einholen kann. Dies gilt auch für Auskunftsbegehren über eine Vielzahl namentlich bezeichneter Einwohner. Die Weitergabe der Statusangabe "Asylbewerber" durch das Meldeamt wäre jedoch nicht zulässig; dieses Datum darf dort überhaupt nicht gespeichert werden.

Sicherlich habe ich Verständnis für das Bestreben der DBP Telekom, Einnahmeverluste so gering wie möglich zu halten. Auch erkenne ich, daß das Fernmeldeamt wegen seiner Gemeinwohlverpflichtung einem sog. Kontrahierungszwang unterliegt, d.h. grundsätzlich Telefonanschluß-Anträgen entsprechen muß. Dies berechtigt aber nicht zu Anfragen ins Blaue hinein und schon gar nicht zu deren Beantwortung.

Nach § 11 Abs. 1 NDSG ist eine Datenübermittlung zulässig, wenn "Angaben der Betroffenen überprüft werden müssen, weil Anhaltspunkte für deren Unrichtigkeit bestehen". Die DBP Telekom muß also die Frage der Zahlungsfähigkeit zunächst gegenüber der jeweils antragstellenden Person klären. Ob ein Asylantrag gestellt worden ist, dürfte zur Feststellung der Zahlungsfähigkeit weder geeignet noch erforderlich sein. Darin käme ein pauschaler diskriminierender Verdacht zum Ausdruck, Asylsuchende würden ihren Zahlungspflichten nicht nachkommen. Das Führen eines ausländischen Namens ist in jedem Fall kein Anhaltspunkt dafür, daß eine Antrag-

stellerin bzw. ein Antragsteller den Zahlungsverpflichtungen nicht nachkommen kann. Eine Beantwortung der Anfragen des Fernmeldeamtes sah ich daher für unzulässig an. Der DBP Telekom bleibt also gegenüber ausländischen Bürgerinnen und Bürgern kein anderer Weg als gegenüber Deutschen: die Sperrung des Telefonanschlusses bei Zahlungsverzug (§ 16 TKV). Dies wird inzwischen auch von der DBP Telekom so gesehen. Diese teilte dem von mir eingeschalteten Bundesbeauftragten für den Datenschutz mit, daß die Einholung der Auskünfte nicht generell praktiziert werde; die Anfragen des genannten Fernmeldeamtes sei eine "Einzelerscheinung, die zwischenzeitlich abgestellt wurde". Die Ausländerbehörden wurden über die Bezirksregierungen auf die Rechtslage hingewiesen. Es ist daher davon auszugehen, daß künftig keine entsprechenden Mitteilungen mehr an die DBP Telekom erfolgen.

13.8 Aufnahme jüdischer Emigranten aus der ehemaligen UdSSR

Auch in Niedersachsen werden jüdische Aussiedler aus der ehemaligen UdSSR im Rahmen eines besonderen Verfahrens aufgenommen. Im Rahmen dieser Aufnahmeaktion ist es für die Erteilung der Aufenthaltsgenehmigung erforderlich, daß die Zugehörigkeit zur jüdischen Gemeinschaft festgestellt wird. Soweit diese Feststellung nicht schon vor der Einreise erfolgt ist, werden entsprechende Bestätigungen mit dem Einverständnis der Betroffenen bei den jüdischen Gemeinden bzw. dem Landesverband der jüdischen Gemeinden eingeholt. Nachdem klargestellt wurde, daß die Einbeziehung der Gemeinden nicht erforderlich ist, wenn die Zugehörigkeit zum Judentum anderweitig festgestellt werden kann, hatte ich keine Bedenken gegen dieses Verfahren.

Für problematisch erachte ich jedoch die in einem Erlaß des Innenministeriums festgeschriebene Praxis, den jüdischen Gemeinden ohne Einwilligung der Betroffenen jeweils eine Liste der Neuankömmlinge zuzuleiten. Die Übermittlung unterbleibt nur bei ausdrücklichem Widerspruch. Begründet wird dieses Vorgehen damit, daß die Aufnahmeaktion nicht vom historischen Hintergrund dieser Aufnahme losgelöst betrachtet werden könne und die Ausländerbehörden ausnahmsweise auch die Aufgabe der Integration hätten. Selbstverständlich unterstütze ich das Bestreben, die Verantwortung Deutschlands hinsichtlich der nationalsozialistischen Judenverfolgung bei der Aufnahme jüdischer Bürgerinnen und Bürger zu berücksichtigen. Doch mußte ich das Innenministerium darauf hinweisen, daß es für die Datenübermittlung an die jüdischen Gemeinden keine gesetzliche Grundlage gibt. Die Kontaktaufnahme zu den jüdischen Gemeinden kann auch dadurch ermöglicht werden, daß den Betroffenen ein Merkblatt ausgehändigt wird, in dem auf die Integrationsangebote der Gemeinden hingewiesen wird.

## 14. Verfassungsschutz

### 14.1 Deregulierung des Verfassungsschutzes?

Entscheidungsspielräume werden erweitert, wenn vorhandene rechtliche Vorgaben reduziert werden oder ganz wegfallen (Deregulierung). Eine geplante Änderung des Niedersächsischen Verfassungsschutzgesetzes (NVerfSchG) scheint mir in diese Richtung zu gehen. Allerdings stimmt mich die Möglichkeit größerer Entscheidungsspielräume beim Verfassungsschutz eher nachdenklich.

Ende 1992 trat das neue NVerfSchG in Kraft (vgl. XI 14.1). Nach Meinung vieler stellte das Gesetz insgesamt einen Meilenstein zu mehr Liberalität, Transparenz und Datenschutz dar. Ein zentrales Anliegen z.B. war es, durch deutliche Vorgaben des Gesetzgebers jegliche Möglichkeit einer "Gesinnungsschnüffelei" auszuschalten. Bestrebungen durften hiernach nur dann beobachtet werden, wenn deren Verhaltensweisen auf Anwendung von Gewalt gerichtet sind oder sich in aktiv kämpferischer, aggressiver Weise gegen die freiheitliche demokratische Grundordnung richten (Aggressionsklausel). Bereits ein Jahr später, Ende 1993, kamen aber schon aus den Reihen der Parlamentsmehrheit erste Ankündigungen, die Voraussetzungen für die Beobachtung durch den Verfassungsschutz wieder zu erleichtern. Inzwischen hat die Landesregierung dem Landtag den Entwurf eines "Gesetzes zur Änderung des niedersächsischen Verfassungsschutzschutzgesetzes" zugeleitet (LT-Drs. 13/420). Danach soll u.a. durch Streichung der "Aggressionsklausel" eine Beobachtung durch den Verfassungsschutz erleichtert werden. Weshalb soll ein vor kurzem noch als "zentrales Anliegen" qualifiziertes Ziel schon wieder über Bord geworfen werden?

Das Verwaltungsgericht Hannover hatte dem Land Niedersachsen untersagt, die "Republikaner" mit nachrichtendienstlichen Mitteln zu beobachten. Nach Meinung des Gerichts hatte das Land, jedenfalls zum Zeitpunkt der Entscheidung, keine hinreichenden Verdachtsmomente für das Vorliegen der Voraussetzungen der "Aggressionsklausel" dargetan. Das Land legte gegen diese Entscheidung zwar Berufung ein, begründete sie aber trotz dreimaliger Aufforderung des Gerichts neun Monate lang nicht. Das Niedersächsische Oberverwaltungsgericht (OVG) entschied über die Berufung dann nach Aktenlage, so wie sie sich vor dem Verwaltungsgericht dargestellt hatte. Das Land verlor den Prozeß.

Es steht außer Frage, daß als extremistisch eingestufte Bestrebungen mit allen dem Rechtsstaat zu Gebote stehenden demokratischen Mitteln entgegenzutreten ist. Wenn die Landesregierung hierzu auch die Möglichkeiten des Verfassungsschutzes nutzen will, so frage ich mich, warum sie dieses Ziel nicht zielstrebig verfolgt. Niemand hat das Land gehindert, das Berufungsverfahren vor dem OVG durch eigenen Sachvortrag inhaltlich zu führen oder als "Zeugen" für kämpferisch, aggressive Verhaltensweisen der Partei ehemals führende Vertreter der Republikaner, die während des Jahres aus der Partei ausgetreten sind, zu benennen. Auch jetzt noch gäbe es die

Möglichkeit, ein neues Beobachtungsverfahren - bei gleicher Gesetzeslage - anzuordnen. Immerhin liegt nach Meinung des Niedersächsischen Innenministeriums neues Material vor, das den Nachweis des geforderten Verhaltens erbringt (vgl. Nordreport vom 1. September 1994). Das geltende NVerfSchG hat sich im übrigen gerade in diesem Punkt in einem anderen Verfahren vor Gericht bewährt. Sollte die geplante Änderung des Verfassungsschutzgesetzes verabschiedet werden, so wäre eine Beobachtung auch anderer Gruppierungen nicht ausgeschlossen. Diese "flächendeckende" Wirkung läßt mich zweifeln, ob der sehr spezifische Anlaß die Gesetzesänderung wirklich trägt.

Im Gesetzentwurf vorgesehen ist außerdem die Erweiterung der Aufgaben des Verfassungsschutzes um die Beobachtung von Bestrebungen, die sich gegen den Gedanken der Völkerverständigung richten. Vom Beratungsverfahren erhoffe ich mir näheren Aufschluß darüber, welche Verhaltensweisen geeignet sind, hiergegen zu verstoßen. Leider wird diese neue Aufgabe nämlich nicht - entgegen der sonst vorhandenen Gesetzestechnik - näher im Gesetz beschrieben. Damit bleibt offen, über welche Gruppierungen zukünftig die Datenverarbeitung durch den Verfassungsschutz erlaubt sein soll.

## 14.2 Strategische "Rasterfahndung" des BND

Wer ins Ausland telefoniert (oder vom Ausland angerufen wird) und dabei bestimmte Worte fallen läßt, muß damit rechnen, daß das Gespräch vom Bundesnachrichtendienst (BND) aufgezeichnet, der Anschlußteilnehmer identifiziert wird und die Erkenntnisse an Strafverfolgungsbehörden weitergeleitet werden. Dies ist eine Folge der kurz vor der Bundestagswahl beschlossenen Erweiterung der Befugnisse des BND (BGBl. I 1994 S. 3186).

Das Grundrecht des Post- und Fernmeldegeheimnisses in Art. 10 des Grundgesetzes (GG) steht allen Menschen zu. Es schützt die Privatsphäre des einzelnen bei einer Kommunikation über eine räumliche Distanz, z.B. durch Brief oder Telefonat. Staatliche Eingriffe bedürfen einer gesetzlichen Grundlage. Die Eingriffsermächtigungen für die Nachrichtendienste stehen im G 10-Gesetz. Das Gesetz unterscheidet in Umsetzung der Vorgaben des Art. 10 GG zwei Fälle: Zum einen geht es um Beschränkungen gegen eine Person, die im Verdacht steht, im Gesetz genannte schwere Straftaten gegen den Bestand der Bundesrepublik Deutschland zu planen (Individualkontrolle). Zum anderen geht es um den hier interessierenden Punkt der sog. "strategischen Kontrolle". Danach dürfen zur Wahrung der äußeren Sicherheit des Staates Sachinformationen zur Lage gesammelt werden, deren Kenntnis notwendig ist, um die Gefahr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen. Die strategische Kontrolle in Form der Fernmeldeaufklärung soll im wesentlichen gegen die DDR und die CSSR während des Kalten Krieges eingesetzt worden sein.

Die Wende im Osten hat offenbar auch beim BND dazu geführt, über neue Einsatzmöglichkeiten der Abhöranlagen nachzudenken. Herausgekommen

ist in Art. 13 des Verbrechensbekämpfungsgesetzes eine Erweiterung der im G 10-Gesetz angelegten Befugnisse. Nunmehr kann der BND alle internationalen nicht leitungsgebundenen Fernmeldekontakte (über Kurzwelle, per Richtfunk, über Satellit) belauschen und aufzeichnen, die scheinbar etwas mit Terrorismus, Verbreitung von Kriegswaffen, Import von Betäubungsmitteln, internationaler Geldfälschung und internationaler Geldwäsche zu tun haben. Es ist zu erwarten, daß dabei, wie bei einer Rasterfahndung, eine unvermeidlich große Zahl Unbeteiligter in Abhörmaßnahmen mit einbezogen wird. Zudem soll der BND in der Lage sein, einzelne Personen durch eine bestimmte Wahl von erlaubten Sachsuchbegriffen gezielt zu belauschen. Die Gesetzesänderung erlaubt, die gewonnenen persönlichen Daten u.a. an die Polizei weiterzuleiten.

Die Gewerkschaft der Polizei hat warnend darauf hingewiesen, daß diese Möglichkeiten "einen Einstieg in Geheimdienstmethoden bedeuten könnten, die keinesfalls Mittel der Polizeiarbeit sein dürften". Nach Meinung aller Datenschutzbeauftragten des Bundes und der Länder droht mit der Befugniserweiterung zugunsten des BND die Trennungslinie zwischen den Nachrichtendiensten und der Polizei weiter zu verwischen. Die neuen gesetzlichen Befugnisse des BND können auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen. Unsere Forderung lautet daher, das Trennungsgebot in der Gesetzgebung und dann auch bei der Durchführung der Fernmeldeaufklärung des BND strikt zu beachten (vgl. Anlage 21). Die Zulassung der Datenauswertung durch den BND für die Strafverfolgung bringt, wie ich meine, unübersehbare Risiken für die rechtsstaatliche Transparenz und die gerichtliche Überprüfbarkeit von Strafverfahren. Ich habe die Forderung des Bundesbeauftragten für den Datenschutz unterstützt, zumindest durch eine Festschreibung seiner Kontrollbefugnisse in diesem von ihm bisher nicht überprüfbaren Bereich eine Datenschutz-Prüfinstanz vorzusehen.

Noch eine Anmerkung: Das Bundesverfassungsgericht hat in seinem Beschluß vom 20. Juni 1984 zur "strategischen Kontrolle" folgendes ausgeführt: "Mit Art. 10 GG ist es nicht vereinbar, Überwachungsmaßnahmen zur Gefahrenabwehr für die innere Sicherheit einzusetzen" (BVerfG, DÖV 85, 104 ff., 106).

## 14.3 Unglaubliche Personendossiers durch Sicherheitsüberprüfungen

Sicherheitsüberprüfungen haben entscheidenden Einfluß auf das berufliche Fortkommen. Sie können existenziell sein.

### 14.3.1 Ablauf einer Sicherheitsüberprüfung

Ist jemand für eine Tätigkeit mit besonders vertraulichen Unterlagen vorgesehen, so hat sie oder er sich einer Sicherheitsüberprüfung zu unterziehen (vgl. XI 14.4). Diese Überprüfung soll dem Verrat von als "Verschlußsa-

chen" eingestuften Geheimnissen vorbeugen. Ziel ist es festzustellen, ob der überprüften Person Verschlußsachen anvertraut werden können. Die für Sicherheitsüberprüfungen relevante Einstufung der Verschlußsachen reicht von "Vertraulich" über "Geheim" bis zu "Streng Geheim".

Das Überprüfungsverfahren beginnt bei Beschäftigten des öffentlichen Dienstes mit der Abgabe einer Sicherheitserklärung. Darin werden detaillierte und umfangreiche Angaben gefordert zur eigenen Person, zum Ehegatten / Lebenspartner und zu Familienangehörigen (Eltern, Geschwister, volljährige Kinder). Die Beschäftigten haben u.a. Angaben zu Wohnsitzen, Ausbildung, Beschäftigung, Wehr- und Zivildienstzeiten, finanzielle Situation, Vorstrafen bzw. Ermittlungs-, Straf- und Diszplinarverfahren, Beziehungen zu verfassungsfeindlichen Organisationen, Reisen in bestimmte Länder usw. zu machen. Geht es um den Umgang mit streng geheimen bzw. wichtigen geheimen Unterlagen - fachlich als Ü 3-Verfahren bezeichnet -, so sind weiter mindestens drei Referenzpersonen zu benennen und zwei Auskunftspersonen, die die Identität der oder des Beschäftigten bestätigen können. Der Sicherheitsbeauftragte der Beschäftigungsbehörde überprüft die Personaldaten. Sodann übersendet er die Sicherheitserklärung dem Niedersächsischen Landesamt für Verfassungsschutz (NLfV).

Nunmehr beginnt die im Niedersächsischen Verfassungsschutzgesetz ganz allgemein vorgesehene Mitwirkung des NLfV bei Sicherheitsüberprüfungen. Einzelheiten der Mitwirkung ergeben sich aus den "Sicherheitsrichtlinien"( vgl. XI 14.5 und 14.6). Danach bedeutet die Mitwirkung des NLfV bei Ü 3-Verfahren: Personalienabfragen bei den Datenbeständen der Verfassungsschutzbehörden einschließlich gegebenenfalls BND, MAD und der Polizei; Anfragen beim Bundeszentralregister und bei den Meldebehörden; Nachfragen bei geeigneten Stellen, in der Regel Behörden; Befragung der angegebenen Referenz- und Auskunftspersonen; Befragung anderer - nicht vom Überprüften genannten - Personen, die sachdienliche Hinweise geben können. Alle eingehenden Informationen werden in einer Sicherheitsüberprüfungsakte beim NLfV gesammelt und bewertet. Dieses gibt ein Votum ab mit dem kurzen Ergebnis: "Risiko" oder "Kein Risiko". Die Beschäftigungsbehörde entscheidet dann unter Berücksichtigung dieses Votums, ob dem Beschäftigten z.B. streng geheime / wichtige geheime Unterlagen anvertraut werden können (Erteilung der Ermächtigung).

Bestimmte Daten über die zu überprüfende Person bzw. den einbezogenen Partner werden auch im von den Verfassungsschutzbehörden des Bundes und der Länder gemeinsam genutzten elektronischen Hinweis- und Auskunftssystem NADIS gespeichert. Der Bundesinnenminister gibt die aufgrund von allen Sicherheitsüberprüfungen Ende 1993 gespeicherten Personen mit 515.530 an (vgl. Verfassungsschutzbericht des Bundes, 1993, S. 223). Davon wurden ca. 19.400 Personen von Niedersachsen "eingegeben" (vgl. Verfassungsschutzbericht Niedersachsen, 1993, S. 89).

14.3.2 Ergebnis meiner Kontrolle

Ich habe die Datenverarbeitung im Rahmen von Ü 3-Verfahren überprüft. Gegenstand meiner Kontrolle waren "Risiko-Akten" der letzten 17 Jahre und Sicherheitsüberprüfungsakten mit dem Votum "Kein Risiko". Die dienstliche Stellung der zu überprüfenden (antragstellenden) Personen ist breit gefächert. Betroffen waren sowohl Sekretärinnen als auch Chefs. Auch die Bandbreite der beabsichtigten Tätigkeit ist groß. Es ging um Tätigkeiten im Landesamt für Verfassungsschutz, bei Behörden im Verschlußsachenbereich, im Polizeidienst, bei kommunalen Selbstverwaltungskörperschaften, im Vorzimmer von Behördenleitern oder auch im Bereich der Wehrstrafgerichtsbarkeit.

Ich habe Verfahren angetroffen, die sich über mehrere Jahre hinzogen. Insgesamt waren es 44 Akten mit einem Umfang von über 5000 Seiten. In einem Fall betrug der Umfang der Akte 699 Seiten. Es wäre ein Irrtum zu glauben, bei den 44 Verfahren ginge es um die Überprüfung von - auch nur - 44 antragstellenden Personen. Die tatsächliche Zahl der überprüften Personen ist weitaus höher. Generell läßt sich sagen, daß pro Verfahren Informationen über durchschnittlich 15 Personen gesammelt wurden. Betroffen waren praktisch alle denkbaren Personenkreise: Antragsteller als zu überprüfende Person; Ehegatte / Lebenspartner / Verlobte; Referenzpersonen; selbstbenannte Auskunftspersonen; Verwandte des Antragstellers; Verwandte des einbezogenen Partners und andere Auskunftspersonen. Die Recherchen führten u.a. dazu, daß ein mit Fotos versehener Bericht des "Stern" aus Sicht des Verfassungsschutzes Anlaß gab, den verantwortlichen Redakteur und alle für diese Ausgabe arbeitenden Fotografen in der Akte festzuhalten.

Ich habe bei den durchgeführten Sicherheitsüberprüfungen eine im Vergleich zu anderen Kontrollen große Anzahl von datenschutzrechtlichen Mängeln festgestellt. Im einzelnen:

- Die Überprüfungen waren nicht erforderlich.
  Nach meiner Überzeugung war das durchgeführte Verfahren in fünf Fällen nicht erforderlich. Die beabsichtigte Tätigkeit nötigte zum Teil nicht zu der vorgenommenen umfassenden Überprüfung oder es war z.B. schon nach den Vorangaben klar, daß der Person keine sicherheitsempfindlichen Unterlagen anvertraut werden konnten. So sind überflüssige Datensammlungen entstanden.

- Unnötige Datensammlungen durch gesprächige Referenz- bzw. Auskunftspersonen mit Folgen:
  Die Aussagen von Referenz- und Auskunftspersonen über die zu überprüfende Person bzw. den einbezogenen Partner stellen sich als eine wahre Fundgrube an Informationen über z.B. Vereinstätigkeiten, Hobbys, Krankheiten, Rauchgewohnheiten, Kleidungsverhalten, angeblicher Verschwendungssucht, Kindererziehung und Wirkung auf das andere Geschlecht dar. Einen Bezug zur "staatsbürgerlichen Zuverlässigkeit" vermochte ich bei solchen Angaben nur selten zu erkennen. Banale bis

brisante Aussagen über die zu überprüfende Person / den einbezogenen Partner ergeben zwar ein angebliches Persönlichkeitsprofil; mit der zu fordernden Zielrichtung haben die für speicherungswürdig befundenen Angaben aber nichts zu tun. Eine Auswahl:

... "Als besonderes Hobby sei noch erwähnt, daß er früher ein 'Karl-May-Leser' war."
... "Sie raucht stark (sogar Tiparillos)."
... "Er ist ein grundsolider, fast langweiliger Mensch, eben der Prototyp eines Beamten."
... "Hat für den Verein eine Fahrt ausgearbeitet und auch abgerechnet. Dabei hat er sogar Pfennigbeträge wieder zurückgezahlt ('Das ist bei den Vereinsmitgliedern allerdings nicht gut angekommen')."
... "Versagte während der Ausbildung bei einem Vortrag vor der Klasse. Hat zwei Kinder, davon eine unerwünschte Tochter."
... "Körperlich etwas anfällig mit leichtem Hang zur Wehleidigkeit. Die jüngere Tochter ist unehelich geboren. Der Vater ist ein Taugenichts. Kleidet sich zwar kontrastreich und manchmal zu jung, kauft aber stets preiswerte Kleidung. Leidet vor allem in den Frühjahrsmonaten an Kopfschmerzen und Furunkeln an Kopf und Rücken. Das liegt wohl an dem zu dicken Blut."
... "Vielleicht hat er auch anbandeln wollen und hat eine Abfuhr erlitten."
Sieht relativ gut aus und kam bei den Frauen gut an. Im übrigen kleidet er sich modisch. Dabei trug er die Kleidung oft sehr eng, damit sein männlicher Körperbau zur Geltung kommen konnte."
... Zur Ehefrau: "Sie liebt das Extravagante, hat besondere Ansprüche und gibt das Geld mit beiden Händen aus - so hat sie eine Lederhose für z.B. 600 DM."

Diese Aussagen bzw. Vermutungen haben für die überprüften Beschäftigten Folgen. Sie fließen in Bewertungen zur Frage der "staatsbürgerlichen Zuverlässigkeit" ein. So kommt es, daß Zweifel an der geforderten Zuverlässigkeit - verstanden als außerhalb der Norm liegendes Verhalten - u.a. begründet wurden mit "pflegt lockere Zweitbeziehungen" oder "fährt ein Kabriolett und hat das ganze Jahr hindurch eine überdurchschnittlich braune Gesichtsfarbe (Sonnenbräune) - vermutlich möbelt der Beschäftigte sein Äußeres gezielt durch Besuch eines Sonnenstudios oder Solariums auf." Bisweilen genügte aber auch schon der Grund: "hat die Sicherheitserklärung nicht ganz vollständig ausgefüllt". Ich teile nach alledem die Auffassung eines anderen Landesbeauftragten für den Datenschutz, nach der kaum eine andere Stelle bekannt ist, bei der über einen so langen Zeitraum so systematisch aus so breit gefächerten Quellen persönliche Daten zusammengetragen und gespeichert werden, nach meinen Feststellungen sogar über das sexuelle Verhalten.

- Zu weitgehende Ablichtungen aus fremden Akten:
Die Anforderung von Personalakten, polizeilichen Akten, Akten der Staatsanwaltschaft und Gerichtsakten ist nach meinen Feststellungen eine häufig benutzte Form der Informationsbeschaffung. Anschließend

werden umfängliche Ablichtungen gefertigt, die u.a. dazu führen, daß viel mehr an Informationen festgehalten wird, als aufgabenbezogen erforderlich ist. Speicherungswürdig war z.B. dieTatsache der Mitgliedschaft in der Deutschen Angestelltengewerkschaft (DAG). In einem Fall wurden über 100 Blatt Kopien aus der Personalakte (u.a. mit Zeugnissen der letzten 30 Jahre) und einer Polizeiakte gefertigt. In einem anderen Fall wurde fast die komplette Personalakte mit 50 Blatt abgelichtet. Die Kopien betrafen z.B. eine Unfallanzeige wegen eines Blutergusses durch ein Ausrutschen beim Betreten des Dienstgebäudes.

- Überprüfung von Personen, die nicht überprüft werden durften:
  Entgegen den Vorgaben wurden Ehegatten / Lebenspartner / Verlobte (auch Verstorbene, Geschiedene bzw. Ex-Partner) selbst überprüft, ebenso Verwandte der zu überprüfenden Person. Die Überprüfung durch den Verfassungsschutz erfaßte auch verstorbene Elternteile (ein Vater war z.B. seit dem Krieg vermißt), minderjährige Kinder und ging bis zu Verwandten vierten Grades (Vettern / Kusinen). Betroffen waren auch Verwandte des Partners.

  Ebenso wurden Referenz- und Auskunftspersonen nicht nur befragt, sondern selbst durch den Verfassungsschutz "abgeklärt". Zu derart überprüften Referenzpersonen zählten u.a. ein Bundestagsabgeordneter, Landtagsabgeordnete und ein Minister.

- Kein rechtliches Gehör für die überprüften Antragsteller / einbezogenen Partner:
  Ergebnis meiner Kontrolle war, daß der betroffene Antragsteller in vielen Fällen entgegen den Vorgaben keine Möglichkeit erhielt, zu aufgekommenen sicherheitsrelevanten Umständen Stellung zu nehmen. Selbst wenn Eigenbefragungen durchgeführt wurden, erfolgten sie ganz überwiegend erst am Ende der Recherchen. Nach meinem Eindruck wurde häufig kriminalistisch vorgegangen: Der "Täter" wird eingekreist und dann gestellt. Aus Sicht des Datenschutzes wären frühzeitige Eigenbefragungen als Datenerhebung beim Betroffenen vorzuziehen. Weitere Informationsbeschaffungen ohne Kenntnis des Betroffenen und Datenübermittlungen an Dritte könnten in erheblichem Umfang vermieden werden. Zudem führen die Gesamtrecherchen einschließlich der umfänglichen Aussagen der Referenz- und Auskunftspersonen zu einer Informationssammlung über die überprüften Personen, die sie nicht mehr korrigieren können. Die Betroffenen haben derzeit keinen Anspruch auf Akteneinsicht. Selbst vor Gericht ist es den Betroffenen nicht möglich zu erfahren, was in der Akte steht und was gegebenenfalls gegen sie verwendet wurde (vgl. XI 14.4 am Ende).

- Unzulässige Datenweitergaben:
  Nach meinen Feststellungen wurden persönliche Daten dann, wenn es erlaubt war, nur in ganz wenigen Fällen und ausschließlich für Zwecke der Spionageabwehr weitergegeben. Hingegen wurden Daten, wenn es nicht erlaubt war, in vielen Fällen etwa an personalbewirtschaftende Stellen und Vorgesetzte der überprüften Person übermittelt.

- Unzulässige Aufbewahrung von Sicherheitsüberprüfungsakten:
  Ergebnis der Kontrolle war, daß nach meiner Auffassung viele der überprüften Akten aus unterschiedlichen Gründen schon längst hätten vernichtet und die entsprechenden Dateieneinträge gelöscht sein müssen.

14.3.3 Folgerungen für das geplante Sicherheitsüberprüfungsgesetz des Landes

Übereinstimmung besteht mit dem Niedersächsischen Innenministerium zur Notwendigkeit gesetzlicher Regelungen. Nach den Ankündigungen dürfte ein niedersächsisches Gesetz über Sicherheitsüberprüfungen in Kürze auf den Weg gebracht werden. Ich gehe davon aus, daß meine Kontrollergebnisse Eingang in die Überlegungen zur Formulierung der geplanten Vorschriften finden. Hierzu zählt auch die Erfahrung, daß bei ähnlichen Vorgaben sehr unterschiedliche Handhabungen möglich sind. So war bei den "jüngeren" Überprüfungsverfahren eine Tendenz zu erkennen, in Frage kommende Datenverarbeitungsschritte unter dem Gesichtspunkt der Verhältnismäßigkeit intensiver zu bedenken. Dies spricht dafür, die Steuerungsmöglichkeiten durch normenklare Vorschriften auszuschöpfen.

Auf der Grundlage meiner Kontrolle empfehle ich:
- die von Sicherheitsüberprüfungen erfaßten Personenkreise auf das Unerläßliche zu begrenzen,
- die tätigkeitsbezogene Notwendigkeit der Sicherheitsüberprüfung nachvollziehbar zu dokumentieren,
- die erlaubten Überprüfungsmaßnahmen normenklar festzulegen,
- erforderliche Einsichtnahmen in die Personalakte dem bei der Beschäftigungsbehörde tätigen Sicherheitsbeauftragten zuzuordnen,
- durch Vorgaben sicherzustellen, daß verwendete Befragungsberichte sich auf das sachlich notwendige Minimum beschränken,
- bei der Informationsbeschaffung von fremden Stellen vorrangig Auskunftsersuchen des Landesamtes vorzusehen und die Aktenanforderung als
  ultima ratio auszugestalten,
- ein wirksames rechtliches Gehör für die Betroffenen zu verankern. Dazu gehört eine frühzeitige Gelegenheit zur Stellungnahme und die Möglichkeit zur Auskunft und Einsichtnahme in Akten,
- Datenweitergaben nur für Spionageabwehrzwecke zuzulassen und
- präzise Vorgaben für die Aufbewahrungsdauer von Sicherheitsüberprüfungsakten bzw. Dateieinträge.

14.3.4 Was ist geheim?

Betrachtungen über Sicherheitsüberprüfungen bzw. ein entsprechendes Gesetz allein bleiben verengt und unvollständig, wenn nicht ein Blick auf den "Auslöser" geworfen wird. Sicherheitsüberprüfungen sind kein Naturereignis. Sie sind Folge der Einstufung von Unterlagen als "geheim". Die Entscheidung darüber, ob ein Schriftstück klassifiziert wird, liegt bei der her-

ausgebenden Stelle, also bei den jeweils damit Beschäftigten. Diese müssen sich bei ihrer Einstufung an äußerst allgemein gehaltene verwaltungsinterne Vorgaben (Verschlußsachenanweisung) orientieren. Ein Rückgriff auf etwas Griffiges, wie z.B. eine Definition des Staatsgeheimnisses im Sinne des Strafgesetzbuches, erfolgt nicht. Dieses "Vorfeld" wäre es wert, näher aufgehellt zu werden. Ein Mitglied der Regierungskoalition in Bonn forderte bei der Verabschiedung des Sicherheitsüberprüfungsgesetzes des Bundes zu mehr Gelassenheit auf. Ich unterstütze diese Sichtweise. Sie macht auf den Punkt aufmerksam, daß eine Neigung bestehen könnte, auch eher unbedeutende Vorgänge mit dem "Geheim"-Stempel zu versehen. Die von Hans Magnus Enzensberger nachfolgend beschriebene Behördenmentalität darf nicht Kennzeichnung der Verwaltung in einem Rechtsstaat sein: "Vor allem aber ist geheim, was ein Geheimnis ist und was nicht; dies ist vielleicht das eigentliche Staatsgeheimnis."

## 14.4 Die Stasi, ein stellvertretender Ministerpräsident und die Weiterungen

Der niedersächsische Verfassungsschutz hat Daten über den zum damaligen Zeitpunkt stellvertretenden Ministerpräsidenten des Landes Sachsen Anhalt gespeichert und weitergegeben (vgl. XI 14.2). Seitens des Verfassungsschutzes wurde zur Begründung der Datenverarbeitung auf die Notwendigkeit der Aufklärung von Strukturen des früheren Ministeriums für Staatssicherheit der DDR (MfS) hingewiesen (Spionageabwehr). Nun mag man der einleuchtenden Meinung sein, daß eine Aufbereitung von Strukturen des MfS bei einem parlamentarischen Untersuchungsausschuß, der Gauck-Behörde oder gegebenenfalls bei einem Staatsanwalt besser angesiedelt ist. Datenschutzrechtlich hatte ich zu entscheiden, ob die Datenverarbeitung bei der niedersächsischen Verfassungsschutzbehörde aufgabenbezogen und zeitlich gesehen erforderlich war oder nicht. Und ich stellte fest, daß die Datenspeicherung und -weitergabe zumindest ab einem bestimmten - sehr frühen - Zeitpunkt rechtswidrig war. Meine Auffassung stütze ich im wesentlichen auf Aussagen des Bundes. Das Niedersächsische Innenministerium geht dagegen nach wie vor von der Zulässigkeit der damaligen Informationsverarbeitung aus.

Zwischenzeitlich wurden die beim Niedersächsischen Landesamt für Verfassungsschutz (NLfV) vorliegenden Unterlagen allesamt vernichtet. Dies schließt nicht aus, daß bei anderen Verfassungsschutzämtern wegen der Zusammenarbeit bei der "Aufbereitung der DDR-Vergangenheit" noch entsprechende Informationen vorliegen. Ich habe insoweit meine Kollegen unterrichtet.

Der Vorgang hatte noch zwei weitere Aspekte. Zum einen war mir eine Aufklärung eines Teilsachverhalts erst nach einem Jahr möglich. Ursache hierfür waren Darstellungen, die aufgrund meiner Nachfragen mehrmals "präzisiert" werden mußten. Dies ist im Rahmen der Zusammenarbeit mit anderen Behörden ungewöhnlich. Zum anderen ließ das NLfV erkennen, daß es das Verhalten von Personen mit (behauptetem) MfS-Bezug generell als verfassungsschutzrelevant bewerte. Mit anderen Worten: Dieser Vorgang war

wohl kein Einzelfall. Ich sah mich aufgrund dieser Einschätzung veranlaßt, die Rechtmäßigkeit der Datenverarbeitung über weitere in Frage kommende Personen zu überprüfen. Meine Anfrage nach betroffenen Personen wurde erst auf "Nachfassen" beantwortet. Danach steht fest, daß anfallende Informationen immer weitergeleitet wurden. Näheres zum möglichen Betroffenenkreis konnte aber nicht mehr mitgeteilt werden, da Unterlagen beim NLfV zum Zeitpunkt der Antwort vernichtet und damit nicht mehr vorhanden waren.

## 14.5 NADIS-Richtlinien

Im Berichtszeitraum sind die Richtlinien für das von den Verfassungsschutzbehörden des Bundes und der Länder betriebene nachrichtendienstliche Informationssystem NADIS neu gefaßt worden. Die Datenschutzbeauftragten sind an dem Verfahren erst beteiligt worden, nachdem die Leiter der Verfassungsschutzbehörden den Entwurfstext bereits abgesegnet hatten. Dieser Entwurf widersprach eindeutig den gesetzlichen Vorgaben. Die Rechtsgrundlage für NADIS findet sich in § 6 Abs. 2 des Bundesverfassungsschutzgesetzes. NADIS darf danach nur die Daten enthalten, die zum Auffinden der Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Das System darf demnach nur als reines Aktenhinweissystem geführt werden. Nach herkömmlichem Verständnis reicht für diesen Zweck die Speicherung von Namen, Geburtsdaten und Anschriften von Betroffenen sowie des Aktenzeichens aus. Der Richtlinienentwurf ging über diese gesetzliche Vorgabe weit hinaus. NADIS hätte damit eine neue Zweckbestimmung erhalten, die im Gesetz nicht vorgesehen ist. Die Datenschutzbeauftragten des Bundes und der Länder haben sich in einer Entschließung gegen den Richtlinienentwurf gewandt (vgl. Anlage 16).

Die Richtlinien sind nunmehr verändert in Kraft getreten. NADIS wird jetzt als Datensammlung bezeichnet, in der nur die zum Auffinden von Akten und der dazu notwendigen Identifizierung einer Person, Organisation und eines Sachverhalts erforderlichen Daten enthalten sind. Ob diese Formulierung einen weitergehenden Datenkatalog zubilligt als das Gesetz erlaubt, wird die Praxis zeigen.

## 14.6 Zusammenarbeit mit dem polizeilichen Staatsschutz im Extremismusbereich

Gegenstand einer Überprüfung beim NLfV war dessen Umgang mit persönlichen Daten, die bei der polizeilichen Arbeit im Staatsschutzbereich erhoben wurden. Bei meiner Prüfung ging es nun aber nicht um Personen, die Tatverdächtige waren, sondern um solche aus dem Umfeld von Tatverdächtigen (Kontakt- und Begleitpersonen). Für die Polizei besteht nach dem Niedersächsischen Verfassungsschutzgesetz die Verpflichtung, personenbezogene Daten aus dem Bereich Extremismus dann an das Landesamt weiterzugeben, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß die Übermittlung für die Aufgabenerfüllung des NLfV erforderlich ist.

Meine Kontrolle ergab, daß die gesetzlichen Vorgaben für die Datenverarbeitung eingehalten wurden. Da aus meiner Sicht die Möglichkeit bestand, auch das interne Verfahren datenschutzfreundlicher zu gestalten, hatte ich hierzu einige Empfehlungen ausgesprochen. Das NLfV hat daraufhin in einem nicht unwichtigen Punkt das interne Bearbeitungsverfahren geändert.

### 14.7 Auskunftsanspruch für Betroffene

Seit dem Inkrafttreten des Niedersächsischen Verfassungsschutzgesetzes am 21. November 1992 haben Betroffene gegenüber dem NLfV einen Anspruch auf unentgeltliche Auskunft über die zu ihrer Person gespeicherten Daten. Die Betroffenen brauchen ihren Antrag nicht besonders begründen. Das Landesamt hat allerdings die Möglichkeit, die Auskunft unter den im Gesetz genannten Voraussetzungen zu versagen. Aus datenschutzrechtlicher Sicht ist zu bedauern, daß die Möglichkeiten, ein Auskunftsverlangen abzulehnen, in einer sehr umfassenden Weise formuliert worden sind.

Gegen die gesetzliche Regelung wurden in politischen Kreisen erhebliche Bedenken laut: Der Verfassungsschutz werde zu einer Auskunftei degradiert. Die ersten Erfahrungen mit der neuen Vorschrift zeigen, daß diese Gefahr in keiner Phase bestand. Bis Ende 1993 wurden beim NLfV insgesamt 41 Auskunftsersuchen gestellt. Drei Antragstellern wurden die beim Landesamt vorhandenen Erkenntnisse mitgeteilt. In den übrigen Fällen hatte das Landesamt keine Daten gespeichert. Es war in diesem Zeitraum nicht erforderlich, ein Auskunftsersuchen abzulehnen.

Die Praxis zeigt, daß die Einführung üblicher datenschutzrechtlicher Standards auch bei der Verfassungsschutzbehörde nicht zu einer Beeinträchtigung der Aufgabenerfüllung führt.

### 14.8 Zuverlässigkeitsüberprüfung von Flughafenpersonal

Unter XI 14.7 habe ich zum Entwurf einer Verordnung über die Zuverlässigkeitsüberprüfung von Flughafenpersonal Stellung bezogen. Das Bundesverkehrsministerium hat in der Folgezeit weitere inhaltliche Änderungen vorgenommen, die z.T. auch datenschutzrechtliche Verbesserungen gebracht haben. Bei Zweifeln an der Zuverlässigkeit sollen die Betroffenen nunmehr einen rechtskräftigen Bescheid von der Behörde erhalten, während sie nach dem Vorentwurf nur von dem Unternehmen und lediglich über das Ergebnis der Prüfung zu informieren waren.

Die Verordnung war nach meinem Kenntnisstand bei Redaktionsschluß noch nicht in Kraft getreten. Ursache hierfür ist wohl die Initiative eines Bundeslandes mit der Zielrichtung, in der Verordnung eine Regelung aufzunehmen, nach der bei allen Bewerbenden aus einem neuen Bundesland eine Regelabfrage beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes (BStU) erfolgen soll. Nach der Rechtsauffassung des Bundesjustizministeriums wäre dafür allerdings eine gesetzliche Regelung zu for-

dern, die bereits im Rahmen des Gesetzes zur Neuordnung des Eisenbahnwesens aus politischen Gründen gescheitert ist. Im neuesten Entwurf der Zuverlässigkeitsverordnung ist zwar eine Rechtsgrundlage für die Anfrage beim BStU vorgesehen. Es soll allerdings deutlich zum Ausdruck gebracht werden, daß die Erforderlichkeit des Auskunftsersuchens an den BStU im Einzelfall geprüft werden muß und damit eine Regelanfrage nicht erfolgen darf.

Das Niedersächsische Ministerium für Wirtschaft, Technologie und Verkehr hatte mich gefragt, ob ich datenschutzrechtliche Bedenken hätte, wenn von den Bewerbenden aus einem neuen Bundesland stets die Vorlage einer Selbstauskunft über beim BStU vorhandene Unterlagen gefordert würde. Hierzu ist anzumerken, daß die Vorschriften über die Nutzung der Stasi-Unterlagen durch öffentliche und nichtöffentliche Stellen im Stasi-Unterlagengesetz die Verwertung im Rahmen der Zuverlässigkeitsüberprüfung nach dem Luftverkehrsgesetz nicht vorsehen. Nur bei Personen in leitender Funktion kommt die Verwendung der Unterlagen im gesetzlich vorgegebenen Rahmen in Betracht. Bei der überwiegenden Mehrzahl der Bediensteten auf einem Flughafen können die Unterlagen nicht herangezogen werden. Die Bewerberinnen und Bewerber zur Einholung und Vorlage einer Selbstauskunft beim BStU zu verpflichten, wäre eine Umgehung der gesetzlichen Beschränkungen. Die gesetzgeberische Absicht, Stasi-Unterlagen nur für herausgehobene Funktionen im nichtöffentlichen Bereich zu nutzen, würde unzulässigerweise unterlaufen. Das Ministerium hat daraufhin von der in Aussicht genommenen Verfahrensweise abgesehen.

## 15. Personalwesen

### 15.1 Datenschutz geht nicht nur Männer an: Personalakteneinsicht durch Frauenbeauftragte

Im Berichtszeitraum sind das Zehnte Gesetz zur Änderung der Niedersächsischen Gemeindeordnung und der Niedersächsischen Landkreisordnung vom 14. Juni 1993 (Nds. GVBl. S. 137) sowie das Niedersächsische Landesgleichberechtigungsgesetz (NLGG) vom 15. Juni 1994 (Nds. GVBl. S. 246) in Kraft getreten. Aus datenschutzrechtlicher Sicht war bei diesen Gesetzesvorhaben insbesondere von Interesse, unter welchen Voraussetzungen es Frauenbeauftragten ermöglicht werden sollte, in Personalunterlagen Einsicht zu nehmen.

Ich habe dazu die Auffassung vertreten (vgl. XI 15.2), daß die Frauenbeauftragten zwar das Recht haben sollten, Bewerbungsunterlagen einzusehen, daß die Einsichtnahme in Personalakten aber von der Zustimmung der Betroffenen abhängig gemacht werden sollte. Eine Einsicht in Bewerbungsunterlagen ist gerechtfertigt, weil die Frauenbeauftragte am Bewerbungsverfahren teilnimmt; zu ihrer Meinungsbildung muß sie deshalb über die notwendigen Informationen verfügen können. Eine Einsicht in Personalakten

auch gegen den Willen der Bediensteten wird der Schutzbedürftigkeit dieser Vorgänge jedoch nicht gerecht. Aus diesem Grund hat der Gesetzgeber dem Personalrat, der auch u.a. darüber zu wachen hat, daß jede unterschiedliche Behandlung von Beschäftigten wegen ihres Geschlechts unterbleibt, ein von ihrem Willen unabhängiges Akteneinsichtsrecht verwehrt.

Zwar ist das Niedersächsische Frauenministerium meinen Argumenten bei der Regelung der Rechtstellung der kommunalen Frauenbeauftragten noch ohne weiteres gefolgt. Im später vorgelegten Gesetzentwurf zum Niedersächsischen Gleichberechtigungsgesetz hat das Ministerium jedoch aus unerfindlichen, mir gegenüber nie dargelegten Gründen nachdrücklich darauf bestanden, daß die Frauenbeauftragten in der Landesverwaltung - anders als ihre kommunalen Kolleginnen - auch gegen den Willen der Bediensteten Einsicht in deren Personalakten nehmen dürften. Die Erörterung des Gesetzentwurfs in den zuständigen Landtagsausschüssen hat jedoch schließlich dazu geführt, daß in § 20 NLGG im Interesse des Persönlichkeitsrechts der Beschäftigten und einer gleichartigen Ausgestaltung der Rechte der kommunalen und der staatlichen Frauenbeauftragten die Einwilligung der Betroffenen für die Personalakteneinsicht gefordert wird.

In diesem Zusammenhang wurde mir im Rahmen einer Eingabe vorgetragen, daß bei einem Stellenbesetzungsverfahren eines kommunalen Regionalverbandes die Frauenbeauftragte einer der beteiligten Städte auf Initiative der Frauenbeauftragten der übrigen kommunalen Mitglieder des Verbandes beteiligt und ihr Einsicht in Bewerbungsunterlagen gegeben wurde. Eine solche Verfahrensweise ist nicht zulässig. Aus dem Kommunalverfassungsrecht ergibt sich keine Befugnis einer Frauenbeauftragten zur Einsichtnahme in Unterlagen eines anderen Rechtsträgers. Dies gilt auch dann, wenn die Kommune, bei der die Frauenbeauftragte bestellt ist, an dem Rechtsträger beteiligt ist. Vielmehr kann auf der Grundlage der §§ 5a Abs. 6 NGO und 4a Abs. 6 NLO eine Einschaltung der Frauenbeauftragten nur insoweit in Betracht kommen, als Gleichstellungsfragen der jeweiligen Kommune selbst in Rede stehen.

## 15.2 Informationsrechte des Personalrates

Nach dem Niedersächsischen Personalvertretungsgesetz sind dem Personalrat zur Durchführung seiner Aufgaben alle erforderlichen Daten vorzulegen. Mit dem im konkreten Fall zuständigen Niedersächsischen Kultusministerium bin ich insoweit überein gekommen, daß es rechtlich unbedenklich ist, dem Personalrat (einer Schule) zur Wahrnehmung seiner allgemeinen Aufgaben eine Liste aller Teilzeitkräfte der Dienststelle (ohne spezifische Angaben) zur Verfügung zu stellen. Nach der Rechtsprechung des Bundesverwaltungsgerichts, die ein allumfassendes Informationsrecht des Personalrates zur allgemeinen Kontrolle der Dienststelle verneint, halte ich es jedoch für unzulässig, eine Liste aller Teilzeitbeschäftigten mit Angabe der jeweiligen Stundenzahl und darüber hinaus der angefallenen Plus- und Minusstunden jeder Lehrkraft vorzulegen. Anders zu beurteilen wäre dagegen der Fall, daß sich ein Personalrat in einer Einzelangelegenheit eines Teilzeitbe-

schäftigten mit der Dienststelle auseinandersetzt. In einem solchen Fall dürfen selbstverständlich im Rahmen der Erforderlichkeit die notwendigen Angaben zur betroffenen Teilzeitkraft gemacht werden.

Im Zusammenhang mit dem Informationsrecht des Personalrates ist aber auch auf die Verschwiegenheitspflicht der Mitglieder (§ 9 Nds. PersVG) sowie auf dessen Pflichten bei der Behandlung personenbezogener Unterlagen nach dem neuen Personalvertretungsrecht (§ 61 Nds. PersVG) hinzuweisen:

- Unterlagen mit personenbezogenen Daten, die ihm aus Anlaß seiner Beteiligung an einer bestimmten Maßnahme zur Verfügung gestellt wurden, sind nach Abschluß des Beteiligungsverfahrens (einschließlich eventuell gefertigter Kopien) der Dienststelle zurückzugeben.
- Andere personenbezogene Unterlagen des Personalrates, insbesondere Niederschriften und Personallisten, sind zwar für die Dauer seiner regelmäßigen Amtszeit aufzubewahren, jedoch spätestens nach Ablauf einer weiteren regelmäßigen Amtszeit zu vernichten.

## 15.3 Kontrollrechte der Dienststelle gegenüber dem Personalrat

Eine Kommune hat die Frage aufgeworfen, welche Kontrollbefugnisse ein behördeninterner Datenschutzbeauftragter gegenüber dem Personalrat besitzt. Der Datenschutzbeauftragte wollte in Personalratsvorgänge Einsicht nehmen und dabei zur Überprüfung der Einhaltung datenschutzrechtlicher Bestimmungen auch stichprobenweise Niederschriften über Personalratssitzungen einsehen.

Dies ist nicht zulässig. Im Sinne des Datenschutzrechts ist der Personalrat keine eigenständige öffentliche Stelle; vielmehr ist er als Teil einer Behörde und damit nicht als außenstehender Dritter (vgl. § 3 Abs. 4 NDSG) anzusehen. Es gehört zu den Aufgaben der Dienststelle, sicherzustellen, daß die Grundsätze des Datenschutzes und der Datensicherung vom Personalrat eingehalten werden. Die Dienststelle hat deshalb dafür zu sorgen, daß z.B. die Räumlichkeiten des Personalrats angemessen gesichert sind und daß vom Personalrat ggf. genutzte ADV-Anlagen den datenschutzrechtlichen Anforderungen für die Verarbeitung von Personaldaten entsprechen. Insgesamt hat die Dienststelle die Voraussetzungen dafür zu schaffen, daß der Personalrat die Einhaltung der Datensicherheit innerhalb der eigenen Räumlichkeiten gewährleisten kann. Im Hinblick auf die besondere Stellung des Personalrats ist die Kontrollbefugnis der Dienststelle allerdings eingeschränkt. Da die Personalvertretung an Aufträge und Weisungen nicht gebunden ist, darf ihre gesetzlich gesicherte Unabhängigkeit nicht beeinträchtigt werden. Eine Einsicht in die Niederschriften des Personalrats, die zur Prüfung eines datenschutzgerechten Vorgehens ohnehin kaum geeignet sein dürfte, wäre mit der eigenständigen Aufgabenerledigung der Personalvertretung nicht vereinbar. Aus demselben Grunde kommt auch eine Akteneinsicht in sonstige Personalratsvorgänge nicht in Betracht.

Soweit ein Personalrat personenbezogene Daten in einer Datei verarbeitet, ist eine Dateibeschreibung (§ 8 Abs. 1 NDSG) zu erstellen. Aufgrund der darin enthaltenen Angaben läßt sich jedenfalls zum Teil abschätzen, ob der Personalrat personenbezogene Daten in rechtmäßiger Weise verarbeitet. Auch außerhalb einer dateimäßigen Datenverarbeitung dürfte es nicht ausgeschlossen sein, vom Personalrat z.B. Angaben über die Art und Dauer der gespeicherten Daten zu verlangen. Des weiteren ist eine Kontrolle technisch-organisatorischer Maßnahmen (§ 7 NDSG) zur Sicherstellung des Datenschutzes im Personalrat möglich. Auch diese darf allerdings nur so weit ausgeübt werden, wie dies mit der eigenständigen Aufgabenstellung des Personalrats vereinbar ist.

15.4 Überprüfungen von Personal(neben)akten

Nachdem § 24 NDSG und insbesondere die Verwaltungsvorschriften zum NBG Regelungen zu einem in datenschutzrechtlicher Hinsicht sachgerechten Umgang mit Personalakten getroffen haben, bin ich dabei, mir einen Überblick über die praktische Handhabung der Bestimmungen zu verschaffen.

Zunächst habe ich die Aktenführung - es handelte sich im wesentlichen um Personalnebenakten - in einem Finanzamt und in einer Realschule überprüft. Dabei hat sich erneut die Einschätzung bestätigt, daß in der Vergangenheit bei der Anlage von Personalvorgängen häufig in einer Weise vorgegangen wurde, die mit dem heutigen Datenschutzverständnis nicht zu vereinbaren ist. Bei den Prüfungen habe ich mein Augenmerk jedoch auf die derzeitige Verfahrensweise gerichtet. Hier konnte ich bei beiden Prüfungen erfreulicherweise feststellen, daß die Aktenführung - bis auf wenige geringfügige Mängel - den geltenden Bestimmungen entsprach. Aus den mir vorgetragenen Einzelfällen habe ich dagegen nicht ein gleicherweise positives Bild gewinnen können. Sie deuten vielmehr darauf hin, daß bei der Umsetzung der einschlägigen Rechts- und Verwaltungsvorschriften durchaus noch Defizite bestehen. Ich werde deshalb meine Prüfungen in diesem Bereich künftig verstärken.

15.5 Verwaltungsvorschriften über die Führung von Personalakten in der Steuerverwaltung

Nur zufällig wurde mir bekannt, daß das Niedersächsische Finanzministerium die Richtlinien über die Führung von Personalakten in der Steuerverwaltung neu gefaßt hat. Bei der Erarbeitung dieser Richtlinien wurde ich nicht beteiligt, obwohl auf der Hand liegt, daß die Verwaltungsvorschriften datenschutzrechtliche Belange berühren.

Seit Jahren habe ich immer wieder auf die Notwendigkeit hingewiesen, mir bei der Vorbereitung allgemeiner Regelungen (Gesetze, Verordnungen, Runderlasse), die den Umgang mit personenbezogenen Daten betreffen, Gelegenheit zur Stellungnahme zu geben. Das Niedersächsische Innenministerium hat - nach Abstimmung mit den übrigen Ressorts - mit Ministerschreiben

vom 24. April 1986 - 51.2-01480 - diese Beteiligungspflicht hervorgehoben. In einer Vielzahl von Tätigkeitsberichten habe ich selbst diese Notwendigkeit angesprochen (z.B. VIII 3.2, IX 3.3, X 3.3, XI. 3.3). Schließlich habe ich mit meinem an die Staatssekretärinnen und Staatssekretäre der Ressorts gerichteten Schreiben vom 1. Juli 1992 nochmals gebeten, dafür Sorge zu tragen, daß diese Beteiligung auch erfolgt. Auch die zwischenzeitlich erlassenen Verwaltungsvorschriften Nr. 17.1 zu § 22 NDSG sehen meine Beteiligung bei entsprechenden Regelungen vor. Angesichts dieser vielfältigen Hinweise ist es unverständlich, daß meine Beteiligung im vorliegenden Falle unterblieben ist.

Die Richtlinien halte ich in folgenden Punkten für änderungsbedürftig:

Nach Abschn. III Nr. 1 "bilden" die Personalakten der Bediensteten, für die die personalrechtlichen Befugnisse bei der Oberfinanzdirektion liegen, und die Personalakten der Bediensteten, die bei den Finanzämtern geführt werden, die "Personalhauptakten". Den Begriff "Personalhauptakten" kennt das geltende Beamtenrecht seit längerem nicht mehr. Nach § 56 Abs. 2 BRRG kann die Personalakte in Grundakte und Teilakten gegliedert werden (ebenso die VV zum NBG, Nds. MBl. 1993 S. 93, Nr. 4.1 zu § 101). Die angesprochenen Personalakten der Oberfinanzdirektion bzw. der Finanzämter sind somit Grundakten. An dieser Rechtslage müssen sich auch die Richtlinien der Steuerverwaltung orientieren.

Gemäß Abschn. VIII sind die bei den Finanzämtern vorhandenen Personalnebenakten der Beamtinnen und Beamten nach Beendigung des Dienstverhältnisses mit den Hauptakten bei der Oberfinanzdirektion zu verbinden und dort aufzubewahren. Die Personalakten (Grund- und Nebenakten) der Angestellten und Lohnempfänger verbleiben bei der letzten zuständigen Dienststelle.

Diese Regelung steht im Widerspruch zu Nr. 9.4 der VV zu § 101 NBG, wonach Nebenakten zu vernichten sind, sobald sie nicht mehr benötigt werden. Dies ist nach den VV spätestens mit dem Ausscheiden aus dem Dienst der Fall. Diese Regelung gilt gemäß dem Gem. RdErl. des Finanzministeriums vom 2. Dezember 1992 (Nds. MBl. S. 119) auch für Angestellte und Lohnempfänger.

Ich sehe keinen Grund, von diesen Bestimmungen für den Bereich der Steuerverwaltung abzuweichen. Die Nebenakte enthält grundsätzlich nur Unterlagen, die auch in der Grundakte enthalten sind. Deshalb ist eine Aufbewahrung der Nebenakte nach Ausscheiden eines Bediensteten nicht mehr erforderlich.

## 15.6 Beihilfe für getrennt lebende Angehörige - pragmatische Lösung gesucht

Bei volljährigen Kindern und Ehegatten, die vom beihilfeberechtigten Ehepartner getrennt leben, stößt es auf Unverständnis, wenn sie die Inanspruchnahme ärztlicher Leistungen dem Beihilfeberechtigten offenbaren

müssen, weil sie eine Kostenerstattung nur im Rahmen eines vom Beihilfeberechtigten gestellten Beihilfeantrages erlangen können. Die datenschutzrechtlich überzeugendste Lösung dieses Problems würde darin bestehen, wenn die volljährigen Angehörigen eines Beihilfeberechtigten - wie von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1991 gefordert (vgl. XI S. 243) - einen eigenständigen Beihilfeanspruch erhielten. Dies stößt jedoch auf Schwierigkeiten.

Das Niedersächsische Finanzministerium hat mir mitgeteilt, wiederholte Erörterungen auf Bund-Länder-Ebene hätten ergeben, daß eine Regelung im angesprochenen Sinne nicht möglich sei. Der Fürsorgeanspruch des Beamten sei nicht übertragbar. Das Antragsrecht auf die Gewährung einer Beihilfe sei höchstpersönlicher Natur und könne damit grundsätzlich nicht auf Angehörige übertragen werden. Die Bund-Länder-Kommission für das Beihilferecht habe deshalb eine Bremer Initiative zur Einführung eines Beihilfeantragsrechts für berücksichtigungsfähige Angehörige im Sinne des § 3 der Beihilfeverordnung abgelehnt.

In Bremen wird jedoch inzwischen so verfahren, daß Familienangehörige sich ohne Einschaltung des Beihilfeberechtigten an die Beihilfestelle wenden und die Erstattung beihilfefähiger Aufwendungen beantragen können. Diese Verfahrensweise ist nach Meinung des Finanzministeriums allerdings von der bestehenden Rechtslage nicht gedeckt.

Soweit in Niedersachsen bei Landesbediensteten einschlägige Probleme aufgetreten sind, wurde den Angehörigen nach den im Fachressort vorliegenden Informationen in allen Fällen die Möglichkeit eingeräumt, ihre Rechnungsbelege ohne Beteiligung des Beihilfeberechtigten unmittelbar der Festsetzungsstelle zuzuleiten, sofern der Beihilfeberechtigte einen entsprechenden Hinweis in seinen Beihilfeantrag aufgenommen hatte. Die Belege wurden nach der Auswertung von der Beihilfestelle unmittelbar an die betroffenen Angehörigen zurückgesandt. Nach Angabe des Finanzministeriums konnte mit dieser pragmatischen Verfahrensweise bisher allen aufgetretenen Problemfällen Rechnung getragen werden.

Das geschilderte Verfahren setzt allerdings ein Zusammenwirken von Beihilfeberechtigten und Angehörigen voraus. Fälle, in denen dies vom Beihilfeberechtigten verweigert worden wäre, sind mir nicht bekanntgeworden. Sollte sich ausnahmsweise einmal eine solche Situation ergeben, geht das Finanzministerium davon aus, daß auch in diesem Fall ein geeigneter pragmatischer Lösungsansatz gefunden werden kann.

An die Beihilfestellen der Kommunen und anderer Dienstherren appelliere ich, in gleicher Weise zu verfahren.

15.7 Beurteilungswesen - Beurteilungskonferenzen

Ein Polizeibeamter bemängelte die in seiner Dienststelle bereits im Vorgriff auf eine eventuell zu erwartende Neuregelung des Polizei-Beurteilungswe-

sens durch das Niedersächsische Innenministerium praktizierte Erstellung von Beurteilungen durch ein sog. "Beurteilungsgremium". Dieses Gremium, das sich sozusagen im Wege des vorauseilenden Gehorsams gebildet hatte, bestand zum Teil aus Polizeibeamten, die den zu Beurteilenden weder persönlich kannten noch ihm vorgesetzt waren. Es legte nicht nur allgemeine Beurteilungsmaßstäbe und -kriterien fest, sondern besprach detailliert jede einzelne Beurteilung der Beamtinnen und Beamten.

Die Einsetzung von Beurteilungskonferenzen ist problematisch, wenn für die Beurteilungsfindung sensible personenbezogene Daten einer größeren Personenzahl bekannt werden, die sonst nicht in das Beurteilungsverfahren einbezogen wären. Folgerichtig ist in diesem Zusammenhang zu beachten, daß nach dem Wesen der Beurteilung nur solche Gremiumsmitglieder beteiligt werden dürfen, die die einzelnen zu beurteilenden Beamten genau kennen; Angehörige einer Zentralabteilung, die die Einhaltung gleichmäßiger Bewertungsmaßstäbe sichern sollen, können - falls sie in ihrer Person diese Voraussetzung nicht erfüllen - nur grundsätzlich beratend und ohne Kenntnis konkreter personenbezogener Daten teilnehmen. Ich habe deshalb das Innenministerium nach seinen Regelungsabsichten in diesem Bereich befragt.

Nach langer Bearbeitungszeit teilte mir das Innenministerium mit, daß gegenwärtig eine Projektgruppe damit befaßt sei, Vorschläge und Empfehlungen der Polizeireformkommission zur Neugestaltung des Beurteilungswesens auf ihre Realisierbarkeit zu überprüfen und in einen Richtlinienvorentwurf umzusetzen. Die in Rede stehenden Konferenzen sollten nach derzeitiger Einschätzung grundsätzliche Beurteilungsmaßstäbe festlegen, nicht jedoch besonders schutzwürdige Persönlichkeitsmerkmale und entsprechend personenbezogene Daten erörtern. Die abschließende Beurteilung einschließlich der Festlegung der Beurteilungsnote bleibe ausschließlich dem jeweils zuständigen Erst- und Zweitbeurteiler vorbehalten.

Grundsätzliche Bedenken gegen eine solche Verfahrensweise habe ich nicht. Bei der Neugestaltung des Beurteilungswesens, an dem ich gem. Nr. 17.6 der VV zu § 22 NDSG zu beteiligen bin, wird sich mein besonderes Augenmerk auf
eine datenschutzgerechte Ausgestaltung der Regelungen richten.

## 15.8 Mitteilungen gemäß § 13 Schwerbehindertengesetz - 2. Teil

In meinem letzten Tätigkeitsbericht habe ich unter XI 15.11 mitgeteilt, daß mit dem Niedersächsischen Sozialministerium eine Übereinstimmung dahingehend erzielt sei, daß in den jährlichen Meldungen der Arbeitgeber nach § 13 Schwerbehindertengesetz (SchwbG) an die Arbeitsverwaltung der tatsächliche Grad der Schwerbehinderung der Bediensteten in Prozenten nicht mehr aufzuführen sei; es reiche die Angabe: "SB (= schwerbehindert) und Aktenzeichen des Versorgungsamtes" oder "GL (= Schwerbehinderten gleichgestellte Person) und Aktenzeichen des Arbeitsamtes".

Zu Problemen kam es allerdings, als Dienststellen der Landesverwaltung entsprechend dieser Aussage verfuhren. Das Landesarbeitsamt Niedersachsen-Bremen drängte darauf, auch weiterhin den Grad der Behinderung anzugeben, da die Bundesanstalt für Arbeit die Angabe für unverzichtbar hielt. Die Mitteilung sei notwendig, damit die Arbeitsverwaltung prüfen könne, inwieweit Arbeitgeber ihrer Verpflichtung nachkämen, im Rahmen der Beschäftigung von Schwerbehinderten in angemessenem Umfang auch besondere Gruppen Schwerbehinderter zu berücksichtigen (§ 6 SchwbG). Überdies sei diese Angabe für die Kenntnis über Struktur und Entwicklung der in den Betrieben beschäftigten Behinderten erforderlich, damit die Arbeitsämter zielgerichtet Aktivitäten im Rahmen der beruflichen Eingliederung Behinderter entwickeln und durchführen können.

Aus Sicht des Datenschutzes konnten diese Gesichtspunkte nicht überzeugen. Denn der Grad der Behinderung sagt z.B. über die Zugehörigkeit zu einer der in § 6 SchwbG genannten Personengruppen nichts aus. Nachdem die bisherige Praxis auch bei anderen Landesbeauftragten und in anderen Ländern auf Kritik gestoßen ist, hat das Bundesministerium für Arbeit und Sozialordnung schließlich eingeräumt, daß die Angabe entbehrlich sei. Der Grad der Behinderung braucht also künftig im Verzeichnis nach § 13 Abs. 1 SchwbG nicht mehr aufgeführt zu werden. Ich gehe davon aus, daß die Arbeitsverwaltung den Vordruck für die entsprechenden Meldungen in diesem Sinne ändern wird.

## 15.9 Personalakten und Gesundheitsdaten auf Irrfahrt

Immer wieder kommt es im Zusammenhang mit Personalakten, insbesondere bei der Versendung an andere Dienststellen (z.B. Gesundheitsamt) oder auch der Nutzung innerhalb der Behörde zu anderen Zwecken (z.B. Schadenersatzansprüchen gegenüber Dritten), zu Problemen. Beispielhaft sei hier aufgeführt, daß anläßlich einer Untersuchung der Dienstfähigkeit eines Beamten durch den Amtsarzt die vollständige Personalakte, die sich in mehreren Jahrzehnten mit verschiedenen Teilakten aufgebaut hatte, mitgesandt wurde. Der Amtsarzt wußte mit dem Aktenkonvolut nichts anzufangen und gab die für ihn nicht erforderlichen Aktenteile mit einer entsprechenden Bemerkung sofort an die Beschäftigungsbehörde zurück. Diese beharrte aber gegenüber dem Petenten und mir darauf, daß die Übersendung der gesamten Vorgänge für die amtsärztliche Untersuchung erforderlich gewesen sei.

Aufgrund dieser und anderer Eingaben mußte ich auf die Grundregeln der Personalaktenführung, die an sich hinlänglich deutlich in den Verwaltungsvorschriften zu § 101 des Niedersächsischen Beamtengesetzes (NBG) enthalten sind, hinweisen:

Jede Verarbeitung personenbezogener Daten muß sich auf den zur Aufgabenerfüllung unbedingt erforderlichen Umfang beschränken. In Personalgrundakten und Personalnebenakten dürfen nur Vorgänge abgeheftet werden, die nach den geltenden Grundsätzen einer ordnungsgemäßen Personalaktenführung in diese Akten aufzunehmen sind. Ärztliche Gutachten über

den körperlichen oder geistig-seelischen Gesundheitszustand der Beamtin oder des Beamten sind in der Personalakte in einem verschlossenen Umschlag aufzubewahren, der nur geöffnet werden darf, wenn eine Personalangelegenheit die Einsichtnahme erfordert; Anlaß und Datum sind auf dem Umschlag zu vermerken. Zur klarstellenden Erläuterung merke ich an, daß dem Begriff der ärztlichen Gutachten nicht ausschließlich anlaßbezogene umfangreiche Gutachten, wie z.B. anläßlich § 56 Abs. 2 NBG, zuzurechnen sind. Grundsätzlich gehört hierzu jedes den Gesundheitszustand betreffende und jedes detaillierte ärztliche Schreiben. Demzufolge müssen z.B. auch Ergebnisse einer Einstellungsuntersuchung sowie medizinische Angaben über die zur Schwerbehinderung führenden Gesundheitsschäden (Schwerbehindertenbescheid) und auch im Rahmen von Schadenersatzverfahren bei Körperverletzungen entstandene medizinische Daten entsprechend verschlossen zur Personalakte genommen werden.

Werden Gesundheitsämter um amtsärztliche Zeugnisse oder Gutachten ersucht, so sind - wie auch bei allen sonstigen vorgesehenen Anlässen - nur die tatsächlich erforderlichen Akten beizufügen. Soweit das Erforderlichkeitsprinzip beachtet wird, begegnet es keinen Bedenken, daß der außerhalb der Personalstelle angesiedelten Schadenersatz-Sachbearbeitung fach- oder amtsärztliche Gutachten zugänglich gemacht werden oder daß solche Gutachten zur Anspruchbegründung an eine gegnerische Versicherung weitergegeben werden. Stets dürfen nur die unabdingbar notwendigen - gegebenenfalls auszugsweisen - Unterlagen nach eingehender Prüfung durch die die Personalakte führende Stelle zur Verfügung gestellt werden.

15.10 Auskünfte bei Gehaltspfändungen: Datenschutz schützt nicht vor Gläubigern

Öffentliche Arbeitgeber erhalten vielfach Anfragen zu ihren eigenen Beschäftigten aus dem Kreditgewerbe und von Anwälten im Zusammenhang mit ausstehenden Forderungen; erfragt wird regelmäßig, ob ein Beschäftigungsverhältnis besteht und ob das Einkommen bereits anderweitig gepfändet oder abgetreten ist. Wie ich in Erfahrung bringen konnte, wird offenbar häufig lediglich die Tatsache, daß jemand in einer Dienststelle beschäftigt ist, an anfragende private Stellen weitergegeben; in mir vorgetragenen Einzelfällen sind aber auch weitere Angaben gemacht worden.

Nach § 56d Abs. 2 des Beamtenrechtsrahmengesetzes (BRRG) dürfen Auskünfte an Dritte u.a. erteilt werden, wenn berechtigte, höherrangige Interessen des Dritten die Auskunfterteilung zwingend erfordern. In die Gesetzesbegründung zum gleichlautenden Bundesbeamtengesetz (BBG) ist dazu der erläuternde Hinweis aufgenommen worden, daß dieses Erfordernis z.B. bei vollstreckbarem Zahlungstitel eines Dritten gegen den Beamten vorliegt. Ich gehe davon aus, daß die Regelungen des BRRG in dieser Legislaturperiode in das Niedersächsische Beamtengesetz übernommen werden. Schon jetzt bestimmt § 24 Abs. 1 Satz 3 NDSG, daß eine Übermittlung von Beschäftigtendaten an Personen und Stellen außerhalb des öffentlichen Bereichs nur

zulässig ist, wenn die Empfänger ein rechtliches Interesse glaubhaft darlegen, der Dienstverkehr es erfordert oder die Betroffenen eingewilligt haben.

Ein rechtliches Interesse ist in den angesprochenen Fällen gegeben. Ich habe deshalb keine Bedenken, daß auf entsprechende Anfragen Bestätigungen über die Beschäftigung von Mitarbeiterinnen und Mitarbeitern gegeben werden, wenn diesbezüglich begründete Anfragen eingehen. Eine Rechtsverpflichtung zur Auskunfterteilung besteht allerdings nicht (wegen der Erklärungspflicht des Drittschuldners bei Vorliegen eines Pfändungsbeschlusses gem. § 840 ZPO vgl. 31.12).

## 15.11 Brief- und Postgeheimnis: Immer noch ein Buch mit sieben Siegeln für die Verwaltung?

Immer wieder erreichen mich Schreiben von Landes- oder Kommunalbediensteten, die zu Recht Klage darüber führen, daß ihre Verwaltung ihnen persönliche Schreiben offen und/oder auf dem Dienstweg zustellt, die einen dienstrechtlichen und dabei zum Teil recht prekären persönlichen Inhalt haben. Eine Vielzahl von Vorgesetzten und von Kolleginnen und Kollegen hatte somit Gelegenheit, sich daraus über die Betroffenen zu informieren.

Als Beispiel sei der Fall einer Lehrerin genannt, die in einem unkuvertierten Schreiben von ihrer Bezirksregierung über das zuständige Schulaufsichtsamt und die örtliche Schulsekretärin aufgefordert wurde, sie möge doch bitte zu einer gerade mal knapp fünfstelligen dort vorliegenden Gehaltspfändung Stellung nehmen, wie es überhaupt dazu kommen konnte und wie sie beabsichtige, ihre wirtschaftliche Lage wieder zu konsolidieren.

Es liegt auf der Hand, daß im in Rede stehenden Fall die Verfahrensweise - das Schreiben enthielt Daten aus der Besoldungsakte - nicht rechtmäßig war. Ich halte es für eine Selbstverständlichkeit, Schreiben mit persönlichem Inhalt auch entsprechend zu adressieren und verschlossen zuzustellen.

Dies gebietet das Persönlichkeitsrecht der Betroffenen. Aus § 30 Verwaltungsverfahrensgesetz läßt sich der allgemeine Rechtsgedanke entnehmen, daß Schreiben mit Daten oder Angaben, die Rückschlüsse auf persönliche Verhältnisse zulassen, grundsätzlich verschlossen zu übersenden sind.

Lediglich in den Fällen, in denen der dienstrechtliche Charakter des Schreibens überwiegt und Vorgesetzte im Rahmen ihrer Aufsichts- und Kontrollfunktion über den Inhalt informiert sein müssen (z.B. Einweisungs- oder Abordnungsverfügungen, Anzahl der regelmäßig zu leistenden Arbeitsstunden, Aus- und Fortbildungsmaßnahmen, Sonderurlaub), kann eine Zustellung derartiger Schreiben auf dem Dienstweg in Betracht kommen; gleichwohl sind sie auf den unabdingbar erforderlichen Personenkreis zu beschränken und auch diesem jeweils verschlossen im Kuvert oder in Verschlußmappen zuzuleiten.

15.12 Fahrtenbuchführung: Was machen meine Beschäftigten am Wochenende?

Bedenken habe ich gegen das Verfahren geäußert, in Fahrtenbüchern anerkannter privater Kraftfahrzeuge die Kilometerstände von Beginn und Ende von Dienstfahrten eintragen zu lassen. Dadurch war es der abrechnenden Dienststelle möglich, die während der Freizeit und an den Wochenenden von den Bediensteten privat zurückgelegten Kilometer zu erfahren.

Das Niedersächsische Finanzministerium sah nach Überprüfung für diesen Umfang der Datenerhebung reisekostenrechtlich ebenfalls keine Erforderlichkeit. Die Angaben könnten allenfalls Bedeutung für den Fall haben, daß die Bediensteten die ihnen durch die Benutzung des eigenen Pkw auf der Dienstreise entstehenden Kosten - abzüglich der von der Behörde steuerfrei ersetzten Fahrkosten - als Werbungskosten steuermindernd geltend machen. Hierzu wäre das Fahrtenbuch gegenüber dem Finanzamt ein geeigneter Nachweis; alternativ können dazu aber auch gesondert von den Bediensteten geführte Anschreibungen dienen.

Der Vordruck "Fahrtenbuch" wird nach Angabe des Ministeriums zukünftig datenschutzgerecht gestaltet und im Rahmen der nächsten Drucklegung den Hinweis enthalten, daß die Angabe des Kilometerstandes vor und nach einer Dienstfahrt freiwillig ist.

15.13 Personalvorgang in der Tagespresse?

Ein Richter hatte Aufsehen durch seine Urteilsbegründungen erregt. Diese brachten ihm nicht nur Presseberichte ein, sondern auch ein Verfahren zur Versetzung in den Ruhestand wegen Dienstunfähigkeit. Auch hierüber wurde - mit dem Zusatz, ihm sei durch das Niedersächsische Dienstgericht für Richter am zuständigen Landgericht die Amtsführung vorläufig untersagt worden - in der Presse berichtet. Gutachterliche medizinische Feststellungen wurden zitiert. Der Petent vermutete, daß insbesondere hochrangige Ministeriumsangehörige sowie die hauseigene Pressestelle die Weitergabe dieser sein Persönlichkeitsrecht berührenden Informationen an die Öffentlichkeit betrieben hätten.

Sowohl das Niedersächsische Justizministerium als auch das Gericht teilten mir mit, daß sie nicht von sich aus die Presse unterrichtet hatten. Vielmehr hatte sich das Ministerium auf Befragen gegenüber Pressevertretern geäußert. Im Ergebnis vermochte ich einen Verstoß gegen datenschutzrechtliche Vorschriften nicht zu erkennen und stimmte vielmehr der Ansicht des Fachressorts zu, daß die geschilderte Auskunft gegenüber der Presse im vorliegenden Fall zulässig war. § 4 Abs. 1 des Niedersächsischen Pressegesetzes verpflichtet nämlich die Behörde grundsätzlich zur Auskunftserteilung gegenüber der Presse. Auskünfte können allerdings u.a. dann verweigert werden, wenn ihnen Vorschriften über die Geheimhaltung entgegenstehen oder sie ein überwiegendes schutzwürdiges privates Interesse verletzen würden.

Gesetzliche Schweigegebote, die eine Auskunfterteilung nicht zugelassen hätten, vermochte ich in diesem Fall nicht zu erkennen. Die Bestimmung über die Schweigepflicht (§ 68 NBG in Verbindung mit § 4 Nds. Richtergesetz) stellt keine Geheimhaltungsvorschrift in diesem Sinne dar. Eine Behörde als solche unterliegt nicht der Amtsverschwiegenheit, wie sie für die Bediensteten gilt.

Zwar berührte die Aussage des Fachressorts die privaten Interessen des Petenten. Die vorzunehmende Güterabwägung zwischen der Pressefreiheit und dem allgemeinen Persönlichkeitsrecht des Petenten ergab jedoch bei Berücksichtigung der vorliegenden Umstände für mich keinen Anhaltspunkt für ein rechtswidriges Verhalten der Behörde. Die Vorgänge, die zur Einleitung des Verfahrens zur Versetzung in den Ruhestand geführt hatten, waren nach Darstellung des Ministeriums den Pressevertretern bereits vor den erteilten Auskünften bekannt. Da das richterliche Handeln Öffentlichkeitswirkung besitzt, kann der Presse ein Informationsbedürfnis an der Art der Ausübung dieser Tätigkeit, zumal wenn daran - ob berechtigt oder nicht - Kritik geübt worden ist, nicht abgesprochen werden. Im vorliegenden Fall konnte dieses Informationsbedürfnis auch nicht unter Verzicht auf einen konkreten Personenbezug erfüllt werden. Die bloße Nennung der gesetzlichen Voraussetzung des in Rede stehenden Verfahrens - daß Zweifel an der Dienstfähigkeit des Richters bestanden - berücksichtigt schließlich den Verhältnismäßigkeitsgrundsatz.

In diesem Zusammenhang sei noch anzumerken, daß z.B. bei besonderem Öffentlichkeitsinteresse auch eine Unterrichtung der Medien über die Einleitung förmlicher Disziplinarverfahren grundsätzlich als zulässig angesehen wird. Unvereinbar mit dem Persönlichkeitsrecht des Betroffenen wäre es allerdings gewesen, wenn die Behörde, wie von dem Petenten vermutet, Zitate aus medizinischen Gutachten über seinen Gesundheitszustand an die Öffentlichkeit gebracht hätte. Dies war jedoch nicht der Fall.

## 15.14 Gratulation im Büro? - Ein kleines datenschutzrechtliches Kuriosum

Ein im öffentlichen Dienst tätiger Petent stellte in Frage, ob er sich gegen seinen Willen von Kolleginnen und Kollegen sowie Vorgesetzten zum Geburtstag gratulieren lassen muß. Er habe zum Erstellen einer verwaltungsintern genutzten Liste, die auch sein Geburtsdatum enthalte, sein Einverständnis nicht gegeben; dennoch sei er darin aufgenommen worden.

Nicht nur unter Berücksichtigung der dem Dienstherrn obliegenden Fürsorgepflicht ist es nach hergebrachten dienstrechtlichen Grundsätzen eine gängige Verfahrensweise, daß Vorgesetzte - selbstverständlich ebenso Kolleginnen und Kollegen - den Bediensteten zum Geburtstag gratulieren. Dies entspricht allgemeinen Grundsätzen des zwischenmenschlichen Umgangs und wird deshalb in aller Regel nicht nur hingenommen, sondern auch von den Bediensteten ausdrücklich erwartet. Ein Ignorieren eines solchen (Fest-)Tages wird die Zusammenarbeit und eine offene, kooperative und auf

gegenseitige Achtung aufbauende Ausgestaltung der Arbeitsbeziehungen nicht fördern (vgl. auch "Allgemeine Handlungsziele für die niedersächsische Landesverwaltung und Allgemeine Grundsätze für Zusammenarbeit und Führung in der niedersächsischen Landesverwaltung", Gemeinsamer Runderlaß des Niedersächsischen Innenministeriums, der Staatskanzlei und der übrigen Ministerien vom 12. Januar 1993, Nds. MBl. S. 330). Es ist deshalb aus datenschutzrechtlicher Sicht unproblematisch, wenn Vorgesetzte sowie Kolleginnen und Kollegen im abgesteckten Rahmen einer zusammenarbeitenden Organisationseinheit Kenntnis über die Geburtstage der Beschäftigten dieses Bereichs erhalten; die Angabe des Geburtsjahres ist in diesem Zusammenhang allerdings entbehrlich.

Datenschutzrechtliche Bedenken wären allerdings zu erheben, wenn in einer solchen Geburtstagsliste die Geburtstage aller Bediensteten einer größeren Behörde (wie z.B. einer Bezirksregierung) enthalten wären bzw. wenn eine - an sich zulässige - Liste jedermann - also auch unbeteiligten Dritten und Außenstehenden wie z.B. Besuchern - zugänglich aufgehängt würde ("Schwarzes Brett"); bei der letztgenannten Fallkonstellation läge auch eine Übermittlung an Personen außerhalb des öffentlichen Bereichs vor, für die die Empfänger kein rechtliches Interesse an der Kenntnis gemäß § 13 Abs. 1 Satz 1 Nr. 2 NDSG geltend machen könnten.

Wenn jemand jedoch - ungeachtet der datenschutzrechtlichen Zulässigkeit - aus wie auch immer gearteten Gründen die Aufnahme ihres oder seines Geburtstags in eine solche Geburtstagsliste ablehnt, sollte diesem Wunsch Rechnung getragen werden.

## 15.15 Einsatz von öffentlichen Bediensteten als Wahlhelfer oder Betreuer

Besonders im "Superwahljahr" 1994 ist wieder häufig die Frage gestellt worden, ob Behörden Daten der bei ihnen Beschäftigten ohne deren Einwilligung für einen Einsatz als Wahlhelfer an Gemeinden übermitteln dürfen. Die gleiche Problematik ergibt sich bei einer beabsichtigten Bestellung von Angehörigen des öffentlichen Dienstes zu Betreuern nach dem Betreuungsgesetz oder für andere ehrenamtliche Aufgaben.

Da eine solche Datenübermittlung nicht zur Abwicklung des Dienst- oder Arbeitsverhältnisses oder für einen anderen in § 24 NDSG genannten Zweck erforderlich ist, stellt sie - unabhängig davon, ob die Daten innerbehördlich oder an dritte Stellen weitergegeben werden - eine Zweckänderung dar. Diese ist, wenn man vom Fall der Einwilligung der Betroffenen absieht, hier nur zulässig, wenn eine Rechtsvorschrift sie vorsieht (§ 10 Abs. 2 Satz 1 Nr. 2 NDSG). Für die Datenübermittlung zum Einsatz als Wahlhelfer hat der niedersächsische Gesetzgeber mit Art. 1 Nr. 8 - § 25 Abs. 2 - des Gesetzes zur Änderung des Niedersächsischen Landeswahlgesetzes (NLWG) vom 26. Mai 1993 (Nds. GVBl. S. 119) eine entsprechende Rechtsgrundlage geschaffen. Hiernach sind niedersächsische öffentliche Stellen nicht nur berechtigt, sondern verpflichtet, auf Ersuchen der Gemeinden aus dem Kreis ihrer Bediensteten Personen zu benennen, die für eine Berufung

als Beisitzer geeignet sind und im Gebiet der ersuchenden Gemeinde wohnen.

Diese Regelung bezieht sich allerdings nur auf die niedersächsischen Landtagswahlen. Der Bundesgesetzgeber hat für die Europawahlen und die Bundestagswahlen eine vergleichbare Rechtsgrundlage nicht geschaffen. Entsprechende Datenübermittlungen sind deshalb unzulässig, sofern keine Einwilligung der Betroffenen vorliegt. Für diese Wahlen darf eine Gemeinde auch nicht auf eine Wahlhelferdatei zurückgreifen, in denen sie Beschäftigtendaten gespeichert hat, die ihr nach § 25 Abs. 2 NLWG übermittelt worden sind. Ebenso ist es nicht zulässig, Bedienstete anhand sonstiger Unterlagen der Beschäftigungsdienststelle, z.B. des dienstlichen Telefonverzeichnisses, zur Übernahme eines Wahlehrenamtes heranzuziehen. Auch darin läge eine unzulässige Zweckänderung.

Aus dem gleichen Grund darf eine Weitergabe von Beschäftigtendaten von der Personalverwaltung einer öffentlichen Stelle an ein Jugendamt zur Bestellung von Betreuern nach dem Betreuungsgesetz nicht erfolgen. Da ein gesetzlicher Zulässigkeitstatbestand hierfür fehlt, kann nur an die Bediensteten appelliert werden, sich freiwillig als Betreuer zur Verfügung zu stellen.

## 15.16 Telefonverzeichnisse im Netz - "Mäuschen" auf Abwegen

Eine niedersächsische Universität wollte sich ansprechbereit zeigen: Dazu sollte ein uni-internes Telefonverzeichnis, das neben den Namen und Dienstanschriften auch Titel, Berufsbezeichnungen, Institutszugehörigkeit sowie dienstliche und zum Teil sogar private Rufnummern enthält, in das elektronische Auskunfts- und Mailbox-System "gopher" (= "Mäuschen") eingespeist und dadurch weltweit für alle an diesem Verbund beteiligten Nutzer (hauptsächlich in Hochschulen und Forschungseinrichtungen) zum Abruf zur Verfügung gestellt werden.

Die vorsorglich an mich gerichtete Frage nach der Zulässigkeit eines derartigen Verfahrens konnte aber auf der Grundlage des § 24 NDSG, der die Datenverarbeitung bei Dienst- und Arbeitsverhältnissen regelt, nur verneint werden. Schon eine Weitergabe dienstlicher Fernsprechverzeichnisse an andere öffentliche Stellen ist nicht immer zulässig. Sie wird nur gegenüber solchen öffentlichen Stellen in Betracht kommen können, mit denen ein dienstlicher Verkehr besteht. Auch dann sehe ich für eine Übermittlung privater Telefonnummern aber grundsätzlich keine Notwendigkeit. Eine Weitergabe von Fernsprechverzeichnissen an private Dritte setzt voraus, daß der Dienstverkehr sie erfordert (§ 24 Abs. 1 Satz 3 NDSG). Davon kann ausgegangen werden, wenn es um die dienstlichen Telefondaten solcher Beschäftigter geht, die im Rahmen ihrer Dienstausübung häufig in Kontakt mit Bürgerinnen und Bürgern stehen. Denn sie müssen selbstverständlich für jedermann fernmündlich erreichbar sein. Unzulässig ist jedoch die Übermittlung von Telefondaten solcher Mitarbeiterinnen und Mitarbeiter, die - wie z.B. Schreibkräfte und andere Angehörige des Inneren Dienstes - in

der Regel derartige Kontakte nicht unterhalten. Eine Weitergabe des gesamten Telefonverzeichnisses kann deshalb nicht in Betracht kommen.

Auch sofern hiernach eine Datenübermittlung denkbar ist, sehe ich für eine Übermittlung von Vornamen und privaten Telefonnummern grundsätzlich keine Notwendigkeit. Die Angabe des Vornamens bzw. einer entsprechenden Abkürzung kann - auch bei einem nur behördenintern genutzten Telefonverzeichnis - allerdings zulässig sein, wenn sie als Unterscheidungsmerkmal bei Namensgleichheit erforderlich ist. Private Telefonnummern dürfen ohne Einwilligung der Betroffenen nur weitergegeben werden, wenn die Bediensteten außerhalb der Dienstzeit für Bürgerinnen und Bürger erreichbar sein müssen. Diese Voraussetzung dürfte nur in Einzelfällen vorliegen. Vorname und private Telefonnummer dürfen deshalb - sofern nicht die genannten Ausnahmefälle vorliegen - nur mit schriftlicher Einwilligung der Betroffenen weitergegeben werden. Dabei ist § 4 Abs. 2 NDSG zu beachten. Auch im Falle der Universität könnte deshalb eine Einspeisung der Daten des Fernsprechverzeichnisses in das System "gopher" nur mit (schriftlicher) Einwilligung der Betroffenen in Betracht kommen. Zudem wäre wegen der Möglichkeit des automatisierten Abrufs eine Zulassung dieses Verfahrens nur durch eine Rechtsvorschrift nach § 12 NDSG zulässig. Zu beachten wären außerdem die Vorschriften des § 14 NDSG, da die Übermittlung der Daten auch in das Ausland beabsichtigt war.

Nachdem auch im Kommunalbereich mehrere Anfragen zur Zulässigkeit der Weitergabe von Telefonverzeichnissen gestellt worden sind, hat das Niedersächsische Innenministerium in den Verwaltungsvorschriften zum NDSG (s. dort Nr. 18.4 zu § 24) die Problematik im oben dargestellten Sinne angesprochen.

## 16. Kommunalverwaltung

### 16.1 Wer andern eine Grube gräbt ...

Ein Bürger hatte im November 1993 kurz nacheinander zwei Telefaxe an den Oberstadtdirektor einer Stadt gesandt. Im ersten Fax stellte der Petent unter Umweltschutzgesichtspunkten kritische Fragen nach der Einsatzweise eines städtischen Kraftfahrzeuges, im zweiten Fax übte er Kritik daran, daß die Stadt ein kostenträchtiges Gutachten zur Einrichtung von Fahrradstraßen in Auftrag geben wollte. Als Absender gab er seine Privatanschrift an. Außerdem enthielt der Briefkopf seine Telefon- sowie seine Fax-Nummer. Da der Petent die Schreiben über das Fax-Gerät seines Arbeitgebers übermittelte, enthielten sie dessen Absenderkennung.

Das Büro des Hauptverwaltungsbeamten, das offenbar so viel Kritik in so kurzer Zeit nicht verkraften konnte, antwortete nicht nur dem Petenten, sondern unterrichtete gleichzeitig dessen Arbeitgeber von den privaten Schreiben seines Beschäftigten. Hierüber ließ die Stadt den Petenten auch nicht

im unklaren. Eine städtische Bedienstete teilte ihm vielmehr mit, da er seine Schreiben in beiden Fällen über das Fax-Gerät seines Arbeitgebers übermittelte, habe man nicht eindeutig feststellen können, ob es sich nur um Privatschreiben oder auch um Mitteilungen der Firma gehandelt habe. Damit das Schreiben in dem großen Unternehmen des Bediensteten auch gleich an die richtige Stelle kam, scheute die Stadt keine Mühe. Sie ermittelte, in welcher Abteilung der Arbeitnehmer tätig war und brachte auch den Namen seines Abteilungsleiters in Erfahrung. So konnte der Vorgesetzte zielgerichtet über die Privatangelegenheiten seines Mitarbeiters unterrichtet werden.

Die Rechtswidrigkeit dieses Handelns liegt auf der Hand. Die Datenübermittlung an das Unternehmen verstößt gegen § 13 NDSG. Die Information des Arbeitgebers war weder zur Aufgabenerfüllung der Stadt erforderlich, noch hatte das Unternehmen ein berechtigtes oder gar ein rechtliches Interesse an einer Unterrichtung über diese privaten Aktivitäten ihres Mitarbeiters. Die Stadt mochte sich dieser Einschätzung jedoch zunächst nicht anschließen. Sie
wandte ein, wegen der Angabe der Absenderkennung sei zweifelhaft gewesen, ob auch die Firma eine Beschwerde über das Verhalten der Stadt geführt habe. Als Petentin aber habe das Unternehmen einen grundgesetzlich verbürgten Anspruch auf behördliche Stellungnahme.

Diese Einlassung lag nun völlig neben der Sache. Schon die Annahme, ein großes Unternehmen würde sich in einer Firmenangelegenheit unter dem Namen und der Privatanschrift eines Mitarbeiters an eine Behörde wenden, ist nicht nachvollziehbar. Auch ergab sich aus den Eingaben auf den ersten Blick, daß es sich bei dem Inhalt der Faxe nicht um Angelegenheiten des Unternehmens handeln konnte. Schließlich kann aus der Absenderkennung eines behördlichen oder firmeneigenen Fax-Gerätes nicht ohne weiteres geschlossen werden, es handele sich um eine Mitteilung des Fax-Geräteinhabers. Denn Unternehmen und Verwaltungsbehörden, darunter die hier angesprochene Stadt, erlauben ihren Mitarbeitern häufig, gegen Kostenerstattung dienstliche Fax-Geräte für die Übermittlung privater Nachrichten zu nutzen, ohne daß jemand auf den Gedanken käme, diese als Firmen- oder Behördenmitteilungen anzusehen.

Nachdem ich das Verhalten der Stadt beanstandet hatte, hat sie sich meiner rechtlichen Bewertung angeschlossen. Dankenswerterweise hat sie den Vorfall zum Anlaß genommen, ihre Mitarbeiterinnen und Mitarbeiter entsprechend zu unterrichten, um ähnliche Vorkommnisse für die Zukunft auszuschließen. Für die übereifrige städtische Bedienstete blieb der Vorfall nicht folgenlos. Die Mitarbeiterin hat mit der Datenübermittlung an den Arbeitgeber personenbezogene Daten über den Bürger zweckwidrig (nämlich nicht zur Prüfung seiner Eingaben) verwendet und damit gegen das Datengeheimnis (§ 5 NDSG) verstoßen. Zudem bestand der Verdacht, in Schädigungsabsicht gegenüber dem Petenten gehandelt zu haben. Die Staatsanwaltschaft leitete deshalb ein strafrechtliches Ermittlungsverfahren wegen Verstoßes gegen § 28 NDSG ein. Es wurde schließlich gegen Zahlung einer nicht unerheblichen Geldbuße eingestellt.

16.2 Schreibtisch auf - der Ratsherr kommt!

Nach § 7 Abs. 4 NDSG haben die öffentlichen Stellen personenbezogene Daten in Akten insbesondere vor dem Zugriff Unbefugter zu schützen. Eingaben lassen darauf schließen, daß dies im Kommunalbereich gelegentlich zu Problemen führt, weil zumindest in Einzelfällen Ratsmitglieder ihre Wißbegier offenbar nur schwer zügeln können. Insbesondere von Vertretern kleiner Fraktionen wurde hierüber Klage geführt.

So ist mir unverständlich, aus welchem Grunde z.B. - wie mir eine Gemeinde schrieb - in der Poststelle der Behörde ein "Durchgangsverkehr" von Ratsmitgliedern stattfindet. Bei aller Anerkennung eines engagierten Einsatzes für kommunale Belange kann einem Ratsmitglied doch nicht die Möglichkeit eröffnet werden, sich auf diese Weise einen - und sei es noch so begrenzten - Überblick über die Verwaltungseingänge zu verschaffen. Ebenso halte ich es nicht für hinnehmbar, wenn Ratsangehörige während der Dienstzeit Diensträume aufsuchen und dort ohne weiteres Unterlagen mit personenbezogenen Daten zur Kenntnis nehmen können. Auch wenn eine Kommune zum "besseren Verständnis und der konstruktiveren Zusammenarbeit der Organe Rat und Verwaltung" eine "Möglichkeit der kurzen Wege" zwischen Ratsmitgliedern und Mitarbeiterinnen und Mitarbeitern der Verwaltung schafft, darf dies nicht dazu führen, daß es Ratsangehörigen dadurch ermöglicht wird, ungehindert in Verwaltungsvorgänge Einsicht zu nehmen. Schließlich muß selbstverständlich einer Weitergabe personenbezogener Daten durch Bedienstete an Ratsmitglieder unter Verletzung von Dienstpflichten entgegengewirkt werden.

Ich habe angeregt, die Bediensteten schriftlich auf ihre datenschutzrechtlichen Pflichten hinzuweisen. Nach § 5 NDSG ist es den Beschäftigten untersagt, personenbezogene Daten zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren. Hierunter fällt auch eine unerlaubte Weitergabe von personenbezogenen Daten an Ratsmitglieder. Ein solches Verhalten stellt gemäß § 29 Abs. 1 Nr. 1 NDSG eine Ordnungswidrigkeit dar; zugleich liegt darin eine Dienstpflichtverletzung. Dies sollte den Bediensteten vor Augen geführt werden. Die Mitarbeiterinnen und Mitarbeiter haben auch dafür Sorge zu tragen, daß Verwaltungsvorgänge Dritten nicht zugänglich sind. Beim Verlassen des Dienstzimmers müssen die Räume deshalb gegebenenfalls abgeschlossen werden. Auch die Ratsmitglieder müssen darauf hingewiesen werden, daß sie personenbezogene Daten nur im Rahmen der kommunalverfassungsrechtlichen Vorschriften zur Kenntnis erhalten dürfen.

16.3 Streit im Gemeinderat

In einer Gemeinde hatte die Verpachtung eines gemeindeeigenen Grundstücks erheblichen politischen Wirbel ausgelöst. Der Fraktionsvorsitzende einer im Rat vertretenen Partei hatte dabei mehrfach die Gemeinde kritisiert. Als das Grundstück - wie vorgesehen - vom Pächter bebaut wurde, wandte sich der Ratsherr - ohne Hinweis auf seine Funktion als Ratsmitglied -

schriftlich an die Kreishandwerkerschaft. Er äußerte den Verdacht, daß beim Bau Schwarzarbeiter eingesetzt würden und die Gemeinde dies durch ihr Verhalten begünstige. Nachdem auf Antrag des Fraktionsvorsitzenden die Vorgänge um die Grundstücksbebauung auf die Tagesordnung der kommenden Ratssitzung gesetzt worden waren, händigte der Gemeindedirektor den Ratsmitgliedern Ablichtungen des Schreibens des Fraktionsvorsitzenden an die Kreishandwerkerschaft und der dazu abgegebenen Stellungnahme der Gemeinde mit dem Bemerken aus, jeder möge sich hierzu seine Gedanken machen. Zu einer inhaltlichen Diskussion in der öffentlichen Ratssitzung kam es wegen eines in der Sache anhängigen Rechtsstreits nicht. Der Fraktionsvorsitzende sah sich durch die Weitergabe der Unterlagen an die Ratsmitglieder in seinem Persönlichkeitsrecht beeinträchtigt.

Datenschutzrechtlich ist das Verhalten der Gemeinde jedoch nicht zu beanstanden. Der Gemeindedirektor hat nach § 62 Abs. 3 NGO insbesondere den Rat und den Verwaltungsausschuß über wichtige Angelegenheiten zu unterrichten. In dieser Sache hatte es bereits heftige politische Diskussionen gegeben. Schon deshalb bestanden keine Bedenken, daß der Hauptverwaltungsbeamte die Ratsmitglieder über eine weitere Entwicklung in dieser Angelegenheit informierte, zumal diese auf der Tagesordnung der Ratssitzung stand. Auch ein Bürger, der unmittelbar gegenüber einer Gemeinde Beschwerde führt, muß letztlich nach § 62 Abs. 3 NGO damit rechnen, daß das von ihm vorgetragene Anliegen auch unter seiner Namensnennung im Rat oder Verwaltungsausschuß erörtert wird. Sofern es zu einer öffentlichen Ratssitzung kommt, muß allerdings im Einzelfall abgewogen werden, ob seine persönlichkeitsrechtlichen Belange es gebieten, daß von einer Namensnennung abgesehen oder die Angelegenheit in nichtöffentlicher Sitzung behandelt wird (§ 45 Satz 1 NGO).

## 16.4 Kindergartenbeiträge - viel Arbeit für den Landesbeauftragten

Mich haben sehr viele Eingaben von Bürgerinnen und Bürgern aus allen Lan- desteilen Niedersachens sowie Anfragen von Gemeinden und freien Trägern von Kindertagesstätten erreicht, die Kritik an den neuen "Kindergartenbeiträgen" übten und fragten, ob das Antragsverfahren mit dem Datenschutz vereinbar sei. Das Niedersächsische Gesetz über Tageseinrichtungen für Kinder (KiTaG) vom 16. Dezember 1992 (Nds. GVBl. S. 353) schreibt im § 20 vor, daß sich die Elternbeiträge nach der wirtschaftlichen Leistungsfähigkeit der Sorgeberechtigten unter Berücksichtigung der Zahl der Kinder richten sollen. Die Elternbeiträge sind so zu bemessen, daß die wirtschaftliche Belastung für die Sorgeberechtigten zumutbar ist. Die Wahl des Antragsverfahrens sowie die Entscheidung über die Einkommensstufen ist den Trägern der Kindertagesstätten überlassen worden; das Kultusministerium hat bewußt darauf verzichtet, das Antragsverfahren im einzelnen zu regeln.

Die mir durch die Eingaben bekanntgewordenen Datenerhebungen reichen von sehr umfangreichen Fragebogen, die einer Einkommensteuererklärung kaum nachstehen, bis zu der sog. Selbsteinstufung, bei der die Sorgeberech-

tigten keine Nachweise vorzulegen brauchen, sich aber mit deren Vorlage auf Anforderung im Wege einer Stichprobe einverstanden erklären müssen. Diese letztere Verfahrensweise ist die datenschutzfreundlichste Lösung, da sie mit dem geringsten Eingriff für die Betroffenen verbunden ist. Natürlich anerkenne auch ich, daß sozialstaatliche Leistungen Daten der Empfänger und Kontrollen erfordern. Die Erhebung muß jedoch auf das wirklich Erforderliche begrenzt werden.

Die große Anzahl von Eingaben bei mir, die vielen an das Kultusministerium gerichteten Protestbriefe, die lebhafte Diskussion in den Medien und gerichtliche Auseinandersetzungen haben das Kultusministerium dazu gebracht, in einem Erlaß an die Träger der Kindertagesstätten Hinweise zum Datenschutz herauszugeben. Der Erlaß wurde mit mir abgestimmt. Auch konnte ich durch Gespräche und Schriftwechsel mit den Trägern der Kindertagesstätten Verfahrensverbesserungen erreichen.

16.5 Fremdenverkehrsbeiträge - ein "Dauerbrenner"

Wenn es um das liebe Geld geht, entwickeln viele ein ausgeprägtes Datenschutzbewußtsein. So problematisierte eine zahnärztliche Standesvertretung, daß eine Gemeinde Angaben über den steuerbaren Umsatz, das Finanzamt, die Steuernummer und die Zahl der Arbeitskräfte erfragte, um danach den Fremdenverkehrsbeitrag berechnen zu können. Ich teilte der Kammer mit, daß Rechtsgrundlage für die Datenerhebung der § 9 Abs. 3 des Niedersächsischen Kommunalabgabengesetzes i.d.F. vom 11. Februar 1992 (Nds. GVBl. S. 29) ist. Nach dieser Vorschrift haben alle in dem anerkannten Gebiet selbständig tätigen Personen und Unternehmen der Gemeinde auf Verlangen die zur Beurteilung ihrer Beitragspflicht und zur Schaffung der Bemessungsgrundlagen für den Beitrag erforderlichen Auskünfte schon vor Erlaß einer Satzung zu erteilen, sobald der Rat einen Beschluß zum Erlaß einer Fremdenverkehrsbeitragssatzung gefaßt hat. Diese Beschlußfassung war in dem angesprochenen Fall erfolgt. Dabei waren auch die Erhebungsmerkmale bereits festgelegt worden.

16.6 Geburtsdatum in der Kurbeitragsanmeldung

Der Umfang der Datenerhebung zur Festsetzung von Kurbeiträgen war wieder des öfteren Gegenstand von Eingaben und Beschwerden. Dabei wurde z.B. auch gefragt, ob das genaue Geburtsdatum der Kurgäste zur Beitragsfestsetzung erforderlich sei. Ich habe bereits vor längerer Zeit dem Niedersächsischen Innenministerium vorgeschlagen, zumindest auf das Geburtsdatum der Kinder zu verzichten und die Geburtsangaben insgesamt auf der Durchschrift der Kurbeitragsanmeldung für den Vermieter entfallen zu lassen. Das Innenministerium will eine Entscheidung hierüber erst nach Anhörung der Kommunalen Spitzenverbände im Rahmen einer künftigen Satzungsmusterüberarbeitung treffen. Ein genereller Verzicht auf die Angabe des Geburtsdatums für Kinder könne in bestimmten Fällen die Feststellung der tatbestandsmäßigen Voraussetzungen der Beitragspflicht, die zutreffen-

de Festsetzung der Beitragshöhe sowie die zutreffende Gewährung von Teilbefreiungen und Befreiungen beeinträchtigen. Stichprobenartige Überprüfungen in Gemeinden, in denen die Meldevordrucke ausschließlich nach dem Lebensalter fragen, hätten gezeigt, daß die Betroffenen eher geneigt seien, hierzu Falschauskünfte zu erteilen. Dabei sei das Lebensalter häufig zu niedrig angegeben worden, um geringere oder keine Kurbeiträge entrichten zu müssen.

## 17. Natur und Umweltschutz

### 17.1 Einsichtsrecht in Umweltakten

Mit dem Gesetz vom 8. Juli 1994 (BGBl. I S. 1490) ist die EG-Richtlinie vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (vgl. X 17.1) in nationales Recht umgesetzt worden. Eine Umsetzung durch Landesrecht hat sich damit weitgehend erledigt.

Nach diesem Umweltinformationsgesetz (UIG) hat jeder Anspruch auf freien Zugang zu Informationen über die Umwelt, die sich in der Obhut einer Behörde oder einer Person des Privatrechts befinden, die öffentlich-rechtliche Aufgaben im Bereich des Umweltschutzes wahrnimmt und die der Aufsicht von Behörden unterstellt ist. Die Behörde kann auf Antrag Auskunft erteilen, Akteneinsicht gewähren oder Informationsträger in sonstiger Weise zur Verfügung stellen. Der Informationsanspruch besteht allerdings nicht uneingeschränkt. Nach den §§ 7 und 8 UIG kann der Anspruch zum Schutz öffentlicher und privater Belange ausgeschlossen und beschränkt werden. Zum Beispiel besteht der Anspruch nicht, soweit das Bekanntwerden der Informationen eine erhebliche Gefahr für die öffentliche Sicherheit verursachen kann (§ 7 Abs. 1 Nr. 1 UIG), während der Dauer eines Gerichtsverfahrens oder eines strafrechtlichen Ermittlungsverfahrens (Nr. 2 ebenda) oder wenn behördliche Maßnahmen zum Schutz der Umwelt gefährdet werden könnten ( Nr. 3 ebenda). Zur Wahrung des Rechts auf informationelle Selbstbestimmung ist das Einsichtsrecht ausgeschlossen, soweit infolge der Offenbarung personenbezogener Daten schutzwürdige Interessen der Betroffenen beeinträchtigt würden (§ 8 Abs. 1 Nr. 1 UIG).

### 17.2 Niedersächsisches Abfallgesetz

In XI 17.3 hatte ich festgestellt, daß eine allgemeine Regelung der Datenverarbeitung im Niedersächsischen Abfallgesetz (NAbfG) fehlt. Während der Vorarbeiten für eine 2. Novelle zum NAbfG habe ich gegenüber dem Niedersächsischen Umweltministerium die Erforderlichkeit datenschutzrechtlicher Vorschriften dargelegt und auf beispielhafte Regelungen im Landesabfallwirtschaftsgesetz des Landes Schleswig-Holstein hingewiesen.

Am 15. Juni 1994 hat der Landtag das Zweite Gesetz zur Änderung des Niedersächsischen Abfallgesetzes beschlossen (Neufassung in Nds. GVBl. S. 467). Das Ergebnis der getroffenen Datenschutzregelungen ist jedoch enttäuschend. Anstelle normenklarer Bestimmungen hat der Gesetzgeber mit § 45 lediglich eine Generalklausel geschaffen, nach der die entsorgungspflichtigen Körperschaften, die zuständigen Behörden und die Zentrale Stelle für Sonderabfälle die erforderlichen personenbezogenen Daten verarbeiten dürfen. Ergänzend wird auf die Datenverarbeitungsregeln des Niedersächsischen Gefahrenabwehrgesetzes (NGefAG) verwiesen. Diese umfassende Verweisung auf das NGefAG unter Verzicht auf eigene Regelungen ist meines Erachtens nicht haltbar. Das NAbfG ist nur zum Teil dem Polizeirecht im weiteren Sinne zuzuordnen. Es ist im wesentlichen ein Gesetz der Daseinsvorsorge. Der generelle Verweis auf das NGefAG kann daher die typischen Datenverarbeitungssituationen in Ausführung des Abfallgesetzes nicht treffen.

## 17.3 Altlasten

Meine Hoffnung, daß bereichsspezifische Datenschutzvorschriften im Rüstungsaltlastenfinanzierungsgesetz geschaffen würden (vgl. XI 17.4), waren unberechtigt. Eine entsprechende niedersächsische Bundesratsinitiative ist leider gescheitert. Auf Landesebene sind Rüstungsaltlasten nunmehr allerdings ausdrücklich in das NAbfG mit aufgenommen worden (vgl. § 31 Abs. 2 Nr. 2), so daß dessen Regelungen über die Verarbeitung personenbezogener Daten Anwendung finden (17.2).

## 17.4 Niedersächsisches Wassergesetz

Bedauerlicherweise hat es auf dem Sektor des Wasserrechts keine datenschutzrechtlichen Verbesserungen gegeben. Es fehlen nach wie vor bereichsspezifische Regelungen für die im Gesetzesvollzug praktizierte Datenverarbeitung. Das gilt auch für die im letzten Tätigkeitsbericht (vgl. XI 17.2, 17.6 und 17.8) angesprochene Indirekteinleiterverordnung sowie die Speicherung von Daten in Abwasserkatastern. Das Niedersächsische Umweltministerium ist mit mir der Auffassung, daß datenschutzrechtliche Regelungen im Niedersächsischen Wassergesetz (NWG) für verschiedene Regelungsbereiche erforderlich sind. Es hat mitgeteilt, daß diese Thematik für die nächste Novelle des NWG vorgemerkt sei. Derartige Regelungen sind auch für regelmäßige Datenübermittlungen nötig. Eine Verordnung nach 12 Abs. 2 NDSG genügt als Rechtsgrundlage nicht.

## 17.5 Gülle, Jauche, Stallmist - und Datenübermittlungen im Übermaß

Wenn Gülle, Jauche und Stallmist auf Felder aufgebracht werden, kommt es möglicherweise zur Überdüngung landwirtschaftlicher Flächen mit der Folge, daß Schadstoffe in das Grundwasser gelangen. Ein Landkreis, in dessen Bereich intensive Tierhaltung betrieben wird, hatte im Jahre 1990 etwa

3.000 Tierhalter aufgefordert nachzuweisen, wie der in ihrer Tierhaltung anfallende Wirtschaftsdünger entsorgt wird.

Ich habe festgestellt, daß weder das Abfallgesetz des Bundes noch das NAbfG für diese "Aktion 3000" ausreichende Befugnisnormen enthalten. Zwar legt die Gülleverordnung die Menge der zulässigen Dungeinheiten fest, die auf landwirtschaftlich, gärtnerisch oder forstwirtschaftlich genutzte Böden aufgebracht werden dürfen; sie enthält jedoch keine Befugnisnormen für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden. Von der Verordnungsermächtigung in § 40 NAbfG hat die Landesregierung keinen Gebrauch gemacht. Das Umweltministerium sieht für die Landkreise zwar auf der Grundlage des § 11 Abs. 4 Abfallgesetz die Möglichkeit, Auskünfte einzuholen; dies gilt gemäß § 15 Abs. 5 Satz 2 Abfallgesetz jedoch erst dann, wenn das übliche Maß der landwirtschaftlichen Düngung mindestens in einem Fall überschritten wurde.

Für die Zukunft ergibt sich folgendes: In Ermangelung einer bundesrechtlichen Regelung für eine wirksame Überwachung der Ausbringung von Wirtschaftsdünger werden die oberen Landesbehörden (Bezirksregierungen) durch § 40 NAbfG ermächtigt, durch Verordnung für bestimmte Gebiete ihres Bezirkes vorzuschreiben, daß die Abgabe und das Aufbringen von Wirtschaftsdünger in einem Wirtschaftsdüngerverzeichnis zu erfassen sind. In der Verordnung sind insbesondere die Auskunftspflicht sowie die Art der zu erfassenden Informationen zu regeln. Eine ausreichende datenschutzrechtliche Grundlage für die von dem Landkreis vorgenommene flächendeckende Erhebung wäre erst nach Schaffung einer entsprechenden Verordnung durch die zuständige Bezirksregierung vorhanden.

## 18. Bau-, Wohnungs- und Vermessungswesen

### 18.1 Vollständige Kaufverträge an die Gemeinden

Die Landesregierung hat gegen die Übernahme der von mir im XI. TB unter 18.2 beschriebenen "bayerischen Zweistufenlösung" keine grundsätzlichen Bedenken. Nach diesem Vorschlag teilt der Notar einer Gemeinde nicht den gesamten notariellen Kaufvertrag, sondern zunächst nur die für eine Grundentscheidung der Gemeinde notwendigen Fakten mit. Erst wenn die Ausübung eines Vorkaufsrechts in Betracht kommt, erhält die Gemeinde auf Verlangen den vollständigen Inhalt des Kaufvertrages übermittelt. Das Justizministerium hat die Notarkammern und die für die Notarprüfung zuständigen Oberlandesgerichte entsprechend unterrichtet. Auch den Gemeinden wird empfohlen, eine Vorgehensweise entsprechend der beschriebenen "bayerischen Zweistufenlösung" im Interesse des Datenschutzes zu akzeptieren. Nach Auffassung der Landesregierung besteht jedoch keine Möglichkeit, die für die Verkäufer handelnden Notare an die von mir vorgeschlagene Verfahrensweise zu binden.

18.2 Fragebogen zur Führung der Kaufpreissammlung

Viele Grundstückskäufer wundern sich, daß sich - kurz nach Vertragsunterzeichnung - eine Behörde mit einem umfangreichen Fragebogen an sie wendet. Zur Führung der amtlichen Kaufpreissammlung will die Geschäftsstelle des Gutachterausschusses weitere Daten über die gerade erworbene Immobilie und deren Nutzung wissen. Die Erhebung von Daten der Einnahmesituation für Wohnungs-/Teileigentum (Ein- oder Zweifamilienhäuser, Eigentumswohnungen) hat das Niedersächsische Innenministerium damit begründet, daß sich nach den Beobachtungen der Gutachterausschüsse das Marktverhalten in den letzten Jahren nicht unerheblich verändert habe. Das üblicherweise eigengenutzte Einfamilienhaus habe sich, ähnlich wie die Eigentumswohnung, mehr und mehr zu einem Anlage- und somit auch zu einem Renditeobjekt entwickelt. Entsprechend komme der Beurteilung der Einnahmesituation im Falle der Vermietung erhöhte Bedeutung zu, weil zur Wertermittlung nunmehr auch auf das Ertragswertverfahren, das Kenntnis des Mietniveaus und des aus den Kaufpreisen und Mieten abgeleiteten Liegenschaftszinses voraussetzt, zurückgegriffen werden könne. Diese Begründung ist für mich nachvollziehbar.

18.3 Novellierung des Vermessungs- und Katastergesetzes

Das Niedersächsische Vermessungs- und Katastergesetz ist zu novellieren, damit es den Grundsätzen des Volkszählungsurteils entspricht. Zukünftig sollte, wie z.B. in Hamburg und Bremen, der zulässige Umfang der gespeicherten Daten im Gesetz abschließend aufgezählt werden. Auch sollte im Gesetz festgelegt werden, welche Behörden und sonstigen öffentlichen Stellen Daten des Liegenschaftskatasters erheben dürfen. Die vielen Zwecke des Liegenschaftskatasters, die Übermittlungs-, Abruf- sowie die Auskunftsbefugnisse sollten im Gesetz ausdrücklich aufgeführt werden.

Für die seit Jahren praktizierten Übermittlungs- und Abrufverfahren fehlen noch die nach § 12 NDSG vorgeschriebenen Rechtsvorschriften. Allerdings arbeitet das Innenministerium mit "Hochdruck" daran. Entwürfe wurden mit mir abgestimmt.

18.4 Auskünfte aus einem Baulückenverzeichnis

Ich mußte den Elan einer Gemeinde bremsen, die ein Baulückenverzeichnis mit Angaben über Grundstückseigentümer erstellen und hieraus Bauinteressenten, Bauwilligen und Maklern Auskünfte erteilen wollte. Ein solches Vorgehen ist nicht so ohne weiteres möglich. Rechtsgrundlage für entsprechende Auskünfte ist § 13 NDSG, weil es hierfür keine bereichsspezifischen Regelungen gibt. Die Voraussetzungen des § 13 Abs. 1 Satz 1 Nr. 3 NDSG dürften zwar erfüllt sein. Vor einer Datenübermittlung sind die betroffenen Grundstückseigentümer jedoch über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise und rechtzeitig zu unterrichten sowie auf ihr Widerspruchsrecht hinzu-

weisen. Eine solche Unterrichtung könnte nach Aufnahme der Betroffenen in das Baulückenverzeichnis durch ein entsprechendes Anschreiben erfolgen.

## 19. Finanzverwaltung

### 19.1. Die Abgabenordnung - noch immer ohne Datenschutzregelungen

Seit 1988 versuchen die Datenschutzbeauftragten des Bundes und der Länder das Bundesministerium der Finanzen zur Aufnahme datenschutzrechtlicher Regelungen in die Abgabenordnung (AO) zu bewegen (vgl. XI 19.1). Anders als im Vorentwurf zielt der jetzt vorliegende Entwurf (AOÄG 1994) nicht mehr darauf ab, bereichsspezifische Datenschutzvorschriften für den Bereich der AO festzuschreiben. Begründet wird dies u.a. damit, daß schon einige Regelungen in das Gesetz zur Bekämpfung des Mißbrauchs und zur Bereinigung des Steuerrechts (StMBG) übernommen worden seien. Ich vertrete weiterhin die Ansicht, daß die Abgabenordnung um detaillierte bereichsspezifische Regelungen zum Datenschutz zu ergänzen ist. Das Niedersächsische Finanzministerium teilt meine Rechtsauffassung und versprach, mich zu unterstützen.

### 19.2 Verordnungen über Kontrollmitteilungen und Steuerdaten-Abruf

Die seit Jahren von den Datenschutzbeauftragten geforderte Rechtsverordnung zu § 93a AO, nach der die Behörden verpflichtet werden sollen, Kontrollmitteilungen abzugeben, ist endlich am 7. September 1993 (BGBl. I S. 1554) erlassen worden (IX 19.3; X 19.2; XI 19.2). Danach fallen Sozialdaten nicht unter die Übermittlungspflicht. Eine Mitteilung hat nur zu erfolgen, wenn - mit Ausnahme wiederkehrender Zahlungen - die an denselben Empfänger geleisteten Zahlungen 3.000 DM im Kalenderjahr erreichen. Die mitteilungspflichtige Behörde hat den Betroffenen spätestens bei Übersendung der ersten Kontrollmitteilung über ihre Verpflichtung, Kontrollmitteilungen zu erstellen, zu unterrichten.

Auch die Beratungen über die Steuerdaten-Abruf-Verordnung wurden abgeschlossen. Im Hinblick darauf, daß § 30 Abs. 6 AO als Rechtsgrundlage für die Zulässigkeit von automatisierten Abrufen durch die Rechnungsprüfungsbehörden nicht ausreicht, soll eine Änderung der AO erfolgen. Die Rechnungsprüfung soll Verfahren i.S.d. § 30 Abs. 2 Nr. 1a und b gleichgestellt werden. Im Verordnungsentwurf erhalten die Rechnungsprüfungsbehörden die Möglichkeit, Amtsträger, soweit sie mit der Rechnungsprüfung bei den Finanzämtern beauftragt sind, zum automatisierten Abruf von Steuerdaten zu ermächtigen.

19.3 Datenerhebung durch die Finanzämter

In einer Vielzahl von Eingaben beschwerten sich Bürgerinnen und Bürger über die Datenerhebung durch die Finanzämter. In Gesprächen mit dem Niedersächsischen Finanzministerium konnte ich in vielen Fällen den Petentinnen und Petenten helfen und durch eine Änderung der Verfahrensvorschriften Fortschritte für den Datenschutz erzielen:

- So wurde die Niedersächsische Geschäftsordnung für die Finanzämter in Bezug auf den Verbleib der Spendenbelege geändert. Auch die AO-Referatsleiter stellten fest, daß es für den dauernden Verbleib von Original-Spendenbelegen der Steuerpflichtigen bei den Steuerakten keine Rechtsgrundlage gibt. Solche Belege sind daher in jedem Fall nach abschließender Überprüfung an die Steuerpflichtigen zurückzusenden.
- Bei Vordrucken dürfen nur Tatsachen abgefragt werden, die steuerlich relevant sind. Es dürfen keine Daten erhoben werden, die Angaben über andere Personen enthalten. So können Aufwendungen für Fachliteratur bei einer Lehrerin oder einem Lehrer als Werbungskosten anerkannt werden, wenn diese ausschließlich oder weitaus überwiegend beruflich genutzt werden. Die berufliche Nutzung kann dadurch nachgewiesen werden, daß angegeben wird, welche Zeitschrift bzw. welches Buch in welcher Zeit in welcher Klasse zu Unterrichtszwecken benutzt wurde. Auf die Vorlage von Auszügen aus Klassenbüchern wird im allgemeinen verzichtet. Sollte im Einzelfall eine Nachweisführung durch Kopien aus dem Klassenbuch erforderlich sein, sind die personenbezogenen Daten anderer Personen unkenntlich zu machen. Alternativ wäre eine Vorlage der Unterrichtspläne o.ä. möglich.
- Ich konnte mich mit meiner Meinung durchsetzen, daß eine Angabe des genauen Heiratsdatums in der Einkommensteuererklärung nicht erforderlich ist. Das Finanzministerium will die Angelegenheit im Rahmen der Vordruckarbeiten für die Einkommensteuererklärungen 1994 nochmals aufgreifen.
- Bei dem derzeitigen Verfahren zur Beantragung einer Wohnungsbauprämie muß die Bausparerin bzw. der Bausparer gegenüber der Bausparkasse eine Anzahl von Steuerdaten offenbaren, die dort für die Bescheinigung der prämienbegünstigten Aufwendungen nicht benötigt werden. Ich habe vorgeschlagen, daß die steuerlichen Angaben der Bausparerinnen und Bausparer im Rahmen der Einkommensteuererklärung ausschließlich beim Finanzamt nachzuweisen sind, und einen geänderten Verfahrensvorschlag unterbreitet. Das Niedersächsische Finanzministerium meint, daß mein Änderungsvorschlag zu einer erheblichen Mehrbelastung der Finanzämter führen würde. Das Bundesministerium der Finanzen will hierzu die Länder hören und dann entscheiden.

19.4 Verwertung von beschlagnahmten oder gepfändeten EDV-Systemen

Die Pfändung sowie die Sicherungsübereignung von EDV-Systemen stellen dann ein Datenschutzproblem dar, wenn darauf personenbezogene Daten gespeichert sind. Die Datenschutzbeauftragten fordern ihre Löschung. Die

Beschlagnahme findet ihre Grundlage in den §§ 281 ff. AO. Damit sind die auf den Systemen einschließlich der dazugehörigen Datenträger befindlichen personenbezogenen Daten in einem Verwaltungsverfahren in Steuersachen gewonnen worden und unter den Schutz des Steuergeheimnisses nach § 30 AO gestellt. Die Löschung aller personenbezogenen Daten vor einer wirtschaftlichen Verwertung beschlagnahmter Computer und der dazugehörigen Datenträger ist also gesetzlich geboten (vgl. 31.12.2).

## 20. Sozialwesen

### 20.1 Offenbarung von Vorerkrankungszeiten gegenüber den Trägern der gesetzlichen Unfallversicherung

Die Träger der gesetzlichen Unfallversicherung verlangen häufig von den Krankenkassen Angaben über alle Erkrankungen der Versicherten.

Gemäß § 1502 Reichsversicherungsordnung (RVO) kann ein Träger der Unfallversicherung jederzeit von der Krankenkasse Auskunft über die Behandlung und den Zustand des Verletzten verlangen. Die Krankenkasse ist zur Auskunft verpflichtet (§ 1502 Abs. 2). Um die Auskunft von vornherein auf den erforderlichen Umfang zu beschränken, ist der Unfallversicherungsträger gehalten, den Zeitraum und die Art der Vorerkrankungen in seinem Auskunftsersuchen so weit wie möglich zu präzisieren. Mit dem Niedersächsischen Sozialministerium und dem Hauptverband der gewerblichen Berufsgenossenschaften bin ich der Auffassung, daß zudem von der Krankenkasse vor einer Offenbarung an die Träger der Unfallversicherung eine überschlägige Überprüfung der zu übermittelnden Angaben unter dem Gesichtspunkt der Erforderlichkeit durchzuführen ist. Eine vertiefte Prüfung durch den ersuchten Leistungsträger kann nur im Zweifelsfall in Betracht kommen, zumal von den Sachbearbeiterinnen und Sachbearbeitern der Krankenkassen und des Unfallversicherungsträgers fachärztliche Kenntnisse bei der Bestimmung des Auskunftsersuchens nicht erwartet werden können. Erst der vom Unfallversicherungsträger eingeschaltete medizinische Gutachter wird im Einzelfall klären können, ob und ggf. welche Vorerkrankungen für die Klärung von Zusammenhangsfragen oder die Gewinnung von Anhaltspunkten für die zu treffende Feststellung der Minderung der Erwerbsfähigkeit von Bedeutung sind.

### 20.2 Akteneinsicht von Rentenausschußmitgliedern

Im Bereich der gesetzlichen Unfallversicherung sind die Leistungen durch schriftlichen Bescheid festzustellen. Der nach den entsprechenden Vorschriften der RVO bzw. des SGB IV bestellte Rentenausschuß hat in bestimmten Fällen einen förmlichen Bescheid zu erteilen. Der bei fast allen Unfallversicherungsträgern gebildete Rentenausschuß besteht in der Regel je aus einem Vertreter der Versicherten und der Arbeitgeber. Es hat sich die

Frage gestellt, ob die Mitglieder des Rentenausschusses Einsicht in die Unfallakten erhalten dürfen.

Ich halte eine Einsicht der Ausschußmitglieder in Unfallakten zur Wahrnehmung dieser Aufgabe für zulässig. Die Ausschußmitglieder können ihr Amt nur dann ordnungsgemäß wahrnehmen, wenn sie die erforderlichen Informationen erhalten. Deshalb geht § 63 Abs. 3a i.V.m. § 36a Abs. 1 Satz 1 Nr. 2 SGB IV davon aus, daß im Rahmen der Vorbereitung einer Beratung personenbezogene Daten an Ausschußmitglieder weitergegeben werden dürfen. Diese Datenweitergabe kann nicht auf mündliche oder schriftliche Informationen durch Bedienstete des Unfallversicherungsträgers beschränkt werden. Um ihrer Verantwortung gerecht werden zu können, müssen die Ausschußmitglieder vielmehr auch die Möglichkeit haben, die einschlägigen Unfallakten einzusehen, soweit dies für die Entscheidungsfindung erforderlich ist. Hinsichtlich des Erforderlichkeitskriteriums besteht zunächst eine Beurteilungsprärogative für die Ausschußmitglieder.

Soweit die Akteneinsicht im Einzelfall unvermeidbar dazu führt, daß ein Ausschußmitglied auch solche personenbezogenen Daten zur Kenntnis nimmt, die er für die konkrete Entscheidung nicht benötigt, muß dies hingenommen werden. Bei einer Weitergabe von Daten in Akten läßt sich der das Datenschutzrecht beherrschende Erforderlichkeitsgrundsatz nicht lückenlos einhalten. Die allgemeinen Datenschutzgesetze des Bundes und der Länder tragen deshalb den besonderen Umständen bei der Übermittlung/Weitergabe von in Akten gespeicherten Daten durch entsprechende Regelungen Rechnung. Diese Besonderheiten können auch hier nicht außer acht gelassen werden. Die Akteneinsicht hat in den Diensträumen zu erfolgen (vgl. § 29 Abs. 3 Satz 1 VwVfG).

20.3 Weiterleitung von Kindererziehungsleistungen an Heimbewohner

In Erfüllung der Verpflichtung nach § 297 Abs. 3 SGB VI bedienen sich die Sozialhilfeträger in der Regel der Altersheime als Auszahlungsstelle für die Leistungen für Kindererziehung. Diese Verfahrensweise ist in datenschutzrechtlicher Hinsicht, aber auch wegen der Versuche von Heimen, diese Leistungen mit eigenen Forderungen aufzurechnen, auf Kritik gestoßen.

Das Niedersächsische Sozialministerium hat dazu auf folgendes hingewiesen: Sofern Leistungen für Kindererziehung Bestandteil von Rentenzahlungen sind, ist § 297 Abs. 3 SGB VI einschlägig. Hiernach erhält der für die Heimunterbringung aufkommende Sozialhilfeträger die Kindererziehungsleistung gemeinsam mit der Rente überwiesen. Der Sozialhilfeträger ist verpflichtet, die auf die Kindererziehung entfallende Leistung den anspruchsberechtigten Müttern ungekürzt auszuzahlen. Erfahrungsgemäß gehen die Sozialhilfeträger vermehrt dazu über, die gesamte Rente direkt auf ein Konto des betreffenden Heimes überweisen zu lassen. Der zuständige Rentenversicherungsträger sieht in derartigen Fällen einen Erstattungsanspruch des Sozialhilfeträgers nach § 104 Abs. 1 Satz 4 SGB X weiterhin als gegeben an, so daß auch die Leistung für Kindererziehung zusammen mit der Rente an

das Altersheim ausgezahlt wird. Der Sozialhilfeträger hat hierbei dafür Sorge zu tragen, daß das betreffende Altenheim den auf die Kindererziehung entfallenden Leistungsanteil der anspruchsberechtigten Bewohnerin auszahlt. Diese Verfahrensweise hat in der Praxis bisher zu keinerlei Problemen geführt, so daß aus der Sicht der Rentenversicherungsträger diesbezüglich kein Änderungsbedarf besteht. Sofern jedoch eine auf Kosten des Sozialhilfeträgers im Heim untergebrachte Mutter gesonderte Überweisung der Leistung für Kindererziehung auf ein eigenes Konto wünscht, wird dem seitens des Rentenversicherungsträgers Rechnung getragen. Eine getrennte Auszahlung der Kindererziehungsleistung verursacht eine erhebliche Mehrarbeit, weil eine automatisierte Abwicklung vorerst nicht zu realisieren ist. Derartige Fälle bleiben von der alljährlichen Rentenanpassung durch die Deutsche Bundespost ausgenommen. Die Kindererziehungsleistung müßte daher alljährlich manuell angepaßt werden, so daß eine termingerechte Anpassung der Leistung kaum möglich ist. Die aus Anlaß der Auszahlung von Kindererziehungsleistungen durch die Träger der Sozialhilfe vorgenommene Offenbarung von Sozialdaten ist auf der Grundlage des § 69 Abs. 1 Nr. 1 SGB X zulässig.

20.4 Angabe von Heilstätten gegenüber Arbeitgebern

Im Rahmen eines von den Rentenversicherungsträgern praktizierten Verfahrens erhält ein Arbeitnehmer, wenn ihm eine Kur bewilligt wird, zunächst eine allgemeine Bestätigung hierüber, die zugleich eine "Bescheinigung für den Arbeitgeber gemäß § 7 Abs. 2 Lohnfortzahlungsgesetz" darstellt. Den exakten Beginn der Kur und den Entlassungstag teilt der Arbeitnehmer seinem Arbeitgeber unter Vorlage des Einberufungsschreibens bzw. der Entlassungsmitteilung der Behandlungsstätte mit.

Hiergegen hatte ich datenschutzrechtliche Bedenken, da erfahrene Personalsachbearbeiter anhand der Behandlungsstätte und teilweise sogar allein aufgrund des Behandlungsortes auf die Art der zu behandelnden Erkrankung schließen können. Mit diesem Problem hat sich eine Arbeitsgruppe des Verbandes deutscher Rentenversicherungsträger intensiv beschäftigt. Als Ergebnis ist festzustellen, daß der Verband deutscher Rentenversicherungsträger empfiehlt, die Rehabilitationseinrichtungen darüber zu unterrichten, daß Versicherte auf ihren Wunsch auch Bescheinigungen über Beginn und Ende der stationären Heilbehandlung erhalten können, ohne daß die Art der Behandlungseinrichtung durch deren Briefkopf oder Stempel ersichtlich ist.

20.5 Auskünfte aus den örtlichen Fahrzeugregistern für die Überprüfung der Sozialhilfe

Durch das Gesetz zur Umsetzung des föderalen Konsolidierungsprogramms ist § 117 in das Bundessozialhilfegesetz (BSHG) aufgenommen worden. Absatz 3 der Vorschrift gibt den Trägern der Sozialhilfe die Möglichkeit, zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe bei den Kraftfahrzeugzulassungsstellen nachzufragen, ob für einen Hilfeempfänger

ein Kraftfahrzeug zugelassen worden ist. Das Niedersächsische Ministerium für Wirtschaft, Technologie und Verkehr hat hierzu mit Erlaß an die Kfz-Zulassungsstellen klargestellt, daß bei Auskünften gegenüber Sozialämtern weitere Angaben, z.B. über das Fahrzeug oder andere im Zusammenhang mit der Zulassung erhobene Daten, nicht gemacht werden dürfen. Darüber hinaus erhob sich die Frage, ob ein regelmäßiger automatisierter Datenabgleich durch die Bestimmung gedeckt wird. Hierzu vertrete ich gemeinsam mit dem Niedersächsischen Sozialministerium die Auffassung, daß nur in § 117 Abs. 1 und 2 BSHG ein regelmäßiger automatisierter Datenabgleich als Weg der Überprüfung des Bezuges von Leistungen von den dort genannten Stellen vorgesehen ist. § 117 Abs. 3 BSHG erwähnt dagegen den automatisierten Datenabgleich nicht; er kann daher für die dort genannten Überprüfungen von Daten nicht verwendet werden. Die Überprüfung eines Hilfeempfängers als Kraftfahrzeughalter bei den Kraftfahrzeugzulassungsstellen ist nach § 117 Abs. 3 Satz 1 BSHG nur zulässig, soweit diese Daten für die Erfüllung der Aufgaben der Sozialhilfegewährung erforderlich sind. Bei der Erforderlichkeitsprüfung einer Datenrecherche bei anderen Stellen und Unternehmen sind Datenschutzüberlegungen und die §§ 60 ff. SGB I mit zu berücksichtigen. Es ist jeweils eine Einzelfallprüfung vorzunehmen, Sammel- und Gruppenverfahren sind nicht zulässig. Bei der vorzunehmenden Einzelfallprüfung gelten demzufolge die Vorschriften des § 69 SGB X, d.h. auch der Vorrang der Erhebung beim Betroffenen und die Notwendigkeit eines Anlasses im Einzelfall. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit diesen Fragestellungen beschäftigt. Insofern verweise ich auf die Anlagen 2 und 12.

20.6 Fragenbogen zur Überprüfung der Einkommens- und Vermögensverhältnisse des Unterhaltspflichtigen

Nach § 116 Abs. 1 BSHG müssen die Unterhaltspflichtigen dem Träger der Sozialhilfe über ihre Einkommens- und Vermögensverhältnisse Auskunft geben, soweit die Durchführung des BSHG es erfordert. Leben Kinder oder sonstige Angehörige im Haushalt des Unterhaltspflichtigen, so ist zu prüfen, ob für diese Personen ein Mietanteil anzurechnen ist oder sie einen vorrangigen Unterhaltsanspruch gegen den Unterhaltspflichtigen haben. Insoweit ist es für das Sozialamt wichtig zu erfahren, welche Personen noch im Haushalt des Unterhaltspflichtigen leben, wie alt sie sind, in welchem Verwandtschaftsverhältnis sie zum Unterhaltspflichtigen stehen, welchen Familienstand sie haben und wie hoch ihr Einkommen und Vermögen ist. Die auf den Unterhaltspflichtigen entfallenden Kosten der Unterkunft sowie seine sonstigen Verpflichtungen wirken sich auf die Höhe des zu fordernden Unterhaltsbetrages aus, so daß das Sozialamt auch hierüber Angaben und Unterlagen benötigt, um den Unterhaltsbetrag sachgerecht errechnen zu können. § 116 Abs. 1 BSHG verbietet es den Sozialhilfeträgern nicht, die Unterhaltspflichtigen um weitergehende Auskünfte zu bitten. Soweit diese Auskünfte erforderlich sind, um den ggf. zu fordernden Unterhaltsbetrag in sachgerechter Weise ermitteln zu können, verstößt dies nicht gegen gesetzliche Vorschriften. Während der Unterhaltspflichtige die in § 116 Abs. 1 genannten Angaben machen muß, kann er jedoch die Erteilung weitergehender

Auskünfte verweigern und die sich dadurch für ihn ergebenden nachteiligen Folgen in Kauf nehmen. Sein Recht auf informationelle Selbstbestimmung wird hierdurch nicht verletzt. Das Niedersächsische Sozialministerium hat mit Erlaß vom 8. September 1993 an die örtlichen Sozialhilfeträger festgelegt, daß in dem Fragebogen oder einem dazugehörigen Anschreiben auf die Freiwilligkeit der Beantwortung von Fragen aufmerksam gemacht werden muß, die über die Auskunftspflicht nach § 116 Abs. 1 BSHG hinausgehen. Ein entsprechender Hinweis sollte dabei auch auf die möglicherweise nachteiligen Folgen einer Verweigerung weitergehender Auskünfte eingehen.

20.7 Überprüfungsbogen "Wohn- und Wirtschaftsgemeinschaft/eheähnliche Gemeinschaft"

Derartige Überprüfungsbogen werden sowohl beim Wohngeld als auch in der Sozialhilfe verwendet. Nach dem Wohngeldgesetz kann Wohngeld nur dann einheitlich für einen Haushalt gewährt werden, wenn dieser aus Familienmitgliedern besteht. Besteht ein Haushalt nicht nur aus Familienmitgliedern (Haushaltsvorstand, Ehegatte, Verwandte und Verschwägerte bis zu einem gesetzlich bestimmten Grade und Pflegekinder), so ist zu prüfen, ob eine "Wohn- und Wirtschaftsgemeinschaft" (§ 18 Abs. 2 Nr. 2 Wohngeldgesetz) vorliegt. Im Hinblick auf Art. 6 GG soll damit sichergestellt werden, daß antragsberechtigte Personen in einer Wohn- und Wirtschaftsgemeinschaft nicht besser gestellt werden als solche in einem Familienhaushalt entsprechender Größe. Wenn die oder der Antragsberechtigte und die Nichtfamilienmitglieder Wohnraum gemeinsam bewohnen, wird das Bestehen einer Wirtschaftsgemeinschaft gesetzlich vermutet. Insofern ist die Erhebung dieser Daten zur Aufgabenerfüllung der Wohngeldstelle erforderlich.

Nach § 20 SGB X ermittelt die Behörde den Sachverhalt von Amts wegen. Sie bedient sich dabei der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält (§ 21 SGB X). Die bloße Behauptung des Antragstellers, eine Wohn- und Wirtschaftsgemeinschaft liege nicht vor, reicht nicht aus, die vorgenannte gesetzliche Vermutung auszuräumen. Um die Feststellungen über das Vorliegen bzw. Nichtvorliegen einer Wohn- und Wirtschaftsgemeinschaft treffen zu können, bedarf es in der Regel eines ausführlichen Gesprächs bzw. einer Befragung. Wenn hierbei aus verwaltungsökonomischen Gründen auch Fragebogen herangezogen werden, bestehen aus wohngeldrechtlicher Sicht dagegen keine Bedenken. Das gleiche gilt gemäß § 122 BSHG für die Sozialhilfe.

Hinsichtlich des Inhalts dieser Fragebogen halte ich jedoch bestimmte Fragen für überzogen. So wollen Kommunen manchmal z.B. wissen, wer die Räume pflegt, wie Lebensmittel eingekauft und wie sie aufbewahrt werden, wer die Wäsche bügelt und wer sie in die Schränke sortiert. Abgesehen davon, daß die Richtigkeit entsprechender Angaben von der Behörde wohl kaum überprüft werden kann, müssen sich hier Zweifel aufdrängen, daß solche Angaben zur Prüfung des Wohngeldanspruchs erforderlich sind. Daß Fragen zu geschlechtlichen Beziehungen zwischen Antragsteller und Mitbe-

wohner nicht gestellt werden dürfen, sollte im Hinblick auf den Schutz der Intimsphäre selbstverständlich sein. Das Bundesverfassungsgericht hat im übrigen in einer Entscheidung (BVerfGE 87, 234) zur eheähnlichen Gemeinschaft im Sinne des Arbeitsförderungsgesetzes betont, daß die Annahme einer "eheähnlichen" Gemeinschaft nicht die Feststellung voraussetzt, daß zwischen den Partnern geschlechtliche Beziehungen bestehen.

20.8 Landeskrankenhäuser sollen über ehemalige Sozialhilfeempfänger berichten

Einige örtliche Sozialhilfeträger im Einzugsbereich der Landeskrankenhäuser begehren die Meldung aller Patienten, die vor ihrem stationären Krankenhausaufenthalt Sozialhilfeleistungen erhielten. Die Sozialhilfeträger berufen sich dabei auf die Vorschrift des § 69 Abs. 1 Ziffer 1 SGB X. Hierzu stelle ich fest, daß § 69 SGB X nur anwendbar wäre, wenn Daten von den Leistungsträgern, d.h. den örtlichen Sozialhilfeträgern, an die Landeskrankenhäuser übermittelt würden. Hier soll der Datenfluß jedoch umgekehrt erfolgen. Die Landeskrankenhäuser sind keine in § 35 i.V.m. §§ 18 bis 29 SGB I genannten Sozialleistungsträger. Anderweitige Zulässigkeitsvorschriften sind nicht ersichtlich, so daß § 60 Abs. 1 Nr. 1 SGB I zum Tragen kommt. Danach ist ein Sozialleistungsempfänger verpflichtet, alle Tatsachen anzugeben, die für die Leistung erheblich sind, und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen. Es muß demnach bei einer Anfrage durch einen örtlichen Sozialleistungsträger die Einwilligung zur Übermittlung von personenbezogenen Daten durch die Landeskrankenhäuser beim Betroffenen eingeholt werden.

20.9 Arztbriefe für Sozialämter

Im Kostenübernahmeverfahren der Sozialämter bei stationärem Aufenthalt von Patienten in den Landeskrankenhäusern verlangen die Kommunen vor der Hilfegewährung häufig Arztbriefe, die detaillierte personenbezogene Daten enthalten. Diese Informationen gelangen, wie mir mitgeteilt worden ist, nicht an die Mediziner im Gesundheitsamt des örtlichen Sozialhilfeträgers, sondern unmittelbar an die Sachbearbeiterin bzw. den Sachbearbeiter des Sozialamtes. Dies kann soweit gerechtfertigt werden, als die medizinischen Voraussetzungen für die Behandlungsbedürftigkeit im Krankenhaus ärztlich bescheinigt werden müssen. Das Niedersächsische Sozialministerium weist allerdings darauf hin, daß für die Entscheidung des örtlichen Trägers eine auf die notwendigen Angaben beschränkte ärztliche Stellungnahme, die keine detaillierten medizinischen Befunde enthält, ausreicht. Dieser Auffassung ist zuzustimmen. Im Einzelfall mag es allerdings gelegentlich zweifelhaft sein, wie weit die ärztliche Begründungspflicht geht. In einem solchen Fall empfiehlt es sich, die Einwilligung des Betroffenen einzuholen.

20.10 Pauschale Einwilligungserklärungen oder: Ist es auch Unsinn, hat es doch Methode

Auch heute noch beschweren sich Petenten bei mir wegen pauschaler "Einwilligungserklärungen" in Sozialhilfeantragsformularen. Das Problem habe ich bereits unter IX 20.2 umfassend dargestellt. Wie schwer es offenbar in der Praxis einigen Sozialamtsbedienstete noch immer fällt, sich auch in diesem Punkt datenschutzgerecht (und rechtmäßig) zu verhalten, zeigt das Beispiel eines Landkreises. Auf meine Frage, warum er von Antragstellerinnen und Antragstellern eine pauschale, völlig unklare Einwilligungserklärung verlange, antwortete er mir: "Ich gehe davon aus, daß auch Ihnen bekannt ist, daß der von mir bislang verwendeten pauschalen Einwilligungserklärung letztlich keine praktische Bedeutung mehr zukommt, weil in Einzelfällen konkrete spezifizierte Erklärungen notwendig sind, um die erforderlichen Auskünfte zu erhalten." In diesem wie in anderen Fällen habe ich die Verwendung pauschaler Einwilligungserklärungen beanstandet.

20.11 Räumliche Verhältnisse gefährden das Sozialgeheimnis

Die räumlichen Verhältnisse in Sozialämtern, wo z.T. zwei Bedienstete in einem Büro sitzen und Beratungen durchführen oder wo die Verbindungstüren zwischen den Zimmern der einzelnen Bediensteten offen stehen, können das Sozialgeheimnis gefährden. Bei den Beratungsgesprächen können Hilfesuchende personenbezogene Daten anderer Personen erfahren. Die Begründung, daß die Türen offen stehen sollen, wird mit gelegentlichen Angriffen auf Sachbearbeiterinnen und Sachbearbeitern bzw. massiven Bedrohungen gegenüber diesen gerechtfertigt. In diesem Zusammenhang muß geprüft werden, welche anderen Sicherheitsvorkehrungen getroffen werden können, so daß in Zukunft die Verbindungstüren möglichst geschlossen gehalten werden können. In Betracht kommt der Einbau von Alarmanlagen, mit denen bedrohte Bedienstete Hilfe durch ihre Kolleginnen und Kollegen herbeiholen können. Eine weitere Möglichkeit besteht darin, daß - wenn mehrere Sachbearbeiter in einem Büro sitzen - dem Hilfesuchenden die Möglichkeit eröffnet wird, in einem separaten Büro beraten zu werden.

20.12 Weitergabe von personenbezogenen Daten vom Versorgungsamt an die Straßenverkehrsbehörde zum Zwecke der Überprüfung der Eignung zum Führen von Kraftfahrzeugen

Dürfen Sozialdaten im Einzelfall ohne eine ausdrückliche Befugnis zur Offenbarung im SGB X, gestützt auf den "übergesetzlichen" rechtfertigenden Notstand i.S. des § 34 Strafgesetzbuch (StGB), an die Straßenverkehrsbehörden zur Wahrung eindeutig höherwertiger Rechtsgüter weitergegeben werden? Ich neige der Auffassung zu, daß der Gesetzgeber in §§ 67 ff. SGB X die aus seiner Sicht notwendigen Durchbrechungen des Sozialgeheimnisses abschließend regeln wollte. Darauf weist der Gesetzeswortlaut (§ 35 Abs. 2 SGB I, § 67 Satz 1 SGB X) ausdrücklich hin. Auch aus dem Enumerationsprinzip, das diesen Regelungen zugrunde liegt, ergibt sich das

Ziel der Gesetzgebung, einen Numerus clausus der Offenbarungsbefugnisse zu schaffen. Dieser gesetzliche Ansatz würde grundlegend in Frage gestellt, wenn andere als die vom Gesetzgeber vorgenommenen Interessenabwägungen zum Schutz höherwertiger Rechtsgüter ohne weiteres eine Offenbarung nach § 34 StGB zulassen würden. Hinzukommt, daß diese Vorschrift für den Bürger nicht normenklar erkennen läßt, unter welchen Voraussetzungen in sein Grundrecht auf Datenschutz eingegriffen werden darf. Der Einwand, die unter § 34 StGB zu subsumierenden Fallkonstellationen seien dem Gesetzgeber über § 69 Abs. 1 Nr. 1 und § 71 Abs. 1 Satz 1 Nrn. 1 und 2 SGB X hinaus nicht mehr regelbar erschienen, überzeugt nicht. Das Zweite Gesetz zur Änderung des Sozialgesetzbuches regelt in § 68 SGB X, daß personenbezogene Daten zu Zwecken der Gefahrenabwehr an die Gefahrenabwehrbehörden übermittelt werden dürfen. Diese Regelung bekräftigt einerseits das Enumerationsprinzip der Offenbarungsbefugnisse und macht andererseits deutlich, daß eine konkrete Regelung entsprechender Probleme durchaus möglich ist. Ich halte es für unerläßlich, eine solche Regelung auch für die angesprochenen Fallkonstellationen zu schaffen. Wenn die Absicht des Gesetzgebers erkennbar wird, eine entsprechende Ergänzung des SGB X vorzunehmen, halte ich es für hinnehmbar, in der Übergangszeit bis zum Inkrafttreten der Gesetzesänderung im Rahmen des unbedingt Erforderlichen zur Abwehr einer drohenden Gefährdung des Lebens oder einer schweren Gesundheitsgefährdung von Verkehrsteilnehmern nach dem Rechtsgedanken des § 34 StGB eine Datenübermittlung an Straßenverkehrsbehörden zuzulassen.

### 20.13 Krankenversichertenkarte

Ab 1. Oktober 1994 gibt es auch in Niedersachsen die computerlesbare Krankenversichertenkarte. Der Gesetzgeber hat in § 291 SGB V den Inhalt dieser Karte abschließend festgelegt (vgl. XI 20.1). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Sitzung am 9./ 10. März 1994 hierzu einen Beschluß gefaßt (Anlage 10).

### 20.14 Werbung durch Krankenkassen

In mehreren Fällen hatten Arbeitgeber die personenbezogenen Daten ihrer Auszubildenden an Krankenkassen übermittelt, ohne daß eine Einverständniserklärung der Betroffenen für diese Datenübermittlung vorlag.

Das Bundesministerium für Arbeit und Sozialordnung hat bereits im Jahre 1987 darauf hingewiesen, daß eine Krankenkasse Adressenmaterial für Aufklärung und Werbung nicht verwenden darf, wenn die Möglichkeit besteht, daß es unter Verstoß von Datenschutzbestimmungen erlangt oder weitergegeben wurde. Ist der Übersender einer Adresse ein Arbeitgeber oder ein zur Verschwiegenheit über Personaldaten Verpflichteter, hat die Krankenkasse deshalb vor einer Werbung stets die Erklärung der Übersenders einzuholen, daß der Arbeitnehmer schriftlich in die Verwendung seiner Daten zu Werbezwecken der Krankenkassen eingewilligt hat. Die Übermittlung

der Daten vom Arbeitgeber an die Krankenkasse ist gemäß § 28 BDSG nur mit Einwilligung der Betroffenen statthaft.

In den betreffenden Fällen berief sich die Krankenkasse auf § 13 SGB I und § 284 Abs. 1 SGB V. Auf diese Vorschriften kann sich die Krankenkasse jedoch nicht stützen. § 13 SGB I hat zum Inhalt, daß die Bevölkerung über die Rechte und Pflichten nach dem Sozialgesetzbuch aufgeklärt wird. Die Vorschrift wendet sich dem Wortlaut nach an einen unbestimmten Adressatenkreis (Bevölkerung), der in allgemeiner Form aufgeklärt werden soll. Dabei geht es grundsätzlich nicht um eine individuelle Beratung im Einzelfall. Darüber hinaus dürfen Krankenkassen personenbezogene Daten nur dann erheben und speichern, soweit dies für bestimmte, im einzelnen in § 284 Abs. 1 SGB V aufgeführte Zwecke erforderlich ist. Die Mitgliederwerbung ist dort aber als die Speicherung rechtfertigender Zweck nicht erwähnt. Auch § 284 Abs. 1 Nr. 1 SGB V, der eine Erhebung und Speicherung von personenbezogenen Daten durch Krankenkassen zuläßt, soweit dies für die Feststellung des Versicherungsverhältnisses und der Mitgliedschaft erforderlich ist, rechtfertigt diese Praxis nicht. Diese Bestimmung läßt eine Datenerhebung und -speicherung nur zu, wenn das Versicherungsverhältnis bereits besteht oder gerade begründet wird, wobei die Daten dann in das von der Krankenkasse zu führende Versichertenverzeichnis aufzunehmen sind. Schließlich findet auch der von einem Landesverband angeführte § 14 SGB I hier keine Anwendung. Diese Vorschrift setzt voraus, daß sich eine Bürgerin oder ein Bürger an die Krankenkasse wendet und um Beratung nachsucht, was in den vorliegenden Fällen nicht der Fall war. Insofern habe ich festgestellt, daß die Verwendung der von dem Ausbildungsbetrieb ohne Einverständnis der Betroffenen übermittelten Daten durch die Krankenkasse rechtswidrig ist. Ich habe das Niedersächsische Sozialministerium gebeten, insbesondere unter dem Gesichtspunkt der ab 1. Januar 1996 geltenden Wahlfreiheit bei Krankenkassen entsprechende Hinweise für Werbemaßnahmen zu geben.

Des weiteren ergab sich das Problem, ob eine gesetzliche Krankenkasse die Adressen ihrer Mitglieder nutzen darf, um diese im Zusammenhang mit Betriebskrankenkassen-Neugründungen zu beraten. Ich beurteile diese Frage wie folgt:

Das Landesozialgericht (LSG) Baden-Württemberg hat in seinem Beschluß vom 30. August 1989 (L 4 Kr 1430/89 e A) u.a. ausgeführt, daß eine AOK gemäß §§ 13 bis 15 SGB I ihre Mitglieder über die bei der Abstimmung über die Gründung einer Betriebskrankenkasse zu bedenkenden Umstände und die Folgen, die eine solche Gründung haben kann, unterrichten darf. Sie darf dabei jedoch weder irreführende Angaben machen noch ihre Mitglieder unsachgemäß beeinflussen. Unter § 13 SGB I, der die Aufklärung der Bevölkerung über die Rechte und Pflichten nach dem Sozialgesetzbuch regelt, fallen auch alle Mitarbeiterinnen und Mitarbeiter einer Firma, die durch Rundschreiben oder sonstige allgemeine Hinweise aufgeklärt werden sollen. Die Rechtsgrundlage für diese Datenverwendung findet sich in § 284 Abs. 3, 2. Alt. SGB V.

In einem konkreten Fall hatte eine AOK, deren Versicherte z.T. von der Neugründung einer BKK betroffen waren, anderen AOKs die Versichertendaten ohne deren Einverständnis übermittelt und diese gebeten, die Versicherten persönlich über das "Pro und Contra AOK/BKK" zu informieren.

Auch wenn nach dem Urteil des LSG Baden-Württemberg entsprechende Aufklärungsaktionen als Aufgabe einer AOK anzusehen sind, darf eine Offenbarung personenbezogener Daten nach § 69 Abs. 1 Nr. 1 SGB X nur erfolgen, wenn sie zur Aufgabenerfüllung erforderlich ist. Ob eine Verarbeitung personenbezogener Daten erforderlich ist, kann in gewissem Maße auch vom Aufgabenverständis der zuständigen Stelle abhängen. Will sie eine bestimmte Aufgabe besonders nachdrücklich wahrnehmen, so wird die dafür notwendige Datenverarbeitung nicht ohne weiteres mit dem Argument in Zweifel gezogen werden können, daß bei weniger intensiver Aufgabenwahrnehmung personenbezogene Daten nur in geringerem Umfang verarbeitet würden. Das Erforderlichkeitsprinzip wird auch dann nicht verletzt, wenn eine Behörde eine Handlungsalternative (z.B. Anfrage an eine andere als die angesprochene Stelle) hat, die aber nicht zu einer geringeren Belastung für den Betroffenen führt als die gewählte Vorgehensweise. In dem vorliegenden Fall ist es daher der AOK zwar unbenommen, neben oder anstelle von schriftlichen Erläuterungen die Versicherten auch mündlich über die Problematik eines Beitritts zu einer Betriebskrankenkasse aufzuklären. Im Hinblick auf das informationelle Selbstbestimmungsrecht der Betroffenen sind diese Möglichkeiten als gleichwertig anzusehen. Die Einschaltung anderer Ortskrankenkassen im Wege der Amtshilfe führt dagegen zu einer zusätzlichen Offenbarung der Versichertendaten. Die entsprechende AOK hätte ihr Ziel, auch mit den außerhalb ihres Bereichs wohnenden Versicherten Aufklärungsgespräche zu führen, ohne weiteres durch einen entsprechenden Hinweis an die Betroffenen und einen einschlägigen Beratungswunsch erreichen können. Diese Vorgehensweise wäre aus meiner Sicht nicht nur datenschutzgerechter, sondern im Hinblick auf das Erforderlichkeitsprinzip auch notwendig gewesen. Die von der AOK gewählte Praxis genereller Datenübermittlungen an andere AOK zur Amtshilfe durch Werbebesuche geht insofern über das erforderliche Maß hinaus und ist insofern rechtswidrig.

20.15 Auskünfte der Krankenkassen an Arbeitgeber bei möglichen Schadensersatzansprüchen

Durch die Übersendung eines Unfallerhebungsbogens weisen Krankenkassen oftmals Arbeitgeber auf das Vorliegen eines eventuellen Drittverschuldens hin, wenn eine Arbeitnehmerin oder ein Arbeitnehmer einen Körperschaden erlitten hat. Zu dieser Verfahrensweise ist zu bemerken, daß eine gesetzliche Befugnis zu Auskünften der Krankenkassen an Arbeitgeber nicht existiert, weil die Hilfe zur Verwirklichung zivilrechtlicher Schadensersatzansprüche des Arbeitgebers keine soziale Aufgabe der Krankenkassen ist. Deshalb ist eine Unterrichtung des Arbeitgebers nur mit ausdrücklicher Zustimmung der Versicherten zulässig. Mit den Landesverbänden der Krankenkassen ist ein Text für Unfallfragebogen abgestimmt worden. Hierzu ist

besonders zu betonen, daß die Einwilligung auch dann als nicht erteilt gilt, wenn nichts angekreuzt wird. Hierüber werden die Versicherten deutlich aufgeklärt.

20.16 Erhebung von Daten über Mitarbeiter der Leistungserbringer

Die Versicherten gesetzlicher Krankenkassen können Leistungen der häuslichen Krankenpflege, der häuslichen Pflegehilfe, der häuslichen Pflege und der Haushaltshilfe beanspruchen. Ist die Krankenkasse nicht in der Lage, diese Leistung durch eigenes Personal zu erbringen, schließt sie auf der Grundlage des § 132 Abs. 1 SGB V Verträge mit entsprechenden Leistungserbringern. Darin werden Inhalt, Umfang, Vergütung sowie Prüfung der Qualität und der Wirtschaftlichkeit der Dienstleistungen geregelt. Die Träger der gesetzlichen Krankenversicherungen sind hierbei gehalten, die in Betracht kommenden Leistungserbringer nach fachlichen und wirtschaftlichen Gesichtspunkten auszuwählen und dabei insbesondere sicherzustellen, daß eine den Bedürfnissen der Pflegebedürftigen gerechtwerdende, wohnortnahe und qualifizierte Pflegeleistung gewährleistet ist. Damit wird klargestellt, daß nicht die preisgünstigste Möglichkeit der Leistungsgewährung zu wählen ist, sondern im Rahmen des Wirtschaftlichkeitsgebots auch qualitative Gesichtspunkte und berechtigte Interessen der Versicherten zu berücksichtigen sind. Die hier thematisierte Erhebung von Daten der von den Leistungserbringern eingesetzten Pflegepersonen wird von § 284 SGB V als Spezialnorm nicht erfaßt. Anwendbar ist § 79 Abs. 1 und 3 SGB X, über den der zweite Abschnitt des BDSG mit § 13 anwendbar ist. Nach § 13 Abs. 1 BDSG dürfen Daten erhoben werden, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Angesichts des Qualitätssicherungsgebotes i.S. von § 70 Abs. 1 Satz 1 SGB V, dem die Kassen im Rahmen der Gewährung von Leistungen unterliegen, ist das Vorliegen des Tatbestandes des § 13 Abs. 1 BDSG zu bejahen.

Eine weitere Frage ist, ob die betreffenden Angaben auch ohne Mitwirkung der Betroffenen, also des von dem Leistungserbringer eingesetzten Pflegepersonals, erhoben werden dürfen. Diese Frage ist nach § 13 Abs. 2 Nr. 2a BDSG zu bejahen. Die Verträge nach § 132 SGB V werden mit Leistungserbringern abgeschlossen, bei denen es sich in aller Regel um öffentliche oder Verbandseinrichtungen (z.B. Sozialstationen) oder aber um private Einrichtungen (z.B. Pflegedienste) handelt. Die Mitarbeiter, um deren personenbezogene Daten es hier geht, sind Bedienstete dieser Einrichtungen oder ihrer Träger, oder sie sind anderweitig vertraglich an diese gebunden. Schon aus dem entsprechenden Vertragsverhältnis mit ihnen ergibt sich die Notwendigkeit einer entsprechenden Nachweisführung und damit Datenerhebung durch diese Einrichtungen als Vertragspartner der Pflegepersonen. Anhaltspunkte für eine Beeinträchtigung schutzwürdiger Interessen sind auch deshalb nicht zu sehen, weil zuvor bereits ein entsprechender Qualifikationsnachweis der Pflegepersonen gegenüber ihrer Einrichtung zu erbringen war. Die Notwendigkeit, einen entsprechenden Nachweis auch gegenüber der Kasse zu führen, kann nicht anders bewertet werden. Das Ausmaß der rechtlich vertretbaren Nachweispflicht nach den abzuschließenden Ver-

trägen mit den Kassen dürfte sich nach dem Grundsatz vernünftiger Auslegung des Begriffs "Prüfung der Qualität" richten. Es wird den Kassen nicht verwehrt werden können, sich für die Fälle der häuslichen Pflegehilfe bei schwer pflegebedürftigen Versicherten vertraglich auch den Nachweis der Pflegeerfahrung einer eingesetzten Pflegeperson für die Ausübung von Stichprobenkontrollen auszubedingen.

## 21. Gesundheitswesen

Es ist schon fast ein Ritual, daß ich in meinen Tätigkeitsberichten gesetzliche Grundlagen für die Datenverarbeitung im Gesundheitswesen einfordere (vgl. XI 21, X 21, IX 21 usw.). Noch immer werden über einen der sensibelsten Lebensbereiche von unterschiedlichsten Stellen gewaltige Mengen an Daten konventionell und rapide zunehmend auch elektronisch verarbeitet, ohne daß dafür gesetzliche Grundlagen existieren. Ich konnte mich in den letzten beiden Jahren wieder davon überzeugen, daß dieser Mangel dazu führt, daß den im Gesundheitsbereich arbeitenden Menschen oft nicht klar ist, welche Daten sie unter welchen Voraussetzungen verarbeiten und insbesondere übermitteln dürfen. Zwar ist den meisten das Arztgeheimnis als Begriff geläufig. Daß ein Verstoß gegen das Arztgeheimnis strafbar ist (§ 203 StGB), ist auch bekannt. Da aber weitgehend unklar ist, wem Arztgeheimnisse offenbart werden dürfen, und bekannt ist, daß Verstöße praktisch nie strafrechtlich verfolgt und geahndet werden, interpretieren viele die Reichweite des Arztgeheimnisses nach eigenem Gusto. Für eine Strafverfolgung ist ein Strafantrag der Betroffenen erforderlich, der drei Monate nach Kenntniserlangung vom Verstoß gestellt werden muß (§§ 205, 77, 77b StGB). Aus verständlichen Gründen verzichten viele der Betroffenen auf einen solchen Antrag. Offensichtlich wird auch in der medizinischen Ausbildung wenig Wert auf die Vermittlung von Bedeutung und Reichweite des Arzt-Patienten-Geheimnisses gelegt.

Dies hat zur Folge, daß mir im Rahmen meiner Beratungs- und Kontrolltätigkeit am laufenden Band Verstöße bekannt werden, die zumeist nicht auf Böswilligkeit, sondern auf Unkenntnis und Gedankenlosigkeit beruhen. Für die Betroffenen kann dies gravierende Folgen z.B. am Arbeitsplatz, in der Familie, im Bekanntenkreis oder im sonstigen sozialen Umfeld haben. Der Umstand, daß Unbefugte von einer psychischen Krankheit, einer HIV-Infektion, einer Sucht, einer Behinderung usw. erfahren, ist außerdem gewiß nicht förderlich für die Gesundheit der Betroffenen. Bei der Bearbeitung von Einzelfällen erziele ich nur eine beschränkte "pädagogische" Wirkung. Erfreulich war es daher, daß in den letzten zwei Jahren Berufsverbände und Einrichtungen im Gesundheitsbereich verstärkt an mich mit der Bitte um Vorträge zum Thema "Datenschutz und Medizin" herangetreten sind. Bei diesen Vorträgen konnte ich mit vielen Angehörigen von Gesundheitsberufen einen konstruktiven Dialog führen und einer Vielzahl von Vorurteilen gegenüber dem Datenschutz begegnen. Auch aus Sicht der im Gesundheitsbereich Beschäftigten sind gesetzliche Regelungen mehr als überfällig. Der Gesetzgeber steht zudem nicht zuletzt gegenüber kranken Menschen in der

Pflicht, diesen aufzuzeigen, was mit deren medizinischen Daten gemacht werden kann und welche Rechte sie haben.

Im vorliegenden Tätigkeitsbericht muß ich erneut die schlechte Nachricht überbringen, daß trotz der guten Absichten der letzten Regierungskoalition (vgl. XI 21) in der 12. Legislaturperiode des Niedersächsischen Landtags keine Datenschutzgesetze im Gesundheitsbereich verabschiedet worden sind. Allerdings tut sich etwas. Bereichsspezifische Regelungen für den öffentlichen Gesundheitsdienst und für die Psychiatrie sind so weit vorbereitet, daß mit einer baldigen parlamentarischen Behandlung und Verabschiedung der entsprechenden Gesetze zu rechnen ist. Weiterhin Fehlanzeige ist zu vermelden für den Maßregelvollzug und den Krankenhausbereich. Hier kann ich nicht mehr tun, als erneut und mit Nachdruck die nötigen Gesetze einzufordern. Mein Angebot zur konstruktiven Zusammenarbeit ist den verantwortlichen Stellen seit Jahren bekannt.

## 21.1 Gesundheitsdienstgesetz in Sicht ! - mit einer Regelung zu "anonymen Tests"

Ein Lichtblick war es für mich, als mir im September 1993 zur informellen Unterrichtung der Entwurf eines Niedersächsischen Gesundheitsdienstgesetzes (GDG) übersandt wurde. Seitdem hat mich das Niedersächsische Sozialministerium in die Beratungen hierüber in begrüßenswerter Weise einbezogen. Aufgrund meiner Anregung wurde in den Entwurf eine Regelung zur externen Datenverarbeitung (Datenverarbeitung im Auftrag) und zur Forschung aufgenommen. Auch die Auswertung von Todesbescheinigungen für Forschungszwecke wird endlich einer Regelung zugeführt (vgl. XI 21.4 u. 24.3).

Keine Begeisterung auslösen konnte bei mir der Regelungsvorschlag zum AUT. AUT steht für "anonymous unlinked testing". Die geplante Regelung zum AUT erlaubt die anonymisierte Untersuchung von medizinischen Gewebeproben, die aufgrund von Gesetzen, aber auch aufgrund von Einwilligungen erhoben wurden. Hintergrund dieses Regelungsvorschlages ist eine vom Niedersächsischen Sozialministerium für das Jahr 1993 durchgeführte AUT-Testreihe im Rahmen des "Neugeborenen-Screenings" zur Erlangung verbesserter HIV-Daten. Hierbei wurde das Blut, das neugeborenen Kindern mit Einwilligung der Eltern abgenommen wurde, auf Stoffwechselerkrankungen untersucht. Die Eltern hatten bei Erteilung ihrer Einwilligung keine Ahnung, daß die Blutproben nach Anonymisierung auch auf AIDS untersucht werden. Dieses Vorgehen wurde damit begründet, daß viele Eltern die entsprechende Einwilligung verweigern würden und somit die Repräsentativität der Vollerhebung verloren ginge. Das Niedersächsische Sozialministerium vertrat zunächst unter Verweis auf Material aus dem Bayerischen Innenministerium die Ansicht, AUT habe wegen der Anonymisierung der Blutproben überhaupt keine datenschutzrechtliche Relevanz. Ich stellte daraufhin klar, daß auch bei einer sofortigen Anonymisierung die vorherige Datenerhebung wohl einen Eingriff ins Recht auf informationelle Selbstbestimmung darstellt. Werden Daten mit Einwilligung erhoben, so müssen die

Betroffenen über alle geplanten Verwendungszwecke der Daten informiert werden. Alles andere würde auf eine Täuschung der Betroffenen hinauslaufen. Auch die Heranziehung der Forschungsklausel (§ 25 NDSG), auf die sich das Sozialministerium schließlich berief, wurde von mir mit dem Hinweis auf den Vorrang der Einwilligung und das Entgegenstehen schutzwürdiger Betroffeneninteressen abgelehnt. Wegen der gegensätzlichen Standpunkte ist es daher meines Erachtens sinnvoll, eine gesetzliche Regelung zu fassen. Sollte es der gesetzgeberische Wille sein, das AUT-Verfahren zuzulassen, so sollte ein ausdrückliches Reidentifizierungsverbot ins Gesetz mit aufgenommen werden, da es bei menschlichen Gewebeproben mit einem gewissen Aufwand immer möglich ist, diese einer bestimmten Person zuzuordnen.

Abgesehen von dem Sonderfall AUT kann ich dem neuesten mir vorliegenden Entwurf zum GDG bescheinigen, daß hier datenschutzrechtliche Belange weitgehend berücksichtigt worden sind.

## 21.2 Hoffen auf ein PsychKG

Weiter fortgeschritten als die Vorarbeiten für ein GDG sind die Pläne zur völligen Überarbeitung des Niedersächsischen Gesetzes über Hilfen für psychisch Kranke und Schutzmaßnahmen (PsychKG). Nachdem das Niedersächsische Polizeirecht um informationsrechtliche Regelungen ergänzt worden ist, erscheint mir die PsychKG-Novellierung von erhöhter Dringlichkeit, da nach dem derzeit geltenden § 6 Abs. 5 PsychKG die sehr weitgehenden polizeilichen Befugnisse auch bei der Durchführung von Schutzmaßnahmen nach dem PsychKG gelten würden, was aus fachlicher wie auch aus datenschutzrechtlicher Sicht nicht akzeptiert werden kann. Das Diskriminierungsrisiko bei der Nutzung psychiatrischer Daten ist besonders hoch, so daß es von größter Bedeutung ist, daß psychiatrische Daten nur in wenige hierfür berufene Hände geraten und daß diese einer strengen Zweckbindung unterworfen werden.

1993 übermittelte mir die SPD-Landtagsfraktion zwei Vorentwürfe zur Änderung des Gesetzes. Während die erste Regelungsalternative wegen ihrer viel zu weit gehenden Ermächtigungen von mir abgelehnt wurde, hielt ich den zweiten Vorschlag für eine geeignete Diskussionsgrundlage. Dabei handelte es sich um einen aufgrund meiner Änderungsvorschläge überarbeiteten Entwurf der Niedersächsischen Fachkommission für Psychiatrie. Die Fraktionen der SPD und Bündnis 90/Die Grünen brachten den auf die Fachkommission zurückgehenden Entwurf noch in der 12. Legislaturperiode im Landtag ein.

Der Entwurf differenziert zwischen Hilfen für psychisch Kranke und Schutzmaßnahmen. Bei den Hilfen wird sichergestellt, daß die Betroffenen über die zu ihrer Person gemachten Feststellungen selbst verfügen können. Das Zweckbindungsprinzip wird in dem Entwurf erfreulicherweise nur eingeschränkt, soweit ein dringendes Erfordernis dafür besteht. Dabei wird in der Begründung ausdrücklich darauf verwiesen, daß "Hilfen" einen anderen

Zweck verfolgen als "Schutzmaßnahmen". Während Hilfen freiwillig erfolgen, kommt Schutzmaßnahmen Zwangscharakter zu. Daten, die im Zusammenhang mit Hilfen vom Sozialpsychiatrischen Dienst erhoben worden sind, dürfen nicht gleichzeitig für Schutzmaßnahmen verarbeitet werden. Eine Ausnahme gilt, wenn eine Gefahr für Leib und Leben nicht anders abgewendet werden kann. Ohne die saubere Trennung der beiden Zwecke bestünde die Gefahr, daß die Bereitschaft zur Inanspruchnahme freiwilliger Hilfen aus Furcht vor Zwangsmaßnahmen torpediert würde. Die Entwurfsregelung zur in engen Grenzen zugelassenen Postzensur stellt sicher, daß deren Ergebnisse nur im überwiegenden Sicherheitsinteresse und zur Strafverfolgung genutzt werden dürfen. Begrüßt wird von mir auch die Regelung zur Datenspeicherung. Danach ist eine elektronische Speicherung nur dann zulässig, wenn die Aufnahme in Akten zur Erfüllung der Aufgaben nicht ausreicht. Besonders schutzbedürftige Angaben müssen von den sonstigen Daten getrennt aufbewahrt werden. Der Entwurf wurde für die laufende Legislaturperiode erneut vorgelegt (LT-Drs. 13/200). Es ist zu hoffen, daß er baldmöglichst verabschiedet wird.

## 21.3 Krankheitsregister

Angesichts des Auftretens neuer bzw. der massiven Zunahme bekannter zivilisationsbedingter Krankheiten wird von seiten der Politik und der medizinischen Forschung massiv der Aufbau medizinischer Forschungsregister gefordert. Dabei wird der Eindruck erweckt, daß der Aufbau derartiger Register schon der halbe Erfolg bei der Bekämpfung der jeweiligen Krankheit wäre. Meines Erachtens ist insofern Skepsis am Platz. Die epidemiologische Vollerfassung von Krankheiten ist nur selten der Schüssel zur Aufdeckung von Krankheitsursachen. Außerdem sind die besten epidemiologischen Erkenntnisse über Krankheitsursachen nutzlos, wenn das Geld und der politische Wille fehlen, diese Ursachen zu bekämpfen. Völlig aus dem Blickfeld gerät bei der medizinischen Erfassungseuphorie, daß jede Krankheitsregistrierung einen Eingriff ins Grundrecht auf Datenschutz und die Offenbarung von Arztgeheimnissen bedingt. Dabei werden hochsensible Daten erfaßt, die den Patientinnen und Patienten selbst oft aus ärztlicher Fürsorge vorenthalten werden. Deshalb ist es wichtig, darauf hinzuweisen, daß Krankheitsregister grundsätzlich nur mit Daten beliefert werden dürfen, wenn die Betroffenen nach Unterrichtung über die Zwecke der Registrierung und den Umfang der Verarbeitung ihre Einwilligung erteilt haben. Ist bei Erstellung eines Registers schon erkennbar, daß neben Behandlung, Nachsorge oder Qualitätssicherung auch Forschung betrieben werden soll, so muß dies schon beim Einholen der Einwilligung miterwähnt werden. Eine Ausnahme sind reine Behandlungsregister, die vom behandelnden Arzt geführt werden. Hier ist die Datenverarbeitung durch den Behandlungsvertrag abgedeckt. Dies sollte die Ärztinnen und Ärzte nicht daran hindern, ihre Patientinnen und Patienten über die Existenz solcher Register zu unterrichten.

In allen anderen Fällen bedarf es zum Führen von Krankheitsregistern eines speziellen Gesetzes. Datenschutzrechtliche Forschungsklauseln genügen für deren Betreiben nach Beendigung der Testphase nicht, da mit Hilfe der Re-

gisterdatensätze eine Vielzahl von Forschungsvorhaben durchgeführt werden sollen, die thematisch und methodisch noch nicht bestimmt sind. Neben dem eher formalen Erfordernis einer normenklaren gesetzlichen Grundlage, sind bei Krankheitsregistern spezielle Datenschutzsicherungen erforderlich. Es ist insbesondere sicherzustellen, daß bei der statistischen Auswertung durch Forschende für diese keine Identifikation der Betroffenen möglich ist. Dies kann dadurch gewährleistet werden, daß die identifizierenden Personangaben nicht im Register selbst, sondern in einer Treuhand- oder Vertrauensstelle gespeichert werden. Diese ist zu beteiligen, wenn über eine schon gespeicherte Person eingehende Meldungen mit Hilfe von einer Kontrollnummer dem existierenden Datensatz zugeordnet werden müssen oder wenn für Einzelforschungsvorhaben, sog. Fall-Kontroll-Studien, der Personenbezug wieder hergestellt werden soll.

## 21.4 Mißbildungs- oder Fehlbildungsregister

Nach der Veröffentlichung von Medienberichten im Frühjahr 1994 über das gehäufte Auftreten von Mißbildungen bei Kindern in bestimmten niedersächsischen Regionen entnahm ich der Presse, daß Niedersachsen als das erste Bundesland ein flächendeckendes Melderegister über Fehlbildungen bei Kindern einzurichten gedenkt. Die Meldungen an dieses Register sollten durch Hebammen, Geburtskliniken und Kinderärzte erfolgen. Angeblich stand schon der Entscheidungstermin des Landeskabinetts fest. Zuvor noch wollte man "auch mit Datenschützern in einen Dialog treten". Da niemand mit mir den Dialog gesucht hatte, wandte ich mich an das Sozialministerium und bat um Mitteilung über den Sachstand. Anstelle einer Antwort aus diesem Haus konnte ich zu meiner Verwunderung ca. zwei Monate später wieder in der Presse lesen, das Sozialministerium sei weiterhin "Mißbildungen und Allergien mit Register auf der Spur". Ein "Zentrum für medizinische Register" solle eingerichtet werden, das nicht nur für Mißbildungen und das geplante Krebsregister zuständig sein solle, sondern für Sammlungen aller "Informationen und Auffälligkeiten, die in Zusammenhang mit Allergien, Rinderwahnsinn oder Infektionskrankheiten stehen". Wieder wurden Gespräche "mit Datenschützern" angekündigt. Ich teilte daraufhin dem Sozialminister erneut mein gesteigertes Interesse für seine Planungen mit. Schon die Frage, "ob" Gesundheitsregister eingerichtet werden, sei datenschutzrechtlich relevant, nicht nur die Frage nach dem "wie". Ich wies darauf hin, daß medizinische Register nicht per se zu einer Verbesserung der Gesundheitsversorgung führen. Es ist ein vorsichtiges Vorgehen geboten. Daß entsprechende Register zu inhumanen Zwecken mißbraucht werden können, hat deren Verwendung zur Zeit des deutschen Nationalsozialismus gezeigt.

Die Antwort des Sozialministers zeigte, daß die Planungen entgegen dem von der Presse verbreiteten Eindruck noch in den Kinderschuhen stecken. Zur Aufklärung gehäufter Fehlbildungen würden derzeit lediglich übliche epidemiologische Inzidenz- und Fall-Kontroll-Studien durchgeführt. Ein umfassenderes Konzept habe aus Kostengründen aufgegeben werden müssen. Es werde lediglich über die Umstrukturierung nachgeordneter Behörden nachgedacht. Der Sozialminister stimmte mir zu, daß Krankheitsregister

über die Pilot- bzw. Studienphase hinweg einer gesetzlichen Grundlage bedürfen. Meine Hinweise auf das Erfordernis einer Technikfolgenabschätzung (§ 7 Abs. 3 NDSG) nahm er mit Interesse zur Kenntnis. Schließlich sagte er mir zu, mich über Planungen unaufgefordert zu unterrichten, sobald Konzepte erarbeitet sind.

## 21.5 Krebsregistrierung in Niedersachsen

### 21.5.1 Krebsregistrierung heute

Derzeit gibt es in Niedersachsen sechs in der Trägerschaft der Kassenärztlichen Vereinigung Niedersachsen (KVN) betriebene sog. Nachsorgeleitstellen (Braunschweig, Göttingen, Hannover, Osnabrück, Oldenburg, Stade), in denen zum Zweck der Langzeitbetreuung und der Qualitätssicherung umfangreiche Daten von Krebspatientinnen und -patienten gesammelt werden. Rechtsgrundlage für die Datenverarbeitung ist die Einwilligung der Patientinnen und Patienten. In den Städtischen Kliniken Oldenburg wird weiterhin ein Epidemiologisches Krebsregister Weser-Ems geführt. Außerdem gibt es zwei Tumorzentren an der Medizinischen Hochschule Hannover (MHH) und an der Universität Göttingen. Ein im Jahr 1982 beim Reinhard-Nieter-Krankenhaus in Wilhelmshaven eingerichtetes regionales Tumorregister wird seit 1988 als internes Behandlungsregister weitergeführt.

### 21.5.2 Pilotphase für ein Niedersächsisches Krebsregister

Nach der Koalitionsvereinbarung vom 19. Juni 1990 sollte ein landesweites Krebsregister unter Beachtung der datenschutzrechtlichen Anforderungen eingerichtet werden. Ende 1991 wurde ein vom Niedersächsischen Sozialministerium in Auftrag gegebener Bericht vorgelegt, der die Notwendigkeit eines solchen Registers bestätigte. Daraufhin wurden zur Erarbeitung des weiteren Vorgehens Arbeitsgruppen eingesetzt. Eine Arbeitsgruppe Datenschutz legte datenschutzrechtliche Eckpunkte für die Krebsregistrierung in Niedersachsen fest: klar definierter Datensatz, anonymisierte Speicherung, eindeutige Regelung der Reidentifizierung, Rückfragen bei Patienten nur über die Vermittlung des behandelnden Arztes, personenbezogene weitere Verarbeitung nur mit Patienteneinwilligung. Das Niedersächsische Krebsregister wurde dann in den Jahren 1993 und 1994 im Rahmen einer Pilotphase vorbereitet.

Um den datenschutzrechtlichen Anforderungen gerecht zu werden, sind eine die Anonymisierung und evtl. die Reidentifizierung vornehmende Vertrauensstelle und eine getrennt davon geführte, mit anonymen Daten arbeitende Registerstelle geplant. Die Datensätze in der Vertrauensstelle werden jeweils mit eindeutigen Kontrollnummern versehen, die durch ein Einwegverschlüsselungsverfahren aus den identifizierenden Angaben gebildet wird. Weiterhin wird mit den personenidentifizierenden Angaben ein asymetri-

sches Verschlüsselungsverfahren durchgeführt, bei dem nicht durch einfache Umkehrung des Verfahrens Rückschlüsse auf die Ursprungsdaten gezogen werden können. Die Reidentifizierung ist nur über einen völlig anderen, geheimen Schlüssel möglich. Dieser Schlüssel soll bei einer dritten Stelle hinterlegt werden.

In der bis Ende 1994 vorgesehenen Pilotphase sollte die prinzipielle Machbarkeit des Konzeptes prototypisch nachgewiesen werden. Ich wurde vom Niedersächsischen Sozialministerium regelmäßig über den Stand der Projektplanung unterrichtet. In Ermangelung einer datenschutzrechtlichen Erprobungsregelung mußte ich bei der Bewertung der Zulässigkeit regelmäßig auf die Forschungsklausel des § 25 NDSG zurückgreifen, da sonstige spezialgesetzliche Vorschriften nicht vorliegen. Diese sollen erst aufgrund der Ergebnisse während der Erprobung erarbeitet werden. Ich stellte klar, daß § 25 NDSG im besten Fall eine Nutzung für Zwecke der Pilot- bzw. Erprobungsphase zulassen könne.

Als Studienregion für die Pilotphase wurde die Weser-Ems-Region ausgewählt. Als Datenmaterial für diese Phase wurden 13.000 Datensätze der Nachsorgeleitstelle Oldenburg der Kassenärztlichen Vereinigung (KVN) herangezogen. Diese Datenübernahme habe ich in entsprechender Anwendung des § 25 NDSG akzeptiert. Meine Vorschläge zur Verbesserung der Datensicherheit wurden umgesetzt. Während der Pilotphase waren vier Projekte geplant:

- Im Projekt I sollten Pathologen als Melder aktiv in das Krebsregister einbezogen werden, da praktisch jede Krebsdiagnose durch eine pathologische oder zytologische Untersuchung gesichert wird. Gegen die Weitergabe der im Rahmen des Projektes anfallenden Pathologenmeldungen an die Nachsorgeleitstelle für deren eigene Zwecke meldete ich Bedenken an. Nach Angaben des Sozialministeriums kam es im Rahmen des Pilotprojektes dann auch nicht zu personenbezogenen Datenübermittlungen.
- Die Chiffrierung und Dechiffrierung personenidentifizierender Variablen sollte in einem Projekt II getestet werden. Die Erprobung der Kontrollnummerngenerierung und des asymetrischen Verschlüsselungsverfahrens durch die mit Mitarbeitern der Nachsorgeleitstelle besetzten Probevertrauensstelle erwies sich offensichtlich als erfolgreich.
- Zur Steigerung der Qualität war in einem Projekt III die Integration externer Datensätze zu erproben. Als externe Datensätze wurden die Angaben von Totenscheinen aus dem Gesundheitsamt Oldenburg herangezogen. Ca. 5000 Totenscheine aus den Jahren 1990 bis 1992 wurden zur Kontrollnummerngenerierung genutzt. Eines der Ziele war es, das Problem der Synomyme und Homonyme zu lösen. Bei den Synonymen werden z.B. wegen Namensänderungen oder Schreib- und Hörfehlern bei Meldungen einer Person unterschiedliche Kontrollnummern zugeordnet, so daß der Eindruck entsteht, es handele sich um zwei Krebsfälle. Homonyme entstehen bei Patienten mit ähnlichen Identifikationsdaten (z.B. gleicher Name), indem fälschlicherweise deren Daten über gleiche oder ähnliche Kontrollnummern einer Person zugeordnet werden. Die Datensätze der Nachsorgeleitstelle der KVN Oldenburg wurden mit den

Angaben der Totenscheine abgeglichen, um den Vitalstatus der gespeicherten Patientinnen und Patienten und die sog. Death-Certificate-Only-(DCO)-Fälle zu erkennen. Dabei geht es um die Fälle, bei denen erst anläßlich des Todes die Krebserkrankung dem Register bekannt wurde.

- Projekt IV hatte das Ziel, ein aktives Datenbanksystem zu entwickeln, mit dem die epidemiologische Auswertung der Registerstelle nach geographischen Gesichtspunkten möglich ist. Als Datenmaterial wurde auf anonymisierte Daten des Landesamtes für Statistik zurückgegriffen.

### 21.5.3 Das niedersächsische Meldemodell

Im Zentrum der Erprobung des niedersächsischen Krebsregisters soll ein neues niedersächsisches Meldemodell stehen. Dabei ist ein doppelter Meldeweg vorgesehen:
A. Meldungen von diagnostizierenden Ärzten, z.B. Pathologen,ohne Einwilligung mit reduziertem, vor allem histologischem Datensatz und sofortiger und endgültiger Anonymisierung bei der Vertrauenstelle,
B. Arztmeldungen mit informierter Einwilligung.

Zu A: Dabei übermitteln Pathologen, die keinen direkten Patientenkontakt haben und daher selbst keine Einwilligung einholen können, direkt - also nicht über den behandelnden Arzt - an die Registerstelle einen anonymisierten Datensatz mit einer Registriernummer, dem vollständigen histologischen Befund, dem Alter der Patientin bzw. des Patienten und eine großbe Angabe zum räumlichen Bezug der Wohnung. Bei der Meldung der medizinischen Daten soll der speziell für Krebserkrankungen entwickelte ICD-O-Schlüssel verwendet werden, der mehr als 1000 Differenzierungen enthält. Der ICD-O-Schlüssel untergliedert sich in zwei Hauptbereiche, einen Histologieschlüssel (Gewebeart des Tumors) und einen Lokalisationsschlüssel (Krebslage im Körper). Eine zweite Meldung nur mit den personenidentifizierenden Angaben und der Registriernummer des Pathologen geht an die Vertrauensstelle. Die Vertrauensstelle generiert mit einem Einwegverschlüsselungsverfahren die Kontrollnummer und übermittelt Kontroll- und Registriernummer der Registerstelle. Danach wird die identifizierende Meldung durch die Vertrauenstelle vollständig gelöscht. Die Registerstelle verknüpft über die Registriernummer die generierte Kontrollnummer mit dem anonymisierten direkt von den Pathologen an die Registerstelle gemeldeten medizinischen Datensatz.

Zu B: Die behandelnden Ärztinnen und Ärzte mit direktem Patientenkontakt holen dagegen in jedem Fall eine informierte schriftliche Einwilligung ein. Die medizinischen und die identifizierenden Daten werden an die Vertrauensstelle weitergeleitet. Diese nimmt die Einwegverschlüsselung der identifizierenden Daten zu der Kontrollnummer vor und chiffriert die per Einwilligung erhaltenen Personendaten. Den medizinischen Datensatz mit der Kontrollnummer sowie dem chiffrierten personenidentifizierenden Datensatz übermittelt die Vertrauensstelle an die Registerstelle. Diese kann anhand

der Kontrollnummer feststellen, ob schon eine Pathologenmeldung vorliegt und führt bei identischer Kontrollnummer die Angaben zusammen.

Mit der Capture-Recapture-Methode kann von der Registerstelle eine hohe Aussagekraft des Registers hergestellt werden. Dabei werden die über den A-Meldeweg und den B-Meldeweg eingehenden Mengen miteinander verglichen. Daraus lassen sich relativ verläßlich Dunkelziffern, Fehlerquoten u.ä. ableiten.

Bei einer ersten datenschutzrechtlichen Bewertung kam ich zu dem Ergebnis, daß das vorschlagene Verfahren akzeptabel ist. Da der Meldeweg A ohne informierte Einwilligung der Betroffenen erfolgen soll, muß das Verfahren in einem Krebsregistergesetz eindeutig geregelt werden. Durch die Trennung der identifizierenden von den histologischen Daten schon beim Pathologen und die sofortige endgültige Löschung der identifizierenden Daten bei der Vertrauensstelle ist das Mißbrauchsrisiko gering einzuschätzen.

### 21.5.4 Die Erprobungsphase

In der 1995 beginnenden Erprobungsphase soll mit neu zu erhebenden personenbezogenen Daten gearbeitet werden. In Ermangelung anderer Rechtsgrundlagen bedarf es dabei jeweils der Einwilligung der Betroffenen. Die Einwilligungserklärungen der Nachsorgeleitstellen sollen entsprechend erweitert werden. Träger des Projektes in der Erprobungsphase wird das Niedersächsische Sozialministerium sein. Die Erprobung soll das gesamte Land Niedersachsen erfassen. Das Erprobungregister soll vom bisherigen Register der Nachsorgeleitstellen vollständig getrennt werden. Die Erprobung erfolgt anhand einiger weniger Zielerkrankungen.

Für die Erprobungsphase sind vier Projekte geplant:

I. Ein selbständiger niedergelassene Pathologe im Nordwesten des Landes, ein Pathologieinstitut der Universität Göttingen sowie evtl. ein mittelgroßes Krankenhaus melden zur Testung der Kontrollnummerngenerierung und vor allem zur Erprobung des unabhängien Meldewegs A ihre personenidentifizierenden Datensätze ohne histologische Befunde. Während der Erprobungsphase sollen die Pathologen die Daten selbst anonymisieren, wozu ihnen die EDV-Voraussetzungen für eine eigene dezentrale Kontrollnummerngenerierung zur Verfügung gestellt werden. Damit entfiele die Zwischenschaltung einer Vertrauensstelle und das Lesen von Klartextangaben durch Registermitarbeitende. Meines Erachtens kann auch auf dieses Projekt § 25 NDSG angewendet werden.

II. Landesweit sollen über einen eigenständigen Meldeweg der Erprobungs-Vertrauensstelle eine Erfassung aller Obduktionen erfolgen, bei denen als Todesursache Krebs oder Krebsgewebe festgestellt wurde. Ich sehe jedoch wegen § 25 Abs. 3 NDSG Probleme, die hierbei gewonnenen Daten in ein späteres Nds. Krebsregister zu überführen.

III. Mit Hilfe eines Datenabgleichs zwischen klinischen Registern (Göttingen, MHH) und den Registern der Nachsorgeleitstellen, in denen

teilweise der gleiche Patientenstamm erfaßt ist, soll die Korrektheit dieser Register untersucht werden. Dazu werden die generierten Kontrollnummern und die Klartext-Identifizierungsdaten miteinander verglichen. Eine personenbezogene Rückmeldung an die Register soll und dürfte auch nicht erfolgen. Bei diesem Verfahren sehe ich insofern Probleme, als für die klinischen Register keine befriedigende Rechtsgrundlage besteht und bei den Nachsorgeleitstellen die Einwilligung diese Datenverarbeitung nicht mit umfaßt.

IV. Schließlich wird der Datenbestand von einer großen Pathologenpraxis quantitiativ ausgewertet. Dabei werden keine personenbezogene Daten übermittelt.

21.5.5 Bundeskrebsregistergesetz

Gemeinsam mit vielen Kollegen und vielen Landespolitikern habe ich Zweifel, ob dem Bund eine Gesetzgebungskompetenz für die epidemiologische Erfassung von Krebsdaten zusteht. Der in Art. 74 Nr. 19 Grundgesetz (GG) verwendete Begriff der "gemeingefährlichen Krankheiten" ist nur auf übertragbare Krankheiten anzuwenden, wozu Krebs nicht gehört. Zudem halte ich es für fraglich, ob es sich bei der Krebsregistrierung um eine "Maßnahme" gegen Krebskrankheiten handelt, da dieses Register nur ein Informationsmittel zur Gewinnung von Kenntnissen über und zur besseren Verhütung von Krebskrankheiten ist. Eine Bundesgesetzgebungskompetenz läßt sich allenfalls mit Art. 73 Nr. 11 GG ("Statistik für Bundeszwecke") begründen. Um für Bundeszwecke eine Krebsstatistik zu regeln, bedarf es aber lediglich der Festlegung eines von den Ländern anzulieferenden, nach in etwa gleichen Methoden erhobenen Datensatzes und der Regelung, wie diese Daten genutzt werden.

Trotz dieser Rechtslage beabsichtigte der Bund, eine Vollregelung zur Krebsregistrierung vorzunehmen. Auf der Basis des Beschlusses der 4. Großen Krebskonferenz vom 5. Dezember 1989 wurden 1990 vom Bundesgesundheitsministerium erste Überlegungen formuliert, die Januar 1993 in einen ausformulierten Referentenentwurf und noch im gleichen Jahr in einen Gesetzentwurf mündeten. Trotz der Bedenken der Länder bezüglich der Bundeszuständigkeit einigte sich der Vermittlungsausschuß auf ein auf fünf Jahre befristetes Krebsregistergesetz (Krebsregistergesetz v. 4. November 1994, BGBl. I S. 3351). Nach Ablauf der fünf Jahre sollen die Krebsregister ausschließlich auf der Grundlage von Landesgesetzen fortgeführt und weiterentwickelt werden.

Danach soll Ärztinnen und Ärzten erlaubt werden, die epidemiologischen Daten von Krebskranken sowie Personenangaben und Angaben über die Krankheitsgeschichte einer Vertrauensstelle zu melden. Diese verschlüsselt die Personenangaben zweifach (einmal nach einem asymetrischen und einmal nach einem symetrischen Verfahren) und gibt den Gesamtdatensatz an die Registerstelle. Dem Robert-Koch-Institut sollen jährlich die epidemiologischen Angaben, Geschlecht, Geburtsmonat, Wohnort, Staatsangehörigkeit und Berufstätigkeit aller Erkrankten mitgeteilt werden. Mit Hilfe einer Kon-

trollnummer sollen sowohl in den einzelnen Registern wie auch bei der bundesweiten Zusammenführung der Daten Doppelmeldungen vermieden werden. Die Patientinnen und Patienten sind vom Arzt über die Meldung frühestmöglich zu informieren und auf ihr Widerspruchsrecht hinzuweisen. Um den Vorbehalten gegen das Gesetz zu begegnen, wurde festgelegt, daß hinsichtlich der Voraussetzungen der Meldung, des Meldeverfahrens und der verschiedenen Phasen der Datenverarbeitung auf Landesebene abweichende Regelungen getroffen werden können.

Ich teilte dem Niedersächsischen Sozialministerium meine Bedenken gegen den ersten Entwurf sowie Verbesserungsvorschläge mit. Mir erscheint bei der vorgesehenen Widerspruchslösung die Hürde zur Wahrnehmung der informationellen Selbstbestimmung sehr hoch. Der Widerspruch muß gegenüber dem behandelnden Arzt, auf dessen Engagement die Patientin oder der Patient in starkem Maße angewiesen ist, erklärt werden. Praktische Probleme werden sicherlich bei der vorgesehenen regelmäßigen "Abgleichung" der verschiedenen Landes-Krebsregister, die nach einer anderen Konzeption arbeiten, entstehen.

### 21.5.6 Landeskrebsregistergesetz

An den Vorbereitungen für ein Niedersächsisches Krebsregistergesetz war ich von Anfang an beteiligt. Die ersten Überlegungen hierzu mündeten Ende 1992 in einen "Endbericht des Arbeitsvorhabens Krebsregistrierung in Niedersachsen" ein. Zum Jahreswechsel 1994/95 sollen die wesentlichen Vorarbeiten für einen Referentenentwurf eines Landeskrebsregistergesetzes abgeschlossen sein.

Für die Register- und die Vertrauensstelle bestanden zunächst Überlegungen, privatrechtliche Organisationsformen zu wählen. Hiergegen meldete ich Bedenken an. Unklar bliebe dabei nicht nur die politische Verantwortlichkeit und die Rechts- und Fachaufsicht. Bezüglich der Aussagepflicht von Bediensteten vor Gericht bestünde kein Genehmigungsvorbehalt (§ 54 StPO i.V.m. § 70 NBG). Es müßte außerdem sichergestellt werden, daß die private Stelle umfassend meiner datenschutzrechtlichen Kontrolle unterworfen wird. Keinen Gefallen konnte ich auch Überlegungen entgegenbringen, die Vertrauensstelle bei der KVN anzusiedeln, da diese als Trägerin der onkologischen Nachsorgeleitstellen in Interessenkonflikte gebracht würde. Die Versuchung wäre zu groß, die Angaben aus dem Krebsregister zum Abgleich bei den Nachsorgeleitstellen zu verwenden oder zur Kontrolle kassenärztlich abrechnender Ärztinnen und Ärzte.

Im Gesetz soll auch vorgesehen werden, daß die während der Erprobungsphase erhobenen Daten schon in das Nds. Krebsregister übernommen werden. Ich halte dies nur dann für akzeptabel, soweit dies schon bei der Einholung der Einwilligung berücksichtigt wird. Bzgl. des weiterhin geäußerten Bedürfnisses, epidemiologische Daten aus den bestehenden klinischen und Nachsorge-Registern für das künftige Krebsregister über die Kontrollnummer anonymisiert zu übernehmen, sehe ich noch Klärungsbedarf.

21.6 Nach dem Abtreibungsurteil zu § 218 StGB: Wie anonym ist die Beratung?

Das Urteil des BVerfG vom 28. Mai 1993 zur Verfassungsmäßigkeit der Fristenlösung bei Schwangerschaftsabbruch (NJW 1993, 1751) hat für alle Beteiligten nicht nur Antworten, sondern auch viele neue Fragen aufgeworfen. Hinsichtlich des Persönlichkeitsschutzes der schwangeren Frauen führt das BVerfG aus: "Dem Anspruch der an der Beratung Beteiligten auf Wahrung ihres Persönlichkeitsrechts wäre dadurch Rechnung zu tragen, daß das Protokoll Rückschlüsse auf die Identität der Beratenen und eventuell hinzugezogener Dritter nicht erlaubt. Damit würde auch der Gefahr begegnet, durch eine Dokumentation das für eine Beratung unerläßliche Vertrauensverhältnis der an ihr Beteiligten zu beeinträchtigen" (NJW 1993, 1762). Die Schwangeren sollen nicht dem Druck ausgesetzt werden, "die Gründe für ihren Abbruchwunsch durch einen Dritten überprüfen und bewerten zu lassen".

Weiter meint das BVerfG, daß es das Grundgesetz nicht zulasse, Leistungen der gesetzlichen Krankenversicherung zu gewähren, wenn die Rechtmäßigkeit des Abbruchs nicht festgestellt ist. Die Schwangere muß also nachweisen, daß eine Beratung erfolgt ist und - eventuell -, daß eine Indikationslage besteht. Nach der Anordnung des BVerfG gemäß § 35 BVerfGG, der vorläufig faktisch Gesetzeskraft zukommt, kann die schwangere Frau auf ihren Wunsch gegenüber der sie beratenden Person anonym bleiben (Nr. 3 Abs. 4). Der Frau muß aber "eine auf ihren Namen lautende ... Bescheinigung" ausgestellt werden. Dies setzt eine eindeutige Identifizierung voraus, die regelmäßig nur über einen Ausweis möglich ist. Wann ein Beratungsgespräch als abgeschlossen angesehen werden kann, bestimmt die beratende Person (Nr. 3 Abs. 5). Eine solche Entscheidung setzt eine gewisse Kooperationspflicht der Beratenen voraus. Gegenüber der beratenden Person sind nach der Anordnung des BVerfG Angaben über "das Alter, den Familienstand und die Staatsangehörigkeit der Beratenen, die Zahl ihrer Schwangerschaften, ihrer Kinder und früherer Schwangerschaftsabbrüche" zu machen, damit diese Angaben in einem Protokoll festgehalten werden können (Nr. 3 Abs. 6). Zu den Auskunfts- und Protokollierungspflichten gehören nach der Anordnung des BVerfG zudem "die für den Abbruch genannten wesentlichen Gründe".

Der den Abbruch durchführenden Ärztin bzw. dem Arzt obliegen detailliert aufgeführte strafbewehrte Pflichten (Anordnung Nr. 6.). Hierzu gehört die Pflicht zur Dokumentation des ärztlichen Handelns. Verlangt wird, daß die Ärztin bzw. der Arzt sich "über die Voraussetzungen vergewissert, von denen nach dem Schutzkonzept einer Beratungsregelung der Ausschluß der Strafdrohung abhängen muß". Nötig ist neben der Feststellung der Identität der Frau die "Prüfung, ob sich die Frau hat beraten lassen". "Weiterhin obliegt es dem Arzt, über die rein medizinischen Aspekte des Schwangerschaftsabbruches hinaus, den Schwangerschaftskonflikt, in dem die Frau steht, im Rahmen ärztlicher Erkenntnismöglichkeiten zu erheben. Dazu hat er sich die Gründe, aus denen die Frau den Schwangerschaftsabbruch verlangt, darlegen zu lassen." Ziel der Erhebung soll sein festzustellen, welches die "tieferliegenden Ursachen des Schwangerschaftskonflikts" sind

und, "ob die Frau tatsächlich den Schwangerschaftsabbruch innerlich bejaht". Läßt sich die Ärztin bzw. der Arzt nicht die Gründe für das Abbruchverlangen und die vorausgegangene Beratung darlegen und werden die für erforderlich erklärten Erhebungen nicht durchgeführt, so ist dies "strafrechtlicher Sanktion zugänglich und im Rahmen eines Beratungskonzeptes bedürftig".

Nach Nr.7. der Anordnung des BVerfG besteht die Pflicht zur Führung einer Bundesstatistik über Schwangerschaftsabbrüche. Dem Gesetzgeber kommt danach eine "Beobachtungspflicht" bzgl. der Wirkungen des Gesetzes zu. Dazu müssen "Daten planmäßig erhoben, gesammelt und ausgewertet werden" (NJW 1993, 1767). Das Gericht nennt als zwingend zu erhebende Angabe lediglich die absolute Zahl der Schwangerschaftsabbrüche. "Auf welche relevanten Tatsachen der Gesetzgeber im übrigen die statistische Erhebung erstrecken will (etwa Mehrfachabbrüche, Alter der Frau, Familienstand, Kinderzahl) und wie er die Erfassung und Auswertung der Daten im einzelnen regelt, obliegt seiner Entscheidung".

Das zitierte Urteil des BVerfG zu § 218 StGB wurde von verschiedener Seite heftig kritisiert. Ausgehend von teilweise widersprüchlichen Grundannahmen des Gerichts sind die daraus abgeleiteten Schlußfolgerungen über Sicherung der Anonymität und über die Informationspflichten konsequent. Die Anordnungen des BVerfG sowie eventuell künftig erlassene gesetzliche Regelungen sind bereichsspezifische Regelungen, die dem allgemeinen Datenschutzrecht vorgehen. Den beteiligten Frauen obliegen danach also bestimmte Mitwirkungspflichten. Dazu gehört aber nicht die Pflicht, bestimmte Unterlagen gegenüber Beratungsstelle oder Arzt vorzulegen. Abgesehen davon, daß die Frau eine eindeutige Identifizierung ihrer Person ermöglichen muß, sind die von ihr gemachten Angaben nicht durch Vorlage von Unterlagen glaubhaft zu machen.

Um eine praktikable Lösung der Zielsetzungen des BVerfG zu erreichen, machte ich dem Niedersächsischen Frauenministerium eine Verfahrensvorschlag, den das Ministerium in leicht modifizierter Fassung akzeptierte:

1. Alle ratsuchenden Schwangeren sind im Eingangsbereich der Beratungsstelle durch entsprechende Schilder und Informationsschreiben und auch mündlich darauf hinzuweisen, daß sie sich anonym beraten lassen können. Bereits bei der telefonischen Kontaktaufnahme zwecks Terminvereinbarung ist die Schwangere auf ihr Recht auf Anonymität hinzuweisen.
2. Der beratenden Person braucht die ratsuchende Schwangere zu keinem Zeitpunkt ihren Namen zu nennen. Ob eine Ratsuchende von sich aus ihren Namen nennen will, ist ihr völlig freigestellt. Unabhängig von der Angabe des Namens ist die beratende Person zur Verschwiegenheit verpflichtet.
3. Die beratende Person vergibt für jede ratsuchende Schwangere eine Beratungsnummer. Diese Nummer wird für das Protokoll und gegebenenfalls auch für die spätere Bescheinigung über die Beratung verwendet.

4. Wenn die Schwangere von dem Angebot Gebrauch machen will, sich bei der Geltendmachung von Ansprüchen, bei der Wohnungssuche, bei der Suche nach einer Betreuungsmöglichkeit für das Kind und bei der Fortsetzung ihrer Ausbildung konkret unterstützten zu lassen, ist diese Unterstützung von einer anderen als der beratenden Person in der Beratungsstelle durchzuführen. Soweit die Schwangere im Interesse ihrer Unterstützung ihren Namen angibt und in die weitere Verwendung ihres Namens gegenüber Dritten einwilligt, ist die unterstützende Person zur Verschwiegenheit gegenüber den beratenden Personen und sonstigen Dritten verpflichtet.
5. Im Protokoll über die Beratung werden in keinem Fall die Namen der Beratenen und der ggf. hinzugezogenen weiteren Personen - ärztlich, psychologisch oder juristisch ausgebildete Fachkräfte oder andere Personen - angegeben. Das Protokoll wird insoweit anonym geführt.
6. Wenn die Beratene nach Abschluß der Beratung eine Bescheinigung beantragt, daß die Beratung in der vorgeschriebenen Weise stattgefunden hat, hat eine andere als die beratende Person die Bescheinigung auszustellen.
   Die Beratene braucht zu ihrer Identifizierung für die Bescheinigung nur ihren Personalausweis oder ein anderes amtliches Dokument mit ihrem Namen vorzuweisen. Ihr Name wird daraufhin allein auf dem Exemplar der Bescheinigung vermerkt, das sie selbst erhält. Im übrigen trägt die Bescheinigung die Beratungsnummer, damit bei späteren Beratungen die dazugehörigen Unterlagen der Beratungsstelle festgestellt werden können.
   Die Person, die die Bescheinigung ausstellt, darf den Namen der Beratenen nicht in sonstiger Weise erfassen und ist zur Verschwiegenheit gegenüber den beratenden Personen und sonstigen Dritten verpflichtet.
7. Die Unterlagen der Beratungsstelle insbesondere mit dem Protokoll werden dort nur befristet aufbewahrt und dann vernichtet. Die Frist läuft jeweils bis zum regelmäßigen nächsten Zeitpunkt, zu dem über die weitere Anerkennung oder erneute Bestätigung der Beratungsstelle behördlich entschieden wird. Diese Frist darf einen nicht zu langen Zeitabstand umfassen und ist in jedem Fall kürzer als die ärztliche Aufbewahrungsfrist von 10 Jahren.
8. Die Bescheinigung ist bei dem Arzt, an den sich die Beratene wegen des Schwangerschaftsabbruchs wendet, zur Prüfung vorzulegen, ob sie sich hat beraten lassen und die Überlegungsfrist zwischen Beratung und Schwangerschaftsabbruch gewahrt ist. Die Feststellung und Beurteilung einer Indikation ist nicht Aufgabe des Arztes. Der Arzt ist zur Verschwiegenheit über den Namen und die weiteren Umstände der Schwangeren verpflichtet.
9. Die Beratene kann die Bescheinigung über die Beratung unter den in Nr. 9 der Anordnung des Bundesverfassungsgerichts genannte Voraussetzungen dazu verwenden, daß Versicherte der gesetzlichen Krankenversicherung und nach Beihilfevorschriften Anspruchsberechtigte - und damit regelmäßig sie selbst - bei einem Abbruch der Schwangerschaft auf Antrag Leistungen erhalten. Die Personen, die auf diese Weise den Namen und weitere Umstände der Schwangeren erfahren, sind zur Ver-

schwiegenheit verpflichtet. Die Kenntnisse, die der Arzt in diesem Zusammenhang erhalten hat, unterliegen der ärztlichen Schweigepflicht.

Das Niedersächsische Frauenministerium beteiligte mich auch bei der Regelung der Finanzierung von nichtindizierten (also rechtswidrigen), aber straffreien Schwangerschaftsabbrüchen als freiwillige Leistung. In den danach erlassenen Richtlinien vom 28. Februar 1994 (Nds. MBl. S. 497) ist vorgesehen, daß das Land die Kosten von Schwangerschaftsabbrüchen dann übernimmt, wenn eine sonstige Finanzierung gesetzlich nicht sichergestellt ist und die Frau bedürftig ist. Die Frau macht Angaben zu ihrer Bedürftigkeit gegenüber der Krankenkasse, bei der sie versichert ist, die dann über den Antrag entscheidet. Nur bei erheblichen Zweifeln an der Richtigkeit der Angaben können die Krankenkassen den Antrag an das Niedersächsische Landesamt für zentrale soziale Aufgaben (NLZSA) abgeben, das dann zu entscheiden hat. Das NLZSA entscheidet auch dann, wenn die Frau dies wünscht oder wenn sie nicht gesetzlich versichert ist. Gegen dieses Verfahren habe ich keine durchgreifenden Bedenken. Meines Erachtens handelt es sich bei der Zuständigkeitsübertragung an die Krankenkassen nicht um eine Funktionsübertragung, sondern um eine Datenverarbeitung im Auftrag. Ich empfahl daher, in der Rahmenvereinbarung des Landes mit den Kassen klarzustellen, daß die hochsensiblen Daten in den Antragsformularen getrennt von den sonstigen Unterlagen der Krankenkassen aufbewahrt werden müssen und nicht für andere Zwecke verwendet werden dürfen. Die Frauen müssen über das Verfahren umfassend unterrichtet werden, um eine informierte Einwilligung in die sie betreffende Datenverarbeitung geben zu können.

## 21.7 Wer darf die Post des Gesundheitsamtes öffnen?

Diese Frage bewegte nicht nur meine Dienststelle, sondern auch die Öffentlichkeit im Landkreis Lüneburg. Von einem Journalisten war ich auf eine Pressemeldung hingewiesen worden, wonach an das Gesundheitsamt Lüneburg gerichtete ärztliche Post aufgrund einer Verfügung vom Mai 1992 von der Posteingangsstelle des Hauptamtes der Kreisverwaltung geöffnet würde. Lediglich Sendungen, die als "Arztsache" gekennzeichnet sind, würden ungeöffnet dem Gesundheitsamt zugeleitet, was aber im Einzelfall auch nicht immer beachtet worden sei. Geöffnet worden sein sollen z.B. ein Schreiben an die Aids-Beratungsstelle des Gesundheitsamtes, das umfangreiche Angaben mit Diagnosen von Klienten enthielt, oder z.B. ein persönlich adressiertes Schreiben, das dann über eine offene Umlaufmappe "zugestellt" wurde.

Der Leiter des Gesundheitsamtes hatte mehrfach erfolglos darauf hingewiesen, daß die Anordnung des Landkreises die Offenlegung intimer Krankheitsdaten gegenüber einem unnötig erweiterten Personenkreis impliziert. Seiner dringenden Bitte, bei Klärung der strittigen Frage den Landesbeauftragten für den Datenschutzbeauftragten, das Niedersächsische Sozialministerium oder die Bezirksregierung einzubeziehen, wurde nicht entsprochen. Erst eine Dienstaufsichtsbeschwerde eines betroffenen Arztes führte dazu, daß in den Fall Bewegung kam. Nach mehr als eineinhalb Jahren wurde schließlich

seitens der Kreisverwaltung verfügt, in Zukunft wie folgt zu verfahren: An das "Gesundheitsamt" adressierte Post soll dem Amtsarzt oder seiner Vertreterin zugeleitet werden. Sofern die Post nicht unter die ärztliche Schweigepflicht fällt, wird diese vom Vorzimmer des Amtsarztes der zentralen Posteingangsstelle des Landkreises zugeleitet und dort entsprechend der Dienstanweisung weiter bearbeitet.

Die ärztliche Schweigepflicht, die ihre rechtliche Ausgestaltung in § 203 StGB sowie in § 2 der Berufsordnung der Ärztekammer Niedersachsen gefunden hat, umfaßt nicht nur Schriftstücke, die das Ergebnis einer Untersuchung, Diagnosen, Anamnesen oder Einzelbefunde enthalten, sondern auch Unterlagen mit Namen, Adressen u.ä., aus denen sich die Tatsache ergibt, daß jemand überhaupt eine Ärztin oder einen Arzt aufsucht. Das Briefgeheimnis nach Art. 10 Abs. 1 GG, das nach § 202 StGB strafrechtlich geschützt ist, ist auch dann verletzt, wenn z.B. ein als "persönlich" oder sonstwie als privat gekennzeichneter, an die Arbeitsstelle des Empfängers adressierter Brief von der Arbeitsstelle geöffnet wird. Bei der ärztlichen Schweigepflicht handelt es sich ebenso wie bei dem Post- und Fernmeldegeheimnis um Datenschutzbestimmungen im Sinne von § 23 Abs. 1 Satz 1 NDSG.

Briefe und sonstige Postsendungen, die direkt an eine namentlich genannte Person gerichtet sind, dürfen nicht von der Dienststelle geöffnet werden. Wird als Adressat einer Postsache, die als "Arztsache" oder ähnlich gekennzeichnet ist, eine Behörde genannt, so darf diese nur durch den zuständigen Arzt oder deren Hilfspersonen nach § 203 Abs. 3 StGB geöffnet werden. Keine Hilfspersonen in diesem Sinne sind die Mitarbeiterinnen und Mitarbeiter der Poststelle des Hauptamtes einer Kreisverwaltung. Dies ergibt sich schon aus dem Umstand, daß sie nicht durch die ärztliche Schweigepflicht gebunden sind. Der Verweis auf die generelle Pflicht zur Amtsverschwiegenheit (vgl. § 203 Abs. 2 StGB, § 5 NDSG, § 39 BRRG, § 68 NBG) reicht nicht aus, um eine Offenbarung von Brief- oder Arztgeheimnissen zu rechtfertigen.

Zwar ist das Gesundheitsamt als rechtlich unselbständiges Fachamt Teil der öffentlichen Stelle "Landkreis". Doch ist dies für die Behandlung ärztlicher Post ohne Bedeutung. Die Datenweitergabe innerhalb einer Stelle ist nicht unbeschränkt zulässig, sondern nach § 11 Abs. 4 NDSG wie eine Übermittlung zu behandeln. Dies gilt in besonderem Maße für sensible Daten, die dem Arztgeheimnis unterliegen. Im Rahmen des Gebots der Verschwiegenheit ist der Träger des Geheimnisses verpflichtet, den Personenkreis, der in das Geheimnis eingeweiht wird, möglichst klein zu halten. Dem Arztgeheimnis unterliegende Daten dürfen zwischen ärztlich tätigen Gehilfen nur so weit weitergegeben und genutzt werden, als dies zur Aufgabenerfüllung erforderlich ist. So gehören in einem Krankenhaus die Angestellten der Krankenhausverwaltung nur hinsichtlich der Verwaltungsvorgänge zu den berufsmäßig tätigen Gehilfen. Nicht mehr dazu zu zählen sind aber bei einem

Gesundheitsamt die Bediensteten in der Posteingangstelle der allgemeinen Kreisverwaltung. Dies ergibt sich schon daraus, daß dem leitenden Amtsarzt gegenüber diesen Bediensteten kein (ärztliches) Weisungsrecht zusteht.

Unterschiedliche Auffassungen werden hinsichtlich der Fälle vertreten, in denen ein Schreiben "z.Hd." adressiert ist. Es ist zwar richtig, daß in diesen Fällen Adressat nicht die genannte Person, sondern die Behörde ist. Doch muß im Hinblick auf das Arztgeheimnis berücksichtigt werden, daß es Patientinnen und Patienten, teilweise auch Bediensteten öffentlicher Stellen nicht klar ist, daß die Bezeichnung "z.Hd." keine Adressatenbenenung ist, sondern nur einen Verteilungsvermerk darstellt. Der Wille der absendenden Stelle dürfte zumindest bei ärztlicher Post dahin gehen, daß eine Versendung "z.Hd." tatsächlich ausschließlich in die Hände der jeweiligen Person gelangt. Im konkreten Fall kam es hierauf aber nicht an. Es ist nämlich unstreitig, daß an eine ärztliche Behörde oder Stelle, also z.B. an das Gesundheitsamt gerichtete Schreiben nicht von einer Verwaltungsbehörde oder -stelle geöffnet werden dürfen.

Entgegen der Einlassung des Landkreises sind als "persönlich" adressierte Schreiben überhaupt nicht an den Landkreis oder das Gesundheitsamt adressiert. Adressat ist die jeweils genannte Privatperson. Die öffentliche Stelle, über die die Zustellung erfolgt, hat kein Recht, diese Post zu öffnen. Wird dies nicht beachtet, so liegt eine objektive Verletzung des Briefgeheimnisses vor.

Das Öffnen der Post an das Gesundheitsamt durch die Eingangsstelle des Hauptamtes war auch nicht erforderlich. Ziel des Öffnens ist ja nicht die Kontrolle des Inhaltes, sondern die Registrierung des Briefeingangs sowie die korrekte Weiterleitung der Schreiben. Es war mir nicht ersichtlich, worin die behauptete erhebliche Erschwerung der Überwachung der ordnungsgemäßen Wahrnehmung der Aufgaben und des Geschäftsablaufes im Gesundheitsamt durch die Vorgesetzten liegen könnte.

Nach § 7 Abs. 1 und 3 NDSG sind nicht-automatisiert gespeicherte Daten vor dem Zugriff Unbefugter zu schützen. In der Verfügung vom 19. Mai 1992 war ausdrücklich vorgesehen, daß an das Gesundheitsamt gerichtete Post - ausschließlich der als "Arztsache" gekennzeichneten Post - von der Eingangsstelle des Hauptamtes geöffnet werden soll. Damit wurde in der grundsätzlichen Verfügung die Verletzung des Arztgeheimnisses und des Briefgeheimnisses strukturell angelegt. Entsprechende Verstöße sind auch erfolgt. Diese Verstöße beruhten auf der Organisationsverfügung. Gegen die nunmehr erlassene Verfügung vom Dezember 1993 bestehen keine durchgreifenden datenschutzrechtlichen Bedenken mehr. Verstöße gegen das Arzt- oder gegen das Briefgeheimnis nach diesem Datum wurden mir auch nicht vorgetragen worden. Auch wenn aufgrund der nun gültigen Verfügung davon ausgegangen werden kann, daß beim Posteingang im Gesundheitsamt Lüneburg künftig die datenschutzrechtlichen Bestimmungen beachtet werden, konnte wegen der Schwere des erfolgten Datenschutzverstoßes auf eine Beanstandung nach § 23 NDSG nicht verzichtet werden.

## 21.8 Arztakten im Müllcontainer

Von einem Journalisten in Hildesheim wurde ich darüber informiert, daß in dessen Redaktion ein Bürger erschien - unter dem Arm eine vollständige und aktuelle Krankenakte aus einem hannoverschen Krankenhaus. Diese Akte hatte der Bürger aus einem Altpapiercontainer "gefischt", in dem sich noch weitere Arztakten befanden. Es wurde zunächst veranlaßt, daß der Container sichergestellt wurde. Die daraufhin eingeleiteten Recherchen ergaben, daß es sich bei dem Aktenfund nur um die Spitze eines Eis- oder besser eines Aktenberges handelte: Der auf einem Gehweg abgestellte Altpapiercontainer enthielt insgesamt 125 Patientenakten, die ein früherer Arzt des Krankenhauses in Hannover zu "entsorgen" versucht hatte. Sie enthielten vollständige Arztberichte, Befunde, Diagnosen und ärztliche Korrespondenz. In dem betroffenen Krankenhaus hatte man schon seit längerem einen Arzt im Verdacht, Akten unterschlagen zu haben, was sich jedoch nicht beweisen ließ. Die vermuteten Unregelmäßigkeiten hatten letztlich schon vor dem großen Fund zur Aufhebung des Dienstverhältnisses mit dem Arzt geführt. Die sichergestellten Akten wurden dem Krankenhaus zurückgegeben.

Ich legte dem Krankenhaus nahe, die betroffenen Patientinnen und Patienten vom Verlust und Wiederauftauchen der Akten in Kenntnis zu setzen, u.a. um diesen zu ermöglichen, nach § 203 StGB, der unter anderem das Arztgeheimnis regelt, Strafanzeige zu erstatten. Davon wollte aber das Krankenhaus nichts wissen. Zu dem betreffenden Arzt habe ein kollegiales Verhältnis bestanden; dieser habe mit dem Unterlassen der Aktenrückgabe keine böse Absicht verfolgt. Der unkorrekte Umgang mit den Akten sei vielmehr Ausdruck einer persönlichen Schwäche. Der Arzt ließ sich dahingehend ein, daß nicht er die Unterlagen in dem Container verstaute, sondern ein mit Aufräumarbeiten beauftragter Verwandter. Auch dies stellt einen strafbaren Bruch des Arztgeheimnisses dar, das auch gegenüber Verwandten des Arztes gilt. Das eingeleitete Strafverfahren wurde letztendlich von der Staatsanwaltschaft gemäß § 153a StPO gegen Zahlung einer Geldbuße in Höhe von 1500 DM an eine gemeinnützige Einrichtung eingestellt.

Verblüffend im konkreten Fall war nicht nur die "Schwäche" des Arztes, sondern auch, daß das Krankenhaus trotz vielfältiger Verdachtsmomente nicht in der Lage war, das Verschwinden der Akten zu unterbinden oder zumindest aufzudecken. Das Krankenhaus hat nunmehr den Ärztinnen und Ärzten neben der üblichen Verpflichtung zum Datenschutz im Rahmen des Dienstantritts per Dienstanweisung auferlegt, Arztbriefe innerhalb von zehn Tagen nach der Entlassung der Patientinnen bzw. Patienten abzudiktieren. Damit soll verhindert werden, daß Bearbeitungsstaus entstehen, die einzelne Ärzte zum Verschwindenlassen von Akten animieren könnten. Außerdem wurde die Ärzteschaft darauf hingewiesen, daß Patientenakten ohne Genehmigung das Haus nicht verlassen dürfen.

21.9 Ist die zentrale Dokumentation von Blut-Chargen in Krankenhausapotheken zulässig?

Der Leiter einer Krankenhausapotheke bat mich zu überprüfen, ob die zentrale Erfassung der verwendeten Chargen von Gerinnungspräparaten mit Patientenname, Geburtsdatum und Lieferfirma in seiner Apotheke zulässig sei. Der Anfrage waren Veröffentlichungen vorausgegangen, daß HIV-kontaminiertes Blut von Blutspenden in medizinischen Präperaten weiterverarbeitet wurde, was zur einer HIV-Infektion von behandelten Patientinnen und Patienten führte. Zweck der Dokumentation solle es sein, bei einer eventuellen Kontamination mit Viren potentiell infizierte Patientinnen und Patienten frühestmöglich zu identifizieren, um damit den Schaden im Umfeld dieser Menschen zu begrenzen.

Es wurde vorgetragen, daß es zu den dokumentarischen Sorgfaltspflichten von Arzt und Krankenhaus gehört, bei einer Bluttransfusion oder bei der Verabreichung von Blutprodukten in der Krankenakte Datum, Konservennummer und Art der Konserve zu vermerken. Um bei einer Serokonversion diejenigen Patienten ausfindig zu machen, denen zuvor von einem infizierten Spender stammende Konserven verabreicht wurden, müsse jedoch die zentrale produkt-, hersteller- und chargenbezogene Dokumentation des Patientennamens einschließlich anfordernder Klinik und Station erfolgen. Auch nach Ansicht des Sozialministeriums ist eine zentrale Erfassung der Liefer-, Abgabe- und Anwendungsdaten von Blut und von Blutprodukten im Krankenhaus im Interesse der Arzneimittelsicherheit unbedingt erforderlich. Es müsse möglich sein, in angemessener Zeit den Weg dieser Produkte vom Spender bis zum Patienten verfolgen zu können. Bei Beanstandung einer Charge bedürfe es der sofortigen Ermittlung der mit dieser Charge behandelten Patienten.

Die Mitteilung personenbezogener Daten durch die behandelnden Ärztinnen und Ärzte an die Apotheke ist eine Offenbarung i.S.v. § 203 StGB. Diese bewegt sich im Rahmen der Behandlung und ist daher befugt. Die Bediensteten der Apotheke sind hinsichtlich der Behandlung "berufsmäßig tätige Gehilfen" nach § 203 Abs. 3 StGB, denen im Rahmen der Erforderlichkeit personenbezogene Mitteilungen gemacht werden können (vgl. §§ 2 Abs. 3 und 6, 3 Ärztl. BerufsO). Auf die Dokumentation selbst ist § 28 Abs. 1 BDSG anwendbar (vgl. § 2 Abs. 2 Satz 1 Nr. 1 NDSG). Danach ist eine Datenspeicherung zulässig, wenn sie im Rahmen der Zweckbestimmung eines Vertragsverhältnisses (hier des Behandlungsvertrags) erforderlich ist. Nach § 39 Abs. 1 BDSG dürfen personenbezogene Daten, die einem Berufsgeheimnis unterliegen, nur für den jeweiligen Zweck verwendet werden. Der datenschutzrechtlichen Zweckbindung sowie der beruflichen Schweigepflicht unterliegen auch Apothekerinnen und Apotheker.

Meine ursprünglichen Bedenken gegen die Dokumentation konnte ich fallenlassen, nachdem mir mitgeteilt worden ist, daß in der Apotheke die Regeln der ärztlichen Dokumentation beachtet werden und daß dort eine ärztliche Leitung und Aufsicht besteht. Durch technisch-organisatorische Maßnahmen (vgl. § 9 BDSG) muß sichergestellt werden, daß die Daten ausschließ-

lich für den vorgesehenen Zweck verwendet werden. Die Nutzung ist in geeigneter Weise zu dokumentieren.

21.10 Was darf die Polizei aus Psychiatrie und Krankenhaus erfahren ?

Von der Mitarbeiterin einer Nervenklinik wurde ich darauf hingewiesen, daß es gängige Praxis sei, daß Polizeidienststellen oder Staatsanwaltschaften telefonisch in Krankenhäusern Auskunft darüber einholen, ob sich eine Patientin oder ein Patient derzeit im Krankenhaus in Behandlung befindet. Teilweise würden weitere Daten erhoben, z.B. die Entlaßadresse. Betroffen seien vorrangig alkohol- oder ansonsten drogenabhängige Personen. Mit den Daten sollen u.a. gerichtliche Vorladungen oder Zustellungen ermöglicht werden. Auch würde derart die Einhaltung von strafrechtlichen Auflagen, z.B. die Durchführung einer Therapie, überprüft.

Gemäß § 20 Niedersächsisches Meldegesetz (NMG) ist die Leitung eines Krankenhauses verpflichtet, aufgenommene Personen unverzüglich in ein Verzeichnis aufzunehmen. Gemäß § 16 Abs. 3 Melderechtsrahmengesetz (MRRG) i.V.m. § 20 Abs. 5 NMG hat die Leitung des Krankenhauses diese so erhobenen Daten u.a. den Polizeibehörden, den Staatsanwaltschaften und den Gerichten in Strafverfolgungs-, Strafvollstreckungs- und Strafvollzugssachen zu übermitteln, wenn diese darum zur Verhütung erheblicher Gefahren für die öffentliche Sicherheit oder für Zwecke der Strafverfolgung sowie zur Aufklärung des Schicksals von Vermißten und Unfallopfern ersuchen. Die genannten Stellen sind befugt, die Daten zu diesem Zweck auszuwerten und zu verarbeiten.

Die Formulierung des Gesetzes "zur Verhütung erheblicher Gefahren für die öffentliche Sicherheit oder für Zwecke der Strafverfolgung" macht deutlich, daß es sich um erhebliche Gefahren oder um eine konkrete Strafverfolgung handeln muß. Bei polizeilichen Routineermittlungen liegt die erforderliche Qualität hinsichtlich der Übermittlungspflicht und -befugnis nicht vor. Es kommt jeweils auf den Einzelfall, dessen Hintergründe und Umstände an. Nach Ansicht des Niedersächsischen Innenministeriums ist es nicht von vornherein ausgeschlossen, daß im Einzelfall die Feststellung des Aufenthalts zum Zweck der gerichtlichen Vorladung Strafverfolgungszwecken dient. Die Überprüfung strafrechtlicher Auflagen könne der Abwehr erheblicher Gefahren für die öffentliche Sicherheit dienen. Diese Ausführungen gelten für Krankenhäuser allgemein, also auch für psychiatrische Kliniken.

Nach Ansicht des Innenministeriums bestehen gegen eine Gleichsetzung der Entlaßadresse und der regelmäßigen Wohnung nach § 20 Abs. 3 NMG keine durchgreifenden Bedenken. Dem kann ich mich so nicht anschließen. Soweit es sich bei der Entlaßadresse um die Wohnadresse handelt, spricht nichts dagegen, diese weiterzugeben. Ist dies aber nicht der Fall, z.B. wenn eine Behandlung in einem anderen Krankenhaus durchgeführt wird, so wird diese Information von den Erlaubnistatbeständen des NMG nicht erfaßt; eine Datenübermittlung ist insofern grundsätzlich unzulässig.

Aufgrund der ärztlichen Schweigepflicht dürfen Ärztinnen, Ärzte und Berufshelfende die anvertrauten oder bekannt gewordenen Berufsgeheimnisse nicht unbefugt offenbaren. Grundsätzlich sind schon Informationen darüber, daß sich eine Person in ärztlicher Behandlung befindet, wo, wann und bei wem sie behandelt wird, der Schweigepflicht unterfallende Sachverhalte. Die ärztliche Schweigepflicht ist Grundlage für eine Arzt-Patienten-Vertrauensbeziehung und damit Basis für eine wirksame Behandlung. Dies gilt in besonderem Maße für die psychiatrische oder psychotherapeutische Behandlung von Patientinnen und Patienten, zumal hier neben objektiven Angaben Gefühle, Ängste, Sorgen, Beziehungsprobleme, persönliche Fehler und Unzulänglichkeiten bis hin zu Angaben über strafbare Handlungen in die Behandlung einfließen. Das NMG rechtfertigt die Offenbarung ärztlicher Geheimnisse. Unter den oben genannten Gründen ist daher eine Durchbrechung der ärztlichen Schweigepflicht gesetzlich erlaubt. Voraussetzung ist aber eine konkrete Gefährdung eines höherwertigen Rechtsgutes.

Soweit die Angaben über eine psychiatrische oder sonstige medizinische Behandlung unter das Sozialgeheimnis fallen, sind zudem die datenschutzrechtlichen Regelungen des Sozialgesetzbuches (SGB) zu beachten. Dies ist der Fall, wenn einer berechtigten Person vorbeugende Gesundheitshilfe oder Krankenhilfe nach dem Bundessozialhilfegesetz gewährt wird. Nach § 68 SGB X ist es zulässig, zur Erfüllung von Aufgaben der Polizeibehörden, der Staatsanwaltschaften, der Behörden der Gefahrenabwehr oder der Justizvollzugsanstalten Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift der Betroffenen sowie Namen und Anschriften der Arbeitgeber zu übermitteln, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

## 21.11 Datenverarbeitung im Geschäftsbereich des Landesamtes für Zentrale Soziale Aufgaben

Der Datenschutzbeauftragte eines niedersächsischen Landeskrankenhauses hatte mir gegenüber den Direktzugriff auf die Basisdokumentation in den Landeskrankenhäusern durch das Niedersächsische Landesamt für zentrale soziale Aufgaben (NLZSA) problematisiert. Als bedenklich wurde insbesondere der Zugriff auf ärztliche Daten im Rahmen der Systembetreuung und damit eine Offenbarung im Sinne von § 203 StGB angesehen.

Die Krankenhäuser sind offensichtlich zur Durchführung der Systembetreuung mit eigenem Personal nicht in der Lage. Seitens des NLZSA wurde die Auffassung vertreten, daß es sich bei der fraglichen Bado-DXD-Datei um eine nichtpersonenbezogene Datensammlung handelt. Ich habe klargestellt, daß die teilweise anonymisierten Daten zumindest über die Referenzdatei reidentifizierbar sind. In der Vergangenheit erfolgte die Systembetreuung ohne Abstimmung mit den Landeskrankenhäusern über ein dauernd eingeschaltetes Modem. Dies ist zweifellos unzulässig. Ich habe von einer Beanstandung in Anwendung von § 23 Abs. 3 NDSG abgesehen. Künftig erfolgt - wie vom Landesamt schriftlich zugesichert - eine vorherige (telefonische)

Abstimmung mit dem Krankenhaus, daß das Modem aktiviert wird. Erst danach kann die Systemwartung durchgeführt werden.

Die Erstellung der Krankenhausdiagnosestatistik für die niedersächsischen Landeskrankenhäuser ist Aufgabe des Landesamtes. Nach der Niedersächsischen Statistikverordnung ist das NLZSA gegenüber dem Landesamt für Statistik berichtspflichtig. Die Anlieferung der Daten erfolgt über bei den Landeskrankenhäusern erstellte Datenträger; die von dort zur Verfügung gestellten Daten werden einer summarischen Vollständigkeitskontrolle unterzogen und direkt an das Landesamt für Statistik übermittelt. Gegen diese Vorgehensweise bestehen aus datenschutzrechtlicher Sicht keine Bedenken.

Unabhängig von zusätzlich notwendigen Regelungen über Datensicherungsmaßnahmen bestand zwischen mir und den Vertretern des Landesamtes Einvernehmen dahingehend, daß bei Erweiterungen der Datenverarbeitungsmöglichkeiten in den Landeskrankenhäusern (Krankenhausinformationssystem) meine Dienststelle frühzeitig beteiligt werden soll.

21.12 Der Totenschein für den Erben

Der Bruder eines Verstorbenen wandte sich an mich mit der Frage, ob ein Gesundheitsamt zu Recht die Herausgabe einer Fotokopie einer Todesbescheinigung verweigert hatte. Ziel des Auskunftsersuchens war es, genauere Kenntnis über die zum Tode des Bruders führende Krankheit zu erlangen. Die Verweigerung der Kopie der Todesbescheinigung durch den Landkreis war ohne nähere Begründung erfolgt.

Das NDSG ist hier direkt nicht anwendbar, da dieses Gesetz nur die personenbezogenen Daten lebender natürlicher Personen erfaßt (§ 3 Abs. 1 NDSG). Zu beachten ist jedoch das Arztgeheimnis. Das Arztgeheimnis schützt das Vertrauensverhältnis zwischen Arzt und Patient über den Tod eines Patienten hinaus. Dieses gilt aber nicht unbeschränkt. Zum Schutz höherwertiger Güter ist eine Offenbarung ärztlicher Geheimnisse zulässig, evtl. sogar geboten. Der Bundesgerichtshof hat in einem Urteil von 1983 erkannt, daß Angehörigen bzw. Erben einer verstorbenen Person ein Recht auf Einsicht in Patientenunterlagen zustehen kann (NJW 1983, 2627). Ausgangspunkt hierfür ist der dem Patienten zu Lebzeiten zustehende Anspruch auf Einsichtnahme, ohne daß dieser ein Informationsinteresse darlegen müßte. Dieser Anspruch geht, zumindest soweit es sich um die Klärung von Schadensersatzforderungen handelt, auf die Erben über.

Das Einsichtsrecht steht nahen Angehörigen bzw. Erben aber nur zu, soweit dies nicht dem geäußerten oder mutmaßlichen Willen des verstorbenen Patienten widerspricht. Im konkreten Fall lag keine positive Willensäußerung des Bruders vor. Bei der Feststellung des mutmaßlichen Willens sind die Gründe für die begehrte Einsichtnahme zu erforschen. Dabei kommt es vor allem darauf an, wie die verstorbene Person sich zu dem Akteneinsichtsbegehren wahrscheinlich gestellt hätte. Die Einsichtsverweigerung durch den

Arzt muß auf nachvollziehbaren Gründen beruhen. Sachfremde Überlegungen können eine Verweigerung nicht begründen. Diese Kriterien sind nicht nur auf Patientenakten anzuwenden, sondern im gleichen Maße für die Angaben auf den Todesbescheinigungen. Im konkreten Fall sah ich keine Gründe, die einer Offenbarung der ärztlichen Angaben entgegenstünden.

### 21.13 Ärztekammer gibt Daten an Gesundheitsämter

Unter XI 21.14 hatte ich meine datenschutzrechtlichen Bedenken gegen die in Niedersachsen geübte Verwaltungspraxis dargestellt, nach der seitens der Ärztekammer regelmäßig die Gesundheitsämter über neue Anmeldungen von Ärztinnen und Ärzten informiert werden. Es gab für mich in den letzten zwei Berichtsjahren keine Veranlassung, von dieser Rechtsauffassung abzurücken. Aus meiner Korrespondenz mit dem Niedersächsischen Sozialministerium ist mir bekannt, daß die Ärztekammer nach wie vor Anmeldungen nach § 5 Abs. 1 HKG an die zuständigen Gesundheitsämter mitteilt. Für diese Datenübermittlung besteht bisher noch keine Rechtsgrundlage, so daß die Praxis als rechtswidrig anzusehen ist. Daran ändert auch der Umstand nichts, daß in einem künftigen Gesundheitsdienstgesetz eine entsprechende gesetzliche Grundlage geschaffen werden soll (vgl. 21.1).

Auf meine Anfrage hin hat die Ärztekammer Niedersachsen ausgeführt, daß die Datenübermittlung als Amtshilfe angesehen werde. Eine Verletzung des Datenschutzes sei nicht zu befürchten sei, da die Kammerangehörigen ihre Meldedaten ohnehin dem zuständigen Gesundheitsamt bekanntgeben müßten. Deren persönliche Rechtssphäre kann nach Auffassung der Ärztekammer nicht verletzt werden, weil diese lediglich behilflich sei, der gesetzlichen Meldepflicht nachzukommen. Zwar waren mir diese Ausführungen nicht gerade nachvollziehbar. Im Hinblick auf die künftige Sanktionierung der derzeit geübten Praxis habe ich aber bislang auf eine Beanstandung der Datenübermittlungen nach § 23 Abs. 1 NDSG abgesehen.

### 21.14 Berufsordnung für Hebammen und Entbindungspfleger

Anfang 1994 leitete mir das Niedersächsische Sozialministerium den Entwurf einer Berufsordnung für Hebammen und Entbindungspfleger zu. Dabei handelt es sich keinesfalls um ein datenschutzrechtlich irrelevantes Thema: Hebammen und Entbindungspfleger genießen einen der ärztlichen Schweigepflicht vergleichbaren beruflichen Vertrauensschutz (§ 203 StGB). Sie sind oft die ersten, die Daten über ein neugeborenes Kind "erheben". Ich hatte an der Berufsordnung grundsätzlich auszusetzen, daß sie mit der rechtlichen Qualität eines Erlasses nicht in der Lage ist, Eingriffe ins Recht auf informationelle Selbstbestimmung zu legitimieren. Andere Länder - wie etwa Bremen oder Schleswig-Holstein - haben hierzu ein förmliches Gesetz erlassen. Ich äußerte zudem Zweifel daran, ob eine Aufbewahrungspflicht der Aufzeichnungen der Hebammen und Entbindungspfleger von 30 Jahren angemessen ist. In den meisten Ländern müssen derartige Unterlagen nur 10 Jahre dokumentiert bleiben. Begrüßenswert ist, daß von der regelmäßigen

Vorlagepflicht der Aufzeichnungen (früher Hebammentagebücher) gegenüber den Gesundheitsämtern abgesehen werden soll.

## 22. Kinder- und Jugendhilfe

Durch das 2. SGB-Änderungsgesetz (2. SGBÄndG vom 13. Juni 1994, BGBl. I S. 1229) wurden auch die Bestimmungen über den Schutz von Sozialdaten im KJHG (4. Kapitel) geändert. Neben einer Anpassung an den Sprachgebrauch des BDSG und einer Konkretisierung der Zweckbindung ist besonders hervorzuheben, daß Sozialdaten im Bereich der Amtspflegschaft und der Amtsvormundschaft nunmehr auch im Hinblick auf den Einzelfall zum Zwecke der Aufsicht, Kontrolle oder Rechnungsprüfung übermittelt werden dürfen (§ 68 SGB III).

Gravierende Auswirkungen haben auch die Änderungen der §§ 73 und 78 SGB X. § 73 betrifft im wesentlichen die Beschlagnahme von Jugendamtsakten und die Zeugenvernehmung von Jugendamtsbediensteten in Strafverfahren. Beides ist nach dem bisher geltenden Recht nur bei Strafverfahren wegen eines Verbrechens möglich. Von der Ausweitung auf "sonstige Straftaten von erheblicher Bedeutung", die nunmehr den Verbrechen gleichgestellt werden, sind z.B. Mißhandlungen von Schutzbefohlenen oder sexueller Mißbrauch von Schutzbefohlenen und Kindern betroffen. Mit solchen Verfahren kommen die Jugendämter wesentlich häufiger in Berührung als mit Verbrechen. In diesen Fällen kann das Jugendamt notwendige Hilfe zur Erziehung oft nur sachgerecht planen und durchführen, wenn es nicht damit rechnen muß, daß es sein Wissen eventuell an Staatsanwaltschaft und Gericht weiterzugeben hat. Interessen des Opferschutzes und des Kindeswohls können deshalb mit dem Strafverfolgungsinteresse kollidieren. Ich halte es für problematisch, daß § 73 SGB X den Belangen der Strafrechtspflege Vorrang vor dem Interesse des Kindeswohls einräumt.

Kritisch beurteile ich auch die Änderung des § 78 SGB X. Hiernach dürfen Polizeibehörden, Staatsanwaltschaften, Gerichte und Behörden der Gefahrenabwehr Sozialdaten, die ihnen übermittelt worden sind, unabhängig vom Zweck der Übermittlung sowohl für Zwecke der Gefahrenabwehr als auch für Zwecke der Strafverfolgung und Strafvollstreckung verarbeiten und nutzen.

### 22.1 Welches Datenschutzrecht gilt für Träger der freien Jugendhilfe?

Die Frage, welche datenschutzrechtlichen Regelungen für Träger der freien Jugendhilfe gelten und welche konkreten Verpflichtungen § 61 Abs. 4 SGB VIII den Trägern der öffentlichen Jugendhilfe auferlegt, ist in hohem Maße klärungsbedürftig. Werden die freien Träger der Jugendhilfe an der Durchführung bestimmter Aufgaben beteiligt oder werden ihnen diese Aufgaben zur Ausführung übertragen, so ist nach dieser Vorschrift sicherzustellen, daß der Schutz von Sozialdaten bei ihrer Erhebung, Verarbeitung

und Nutzung in entsprechender Weise gewährleistet ist. Der Sinn dieser Regelung dürfte darin liegen, daß die Datenschutzbestimmungen, die für den Träger der öffentlichen Jugendhilfe gelten, letztlich auch für den Träger der freien Jugendhilfe Gültigkeit erhalten. Es kann bei der Wahrnehmung von gleichen Aufgaben bei den Trägern der freien Jugendhilfe kein geringerer Datenschutz bestehen als bei den Trägern der öffentlichen Jugendhilfe. In der Praxis besteht offenbar nicht selten Unklarheit darüber, in welcher Weise die Sicherstellung vorgenommen werden sollte. In der Literatur wird die Ansicht vertreten, die Sicherstellung könne durch entsprechende Selbstverpflichtung des freien Trägers oder dessen Zusicherung, durch Nachweis oder vertragliche Vereinbarung erfolgen. Ich sehe in einer vertraglichen Vereinbarung den geeignesten Weg, um der gesetzlichen Forderung zu genügen. Da § 61 Abs. 4 SGB VIII den Träger der öffentlichen Jugendhilfe in die Pflicht nimmt, für einen entsprechenden Sozialdatenschutz zu sorgen, sollte sich der Träger der öffentlichen Jugendhilfe mit einer bloßen Selbstverpflichtung, deren Einhaltung nicht kontrolliert wird, aus meiner Sicht nicht begnügen. Es ist zu überlegen, ob dies durch formularmäßige "Geschäftsbedingungen" geregelt werden kann. Darüber hinaus erhebt sich die Frage, wie sichergestellt werden kann, daß auch die freien Träger "keine Auskunftspflicht, keine Zeugnispflicht und kein Pflicht zur Vorlegung oder Auslieferung von Schriftstücken, Akten, Dateien und sonstigen Datenträgern" trifft (§ 35 Abs. 3 SGB I). Ich stehe wegen dieser Fragen in Diskussion mit dem Niedersächsischen Kultusministerium.

## 22.2 Praktikum in Jugendämtern

Nach § 67c Abs. 3 SGB X liegt eine Zweckänderung nicht vor, wenn vorhandene Daten zu Ausbildungs- und Prüfungszwecken durch die speichernde Stelle verändert oder genutzt werden, soweit nicht überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen. Die Vorschrift ermöglicht somit die Nutzung im Rahmen bestehender Ausbildungsverhältnisse. Ich habe daher keine grundsätzlichen Bedenken gegen die Akteneinsicht durch Auszubildende, soweit sie im Rahmen ihrer Ausbildung im Jugendamt an der Fallbearbeitung beteiligt sind. Dagegen dürfen Personen, die nicht in einem Beschäftigungsverhältnis stehen, wie Studierende oder sonstige Praktikantinnen bzw. Praktikanten, dem Sozialgeheimnis unterfallende Akten nicht einsehen. Dies ist unabhängig davon, ob ein legitimes Interesse anzuerkennen ist und die Praktikantin bzw. der Praktikant sich zur Verschwiegenheit verpflichtet.

## 22.3 Rufbereitschaft

Ein Landkreis hat mir mitgeteilt, daß er fachbezogen für Aufgaben nach dem Kinder- und Jugendhilfegesetz sowie nach dem PsychKG die in § 15 Abs. 6 b BAT tariflich vorgesehene Rufbereitschaftsregelung geschaffen hat. Nach dieser Vorschrift sind Angestellte verpflichtet, sich auf Anordnung des Arbeitgebers außerhalb der regelmäßigen Arbeitszeit an einer dem

Arbeitgeber anzuzeigenden Stelle aufzuhalten, um auf Abruf die Arbeit aufzunehmen (Rufbereitschaft).

Schwerpunkt der Inanspruchnahme außerhalb der regelmäßigen Arbeitszeit sind nach Darstellung des Landkreises Kriseninterventionen in Familienunterbringungsangelegenheiten. Das Jugendamt ist verpflichtet, ein Kind oder einen Jugendlichen in seine Obhut zu nehmen, wenn eine dringende Gefahr für das Wohl des Kindes odes des Jugendlichen die Inobhutnahme erfordert. Die in die Rufbereitschaft eingebundenen Mitarbeiterinnen und Mitarbeiter können darüber hinaus nach Einweisung durch das Gesundheitsamt Aufgaben nach dem Nds. PsychKG bei der Unterbringung von psychisch Kranken übernehmen. Das Verfahren für einstweilige Unterbringung bzw. vorläufige Einweisung ist in den §§ 12, 15 und 16 Nds. PsychKG geregelt. Die Aufgabe der Verwaltungsbehörde im Unterbringungsverfahren besteht darin, die einstweilige Unterbringung nach § 15 Nds. PsychKG beim Amtsgericht zu beantragen bzw. nach § 16 Nds. PsychKG nach Vorliegen eines ärztlichen Zeugnisses eine vorläufige Unterbringung bis zum Ablauf des folgenden Tages anzuordnen, wenn eine gerichtliche Entscheidung nicht rechtzeitig herbeigeführt werden kann.

Der Landkreis hält eine Einbeziehung von Sozialarbeiterinnen und Sozialarbeitern in die Rufbereitschaft aufgrund des Arbeitsvertrages und des Direktionsrechts des Arbeitgebers für zulässig. Er verweist darauf, daß der tarif- und arbeitsvertraglich gezogene Rahmen zumutbarer Tätigkeiten nach dem Ausbildungsprofil beachtet werde. Wenn die Arbeitspflicht arbeitsvertraglich nicht auf eine genau bestimmte Tätigkeit beschränkt sei, könne den Angestellten im Rahmen ihrer Qualifikation jede Tätigkeit übertragen werden, die den Merkmalen der Qualifikation und Vergütungsgruppe entspreche und die ihnen billigerweise zugemutet werden könne. Die Wahrnehmung administrativer Aufgaben gehöre zum regelmäßigen Anforderungsprofil von Sozialarbeiterinnen und Sozialarbeitern und verpflichte sie zur entsprechenden vorübergehenden Wahrnehmung auf Weisung des Arbeitgebers auch in anderen Organisationsbereichen, wenn dadurch die allgemeine Rechtsstellung nicht berührt werde. Diese Auffassung halte ich für zutreffend. In diesem Zusammenhang ist anzumerken, daß es nicht nur bei Einsätzen im Rahmen von Rufbereitschaften, sondern auch bei Urlaubs- oder Krankheitsvertretungen oder beim Wechsel auf einen anderen Arbeitsplatz sowie bei Amtsleitern und Dezernenten vorkommt, daß eine Person in verschiedenen Arbeitsfeldern tätig wird und in das jeweils andere Arbeitsfeld Wissen mitnimmt.

Die Frage, ob Jugendamtsbedienste, die ausschließlich mit Beratungsaufgaben betraut sind, Erkenntnisse aus den auf Vertraulichkeit beruhenden Beratungsgesprächen im Rahmen einer vom Landkreis veranlaßten Rufbereitschaft verwerten dürfen, ist zu verneinen. Das folgt aus der besonderen Schweigepflicht für Daten und Informationen aus der Beratungsstellentätigkeit. Es ist möglich und zumutbar, diese Informationen zu "verdrängen" bzw. für eine Entscheidung nicht zu verwerten. Ein solches Verhalten wird Verwaltungsbediensteten auch in anderen Verwaltungsbereichen abverlangt. Das Landesarbeitsgericht Niedersachsen hat festgestellt, daß eine Tä-

tigkeit in der Erziehungsberatungsstelle, die der Geheimhaltung nach §§ 203 Abs. 1 Nr. 4, 204 StGB unterliegt, eine Tätigkeit in der Rufbereitschaft nicht deshalb ausschließe, weil dort ggf. Erkenntnisse verwertet werden können, die bei der Beratung gewonnen wurden. § 203 Abs. 1 Nr. 4 StGB stellt das unbefugte Offenbaren eines fremden Geheimnisses unter Strafe. Das Gericht hat zu Recht betont, daß die Person in einer Rufbereitschaft, die in dieser Funktion nicht auf Informationen aus der Erziehungsberatung zurückgreift, von vornherein nicht in die Gefahr geraten kann, die genannte Strafvorschrift zu verletzen.

Mitarbeitende des Jugendamtes, die auf anderen Arbeitsfeldern eingesetzt werden, sind insofern nicht (mehr) als Jugendamtsmitarbeitende anzusehen. Erhalten diese im Rahmen der Rufbereitschaft über nächtlich betreute Personen (die bereits Klienten der Beratungsstelle sind oder waren) Informationen, so ist es ihnen nicht gestattet, andere Jugendamtsbedienstete darüber zu informieren. Sie sollten die Betroffenen an die zuständigen Bediensteten verweisen.

Der Landkreis hat im Rahmen eines Rechtsstreits dargelegt, daß Konfliktsituationen durch die Anordnung von Zwangsmaßnahmen gegenüber Personen, die die Mitarbeiterin bzw. den Mitarbeiter des Jugendamtes bereits in der Beratungsstelle aufgesucht haben, wenn überhaupt, nur äußerst selten auftreten werden. Grundsätzlich sollte in diesen Fällen ein anderer Mitarbeiter des Jugendamtes einspringen. Sollte dies ausnahmsweise nicht möglich sein, sei es zumutbar, selbst tätig zu werden.

22.4 Auskunftsrecht über nach dem Betreuungsgesetz betreute Personen

Gemäß § 1896 Abs. 1 BGB erhält eine volljährige Person dann eine Betreuerin oder einen Betreuer, wenn sie aufgrund einer psychischen Krankheit oder einer körperlichen, geistigen oder seelischen Behinderung ihre Angelegenheit ganz oder teilweise nicht besorgen kann. Gemäß § 1896 Abs. 2 BGB wird eine Betreuerin oder ein Betreuer nur für den Aufgabenkreis bestellt, in welchem eine Betreuung auch erforderlich ist. In diesem Aufgabenkreis ist die Betreuerin oder der Betreuer gesetzliche Vertreterin oder gesetzlicher Vertreter der betroffenen Person (§ 1902 BGB). Unabhängig davon hat die Bestellung einer Betreuerin oder eines Betreuers keinen Einfluß auf die Geschäftsfähigkeit der betroffenen Person. Vielmehr gilt die betroffene Person so lange als geschäftsfähig, wie nicht im Einzelfall das Gegenteil festgestellt worden ist. Im Bereich der Gesundheitssorge genügt es darüber hinaus, daß zur Einwilligung in eine ärztliche Behandlung lediglich die Einwilligungsfähigkeit der betroffenen Person gegeben ist. Ist dies der Fall, kommt es ausschließlich auf den Willen der betroffenen Person an.

Dies wiederum kann nicht bedeuten, daß insoweit allein die betroffene Person Anspruch auf umfassende Aufklärung ihrer gesundheitlichen Situation besäße. Die Übertragung der Beratungsaufgabe beinhaltet die Pflicht, innerhalb des Aufgabenkreises für die betroffene Person tätig zu werden oder sie in die Lage zu versetzen, ggf. selbst zu entscheiden. Die Wahrnehmung

der Gesundheitssorge ist nur dann möglich, wenn die Betreuerin oder der Betreuer über alle wesentlichen Gegebenheiten in bezug auf die betroffene Person informiert ist. Die Betreuerin oder der Betreuer hat demzufolge durch die Übertragung dieses Aufgabenkreises einen Anspruch auf umfassende Aufklärung der gesundheitlichen Belange der betreuten Person durch die jeweils behandelnde Ärztin oder den jeweils behandelnden Arzt, damit ggf. die erforderlichen Maßnahmen und Entscheidungen getroffen werden können. Hierfür ist es nicht ausreichend, daß lediglich die Diagnose kommentarlos mitgeteilt wird.

Da nur ein Anspruch auf allgemeine Aufklärung besteht, dürfte es der Ärztin oder dem Arzt überlassen sein, in welcher Art und Weise eine Aufklärung und Information erfolgen. Dies kann durch persönliche umfassende Aufklärung geschehen, durch die Gewährung der Einsichtnahme in Befundberichte oder durch eine andere Ärztin oder einen anderen Arzt anhand der Befundberichte. Hierin besteht Einvernehmen zwischen dem Niedersächsischen Sozialministerium, dem Niedersächsischen Justizministerium und mir.

Das Justizministerium hat ergänzend darauf hingewiesen, daß gemäß § 34 FGG die Möglichkeit der Einsichtnahme in die gerichtlichen Verfahrensakten besteht, die oftmals auch Abdrucke ärztlicher Stellungnahmen enthalten. Die Gerichte werden entsprechende Anträge in eigener Zuständigkeit zu prüfen haben. Für den Bereich der Gebrechlichkeitspflegschaft ist von den Gerichten ein berechtigtes Interesse an einer Akteneinsicht bereits anerkannt worden. Aus den Pflichten der Betreuerin und Betreuer wird im Einzelfall ebenfalls ein rechtliches Interesse gemäß § 13 Abs. 1 Satz 1 Nr. 2 NDSG oder auch ein berechtigtes Interesse gemäß § 34 FGG hergeleitet werden können.

22.5 Täter-Opfer-Ausgleich im Bereich der Jugendhilfe

Der Täter-Opfer-Ausgleich als solcher ist ausdrücklich gesetzlich bisher nur im Jugendgerichtsgesetz (JGG) verankert, und zwar in § 10 JGG als Erziehungsmaßnahme und in § 45 JGG als Bemühen von Jugendlichen, die erzieherischen Maßnahmen gleichstehen. Nach Auffassung des Niedersächsischen Kultusministeriums und des Niedersächsischen Justizministeriums ist die Durchführung des Täter-Opfer-Ausgleichs aber auch eine soziale Leistungsaufgabe der Jugendhilfe im Sinne von § 52 Abs. 1 Satz 2 i.V.m. §§ 27 ff., 41 SGB VIII (also nicht der Jugendgerichtshilfe im engeren Sinne von § 38 JGG bzw. §§ 2 Abs. 3 Nr. 8, 76 SGB VIII). Dementsprechend fördert das Land Täter-Opfer-Ausgleichsangebote von Jugendämtern und freien Trägern der Jugendhilfe als Angebote der Jugendhilfe. Unmittelbarer Adressat der Datenschutzbestimmungen des SGB VIII ist nur das Jugendamt. Wenn eine Jugendhilfeleistung durch einen Träger der freien Jugendhilfe erbracht wird, so ist das Jugendamt berechtigt und verpflichtet, personenbezogene Daten weiterzugeben (§ 69 Abs. 1 Nr. 1 SGB X). Für eine Datenweitergabe durch Staatsanwalt oder Gericht sind §§ 67 ff. SGB X und §§ 61 ff. KJHG nicht maßgeblich.

## 23. Kulturgut- und Denkmalschutz: Wer kassiert, wird kontrolliert

Das Niedersächsische Denkmalschutzgesetz (DenkmalschutzG) bestimmt, daß Kulturdenkmale von ihren Eigentümern instand zu halten und, wenn nötig, instand zu setzen sind. Diese Erhaltungspflicht hat natürlich Grenzen. Soweit die Erhaltung zu einer unzumutbaren wirtschaftlichen Belastung führt, können Erhaltungsmaßnahmen nicht (mehr) gefordert werden. Um die Frage der wirtschaftlichen Zumutbarkeit prüfen zu können, verlangte ein Landkreis neben der Ausfüllung eines umfangreichen Fragebogens die Erklärung des Antragstellers, daß er das jeweilige Finanzamt von der Pflicht zur Wahrung des Steuergeheimnisses vollständig entbinde. Diese Verfahrensweise ging offensichtlich auf eine Dienstbesprechung der unteren Denkmalschutzbehörden mit der zuständigen Bezirksregierung zurück.

Nachdem ich mich eingeschaltet hatte, verzichtete der Landkreis zwar im angeführten Fall auf die Erklärung. Die Bezirksregierung als obere Denkmalschutzbehörde war jedoch der Meinung, für die Zukunft reiche es aus, in den Vordruck einen Hinweis aufzunehmen, daß die Entbindungserklärung freiwillig abgegeben werde und daß eine Verweigerung der Erklärung dazu führen könne, daß u.U. ein geschätzter, ungünstigerer Steuersatz bei der Prüfung der wirtschaftlichen Zumutbarkeit zugrunde gelegt werden könne. Hiermit konnte ich mich nicht einverstanden erklären.

Nach § 7 Abs. 3 DenkmalschutzG ist die wirtschaftliche Belastung durch ein Kulturdenkmal insbesondere dann unzumutbar, wenn die Erhaltungs- und Bewirtschaftungskosten nicht durch Erträge oder den Gebrauchswert des Kulturdenkmals aufgewogen werden können. Der Gesetzgeber geht somit davon aus, daß für die Zumutbarkeit des Unterhaltungsaufwands nicht die gesamte Vermögenslage des Betroffenen ausschlaggebend ist. Es wird (nur) objektbezogen auf die Wirtschaftlichkeit der Unterhaltung des Kulturdenkmals abgestellt. Eine umfassende Ermittlung seiner Einkommensverhältnisse ist deshalb nicht notwendig. Damit ist auch eine uneingeschränkte Entbindung vom Steuergeheimnis nicht erforderlich. Grundsätzlich reicht es aus, von den Betroffenen - soweit notwendig - Nachweise über die Richtigkeit ihrer Angaben vorlegen zu lassen. In Zweifelsfällen muß allerdings die Wirtschaftlichkeit durch die zuständige Denkmalschutzbehörde anhand einer konkreten Wirtschaftlichkeitsberechnung überprüft werden. Hierzu bestimmt § 7 Abs. 3 Satz 2 DenkmalschutzG, daß steuerliche Vorteile anzurechnen sind, die der Verpflichtete in Anspruch nehmen kann. Die konkreten steuerlichen Vorteile sind abhängig von der Höhe des Steuersatzes. In diesen Fällen kann daher der gesetzliche Auftrag nur erfüllt werden, wenn die steuerlichen Vorteile mit Hilfe des (allgemeinen) Steuersatzes des Denkmaleigentümers errechnet werden. Ist der Betroffene dann nicht bereit, seinen Steuersatz nachzuweisen oder das Finanzamt insoweit (eingeschränkt) vom Steuergeheimnis zu befreien, müßte er allerdings damit rechnen, daß sein Steuersatz geschätzt oder der Höchstsatz angenommen werden würde. Mit einer Überprüfung der gesamten Vermögenslage des Verpflichteten hat dies nichts zu tun.

Das Niedersächsische Ministerium für Wissenschaft und Kultur hat den geschilderten Fall zum Anlaß genommen, die unteren Denkmalschutzbehörden darauf hinzuweisen, daß in den benutzten Berechnungsbögen eine Erklärung über die Entbindung vom Steuergeheimnis nicht mehr vorgesehen wird.

## 24. Forschung

### 24.1 Probleme bei der Anwendung der Forschungsregelung

In meinem XI. Tätigkeitsbericht hatte ich unter Ziffer 24.1 darüber berichtet, daß mir in der Vergangenheit eine Vielzahl von Forschungsvorhaben mit der Bitte vorgelegt worden ist, hierzu eine datenschutzrechtliche Unbedenklichkeitsbescheinigung abzugeben. Die an dieser Stelle dargelegten Gründe für die Nichterteilung derartiger Unbedenklichkeitserklärungen haben nach wie vor Gültigkeit.

Mit dem Inkrafttreten des neuen NDSG steht für die datenschutzrechtliche Beurteilung von Forschungsvorhaben mit § 25 eine Regelung zur Verfügung, die zwar nicht in allen Einzelheiten meinen Vorstellungen entspricht, jedoch eine wesentliche Verbesserung der Rechtssituation gebracht hat.

§ 25 regelt als allgemeine "Forschungsklausel" die Verarbeitung personenbezogener Daten für wissenschaftliche Zwecke durch öffentliche Stellen, die Forschung betreiben. Eine solche Vorschrift fehlte im NDSG von 1978. Sowohl die Freiheit der Forschung (Art. 5 Abs. 3 Satz 1 GG) wie auch das Recht auf informationelle Selbstbestimmung haben Verfassungsrang. Mit § 25 wird ein Ausgleich zwischen den beiden Rechtsgütern und den sich widersprechenden Interessen geschaffen. Als wesentliche Voraussetzungen wurden vom Gesetzgeber festgelegt:

- strenge Erforderlichkeitsprüfung
- umfassende, schriftlich aufzuzeichnende Abwägung der Interessen
- strenge Zweckbindung auf das jeweilige Forschungsvorhaben
- frühestmögliche Anonymisierung der Personenangaben
- enge Grenzen bei der Veröffentlichung personenbezogener Forschungsergebnisse (Einwilligung, Personen der Zeitgeschichte).

Werden besonders sensible Daten für Forschungszwecke verarbeitet, so bedarf es u.U. weiterer Einschränkungen. Dies gilt insbesondere für die dem Arztgeheimnis unterliegenden Angaben über den Gesundheitszustand von Bürgerinnen und Bürgern. Aus diesem Grund bleibt der Gesetzgeber aufgefordert, hier noch weitere besondere Schutzvorkehrungen vorzunehmen.

In der Praxis hat sich gezeigt, daß die öffentlichen Stellen im Lande Niedersachsen, die mit Forschungsvorhaben konfrontiert werden, zum Teil noch (verständliche) Anwendungsprobleme mit der Regelung haben. Dies fängt mit der Frage an, ob überhaupt von einem Forschungsvorhaben die Rede

sein kann. Für die Annahme eines Forschungsvorhabens muß der Forschungszweck hinreichend bestimmt festgelegt werden. Wissenschaftliche Forschung ist "alles, was nach Inhalt und Form als ernsthafter, planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist" (BVerfGE 35, 112 f. = NJW 1978, 1176). Forschung ist nicht dadurch ausgeschlossen, daß das Vorhaben auch Ausbildungs- und Prüfungszwecken dient. So sind Dissertations- und Habilitationsvorhaben regelmäßig Forschung, nicht aber eine der Ausbildung dienende Studienarbeit. Keine Forschung sind auch Untersuchungen, die zu Aufsichts-, Organisations- und Kontrollzwecken durchgeführt werden.

Vom Grundsatz bedarf die Verarbeitung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung in allen ihren Phasen der Einwilligung der Betroffenen. Eine Alternative besteht darin, daß eine Rechtsvorschrift die Forschung durch öffentliche Stellen ausdrücklich erlaubt. Rechtsvorschriften sind auch Satzungen von Kommunen oder von sonstigen Selbstverwaltungskörperschaften, wie z.B. den Hochschulen. In jedem Fall bedarf es aber einer gesetzlichen Ermächtigung zum Erlaß dieser Rechtsvorschriften.

Mit § 25 Abs. 2 Nr. 3 NDSG schafft das Gesetz zwei besondere Zweckdurchbrechungstatbestände. Danach ist die Einwilligung verzichtbar, wenn kein Grund zur Annahme besteht, daß die Betroffenen ein schutzwürdiges Interesse an dem Ausschluß ihrer Daten von der Nutzung zu Forschungszwecken haben (1. Alt.) oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens das schutzwürdige Interesse der Betroffenen erheblich überwiegt (2. Alt.). Liegen diese Voraussetzungen vor, so ist die Datenverarbeitung in der jeweiligen Verarbeitungsphase zulässig. Die Prüfung, ob eine dieser Voraussetzungen vorliegt, bereitet den an mich herantretenden Stellen vielfach Probleme. Aus den mir vorgelegten schriftlichen Unterlagen geht oftmals nicht hervor, unter welchen Tatbestand die beabsichtigte Datenverarbeitung für wissenschaftliche Zwecke subsumiert werden soll; das Ergebnis der Abwägung, sofern die 2. Alt. greift, wird z.T. gar nicht oder nur unzulänglich dargestellt.

Um sicherzustellen, daß die Abwägung den Intentionen des Gesetzes Rechnung trägt, ist eine spezielle Dokumentationspflicht und die Unterrichtung des Landesbeauftragten vorgesehen. Die Unterrichtung hat in jedem Fall einer Verarbeitung nach Nr. 3 (1. und 2. Alt.) zu erfolgen. Der gegenüber dem Entwurf vorgenommene Wechsel in der Wortwahl von "anzuzeigen" in "zu unterrichten" soll deutlich machen, daß es nicht Aufgabe des LfD sein kann, den forschenden Einrichtungen datenschutzrechtliche Entscheidungen abzunehmen, zumal er damit schon wegen der Vielzahl der Fälle überfordert wäre. Entstehen bei den forschenden und deren vorgesetzten Stellen Zweifel, so können sie sich selbstverständlich der Sachkunde meiner Geschäftsstelle bedienen. Die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorgaben verbleibt vollständig bei der forschenden Stelle bzw. dem jeweils zuständigen Ressort. Daher sollten sich die Forschenden bei datenschutzrechtlichen Unklarheiten auch zunächst an die übergeordnete Stelle wenden, bevor sie den LfD einschalten.

Die Unterrichtung soll dem LfD die Möglichkeit geben, das Forschungsvorhaben insgesamt oder dessen Ablauf zu überprüfen. Der LfD hat keine Pflicht zur Reaktion auf die Unterrichtung. Aus seinem Schweigen kann jedoch nicht geschlossen werden, daß überhaupt keine datenschutzrechtlichen Bedenken bestehen. Der LfD kann seine datenschutzrechtlichen Bedenken der öffentliche Forschungsstelle unter Angabe der Gründe mitteilen. Soweit möglich, werden datenschutzrechtliche Verbesserungsvorschläge unterbreitet.

Abs. 7 der Vorschrift regelt die Übermittlung an private Stellen zu Forschungszwecken sowie an öffentliche Stellen außerhalb des Geltungsbereichs des NDSG. Die Datenempfänger sind verpflichtet, ihr Forschungsvorhaben konkret zu benennen, für das sie die Daten verarbeiten wollen. Die Zweckbindung und weitere Verarbeitungsvorgaben müssen nach Maßgabe des NDSG durch spezielle Absprachen mit der forschenden Stelle gesichert werden. Die Anzeigepflicht gegenüber dem Landesbeauftragten sorgt für Selbstkontrolle sowie Transparenz und ermöglicht gezielte Kontrollmaßnahmen oder weitere Interventionen, ggf. in Zusammenarbeit mit anderen Kontrollinstanzen, und zwar bevor die Verarbeitung erfolgt. Die Anzeige sollte so früh wie möglich, spätestens aber einen Monat vor Beginn der Verarbeitung erfolgen. Auch hier besteht keine Pflicht des LfD zur Reaktion auf die Unterrichtung.

Im Rahmen meiner Öffentlichkeitsarbeit bereite ich ein Merkblatt "Datenschutz und Forschung - Hilfen zur Auslegung der Forschungsklausel nach § 25 NDSG" vor, das voraussichtlich Anfang 1995 in meiner Dienststelle angefordert werden kann.

## 24.2 Rinderwahnsinn beim Menschen ?

In Presseberichten wird immer wieder die Frage gestellt, ob die insbesondere in Großbritannien verbreitete, unter dem Namen "Rinderwahnsinn" bekannte Tierseuche BSE auf den Menschen übertragbar ist. Dieser Verdacht ist aufgekommen, nachdem zwei Bauern, deren Tiere von der Seuche betroffen waren, an der Creutzfeldt-Jakob-Krankheit erkrankt sind. Diese Krankheit zeigt Ähnlichkeiten mit der Rinderseuche BSE (bovine spongiforme Enzephalopathie). Grund genug, der Frage forschend nachzugehen. Ich wurde um die datenschutzrechtliche Bewertung eines entsprechenden Projektes gebeten, das die Universität Göttingen für die gesamte Bundesrepublik in Rahmen einer europaweiten Studie durchführt. Von der Creutzfeldt-Jakob-Krankheit dürften in der Bundesrepublik ca. 40 Personen betroffen sein. Bei über 90 % der Betroffenen führt die Krankheit über eine schnell voranschreitende Demenz innerhalb eines Jahres zum Tod.

Zur Durchführung des Projektes sollte zunächst eine Meldung der mit der Krankheit in Berührung kommenden Ärztinnen und Ärzte an die Forschungsgruppe erfolgen. Vor Ort sollte dann eine Untersuchung der Betroffenen sowie von Kontrollpatienten erfolgen. Geplant war außerdem die

Durchführung von Genanalysen. Das federführende Niedersächsische Ministerium für Wissenschaft und Kultur teilte mir mit, daß es nach Abwägung aller Gesichtspunkte die Durchführung des Forschungsprojektes befürworte. Es bestünde eine erhebliche Gefährdung für die Bevölkerung, wenn sich der Verdacht bestätigte, daß der "Rinderwahnsinn" durch Fleischverzehr auf den Menschen übertragbar sei.

Ich vertrete die Ansicht, daß § 25 NDSG wegen der besonderen Sensibilität von Patientendaten keine ausreichende Rechtsgrundlage für medizinische Forschungsvorhaben darstellt. Im Hinblick auf die Forschungsfreiheit nach Art. 5 Abs. 3 GG wende ich jedoch wegen des Fehlens sonstiger bereichsspezifischer Regelungen diese Norm zwar entsprechend an, behalte mir jedoch vor, über die Norm hinausgehende Datenschutzsicherungen zu verlangen (vgl. 25.1). Gegen das Verfahren, zunächst eine anonymisierte Meldung vorzunehmen und dann einer Mitarbeiterin bzw. einem Mitarbeiter der Forschungsgruppe unter Beachtung des § 25 NDSG, insbesondere des Abs. 2 Nr. 3 NDSG Einblick in die Patientenakten zu geben, hatte ich keine grundsätzlichen Bedenken.

Für die Durchführung genomanalytischer Untersuchungen halte ich dagegen Einwilligungen der Betroffenen für unverzichtbar. Können diese wegen des gesundheitlichen Zustands der Betroffenen nicht eingeholt werden, so bedarf es zwingend der Einwilligung einer gesetzlich bestellten Betreuerin bzw. eines Betreuers (vgl. §§ 1896, 1904 BGB). Auch hinsichtlich der Verarbeitung von Angehörigendaten sowie der Daten von Kontrollpersonen erachte ich das Einholen von Einwilligungen für möglich und für rechtlich geboten.

Ebenso wie das Sozialministerium meine ich, daß eine rechtliche Einstufung der Forschungsgruppe als mitbehandelnde Ärzte bzw. Gehilfen, die unbeschränkt Zugang zu allen Patientenakten hätten, nicht möglich ist. Unproblematisch, aus medizinischer Sicht sogar wünschenswert ist es dagegen, wenn aus der Forschungsgruppe Anregungen an die behandelnde Ärztin bzw. den Arzt gegeben werden, die besondere Untersuchungen und Behandlungsformen zur Folge haben.

Schließlich wies ich darauf hin, daß die behandelnden Ärztinnen und Ärzte weder zu einer Meldung noch zur Gewährung der Akteneinsicht verpflichtet sind. Ebenso wenig besteht die Verpflichtung zur Erteilung rechtlich erforderlicher Einwilligungen durch die Betroffenen.

## 24.3 Das lange Gedächtnis der Forschung

Vom Datenschutzbeauftragten der Medizinischen Hochschule Hannover (MHH) wurde mir ein Forschungsvorhaben präsentiert, gegen das ich schwerwiegende Bedenken vorbringen mußte: Eine Doktorandin sollte im Rahmen ihrer Arbeit die psychischen Folgen von Schwangerschaftsabbrüchen untersuchen. Zu diesem Zweck sollten aus den Akten einer Frauenklinik die Namen und Adressen von Frauen entnommen werden, die vor mehr

als 10 Jahren einen Schwangerschaftsabbruch durchführen ließen. Die Patientinnen sollten sodann zum Zweck einer standardisierten Befragung namentlich angeschrieben werden. Die volle Anonymität der Patientinnen sollte zugesichert werden.

Forschungsvorhaben sind zulässig, wenn die Betroffenen eingewilligt haben. Auch bei der Einholung der Einwilligung muß jedoch das allgemeine Persönlichkeitsrecht beachtet werden. Der Einblick der Doktorandin in die Patientinnenakten zur Einholung der Einwilligung selbst wäre schon als Datenweitergabe zu qualifizieren gewesen. Die Einwilligung bei den Betroffenen hätte daher in jedem Fall durch die aktenführende Stelle selbst eingeholt werden müssen.

Problematisch erschien mir aber insbesondere der Grundansatz des Forschungsprojektes. Die Bezugnahme auf zehn und mehr Jahre zurückliegende Schwangerschaftsabbrüche hätte dazu geführt, daß die Betroffenen nunmehr mit einer weit zurückliegenden und u.U. psychisch schmerzlichen Erfahrung konfrontiert worden wären. Schon das Anschreiben der Betroffenen hätte eine solche Konfrontation zur Folge gehabt. Ich äußerte daher Zweifel, ob das Projekt schon aus medizinisch-fachlicher Sicht ergiebig und sinnvoll sei.

In der Rechtsprechung des BVerfG ist es anerkannt, daß das allgemeine Persönlichkeitsrecht auch einen "Anspruch auf Vergessen" beinhaltet. Das Sozialstaatsprinzip verlangt eine staatliche Vor- und Fürsorge für Gruppen der Gesellschaft, die durch bestimmte Ereignisse in der Vergangenheit in ihrer persönlichen und sozialen Entfaltung behindert sind (NJW 1973, 1231 f.).

Im Hinblick auf die besondere Sensibilität der Information "Schwangerschaftsabbruch" war nicht auszuschließen, daß im Zusammenhang mit der beabsichtigten Postzustellung an die ehemaligen Patientinnen erhebliche Beeinträchtigungen des informationellen Selbstbestimmungsrechts eintreten. Das persönliche Anschreiben der Adressatinnen hätte keinen ausreichenden Schutz dargestellt, da gerade eine solche persönliche Adressierung bei Mitwohnenden Neugierde und Erklärungszwänge hätte entstehen lassen können, die u.U. letztendlich dazu führten, daß die Betroffenen unfreiwillig die Tatsache eines lange zurückliegenden Schwangerschaftsabbruchs hätten offenbaren müssen.

Aufgrund meiner Stellungnahme sowie eines entsprechenden Votums des Datenschutzbeauftragten der MHH entschloß sich der betreuende Professor, das Projekt nicht durchführen zu lassen.

## 24.4 Auswertung von Akten über nationalsozialistische Gewaltverbrechen (NSG)

Das Niedersächsische Justizministerium beabsichtigte, einen Forschungsauftrag zu erteilen, der die Auswertung von Ermittlungsakten aus Strafver-

fahren gegen nationalsozialistische Gewaltverbrecher ab 1945 bis in die jüngste Vergangenheit beinhaltet. Die Ermittlungsverfahren haben teilweise zu Anklagen und Verurteilungen geführt, teilweise wurden sie vor einer möglichen Anklageerhebung eingestellt. Ausgewertet werden sollten auch beim Niedersächsischen Justizministerium befindliche verfahrensbezogene, nicht personenbezogene Dienstaufsichtsvorgänge, die aufgrund der Meldepflicht von NSG-Verfahren im Niedersächsischen Justizministerium angefallen sind.

Das Ministerium hielt die Nutzung von Akten, in welchen neben den Angeschuldigten Datenangaben Dritter enthalten sind (z.B. Verwandte, Opfer) für problematisch. Unklar war auch die Frage, inwieweit der Datenschutz die Nutzung der Daten von öffentlich Bediensteten, die z.B. sich im Rahmen der NS-Verfahren für Beschuldigte eingesetzt haben, einschließt.

Auf Datenschutzrechte können sich öffentlich Bedienstete gegenüber dem Staat nur berufen, soweit sie diesem als eigenständiger Träger von Rechten und Pflichten gegenübertreten. Dies ist der Fall, soweit etwa bei Beamten das Dienst- bzw. Grundverhältnis berührt wird. Soweit dagegen ein Amtsträger für den Staat handelt, dem diese Tätigkeit auch zugerechnet wird, ist das informationelle Selbstbestimmungsrecht des Bediensteten bei der Verarbeitung seiner personenbezogenen Daten nicht betroffen. Einschränkungen der Befugnisse des Dienstherrn können sich jedoch aus den hergebrachten Grundsätzen des Berufsbeamtentums (Art. 33 Abs. 4 GG) und aus Regelungen des öffentlichen Dienstrechts ergeben.

Zu berücksichtigen waren weiterhin archivrechtliche Regelungen. Zwar war weder das neue NDSG noch das NArchG (vgl. 8.) zum damaligen Zeitpunkt in Kraft getreten. Doch habe ich die in den Gesetzentwürfen enthaltenen Grundüberlegungen bei meiner Bewertung mit herangezogen. Danach hat "jedermann" Zugang zu Archivgut 30 Jahre nach Bearbeitung einer Sachakte sowie 10 Jahre nach dem Tod einer Person, wenn die Akte zu einer Person geführt wird. Eine vergleichbare Regelung enthält übrigens § 73 der Gemeinsamen Geschäftsordnung der Niedersächsischen Ministerien vom 20. September 1955. Es ist aber auch unbestritten, daß bei eindeutig überwiegendem Interesse eine Fristverkürzung erfolgen kann, wobei die schutzwürdigen Interessen von Betroffenen angemessen beachtet werden müssen. Auf Besonderheiten der Forschung über den Nationalsozialismus geht auch das neue NArchG nicht ein. Gerade in diesen Fällen kann eine Interessenlage zugrundeliegen, die mit derjenigen der Aufarbeitung der Geschichte der DDR und des Ministeriums für Staatssicherheit vergleichbar ist (vgl. Stasi-Unterlagen-Gesetz vom 20.12.1991, BGBl. I S. 2272). Das StUG enthält keine Schutzfristen. Auch in der nunmehr geltenden Forschungsregelung des § 25 NDSG fehlen sie. Bei der Bereitstellung der öffentlichen Akten muß daher eine Abwägung des von Art. 5 Abs. 3 GG geschützten Forschungsinteresses mit Datenschutzinteressen vorgenommen werden.

Das Ministerium hat mir kundgetan, daß die Akteneinsicht unter Berücksichtigung meiner Überlegungen ermöglicht werden sollte.

## 25. Hochschulen

Auf Initiative des Datenschutzbeauftragten der Universität Oldenburg haben drei Tagungen der behördlichen Datenschutzbeauftragten der Hochschulen des Landes stattgefunden. Diese dienen dem internen Erfahrungs- und Meinungsaustausch. Durch die Präsenz des Niedersächsischen Ministeriums für Wissenschaft und Kultur sowie meiner Dienststelle ist es möglich, auftauchende Fragen unbürokratisch und einvernehmlich zu klären. Bei den Tagungen stand die Umsetzung der Novellen des NDSG sowie des Hochschulgesetzes im Vordergrund, z.B. die Anwendung der Forschungsklausel oder der Regelung zur Evaluation.

### 25.1 Hochschulgesetz

Unter XI 25.1 stellte ich den Entwurf der im Landtag eingebrachten 5. Novelle zum Niedersächsischen Hochschulgesetz (NHG) vor. Nach langwierigen Verhandlungen konnte diese Ende 1993 im Landtag verabschiedet werden und trat am 1. Januar 1994 in Kraft (Nds. GVBl. 1993 S. 618; Neufassung des NHG: Nds. GVBl. 1994 S. 13). Meine Versuche, noch datenschutzrechtliche Verbesserungen zu initiieren, hatten nur mageren Erfolg. In der Datenschutzregelung des § 38 Abs. 1 NHG wurden lediglich kleine redaktionelle Änderungen vorgenommen, ohne daß die generelle Befugnis zur Nutzung der Immatrikulationsdaten für andere Hochschulzwecke eingeschränkt wurde. Durch den Verweis auf die §§ 2 und 3 NHG dürfen somit Immatrikulationsdaten z.B. für die "Pflege und Entwicklung der Wissenschaften und der Künste durch Forschung und künstlerische Vorhaben sowie durch Lehre, Studium und Weiterbildung" verwendet werden. Es muß nunmehr verhindert werden, daß der Verweis auf diese programmatischen Regelungen nicht dazu benutzt wird, das datenschutzrechtliche Zweckbindungsprinzip zu untergraben.

Von meinem Wunsch, in das NHG ein Verbot der Nutzung privater Personal Computer für dienstliche Zwecke aufzunehmen, ist nicht viel übrig geblieben. § 38 Abs. 3 NHG enthält nur noch die selbstverständliche Feststellung, daß die Verarbeitung von Hochschuldaten dürfe "nur auf Anlagen erfolgen, die der Aufsicht der oder des Landesbeauftragten für den Datenschutz unterliegen".

In den §§ 99 bis 102 NHG sind ausführliche Regelungen zu Frauenbeauftragten aufgenommen worden. Diese haben nunmehr ein umfassendes Informationsrecht, das u.a. die Einsicht in Bewerbungsunterlagen einschließt. Die Einsicht darf aber nur im Rahmen ihrer Aufgabenwahrnehmung, also zur Wahrnehmung der "Belange der Hochschulfrauen" erfolgen. Ich gehe davon aus, daß kein Akteneinsichtsrecht besteht, wenn sich für eine Stelle lediglich Männer beworben haben. In § 102 Abs. 1 Satz 2 NHG ist vorgesehen, daß sich die Frauenbeauftragten einer Hochschule bei der Wahrnehmung ihrer Aufgaben gegenseitig vertreten. Hinsichtlich der Einicht in personenbezogene Akten ist es meines Erachtens erforderlich, daß eine ausdrückliche schriftliche Vertretungsermächtigung vorgelegt wird.

25.2 Der Schrecken aller Lehrenden und Forschenden: Evaluation

Bei Hochschulverwaltungen, Lehrenden und Studierenden besteht offensichtlich große Verunsicherung, in welcher Form hochschulpolitische Gruppen oder Einrichtungen der Hochschule Befragungen über die Studiensituation durchführen, auswerten und veröffentlichen dürfen. Derartige "Evaluationen" können insbesondere für Hochschullehrerinnen und Hochschullehrer unangenehm sein, wenn dabei ein für sie ungünstiges Ergebnis herauskommt. Auf Bitte der Datenschutzbeauftragten der Hochschulen habe ich einige Leitlinien für die Durchführung von Evaluationen, die erstmalig im neuen NHG in § 38 Abs. 2 ausdrücklich erwähnt werden, entwickelt.

Die Notwendigkeit der Regelung wurde vom Ministerium für Wissenschaft und Kultur damit begründet, daß Daten gebraucht würden, mit denen die Ursachen für ein ineffektives Studienangebot und für die teilweise sehr lange Studiendauer ausfindig gemacht werden können (vgl. XI 25.1). Sie erfaßt ausschließlich von den Hochschulen durchgeführte Evaluationen. In diesem Sinne können z.B. folgende Organe tätig werden: Hochschulleitung, Frauenbeauftragte, Leitung der Fachbereiche oder Organe der Studentenschaft (Allgemeiner Studentenausschuß, Fachschaften). Nicht erfaßt sind private Initiativen, z.B. die Erhebung durch einzelne Hochschulangehörige, durch Externe oder durch hochschulpolitische Organisationen von Studierenden. Derartige private Initiativen sind weitgehend zulässig. Es darf dabei aber nicht der Anschein erweckt werden, es handele sich um offizielle Evaluationen (z.B. durch Verwendung universitärer Briefköpfe). Private Evaluationen können keine Auskunftspflicht der Befragten begründen. Bei der Durchführung und der Veröffentlichung von Ergebnissen privater Evaluationen ist darauf zu achten, daß keine ehrverletzenden und unwahren Aussagen gemacht werden. Falsche oder herabwürdigende Tatsachenbehauptungen, Persönlichkeitsverfälschungen, die unerlaubte Erhebung, Speicherung, Verwertung und Verbreitung von Informationen aus der Privatsphäre, aber auch evtl. schwerwiegende Belästigungen und Zumutungen sind nicht zulässig.

§ 38 Abs. 2 NHG erlaubt Hochschulorganen die Erhebung und Verarbeitung von Daten "zur Beurteilung der Bewerbungssituation, der Lehr- und Forschungstätigkeit, des Studienangebots sowie des Ablaufs von Studium und Prüfungen". Möglich sind diese Evaluationen, wenn entweder die erforderlichen Einwilligungen vorliegen oder diese durch Satzung geregelt sind. Für Einwilligungen ist es nach § 4 Abs. 2 NDSG erforderlich, daß die Betroffenen über den Verwendungszweck der Daten und über die Freiwilligkeit des Ausfüllens unterrichtet sind. Werden Daten von Hochschulangehörigen (z.B. über Lehrende od. Forschende) bei Dritten (z.B. Studierenden) erhoben, so bedarf es auch der Einwilligung der betroffenen Hochschulangehörigen. Bei Evaluationen aufgrund einer Hochschulsatzung erfolgt dort die Festlegung des Zwecks, des Inhalts und Umfangs der Auskunftspflicht, der Erhebungsmerkmale und des Erhebungsverfahrens.

Absatz 2 Satz 3 verbietet die Verwendung der Daten für andere als die bei der Erhebung angegebenen bzw. in der Satzung aufgeführten Evaluationszwecke. Damit soll verhindert werden, daß andere als organisatorische und

planerische Konsequenzen aus den Evaluationen gezogen werden. Verboten sind insbesondere disziplinarische und sonstige dienstrechtliche Maßnahmen sowie die Heranziehung bei Prüfungen. Die Pflicht zur frühestmöglichen Anonymisierung nach Absatz 2 Satz 4 entspricht der für den Forschungsbereich geltenden Regelung des § 25 Abs. 4 NDSG. Die Anonymisierungspflicht gilt zunächst bzgl. der Daten der Befragten. Deren Namen müssen bei Vollerhebungen spätestens dann gelöscht werden, wenn die Vollständigkeitskontrolle der Unterlagen beendet ist. Die Anonymisierungspflicht betrifft auch personenbezogene Daten, die im Rahmen der Evaluation entstehen. Sie entfällt jedoch, wenn das Ziel der Evaluation z.B. darin besteht, die konkrete Lehr- und Forschungstätigkeit zu eruieren. Zweck der im Gesetz obligatorisch vorgesehenen Rechenschaftslegung ist die Herstellung universitärer Transparenz.

Inzwischen sind mir erste Beschwerden wegen unangemessener Evalationsvorhaben vorgetragen worden. Wegen der Sensibilität des Bereichs werde ich aber auch unabhängig von Betroffeneneingaben die Anwendung des § 38 Abs. 2 NHG kritisch begleiten.

25.3 Überflüssige Lebensläufe?

Für die Verleihung der Grade "Doktor der Naturwissenschaften" und "Doktor der Wirtschaftswissenschaften" an der Technischen Universität Braunschweig ist geregelt (Nds. MBl. 1985 S. 1024), daß dem Promotionsgesuch "ein Abriß des Lebenslaufes und des Bildungsganges des Bewerbers, ggf. ergänzt durch eine vollständige Liste der wissenschaftlichen Veröffentlichungen" beizufügen ist. Die Vorlage des Lebenslaufes wird auch in anderen Promotionsordnungen gefordert.

Der Datenschutzbeauftragte der TU Braunschweig hat mir mitgeteilt, daß Doktoranden an ihn herangetreten sind mit der Bemerkung, daß derartige Angaben für das Promotionsverfahren überflüssig seien. Die Regelung verstoße nach Auffassung der Betroffenen gegen das Recht auf informationelle Selbstbestimmung. Darüber hinaus erschien mir von Interesse, ob es eine Verpflichtung für die Doktoranden gibt, ihren Lebenslauf gemeinsam mit der Dissertation zu veröffentlichen.

Nach Umfrage des Niedersächsischen Wissenschaftsministeriums bei den niedersächsischen Hochschulen meint dieses, daß die Abgabe eines Lebenslaufes im Zusammenhang mit der Vorlage von Unterlagen für das Promotionsverfahren grundsätzlich gefordert werden darf. Inhaltlich erforderlich sind dabei nach meinem Dafürhalten aber lediglich Angaben, die sich auf den Ausbildungs-, beruflichen und wissenschaftlichen Vorlauf des Bewerbers beziehen. Bei der Veröffentlichung des Pflichtexemplares der Dissertation vermag ich die Erforderlichkeit der Angaben zum Lebenslauf dagegen nicht zu erkennen. Diese nicht erforderliche Übermittlung personenbezogener Daten darf im Rahmen einer Promotionsordnung nicht gefordert werden. Ich habe das Ministerium gebeten, die niedersächsischen Hochschulen dahingehend zu informieren. Spätestens anläßlich anstehender Änderungen

der Promotionsordnungen muß eine Klarstellung hinsichtlich des Umfanges des Lebenslaufes bzw., sofern eine Regelung zur Dissertation erfolgt ist, die Herausnahme des Erfordernisses des Lebenslaufes vorgenommen werden.

25.4 Botschaft will Liste mit Hochschulangehörigen

Die italienische Botschaft in Bonn erbat von der Medizinischen Hochschule Hannover (MHH) eine Liste der dort tätigen italienischen Professoren und Stipendiaten mit Angabe der Funktion, des jeweiligen Forschungs- oder Studienfachs und der Anschrift. Diese Informationen sollten der Kontaktpflege und dem Informationsaustausch unter italienischen Akademikern im Bundesgebiet dienen und in Form einer kleinen Broschüre verbreitet werden.

Die Überlegungen der italienischen Botschaft hinsichtlich einer Verbesserung der Kontaktmöglichkeiten unter den in Deutschland lebenden und tätigen Akademikern ihrer Nationalität waren für mich durchaus nachzuvollziehen. Eine Rechtsgrundlage für die Übermittlung der an der MHH tätigen italienischen Professoren und Stipendiaten mit den gewünschten Angaben gibt es jedoch nicht. Eine Weitergabe der Betroffenendaten kann nur mit deren ausdrücklicher Einwilligung erfolgen.

25.5 Äußerungen eines Uni-Professors

Durch die Ausweitung der Anwendbarkeit des Datenschutzrechts auf aktenmäßige Datenverarbeitung haben öffentliche Stellen in Zukunft verstärkt auf den Schutz der Persönlichkeitsrechte Betroffener zu achten, wenn sie in Presseerklärungen, eigenen Publikationen oder sonstigen Verlautbarungen personenbezogene Daten preisgeben und veröffentlichen. Diese Veröffentlichung ist nichts anderes als eine Datenübermittlung an einen unbestimmten Empfängerkreis.

So erhielt ich von einem Artikel eines studentischen Magazins der Universität Hannover Kenntnis. Hierbei wurde ein Professor mit Angaben über die Bearbeitung eines Versetzungsantrags einer namentlich genannten Sekretariatsmitarbeiterin, über die Entscheidung über einen Arbeitsvertrag einer schwerbehinderten Bewerberin sowie über das persönliche Abstimmungsverhalten bei dieser Entscheidung zitiert. Die Sachverhaltsaufklärung ergab, daß die diesem Professor zugesprochenen Äußerungen teilweise schon in einem früheren Artikel dieser Zeitschrift enthalten waren. Soweit dies nicht der Fall war, hat sich der Professor umgehend bei der betroffenen Person entschuldigt.

Die Veröffentlichung des studentischen Magazins selbst kann keiner datenschutzrechtlichen Kontrolle unterzogen werden, da Herausgeber des Magazins eine nicht-öffentliche Stelle ist, die für sich zudem den Schutz der Pressefreiheit nach Art. 5 Abs. 1 GG in Anspruch nehmen kann. Ein Ansatzpunkt für mich war aber die Informierung der Presse durch eine öffentli-

che Stelle. Auch ein Professor ist als Beamter dienstrechtlich zur Verschwiegenheit verpflichtet und unterliegt als Teil einer öffentlichen Stelle dem Datenschutzrecht. Soweit Personal- und Verwaltungsangelegenheiten der Hochschule betroffen sind, kann sich ein Professor auch nicht auf die Freiheit von Forschung und Lehre (Art. 5 Abs. 3 GG) berufen. Zwar werden Auseinandersetzungen in Hochschulen teilweise mit "harten Bandagen" geführt. Dies entbindet deren Bedienstete jedoch nicht von der Einhaltung des Datenschutzes.

Im konkreten Fall konnte wegen der teilweisen Vorveröffentlichung der Fakten und im Hinblick auf die ausgesprochene Entschuldigung gegenüber der Betrroffenen von einer Beanstandung abgesehen werden.

## 26. Bibliotheken: Erhebung von Personalausweisnummern

Die Bibliothek der Medizinischen Hochschule Hannover (MHH) ist in das landeseinheitliche Bibliotheksautomationssystem PICA integriert (vgl. XI 4.6.5). Im Rahmen des Verbundes dürfen Benutzerdaten mit dem Einverständnis der Betroffenen zwischen den beteiligten Bibliotheken ausgetauscht werden. Die MHH-Bibliothek beabsichtigte nun, bei der Erhebung der Personaldaten auch die Nummer des Bundespersonalausweises bzw. des Reisepasses oder eines EG-Ausweises zu erfassen. Als Begründung wurde angegeben, daß neben den "normalen" Nutzerinnen und Nutzern auch internationale Gastärzte, Semesterlehrbeauftragte und Studierende aus dem Ausland betreut werden. Diese würden häufig umziehen und trotz entsprechender Verpflichtung ihre Adreßänderung oft nicht mitteilen. Mit Hilfe der Ausweisnummer hätte die Bibliothek die Möglichkeit, die Adressen der Benutzenden über die Ausweisnummer zu ermitteln, um ausstehende Gebühren einzutreiben oder Bücher zurückzufordern.

Gewiß habe ich Verständnis für die wirtschaftlichen Interessen der Bibliothek. Ich habe aber Zweifel, ob die Angabe der Ausweisnummer zur Wahrung dieser Interessen erforderlich ist. Mißbrauchsfälle, die Nachforschungen erforderlich machen, dürften relativ selten sein. Für die meisten Fälle würde es sich dagegen um eine unnötige Vorratsdatenerhebung handeln. Von einer freiwilligen Einwilligung zur Erhebung der Nummern kann m.E. nicht die Rede sein, da die Benutzerinnen und Benutzer zumeist darauf angewiesen sind, sich in der Bibliothek Literatur auszuleihen.

Es stellte sich weiterhin heraus, daß nur die Bundesdruckerei darüber Kenntnis hat, welche Behörde welchen deutschen Ausweis ausgestellt hat, so daß hierüber die Anschrift ermittelt werden könnte. Ein adäquater Ermittlungsansatz ergibt sich dagegen über die bei der Benutzeranmeldung zu benennenden Anschrift. Deren Richtigkeit kann durch Vorlage des Ausweises oder einer Meldebestätigung belegt werden. Über die Meldeämter sind die Bibliotheken dann regelmäßig in der Lage, die aktuelle Anschrift zu ermitteln. Die von der Bibliothek der MHH beabsichtigte Verfahrensweise hielt ich daher für unzulässig.

## 27. Schulen

### 27.1 Niedersächsisches Schulgesetz

Die von mir seit langem geforderte bereichsspezifische landesgesetzliche Regelung ist nunmehr durch das 4. Gesetz zur Änderung des Niedersächsischen Schulgesetzes eingeführt worden (NSchG i.d.F. vom 27. September 1993, Nds. GVBl. S. 383). § 31 bestimmt, daß Schulen, Schulbehörden, Schulträger, Schülervertretungen und Elternvertretungen personenbezogene Daten der Schülerinnen und Schüler und ihrer Erziehungsberechtigten nur verarbeiten dürfen, soweit dies zur Erfüllung des Bildungsauftrags der Schule und ihrer Fürsorgeaufgaben erforderlich ist. Dies gilt auch für Gesundheitsämter, soweit sie Aufgaben im Rahmen von Einschulungsuntersuchungen und der Schulgesundheitspflege wahrnehmen, und für die Träger der Schülerbeförderung.

Das Niedersächsische Kultusministerium wird ermächtigt (und zugleich verpflichtet), durch Verordnung zu regeln, welche personenbezogenen Daten der Schülerinnen und Schüler sowie ihrer Erziehungsberechtigten von der Schule verarbeitet und beim Übergang in eine andere Schule übermittelt werden dürfen.

### 27.2 Verordnung über die Verarbeitung personenbezogener Daten der Schülerinnen und Schüler sowie ihrer Erziehungsberechtigten

Das Kultusministerium hat die genannte Verordnung frühzeitig mit mir abgestimmt und ist meinen Anregungen gefolgt. Die Verordnung regelt u.a., welche Daten automatisiert und welche in nicht-automatisierter Form verarbeitet werden dürfen. Die Anlage 1 der Verordnung bestimmt die für die Verarbeitung in Betracht kommenden Daten zur Person der Schülerinnen und Schüler und der Erziehungsberechtigten in Form eines Maximalkatalogs. Die Anlage 2 legt die Daten über die Schullaufbahn, die Anlage 3 die Verwaltungsdaten, die Anlage 4 die Leistungsdaten und die Anlage 5 die Daten über persönliche Eigenschaften fest (Nds. GVBl. 1994 S. 455).

### 27.3 Verordnung über regelmäßige Datenübermittlungen im Geschäftsbereich des Niedersächsischen Kultusministeriums

Seit dem 1. Oktober 1994 dürfen automatisierte Abrufverfahren nur dann eingerichtet werden, wenn eine Rechtsvorschrift, also ein Gesetz oder eine Verordnung, dies zuläßt. Das gleiche gilt nach § 12 Abs. 6 NDSG für regelmäßige Datenübermittlungen. Das Kultusministerium war das erste Ministerium, das mir einen entsprechenden Verordnungsentwurf vorgelegt hat. Dieser ist jedoch datenschutzrechtlich völlig unzureichend.

Die Verordnung soll u.a. regeln, daß personenbezogene Daten der an den Schulen tätigen Landesbediensteten und anderer an den Schulen tätigen Personen regelmäßig von den Bezirksregierungen an das Kultusministerium in umfassender Weise zum Zwecke des Ausgleichs der Unterrichtsversor-

gung, der Personalplanung und des Personaleinsatzes übermittelt werden dürfen. Ebenso ist die umfassende Übermittlung von Daten der Bewerberinnen und Bewerber um Einstellung in den niedersächsischen Schuldienst an das Kultusministerium zur Steuerung des Einstellungsverfahrens und zur Koordinierung der Einstellungen vorgesehen.

Ich habe gegen die vorgesehenen Regelungen massive rechtliche Bedenken erhoben. Der genannte Datensatz - z.B. 27 Einzelangaben über mehr als 75.000 Personen, von der Staatsangehörigkeit bis zur Anzahl der Vertretungsstunden jeder einzelnen Lehrkraft - ist in großen Teilen zur Wahrnehmung der Aufgaben des Fachressorts nicht erforderlich. Z.B. ist auch nicht ersichtlich, wozu das Kultusministerium Angaben über die Religionszugehörigkeit sämtlicher Lehrerinnen und Lehrer im Schuldienst und aller an den Schulen tätigen Personen, also auch der Hausmeister, Schulsekretärinnen, Reinigungskräfte usw. benötigt. Auch das Niedersächsische Innenministerium bewertet die geplante Datenverarbeitung als eine "nach dem Datenschutzrecht nicht zulässige(n) Vorratsdatenhaltung". Ich gehe davon aus, daß der Verordnungsentwurf grundlegend überarbeitet wird.

27.4 Verordnung über die Aufnahme der Schülerinnen und Schüler in den Sekundarbereich I der Gesamtschule

Auch diese Verordnung und die ergänzenden Bestimmungen zu dieser Verordnung sind schon frühzeitig mit mir abgestimmt worden. Meinen Anregungen ist das Niedersächsische Kultusministerium gefolgt. Die Verordnung war aufgrund des § 178 NSchG zu erlassen. Nach dieser Bestimmung kann die Aufnahme in den Sekundarbereich I von Gesamtschulen beschränkt werden. Hierbei ist auch eine entsprechende Regelung für Härtefälle zu treffen. In der Verordnung (Nds. GVBI. 1994 S. 503) werden die Voraussetzungen für die Aufnahme, die Zusammensetzung der Schülerschaft, die Härtefälle und die Durchführung des Aufnahmeverfahrens geregelt.

27.5 Mitteilungen über ausgefallene Berufsschultage an den Arbeitgeber

Dürfen Berufsschulen Arbeitgeber darüber unterrichten, daß der Berufschulunterricht für ganze Tage ausfällt? Einige Berufsschüler hielten dies für problematisch. Ihre Bedenken konnte ich jedoch nicht teilen.

Nach § 7 Berufsbildungsgesetz hat der Ausbildungsbetrieb die Auszubildenden für die Teilnahme am Berufsschulunterricht und an Prüfungen freizustellen. Der Arbeitgeber hat deshalb ein rechtliches Interesse daran zu erfahren, ob und wann die Auszubildenden am Berufsschulunterricht teilzunehmen haben und wann der Unterricht ausfällt. Ein überwiegendes schutzwürdiges Interesse des Auszubildenden an einer Geheimhaltung der Tatsache des Unterrichtsausfalls ist nicht ersichtlich. Gemäß § 13 Abs. 1 Satz 1 Nr. 2 NDSG ist die Mitteilung der Berufsschule an den Ausbildungsbetrieb darüber, daß Unterricht ausfällt, zulässig. Eine Verpflichtung der Schule, bei jedem Unterrichtsausfall alle Arbeitgeber direkt zu benachrichtigen, besteht allerdings nicht. Dies wäre im übrigen wegen des hohen Verwaltungsaufwandes auch nicht leistbar. In der Praxis werden daher im

Regelfall weiterhin die Auszubildenden informiert. Ihnen obliegt es, ihren Pflichten aus ihrem Ausbildungsvertrag nachzukommen und ihren Arbeitgeber zu unterrichten.

27.6 Zulässigkeit von Telefonketten in Schulen

An vielen Schulen werden die Kinder aufgefordert, dem Klassenlehrer die Telefonnummern ihrer Eltern anzugeben, die dann zu einer sog. Telefonkette zusammengestellt werden. Die Schülerinnen und Schüler erhalten eine Liste, auf der die Namen und Telefonnummern ihrer Klassenkameraden in einer bestimmten Reihenfolge aufgeführt sind. In dieser Reihenfolge, an deren Spitze in der Regel der Klassenlehrer steht, sollen die Kinder einander anrufen, falls seitens der Schule oder eines Lehrers für dringend gehaltene Nachrichten - etwa über einen Unterrichtsausfall - allen Schülerinnen und Schülern einer Klasse bekanntgegeben werden müssen.

Nach § 31 NSchG dürfen Schulen personenbezogene Daten der Schülerinnen und Schüler und ihrer Erziehungsberechtigten verarbeiten, soweit dies zur Erfüllung des Bildungsauftrages der Schule und ihrer Fürsorgeaufgaben erforderlich ist. Ich meine ebenso wie das Niedersächsische Kultusministerium, daß die genannten "Telefonketten" zur Erfüllung der Fürsorgeaufgaben zu zählen sind. Deshalb habe ich keine datenschutzrechtlichen Bedenken, daß eine Liste erstellt wird, aus der Name und Telefonnummer hervorgehen. Die Übermittlung wäre im übrigen auch nach § 13 NDSG an die anderen Eltern zulässig, weil sie zur Erfüllung der in der Zuständigkeit der Schule liegenden Aufgaben erforderlich ist.

27.7 Teilnahme von Eltern am Unterricht

Das Niedersächsische Kultusministerium teilte mir mit, daß die Anwesenheit von interessierten Erziehungsberechtigten im Unterricht ihrer Kinder nicht nur zulässig, sondern besonders in der Grundschule im Hinblick auf die Wechselwirkung von schulischen und außerschulischen Erziehungs- und Lerneinflüssen unentbehrlich ist. Das Fachressort hält die Hospitation interessierter Eltern neben Sprechtagen, Hausbesuchen oder Elternabenden zur Förderung der kontinuierlichen Zusammenarbeit zwischen Lehrerinnen bzw. Lehrern und Erziehungsberechtigten gerade in der Grundschule pädagogisch für sinnvoll und zur Erfüllung des Bildungsauftrages der Schule für notwendig. Mit zunehmendem Alter der Schülerinnen und Schüler wird die Bedeutung der Teilnahme von Erziehungsberechtigten am Unterricht für die Erfüllung des Bildungsauftrages zwar abnehmen. Im Grundsatz können jedoch in allen Schulen Erziehungsberechtigte beim Unterricht anwesend sein. Darüber hinaus ist es nach Angabe des Kultusministeriums möglich, geeignete Erziehungsberechtigte mit der Wahrnehmung von Aufsichtsfunktionen zu beauftragen.

Die Schule entscheidet in eigener Verantwortung, ob die Anwesenheit der Erziehungsberechtigten im Einzelfall sinnvoll ist, ohne daß z.B. der Unter-

richt durch die Anwesenheit zu vieler Eltern gestört wird. Daß den am Unterricht teilnehmenden Erziehungsberechtigten hierbei - ebenso wie den Mitschülerinnen und Mitschülern - personenbezogene Daten bekanntwerden können, ist unvermeidbar. Das allgemeine Persönlichkeitsrecht der Betroffenen muß nach meiner wie des Ministeriums Auffassung so weit zurücktreten, wie es die Erfüllung des verfassungsgemäßen Auftrages der Schule erfordert. Dies gilt im Verhältnis zu den im selben Klassenverband unterrichteten Mitschülerinnen und Mitschüler ebenso wie im Verhältnis zu den am Unterricht teilnehmenden Erziehungsberechtigten. Die hierbei zwangsläufig erfolgende Datenweitergabe ist nach § 31 i.V.m. § 11 Abs. 4 NSchG zulässig, wenn man die Erziehungsberechtigten als "Beauftragte" der Schule ansieht, weil sie zur Erfüllung des Bildungsauftrages beitragen. Die an den Unterrichtsveranstaltungen teilnehmenden Erziehungsberechtigten sind zur Verschwiegenheit über die ihnen dadurch bekanntgewordenen personenbezogenen Daten verpflichtet. Hierauf sind die Erziehungsberechtigten hinzuweisen. Die Datenweitergabe wäre aber auch nach § 13 Abs. 1 Satz 1 Nr. 1 NDSG möglich, wenn die Erziehungsberechtigten als Personen außerhalb des öffentlichen Bereichs anzusehen wären.

27.8 Zeugnisnoten auf Abiturarbeiten

Das Niedersächsische Kultusministerium hat mir mitgeteilt, daß es keine Regelung gibt, nach der auf dem Deckblatt von Abiturarbeiten frühere Zeugnis- und Klausurnoten einzutragen sind. Die Eintragung von Noten hat an einigen Gymnasien vermutlich ihre Tradition in der Tatsache, daß in früheren Jahren vor Eintritt in die schriftliche Abiturprüfung eine sog. "Vornote" von der Klassenkonferenz festgesetzt wurde, aufgrund derer bei großen Abweichungen zwischen der Vornote und den Leistungen in der Prüfungsklausur eine mündliche Prüfung anzusetzen war. Bei dieser Entscheidung war die Kenntnis von Noten, die zur "Vornote" geführt hatten, von Fall zu Fall hilfreich.

Auch heute werden mündliche Prüfungen in schriftlichen Prüfungsfächern festgelegt. Dies geschieht durch eine an der Schule tätige Prüfungskommission, die bei ihrer Entscheidung, ob eine mündliche Abiturprüfung in einem schriftlichen Prüfungsfach anzusetzen ist, nicht die einzelne Prüfungsklausur bzw. deren Deckblatt, sondern eine eigens zu erstellende Zensurenübersicht heranzieht, in der auch eine Durchschnittsnote, gebildet aus den bisher erzielten Halbjahresnoten, für die Prüfungsfächer aufgeführt wird.

Eine Eintragung von Zeugnis- und Klausurnoten auf dem Deckblatt von Abiturprüfungsarbeiten ist somit auch aus sachlichen Gründen nicht erforderlich. Die Prüfungskommission kann auch sonst keine Kenntnis der Klausurnoten vergangener Jahre verlangen, weil dies zur Aufgabenerfüllung nicht erforderlich ist. Die Kenntnis dieser Noten ist zur Beurteilung einer Prüfungsklausur, z.B. durch eine Fachberaterin oder einen Fachberater der Bezirksregierung, nach Auffassung des Niedersächsischen Kultusministeriums nicht erforderlich.

Die Klausurnoten (und die Halbjahresnoten) werden u.a. in den Kursheften festgehalten, die als Unterrichtsakten vergleichbar den Klassenbüchern von den Schulen bis zum Ende des Schuljahres, das nach der Abiturprüfung beginnt, aufzubewahren sind. Da die Daten also bereits (vorübergehend) in den Schulakten gespeichert sind, ist weder die Aufbewahrung noch die Weitergabe durch die Kursleiterin oder den Kursleiter erforderlich.

### 27.9 Angabe von Krankheiten auf Entschuldigungen

Die Angabe der Krankheit auf den Entschuldigungsschreiben ist zur Erfüllung des Bildungsauftrages der Schule und der Fürsorgeaufgaben nicht erforderlich.

### 27.10 Sonderpädagogisches Prüfungsverfahren

Mehrere Petenten haben sich bei mir darüber beschwert, daß ihnen Gutachten, die im Rahmen der sonderpädagogischen Prüfung erstellt worden sind, nicht ausgehändigt werden. § 56 Abs. 4 NSchG sieht vor, daß den Erziehungsberechtigten auf Antrag Einsicht in die Entscheidungsunterlagen zu geben ist, die sich u.a. zur Frage der etwaigen sonderpädagogischen Förderung einer Schülerin oder eines Schülers äußern. Die Erziehungsberechtigten müssen zudem Gelegenheit zur Besprechung der Testergebnisse und Gutachten erhalten. Ich würde es begrüßen, wenn den nachfragenden Eltern Gutachten in Kopie überlassen würden.

Betonen muß ich allerdings, daß auch eine bloße Einsichtnahme nach der geltenden Rechtslage nicht als Verstoß gegen das informationelle Selbstbestimmungsrecht von Erziehungsberechtigten und Kindern gewertet werden kann. Dieser läge nur vor, wenn die personenbezogenen Daten hinter dem Rücken der Betroffenen ohne deren Kenntnis zu schulischen Zwecken verarbeitet würden. Die Transparenz, die das Grundrecht auf Datenschutz fordert, wird jedoch hier durch das Akteneinsichtsrecht und durch die Verpflichtung, die Untersuchungsergebnisse mit den Erziehungsberechtigten auf deren Wunsch zu erörtern, im rechtlich notwendigen Maße gewährleistet. Im Rahmen des Gesprächs können z.B. auch gutachterliche Fachbegriffe erläutert werden. Außerdem dürfte es auch hier möglich sein, daß die Erziehungsberechtigten sich durch einen Bevollmächtigten vertreten lassen, um ihre Interessen sachgerecht wahrnehmen zu können.

## 28. Landwirtschaft und Forsten

### 28.1 Integriertes Verwaltungs- und Kontrollsystem

Im XI. TB habe ich damit begonnen, zu den Problemen Stellung zu nehmen, die aus datenschutzrechtlicher Sicht mit der strukturellen Umstellung des

Systems der Landwirtschaftsförderung durch die Europäischen Gemeinschaften (EG) verbunden sind. Die Diskussion hierüber ist fortzusetzen. Um eine mißbräuchliche Verwendung von Fördermitteln zu verhindern, hat die EG die Mitgliedstaaten zur Einführung eines "Integrierten Verwaltungs- und Kontrollsystems (InVeKoS)" verpflichtet. Diese haben integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen. Wegen der Einzelheiten verweise ich auf XI 6.5 und 28.1. Nach der Verordnung (EWG) Nr. 3508/92 vom 27. November 1992 (InVeKoS-VO) erhalten nur die Staaten Mittel für die genannten Fördermaßnahmen, die zu den für 1993 festgelegten Terminen Betriebsdatenbanken realisiert haben. Im Rahmen des Gesamtsystems werden zahlreiche personenbezogene Daten der Landwirte verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder haben eine Entschließung zum Integrierten Verwaltungs- und Kontrollsystem verabschiedet und darin zur Wahrung datenschutzrechtlicher Belange der Betroffenen Forderungen erhoben, die bei der Umsetzung von InVeKoS Berücksichtigung finden sollten (vgl. Anlage 8). Nach dem mir bekannten Stand der Realisierung von InVeKoS im Land Niedersachsen werden die durch die Verordnung eröffneten Möglichkeiten der Fernerkundung (Satellitenüberwachung) nicht eingesetzt. Die erhobenen Daten werden an das Bundesministerium für Ernährung, Landwirtschaft und Forsten als Koordinierungsstelle im Sinne des § 8 Abs. 3 InVeKoS-VO länderbezogen in aggregierter Form geliefert und von dort wiederum aggregiert auf die Bundesebene bezogen weitergeleitet.

Hier könnte sich jedoch in der Zukunft eine Änderung ergeben. Wie unter 7.6 dargestellt, soll die Bundesrepublik in Zukunft im Rahmen der Agrarstatistik auch Individualdaten an die Statistikinstitution der EU (EUROSTAT/EUROFARM, vgl. Anlage 22) liefern. Nach Art. 1 Abs. 3 Satz 3 in Verbindung mit Satz 5 der InVeKoS-VO können die unter InVeKoS erhobenen Daten zu statistischen Zwecken genutzt werden. Im Hinblick auf die Bestrebungen im Rahmen der Statistik, Individualdaten an die EU zu liefern, könnte auch die bisher stets verneinte Lieferung von InVeKoS-Daten an die EU erfolgen. Ich werde mich derartigen Planungen energisch entgegenstellen.

28.2 Hege des Rehwildes

Für die Umsetzung der Hegeziele des Bundesjagdgesetzes (§ 1 Abs. 1) ist nach Mitteilung des Niedersächsischen Ministeriums für Ernährung, Landwirtschaft und Forsten die Erstellung von Abschußplänen und Abschußlisten und ein Austausch von Daten aus diesen Unterlagen zwischen den je nach Forstart unterschiedlichen Behörden erforderlich. Einzelheiten hierzu enthält die Rehwild-Hegerichtlinie vom 29. August 1993 (Nds. MBl. S. 1076). Mit einem Erlaß zur Hege und Bejagung des Rehwildes beabsichtigt das Ministerium für Ernährung, Landwirtschaft und Forsten, nunmehr die Forstämter der Landesforstverwaltung und die Jagdbehörden anzuwei-

sen, ihre Abschußpläne und Ergebnisse gegenseitig offenzulegen, wobei es zur Übermittlung personenbezogener Daten kommt.

Ich habe dem Ministerium mitgeteilt, daß es sich bei der Weitergabe personenbezogener Daten von Revierinhabern oder Pächtern durch die Jagdbehörden an die staatlichen Forstämter um Datenübermittlungen handelt, die als datenschutzrechtliche Eingriffe bei fehlender Einwilligung einer normenklaren gesetzlichen Grundlage bedürfen. Eine derartige Rechtsgrundlage vermag ich weder dem Bundesjagdgesetz noch dem Landesjagdgesetz zu entnehmen. Im Hinblick auf den mit der Rehwild-Hegerichtlinie verfolgten Zweck, nämlich die Ziele des § 1 Abs. 2 Bundesjagdgesetz umzusetzen, habe ich mich der Erforderlichkeit der im Erlaß genannten Datenübermittlungen nicht verschlossen. Ich halte sie für eine Übergangszeit bis zur Schaffung einer gesetzlichen Befugnisnorm für die Datenverarbeitung für zulässig. 11 Jahre nach dem Volkszählungsurteil ist eine Berufung auf den "Übergangs"-Bonus nur noch schwer zu rechtfertigen. Meines Erachtens ist eine Gesetzesnovelle zu Beginn der 13. Legislaturperiode erforderlich, um die Rechtmäßigkeit dieser - und ggf. anderer, hier nicht geprüfter Datenflüsse - in Zukunft sicherzustellen.

## 29. Wirtschaft

### 29.1 Architektenliste

Meine jahrelangen Bemühungen um einen datenschutzgerechten Inhalt im "Antrag auf Eintragung in die Architektenliste" (zuletzt XI 29.3) sind nunmehr erfolgreich abgeschlossen. Das Niedersächsische Ministerium für Wirtschaft, Technologie und Verkehr hat mir mitgeteilt, daß auf die Erhebung einer Reihe von Daten, die im Antragsformular vorgesehen waren, verzichtet wird. So brauchen z.B. antragstellende Architektinnen und Architekten künftig nicht mehr anzugeben, ob sie entmündigt oder unter vorläufige Vormundschaft gestellt sind. Auch ein Führungszeugnis für Behörden wird den Antragstellenden nicht mehr abverlangt. Nicht zuletzt ist die zu erteilende - ursprünglich umfassende - Ermächtigung für die Architektenkammer zur Einholung von Auskünften für die Bearbeitung des Antrages unter Hinweis auf die Vorschriften des NDSG eingeschränkt worden.

### 29.2 Datenschützer als Pfadfinder "per legem ad data"

Eine Gemeinde, die eine Firma unter deren Postfachanschrift angeschrieben hatte, um sie zur Gewerbeanzeige gemäß § 14 Gewerbeordnung (GewO) anzuhalten, blieb ohne Antwort. Die anschließende Anfrage der Gemeinde nach der Anschrift der Firma, um die Gewerbeanmeldung durchzusetzen, lehnte die Deutsche Bundespost unter Hinweis auf § 5 Abs. 1 Postdienst-Datenschutzverordnung (PD-DSV) ab. Danach darf die Deutsche Bundespost Postdienst die Anschrift eines Postfachinhabers nur im Zusam-

menhang mit der Inanspruchnahme des postalischen Dienstleistungsangebots mitteilen. Diesen Zusammenhang sah die Deutsche Bundespost Postdienst zu Recht nicht, denn das Auskunftsersuchen der Gemeinde diente gewerberechtlichen Zwecken (§§ 14, 34c Nr. 1d GewO). Die Lösung war folgende: Der von der Gemeinde beabsichtigte Hinweis an den Postfachinhaber, daß er sein Gewerbe gemäß § 14 GewO anzumelden habe, konnte auch an die Postfachanschrift gerichtet werden. Bleibt dies erfolglos, ist der Gewerbetreibende seiner Anzeigepflicht nach § 14 GewO nicht nachgekommen. Er handelt damit gemäß § 146 Abs. 2 Nr. 1 GewO ordnungswidrig. Im Rahmen des einzuleitenden Ordnungswidrigkeitenverfahrens können oder müssen Schriftstücke an den Betroffenen zugestellt werden. Dies ist jedoch nicht an ein Postfach, sondern nur an die richtige Anschrift möglich (vgl. § 3 Abs. 2 VwZG des Bundes i.V.m. §§ 180 bis 186 und 195 Abs. 2 ZPO). Zu diesem Zweck ist auch eine rechtmäßige Auskunftserteilung durch die Post gegeben, denn die Zustellung gehört zum postalischen Dienstleistungsangebot. Ein praktisches Beispiel wider das Vorurteil, der Datenschutz blockiere die Verwaltungstätigkeit.

29.3 Datenübermittlungen aus der Gewerbedatei an Allgemeine Ortskrankenkassen

Dem Ersuchen einer Allgemeinen Ortskrankenkasse um regelmäßige Übersendung von Kopien der Gewerbeanzeigen-Durchschriften konnte wegen fehlender gesetzlicher Grundlagen nicht entsprochen werden. Die derzeit für die Übermittlung von Daten aus der Gewerbedatei an andere Behörden und sonstige öffentliche Stellen geltende Gewerbeanzeigenverordnung vom 30. Januar 1981 sieht Allgemeine Ortskrankenkassen als Empfänger dieser Daten nicht vor. Da es sich um eine Verwaltungsvorschrift handelt, wäre sie als Rechtsgrundlage für eine Übermittlung darüber hinaus auch nicht in Betracht gekommen. Das verständliche Informationsbedürfnis der Krankenkasse, die Versicherungslücken suchen muß, wird erst befriedigt werden können, wenn das inzwischen verabschiedete Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften in Kraft getreten ist.

29.4 Datenverarbeitung durch Schornsteinfeger

Die Problematik des Datenabgleichs der unteren Wasserbehörden mit Karteien der Bezirksschornsteinfegermeister hat mich seit geraumer Zeit beschäftigt (vgl. VII 29.10). Der seinerzeit festgestellte Mangel an bereichsspezifischen gesetzlichen Vorschriften ist nunmehr durch die Verabschiedung des Gesetzes zur Änderung des Schornsteinfegergesetzes vom 20. Juli 1994 (BGBl. I S. 1624) behoben. In § 19 des Schornsteinfegergesetzes wurden bereichsspezifische gesetzliche Regelungen für die Verarbeitung personenbezogener Daten durch den Bezirksschornsteinfegermeister getroffen. Nach § 19 Abs. 3 Schornsteinfegergesetz darf der Bezirksschornsteinfegermeister die nach den Abs. 1 und 2 erhobenen Daten aus seinen Aufzeichnungen an öffentliche Stellen übermitteln, soweit dies u.a. für die Be-

kämpfung der Luft-, Boden- und Gewässerverschmutzung erforderlich ist. Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten und nutzen, zu dessen Erfüllung sie ihm übermittelt worden sind.

29.5 Handwerksordnung, Handwerksrolle

Mit Verabschiedung des Gesetzes zur Änderung der Handwerksordnung, anderer handwerksrechtlicher Vorschriften und des Berufsbildungsgesetzes vom 20. Dezember 1993 sind bereichsspezifische Bestimmungen zur Verarbeitung personenbezogener Daten geschaffen worden. Sie regeln z.B. Datenübermittlungsbefugnisse der Handwerkskammern, Handwerksinnungen und Kreishandwerkerschaften, Auskünfte und Datenübermittlungen aus der Handwerksrolle, Widerspruchsrechte gegen Datenübermittlungen.

Zu begrüßen ist, daß an die Stelle der Erlaßregelung vom 10. Juni 1991, nach der eine Einverständniserklärung in den Antragsvordruck für Aufnahmebewilligungen nach § 8 der Handwerksordnung aufzunehmen ist (vgl. XI 29.2), nunmehr eine gesetzliche Bestimmung in § 8 Abs. 3 Handwerksordnung getreten ist.

29.6 Der Datendieb in der Handwerkskammer

Der Mitarbeiter einer Handwerkskammer fotokopierte aus ihm dienstlich zugänglichen Akten Honorarabrechnungen eines freien Mitarbeiters, gegen den er einen Zivilrechtsstreit führte. Diese Unterlagen legte er dem Gericht zum Beweis für bestimmte An- bzw. Abwesenheitszeiten seines Prozeßgegners vor. Dieser wandte sich - nach vergeblichen Versuchen, eine Ahndung durch die Handwerkskammer selbst zu erreichen - mit der Bitte um datenschutzrechtliche Weiterverfolgung der Sache an mich. Um eine Stellungnahme gebeten, meinte die Handwerkskammer, von ihrer Seite sei nichts zu veranlassen: Sie selbst habe nicht gehandelt, also sei die Datenübermittlung ihr auch nicht zuzurechnen. Sie habe ihren Mitarbeiter ausreichend über seine datenschutzrechtlichen Verpflichtungen belehrt. Im übrigen hätte er auf ein entsprechendes Ersuchen die Daten auch erhalten, denn die Verwendung in einem Rechtsstreit sei ein rechtliches Interesse.

Hier irrt die Handwerkskammer. Da die Daten allerdings nicht durch ein Handeln der Handwerkskammer selbst offenbart wurden - dies setzt einen Willen der Institution voraus, der nicht vorlag - kann die Datenübermittlung ihr tatsächlich nicht zugerechnet werden. Gleichwohl kann und sollte manches getan werden, nämlich die Prüfung dienstrechtlicher Schritte und die Einleitung eines Ordnungswidrigkeitenverfahrens nach § 29 NDSG gegen den Mitarbeiter wegen des Bruchs des Datengeheimnisses (§ 5 NDSG). Dieser Verstoß bestand darin, daß er nicht dienstlich, sondern für seine privaten Zwecke - als Datendieb - Schriftstücke mit personenbezogenen Daten aus den Akten entnahm. Diese Schriftstücke hätte ihm die Handwerkskammer auch nicht so zu dem verfolgten Zweck aushändigen dürfen. Honorar-

abrechnungen enthalten wesentlich mehr Daten, als für den Nachweis von Anwesenheitszeiten erforderlich wären.

29.7 Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern

Ein Bürger, der bei dem für ihn zuständigen Gewerbeamt ein Gewerbe angemeldet hatte, wunderte sich, daß die vom Gewerbeamt unterrichtete Industrie- und Handelskammer ihm mitteilte, sie beabsichtige, Daten zu seiner Person zu übermitteln, soweit die Kammer von interessierten Unternehmen um deren Übermittlung gebeten werde. Die Industrie- und Handelskammer räumte dem Petenten die Möglichkeit ein, innerhalb von vier Wochen der Datenübermittlung zu widersprechen.

Ich konnte den Petenten auf das "Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHK-G vom 21. Dezember 1992, BGBl. I S. 2133) hinweisen. § 9 Abs. 4 IHK-G bestimmt, daß die Industrie- und Handelskammern Firma, Anschrift und Wirtschaftszweig ihrer kammerzugehörigen Unternehmen zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken an nicht-öffentliche Stellen übermitteln dürfen. Die übrigen in § 9 Abs. 1 IHK-G genannten Daten (Telefonnummer, angebotene Waren und Dienstleistungen, Betriebsgrößenklasse, Name und Alter der Betriebsinhaber, Leiter des Unternehmens) sowie die den Kammern aufgrund besonderer Rechtsvorschriften von öffentlichen Stellen übermittelten Daten dürfen zu den genannten Zwecken an nicht-öffentliche Stellen nur übermittelt werden, sofern der Kammerzugehörige nicht widersprochen hat. Auf die Möglichkeit, der Übermittlung der Daten an nicht-öffentliche Stellen zu widersprechen, sind die Kammerzugehörigen vor der ersten Übermittlung schriftlich hinzuweisen.

Die Neufassung des § 9 IHK-G ist mit Wirkung vom 1. Januar 1994 in Kraft. Sie enthält bereichsspezifische Regelungen zur Datenerhebung (Abs. 1 und 2), zur Datenspeicherung und -nutzung (Abs. 3), Datenübermittlung (Abs. 4), Zweckbindung (Abs. 5) und Veränderung, Sperrung und Löschung (Abs. 6). Aus datenschutzrechtlicher Sicht handelt es sich bei diesen Regelungen um ein erfreuliches Beispiel für normenklare gesetzliche Bestimmungen, wie sie vom BVerfG im Volkszählungsurteil für Eingriffe in das Recht auf informationelle Selbstbestimmung gefordert werden.

## 30. Verkehr

30.1 Millionenschwere Datensammlung geplant: Zentrales Fahrerlaubnisregister

Das Straßenverkehrsrecht kennt bereits heute umfangreiche Datensammlungen, in denen behördliche und gerichtliche Entscheidungen personenbezogen gespeichert werden. So führt jede Zulassung eines Kraftfahrzeuges zur

Speicherung der Halterdaten in einem von der Zulassungsstelle geführten örtlichen Register und zusätzlich zur Speicherung im Zentralen Fahrzeugregister beim Kraftfahrt-Bundesamt (KBA). Dort wird auch das Verkehrszentralregister geführt, in das als sog. Negativregister die belastenden behördlichen Anordnungen und gerichtlichen Entscheidungen gegen Verkehrsteilnehmer eingetragen werden, wie z.B. Entziehung der Fahrerlaubnis oder Verhängung einer Geldbuße. Auf diese Dateien haben zahlreiche Behörden Zugriff. Verstöße gegen straßenverkehrsrechtliche Vorschriften können darüber hinaus auch im Bundeszentralregister und in polizeilichen Dateien gespeichert sein.

Das Bundesverkehrsministerium hatte im September 1993 den Entwurf für ein Gesetz zur Änderung des Straßenverkehrsgesetzes vorgelegt, in dem die Errichtung eines Zentralen Fahrerlaubnisregisters beim KBA vorgesehen war. Damit sollte ein "Positivregister" mit den Daten aller Fahrerlaubnisinhaber mit Wohnsitz in der Bundesrepublik sowie von Personen ohne ständigen Wohnsitz in der Bundesrepublik mit von inländischen Behörden erteilten oder registrierten Führerscheinen entstehen. Man geht davon aus, daß von einem Register dieser Art ca. 50 Mio. Personen betroffen wären.

Die Datenschutzbeauftragten des Bundes und der Länder haben eine stichhaltige Begründung für die Erforderlichkeit einer derartig umfangreichen Datensammlung gefordert. Die bislang angegebenen Gründe sind wenig zufriedenstellend:

- Durch Nachfrage im Zentralen Fahrerlaubnisregister sollen Personen ermittelt werden, die keine Fahrerlaubnis erworben haben und mit einem gefälschten Führerschein fahren. Dieser Ansatz setzt voraus, daß alle Führerscheine, die bei der Abfrage nicht im zentralen Register erfaßt sind, unecht sind. Davon wird man schon wegen des Zeitverzuges zwischen der Erteilung der Fahrerlaubnis und der zentralen Erfassung nicht ausgehen können. Erkennt die Polizei bei Verkehrskontrollen die Fälschung, kann sie im übrigen den Führerschein sicherstellen. Fälschungen, die auf gestohlene Führerscheine zurückgehen, können durch Nutzung des polizeilichen Informationssystems aufgeklärt werden. Alle anderen Fälle lassen sich durch Anfragen an die Fahrerlaubnisbehörden klären, so daß insoweit die Einrichtung des zentralen Registers nicht erforderlich sein dürfte.

- Das Zentrale Fahrerlaubnisregister soll dazu dienen, Personen, die im Besitz mehrerer Führerscheine sind, zu erkennen. Auch dies kann das neue Register nicht rechtfertigen. Fälle, in denen jemand nach dem Entzug der Fahrerlaubnis einen "zur Reserve" erworbenen Zweitführerschein nutzt, können bereits jetzt durch die Speicherung des Fahrerlaubnisentzuges im Verkehrszentralregister festgestellt werden.

- Als Hauptargument für die Errichtung eines Zentralen Fahrerlaubnisregisters wird eine nach europäischem Recht angeblich hierzu bestehende Verpflichtung angeführt. Nach der Zweiten EG-Führerscheinrichtlinie müssen die EG-Staaten in bestimmten Fällen Informationen im Zusam-

menhang mit Fahrerlaubnissen untereinander austauschen. Dieser Mitteilungspflicht kann die Bundesrepublik aber auch ohne Einrichtung dieses Registers nachkommen. In diesem Zusammenhang werden zum Teil Sachverhalte konstruiert, die derartig lebensfremd sind, daß damit ein Register in dem genannten Umfang nicht begründet werden kann. Beispielsweise wird die Situation angeführt, ein Bundesbürger werde in Frankreich ohne Führerschein angetroffen und wisse nicht mehr, welche deutsche Behörde ihm die Fahrerlaubnis erteilt habe, so daß eine Nachfrage durch die französische Stelle nicht möglich sei.

Die zunehmende Integration in Europa darf m.E. nicht dazu führen, daß die Bundesrepublik ihre datenschutzrechtlichen Standards ohne Not aufgibt. Bezüglich der vertraglichen Verpflichtung gegenüber der EG ist zu fragen, ob denn die Bundesrepublik wirklich - trotz des ihr nachgesagten Hangs zum Perfektionismus - im Vergleich zu anderen Mitgliedstaaten noch ihre Hausaufgaben in puncto Verkehrssicherheit erledigen muß. So war beispielsweise in der FAZ vom 11. August 1994 zu lesen, nach Schätzung von Londoner Fahrschulen würden in Großbritannien wöchentlich etwa 1000 Personen einen Führerschein bekommen, obwohl andere für sie die Fahrprüfung abgelegt haben. Der Grund hierfür liegt darin, daß in Großbritannien als Führerschein ein Computerauszug ohne Fotografie des Inhabers dient.

Die Bundesregierung hat den Gesetzentwurf zum Zentralen Fahrerlaubnisregister zunächst zurückgezogen. Es wird wohl in Kürze erneut eingebracht werden.

30.2 Führerschein weg - Datenschutz ade

Die Polizei kann bei Verkehrskontrollen mit ihrem Direktzugriff auf das beim Kraftfahrt-Bundesamt geführte Verkehrszentralregister feststellen, ob einem Verkehrsteilnehmer die Fahrerlaubnis entzogen worden ist. Für mich ist deshalb nicht nachvollziehbar, aus welchen Gründen in Niedersachsen als einzigem Bundesland eine Erlaßregelung geplant war, nach der die Verwaltungsbehörde die Entziehung von Fahrerlaubnissen zusätzlich regelmäßig an die örtliche Polizei melden soll (vgl. XI 30.2). Soll die Polizei mit Hilfe der erhaltenen Informationen gezielt Personen observieren, denen die Fahrerlaubnis entzogen wurde, um festzustellen, ob die Betroffenen sich an das Fahrverbot halten?

Meine Frage nach der Rechtsgrundlage für diese regelmäßigen Meldungen wurde nicht abschließend geklärt. Das Niedersächsische Innenministerium hatte angeregt, im Hinblick auf eine geplante Änderung des Straßenverkehrsgesetzes von der Herausgabe der Erlaßregelung abzusehen. Damit schien die Angelegenheit zunächst erledigt zu sein. Um so überraschter war ich, als in meiner Dienststelle Errichtungsanordnungen für polizeiliche Dateien eingingen, in denen Mitteilungen der Straßenverkehrsbehörden über entzogene Fahrerlaubnisse gespeichert werden. Die hierzu erbetene Stellungnahme des Innenministeriums räumt meine Bedenken nicht aus. Ich ha-

be mich auch dagegen ausgesprochen, die regelmäßigen Meldungen durch eine Verordnung nach § 12 NDSG zuzulassen.

30.3 Speicherung von hartnäckigen Parksündern

In Niedersachsen wird ein automatisiertes Verfahren "Ordnungswidrigkeiten" eingesetzt, das die Speicherung und Erkennung von hartnäckigen Parksünderinnen und Parksündern ermöglicht. Die Erfassung von wiederholten Verstößen gegen straßenverkehrsrechtliche Vorschriften soll eine erhöhte Ahndung ermöglichen. Ich habe unter X 30.2 zu den Rahmenbedingungen bei der Erfassung von wiederholten Verstößen Stellung genommen. Eingaben von betroffenen Personen gaben mir Veranlassung, mich erneut mit der Thematik zu befassen. Dabei komme ich zu dem Ergebnis, daß die Zulässigkeit der Speicherung von wiederholten Verstößen in örtlichen Dateien in Frage zu stellen ist und die Weiterführung der derzeit geübten Praxis überdacht werden sollte:

- Die Berechtigung zum Speichern von wiederholten Verstößen wird auf § 17 Abs. 3 OWiG gestützt. Nach dieser Vorschrift ist bei der Bemessung der Geldbuße der Vorwurf, der den Täter trifft, zu berücksichtigen. Wiederholte Verstöße spielen für den Grad der Vorwerfbarkeit eine Rolle und können zur Erhöhung der festzusetzenden Geldbuße führen. Nach dem Wortlaut des Gesetzes ergibt sich diese Konsequenz allerdings nur für die Entscheidung über die Höhe der Geldbuße im Ordnungswidrigkeitenverfahren, nicht jedoch für die Höhe des Verwarngeldes im Verwarnungsverfahren. Im Fall der Petenten führten deren wiederholte Parkverstöße zu erhöhten Verwarnungsgeldern.
- Das Verwarnungsverfahren zielt darauf ab, ein förmliches Bußgeldverfahren mit einer förmlichen Entscheidung zu ersparen. Seine Besonderheit besteht darin, daß dem Betroffenen das Fehlverhalten lediglich vorgehalten wird, ohne daß darüber definitiv entschieden wird. Mit seinem Einverständnis wird ihm ein "Denkzettel" in Form eines Zahlungsbetrages erteilt. Diesem besonderen Wesen des Verwarnungsverfahrens widerspricht die Speicherung der in der Vergangenheit verhängten Verwarnungen zu dem Zweck, bei erneuten geringfügigen Ordnungswidrigkeiten ein erhöhtes Verwarnungsgeld festzusetzen. Nach der einschlägigen Kommentierung (Göhler, Ordnungswidrigkeitengesetz, 9. Aufl., §17, RdNr. 20c) sollen selbst bei der Bemessung von Geldbußen im förmlichen Ordnungswidrigkeitenverfahren grundsätzlich frühere Verwarnungsgelder außer Betracht bleiben.
- Der Bund-Länder-Fachausschuß für Straßenverkehrsordnungswidrigkeiten ist bei der Erörterung der Problematik zu dem Ergebnis gekommen, daß das Verkehrszentralregister die allein maßgebende Erfassungs- und Auskunftsstelle bezüglich der für die Belange der Verkehrssicherheit bedeutsamen gerichtlichen und verwaltungsbehördlichen Entscheidungen ist. Örtliche Dateien neben dem Verkehrszentralregister sind ohne gesetzliche Grundlage unzulässig. Das Bundesverkehrsministerium vertritt den Standpunkt, die Erfassung der Gesamtheit leichterer Verkehrsverstöße in einer kommunalen Datei sei nicht gerechtfertigt. Dateien, die

schon aus fachlicher Sicht nicht für zulässig und auch nicht für erforderlich gehalten werden, sind auch aus datenschutzrechtlicher Sicht nicht zu akzeptieren.

Einigkeit besteht zwischen dem Niedersächsischen Innenministerium und mir, daß die Speicherung vom Parkverstößen nicht dazu verwendet werden darf, bei zukünftigen Verwarnungsverfahren das Verwarnungsgeld zu erhöhen. Soweit die Verkehrssünderdatei dazu dient, hartnäckige Parksünder zu erkennen, hält das Ministerium die Speicherungen für zulässig. Gegen diesen Personenkreis soll kein Verwarnungsverfahren, sondern gleich ein förmliches Bußgeldverfahren durchgeführt werden. Diese Meinung überzeugt mich nicht. Sie widerspricht der dargestellten Position des Bund-Länder-Fachausschusses sowie des Bundesverkehrsministeriums. Auch wurde mir die für eine solche Datei erforderliche Rechtsgrundlage bis zum Redaktionsschluß nicht genannt.

## 30.4 Frontfotos: Kein Gruppenbild mit Dame

Bußgeldbehörden sind teilweise dazu übergegangen, in Bußgeldverfahren z.B. wegen Geschwindigkeitsübertretungen mit den Anhörungsbögen gleich ein sog. Frontfoto zu übersenden, das den Fahrer des "geblitzten" Fahrzeuges zeigt. Die Behörden versprechen sich von dieser Verfahrensänderung einen spürbaren Rückgang der Einsprüche gegen Bußgeldentscheidungen. Bisher wurden Fotos nur auf Anforderung - meist erst nach Einlegung des Einspruchs - zur Verfügung gestellt.

Zum datenschutzrechtlichen Problem wird diese Verfahrensweise, weil im Zeitpunkt der Anhörung des Halters noch nicht feststeht, ob er mit dem abgebildeten Fahrer identisch ist und weil auf den Frontfotos teilweise auch weitere Fahrzeuginsassen zu erkennen sind. Durch die Übersendung können Situationen entstehen, die von staatlicher Seite ohne Not nicht gefördert werden sollten. Die Verfahrensweise sollte keine ungerechtfertigten Eingriffe in das Recht auf informationelle Selbstbestimmung von Unbeteiligten verursachen. Es ist für den durch die frühe Übersendung des Beweismittels verfolgten Zweck nicht erforderlich, ein Radarfoto mit der Abbildung von weiteren Fahrzeuginsassen zu übersenden.

Ich begrüße, daß das Niedersächsische Innenministerium meine Anregung aufgenommen und die Bußgeldbehörden angewiesen hat, sicherzustellen, daß auf Frontfotoabzügen nur der Fahrer erkennbar ist. Soweit möglich wird die Polizei entsprechende Ausschnittsvergrößerungen anfertigen.

## 30.5 Wenn der Postmann zweimal klingelt

Ein Petent schrieb mir, daß der Postbote ihm eines Tages zwei verschlossene Briefumschläge mit dem Kommentar überreichte, er sei wohl zu schnell gefahren und müsse nun eine Geldbuße in Höhe von 229 DM bezahlen. Wie kam der Postbeamte zu seinem Wissen? Auf einem Umschlag war eine spre-

chende Absenderangabe (Stadt X, Abteilung für Bußgeld und Verwarngeld für Verkehrsordnungswidrigkeiten) gedruckt, die sehr genau auf den Inhalt schließen ließ. Im zweiten Umschlag steckte der vorgefertigte Überweisungsauftrag für die Zahlung der Geldbuße. Durch eine Öffnung konnte der Postbeamte die Höhe des Bußgeldbetrages erkennen.

Bei dieser Verfahrensweise werden zwangsläufig Daten an Außenstehende übermittelt. Im Fall der Ersatzzustellung (der Adressat wird nicht angetroffen) können die Informationen beispielsweise dem Vermieter oder Hauswirt offenbart werden. Eine Rechtsgrundlage gibt es dafür natürlich nicht.

Das Problem der Absenderangabe wurde schnell gelöst. Die Bußgeldbehörde wird zukünftig aus Gründen der Zuordnung bei Rückläufen wegen Unzustellbarkeit in der Absenderangabe eine Organisationsziffer verwenden, die nicht jedermann ohne weiteres deuten kann. Schwieriger gestaltete es sich, die Probleme mit dem Überweisungsträger zu lösen. Die Tücken der Technik wurden für die Erkennbarkeit des zu zahlenden Betrages verantwortlich gemacht. Würde der Umschlag verschlossen, so könnte der Bußgeldbetrag nur im Durchschreibverfahren auf den Überweisungsträger gedruckt werden. Ein automatisiertes Beleglesen wäre dann nicht mehr möglich. Ich habe erreicht, daß die Überweisungsträger zukünftig so erstellt werden, daß nur noch das Kassenzeichen der Behörde für Außenstehende lesbar ist, wodurch Rückschlüsse auf den Gegenstand der Briefsendung schwerlich möglich sind.

Auch wenn letztendlich eine datenschutzgerechte Lösung gefunden wurde, zeigt der Fall doch exemplarisch, wie schnell bei der Automatisierung von Verwaltungsverfahren (vermeintliche) technische Vorgaben als Rechtfertigung für unnötige Eingriffe in das Recht auf informationelle Selbstbestimmung akzeptiert werden.

## 30.6 Akteneinsicht grundsätzlich für den Verteidiger

Ich hatte zu prüfen, ob dem Rechtsanwalt eines Anzeigeerstatters Einsicht in die Akte der Ordnungswidrigkeitenbehörde gewährt werden darf. Rechtlich unbestritten ist, daß den Betroffenen, denen vorgeworfen wird, eine Ordnungswidrigkeit begangen zu haben, ein Recht auf Akteneinsicht zusteht, das grundsätzlich von seinem Verteidiger ausgeübt wird. Anderen Personen als dem Verteidiger ist in der Regel keine Akteneinsicht zu gewähren (vgl. 31.6.1). Für nicht am Bußgeldverfahren beteiligte Personen enthalten die Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) Bestimmungen darüber, inwieweit und in welcher Form Akteneinsicht zu gewähren ist. Diese Verwaltungsvorschriften können nicht als ausreichende Grundlage für Eingriffe in das Recht auf informationelle Selbstbestimmung akzeptiert werden. Sie können allenfalls bis zur Schaffung von gesetzlichen Ermächtigungen im Rahmen des sog. "Übergangsbonus" vorübergehend herangezogen werden.

Nach Nr. 185 Abs. 3 RiStBV kann einem bevollmächtigten Rechtsanwalt Akteneinsicht für die Prüfung bürgerlich-rechtlicher Ansprüche oder für die

Vorbereitung eines Verwaltungsstreitverfahrens gewährt werden, wenn er ein berechtigtes Interesse darlegt und sonst keine Bedenken bestehen (vgl. 31.7). Im Rahmen des "Übergangsbonus" sind an die in den Richtlinien genannten Voraussetzungen strenge Maßstäbe anzulegen. Unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit hat die ersuchte Behörde sorgfältig zu prüfen, ob Anhaltspunkte für das Vorliegen eines berechtigten Interesses bestehen.

Im konkreten Fall hatte die Ordnungswidrigkeitenbehörde die Voraussetzungen der RiStBV nicht beachtet. Sie trug damit unfreiwillig zu einer Situation bei, die für den Petenten fatale Folgen hatte. Der Anzeigeerstatter hatte einen Rechtsanwalt mit der Beantragung der Akteneinsicht beauftragt. Die Ordnungswidrigkeitenbehörde übersandte die Akte entsprechend der üblichen Praxis in die Kanzlei des Rechtsanwalts zur Einsichtnahme. Der Anzeigeerstatter verteilte anschließend Kopien von Unterlagen aus der Ordnungswidrigkeitenakte im Ort (u.a. einen Strafbefehl gegen den Betroffenen wegen Steuerverkürzung). Die Übersendung der Akte an den Rechtsanwalt des Anzeigeerstatters habe ich beanstandet. Weder aus dem Antrag auf Akteneinsicht noch aus der beigefügten Vollmacht ergaben sich Anhaltspunkte für das Vorliegen eines berechtigten Interesses im Sinne der RiStBV. Die Ordnungswidrigkeitenbehörde hätte die Akteneinsicht deshalb ablehnen müssen.

## 31. Rechtspflege

### 31.1 Informationsverarbeitung im Strafverfahren

Leider hat sich seit meiner bereits im X. Tätigkeitsbericht geübten Kritik bzgl. des Fehlens gesetzlicher Verarbeitungsregelungen im Strafverfahren (X 31.1) nichts geändert. Nach wie vor fehlen konkrete gesetzliche Bestimmungen für die Erhebung und Weiterverarbeitung personenbezogener Daten. Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer Konferenz im September 1994 erneut eine Entschließung (vgl. Anlage 19) verabschiedet.

Zu meinem Bedauern wird in der Öffentlichkeit immer wieder der Eindruck erweckt, der Datenschutz stehe einer erfolgreichen Bekämpfung einer immer mehr wachsenden Kriminalität im Wege (so Generalstaatsanwalt Dr. Endler nach einem Bericht der Hannoverschen Allgemeinen Zeitung v. 3. Oktober 1993). Ein Beleg dafür konnte mir noch nicht vorgelegt werden. Ich wende mich allerdings gegen Datenverarbeitung, die ohne erforderliche Rechtsgrundlage oder Notwendigkeit erfolgt, oder deren Folgen in keinem Verhältnis zum erstrebten Zweck steht. Dies ist zum Schutz insbesondere unbeteiligter Dritter, aber auch von Zeugen und Opfern unbedingt erforderlich und entspricht meinem gesetzlichen Auftrag.

31.2 Verbrechensbekämpfungsgesetz - zentrales staatsanwaltliches Verfahrensregister

Das inzwischen vom Bundestag beschlossene Verbrechensbekämpfungsgesetz (BGBl. I 1994 S. 3186) enthält Regelungen von erheblicher datenschutzrechtlicher Bedeutung. Neben dem unter 14.2 dargestellten nunmehr zugelassenen Zusammenwirken von Geheimdiensten und Polizei im Strafverfahren wurde die Einführung eines zentralen staatsanwaltschaftlichen Verfahrensregisters beschlossen. Darin ist die Speicherung der Daten sämtlicher Beschuldigter in Strafermittlungsverfahren vorgesehen. Bisher erfolgte nur eine Speicherung rechtskräftiger Verurteilungen beim Bundeszentralregister (BZR). Ansonsten existieren zentrale Namenskarteien bei jeder Staatsanwaltschaft - im übrigen ohne die dafür erforderliche Rechtsgrundlage (vgl. OLG Frankfurt/M., Beschluß v. 3. Dezember 1993 - 3 VAs 31/93).

Die geplante bundesweite Zentralisierung des Verfahrensregisters bedeutet einen massiven Eingriff in die Rechte der Betroffenen. Die komplette Aufnahme jedes Ermittlungsverfahrens ohne Berücksichtigung der Schwere des Tatvorwurfs steht in keinem Verhältnis zum Interesse an einer wirksamen Strafverfolgung. Dies gilt insbesondere für unbegründete Strafanzeigen, für Fahrlässigkeitsdelikte und Bagatellsachen. Verdachtsfälle von Gewicht und überörtlicher Bedeutung speichert die Polizei im bundesweiten polizeilichen Informationssystem. Diese Informationen stehen somit zur Strafverfolgung neben den im BZR bzw. Verkehrszentralregister erfaßten rechtskräftigen Entscheidungen und Verurteilungen zur Verfügung. Soweit darüber hinaus ein unabweisbarer Bedarf an zentraler Erfassung weiterer Daten über Ermittlungsverfahren besteht, wären gesetzliche Kriterien festzulegen, die einer Abgrenzung der relevanten von den übrigen Verfahren ermöglichen. Deutlich wird diese Problematik auch unter dem Gesichtspunkt des Geldwäschegesetzes (vgl. 31.4). Danach muß jede Meldung über meldepflichtige Transaktionen bei der Staatsanwaltschaft mit einem "Js"-Aktenzeichen versehen werden. Dies hat dann die Meldung zum Bundesregister zur Folge, auch wenn es sich um völlig harmlose Einzahlungen, aber eben über 20.000 DM, handelt.

Die Daten sind nach §§ 474 Abs. 3, 476 Abs. 1 StPO laufend zu aktualisieren. Hierfür trägt die zuständige Staatsanwaltschaft die Verantwortung. Angesichts der allgemein bekannten und nicht zu bestreitenden Belastungen der Staatsanwaltschaften ist nicht davon auszugehen, daß dieses Register auf dem Laufenden gehalten werden kann. Die Eintragung aller Verfahren bekommt durch diesen Umstand besondere Brisanz. Meine Position zu diesem Gesetz fand Eingang in den Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zur "Informationsverarbeitung im Strafverfahren" (vgl. Anlage 11).

31.3 Strafverfahrensänderungsgesetz (StVÄG)

Die in dem o.g. Beschluß erhobenen datenschutzrechtlichen Forderungen erstrecken sich auch auf den Entwurf eines Strafverfahrensänderungsgesetzes 1994 (StVÄG 1994) des Strafrechtsausschusses der Justizministerkonferenz. Bezüglich dieses Entwurfs habe ich gegenüber der Staatskanzlei erhebliche Bedenken an einer Mitantragstellung des Landes Niedersachsen geäußert. Dabei habe ich insbesondere auf den sehr problematischen Bereich der Akteneinsicht (§§ 474 ff. des Entwurfs) hingewiesen.

Es ist ohne weitere Ausführungen für jeden vorstellbar, welche Vielzahl sehr intimer Daten sich in Straf-, aber auch Familienrechts- und Sozialgerichtsakten, um nur einige Beispiele zu nennen, befindet. Nach dem geplanten § 474 Abs. 1 StPO sollen nicht nur Gerichte und Staatsanwaltschaften, sondern auch alle anderen Justiz- und Strafverfolgungsbehörden zum Zwecke der Rechtspflege Akteneinsicht bekommen. Der Begriff der Rechtspflege ist so weit, daß hier kaum noch von einem genau definierten Empfängerkreis ausgegangen werden kann. Die Problematik wird offensichtlich, wenn man die Bestimmung mit der engen Zweckbindungsregelung des § 10 NDSG vergleicht, der in Niedersachsen die eigenen öffentlichen Stellen unterworfen sind. Darüber hinaus enthält die Bestimmung keine Beschränkung auf die erforderlichen Aktenteile oder einen Ausschluß der Einsichtnahme in beigezogene Akten z. B. aus Familienrechtsstreitigkeiten. Nach der Entwurfsfassung könnte gemäß § 475 StPO jede Privatperson über einen Anwalt bei Darlegung eines berechtigten Interesses Auskunft und Akteneinsicht erhalten. An ein solches "berechtigtes Interesse" wären wesentlich geringere Anforderungen zu stellen als an ein "rechtliches Interesse", wie es von datenschutzrechtlicher Seite gefordert wird.

Eine umfassende Auseinandersetzung mit dem Gesetz ist an dieser Stelle nicht möglich. Schon die dargestellten Kritikpunkte zeigen, daß solche Gesetzesvorhaben, die unter dem öffentlichen Druck der Verbrechensbekämpfung diskutiert werden, für jede Person erhebliche stigmatisierende Auswirkungen haben können. Es genügt die Beteiligung an einem Bagatelldelikt oder eine verleumderische Strafanzeige, die schon nach den ersten Überprüfungen in sich zusammengefallen ist.

31.4 Geldwäschegesetz

Mit dem Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) vom 15. Juli 1992, (BGBl. I S. 1302) wurde der Straftatbestand der sogenannten Geldwäsche in das Strafgesetzbuch eingearbeitet (§ 261 StGB). Näheres hierzu regelt das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG) vom 25. Oktober 1993 (BGBl. I S. 1770). Von datenschutzrechtlicher Relevanz ist diese Vorschrift u.a. wegen der in ihr festgelegten Identifizierungspflichten. Identifizierung bedeutet in diesem Zusammenhang Datenerhebung. Es ist - erfreulicherweise - bereichsspezifisch geregelt, wer, nämlich z.B. Geldinstitute, Versicherungen,

Gewerbetreibende, Spielbanken (vgl. §§ 2 bis 4, 14 GwG), wen wie zu identifizieren hat (§ 1 Abs. 5 GwG). Der Name ist anhand eines Personalausweises oder Reisepasses unter Verwendung der Angaben zu Geburtsdatum und Anschrift, soweit sie darin enthalten sind, sowie Art, Nummer und ausstellender Behörde des amtlichen Ausweises festzustellen. Datenspeicherungsvorschriften finden sich in § 9 (Aufzeichnungs- und Aufbewahrungspflicht). Begrüßenswert gewesen wäre eine Bestimmung zur Löschung der Daten (am Ende der - sechsjährigen - Aufbewahrungsfrist). Datenschutzrechtlich positiver zu beurteilen ist die in §§ 10, 11 Abs. 5 vorgeschriebene Zweckbindung der Daten. Problematisch hingegen sind die Bestimmungen über die Datenübermittlung (§ 11). Es bleibt offen, an welche der Strafverfolgungsbehörden die Verdachtsfälle gemeldet werden sollen: Staatsanwaltschaft, Polizei oder Zoll?

Angesichts dieser Unklarheit sind Arbeitsanweisungen für die praktische Umsetzung besonders wichtig, die durch einen Gemeinsamen Runderlaß des Niedersächsischen Innenministeriums und des Justizministeriums (Richtlinien für die Zusammenarbeit von Staatsanwaltschaft und Polizei bei Finanzermittlungen im Rahmen des Geldwäschegesetzes vom 9. September 1994, Nds. MBl. S. 1352) geschaffen wurden. Ich halte den mir vorliegenden Entwurf für problematisch. Im Zuge einer ersten datenschutzrechtlichen Bewertung habe ich z.B. auf das Fehlen von Verfahrensanweisungen für die Fälle hingewiesen, in denen sich ein weiteres Ermittlungsverfahren nicht anschließt, weil der geäußerte Verdacht sich nicht bestätigt hat. Es fehlen insofern Löschungsvorgaben, aber auch Löschungsfristen für den Regelfall. Weiter bin ich davon ausgegangen, daß sich die Datenverarbeitung auf die im GwG genannten Daten beschränkt. Dem ist das Innenministerium entgegengetreten. Es hält neben den Identifizierungsdaten die Verarbeitung noch weiterer Daten für erforderlich. Offene weitere datenschutzrechtliche Fragen werden mit beiden Ministerien noch zu erörtern sein.

## 31.5 Kontrollen

Im Berichtszeitraum wurden von mir im Bereich der Rechtspflege zwei umfangreichere Kontrollen durchgeführt.

### 31.5.1 Kontrolle von Telefonüberwachungsmaßnahmen gemäß §§ 100a ff. StPO

Ich habe bei einem Schwerpunktkriminalkommissariat für organisierte Kriminalität eine dort durchgeführte Telefonüberwachungsmaßnahme kontrolliert. Es handelte sich um ein sehr umfangreiches Verfahren, in dem unter anderem einige Telefonzellen in die Überwachung mit einbezogen waren. Allein aus diesen Telefonzellen heraus wurden einige tausend Gespräche Unbeteiligter aufgezeichnet und ausgewertet.

Ich möchte an dieser Stelle unterstreichen, daß ich mich nicht gegen die Einbeziehung von Telefonzellen in Überwachungsmaßnahmen gem. § 100a

StPO stelle. In der Tat wäre es für jeden Ermittler unerträglich, am überwachten Anschluß die Bemerkung: "Ich gehe jetzt zur Zelle, ich ruf' in fünf Minuten zurück" zu hören und damit am Ende seiner Möglichkeiten zu sein. Andererseits macht aber die Zahl der überwachten Gespräche Unbeteiligter deutlich, daß zu deren Schutz hier besondere organisatorische Maßnahmen getroffen werden müssen, wenn sie schon im Interesse einer effektiven Strafverfolgung den Einbruch in die Privatheit ihrer Gespräche hinnehmen müssen. Dabei ist zu berücksichtigen, daß die Regelungen der §§ 100a ff. StPO nicht für die Überwachung von öffentlichen Telefonanschlüssen "passen". Die Strafprozeßordnung erlaubt von ihrem Wortlaut her auch die Überwachung derartiger Anschlüsse: "Die Anordnung darf sich nur gegen den Beschuldigten oder gegen solche Personen richten, von denen ... anzunehmen ist ..., oder daß der Beschuldigte ihren Anschluß benutzt". Doch macht die Anknüpfung an die Person und nicht an den Anschluß deutlich, daß sie von der Überwachung des Anschlusses des Beschuldigten oder solcher Personen ausgeht, die mit dem Betroffenen in einer wie auch immer gearteten Lebensbeziehung stehen. Aus dieser Beziehung heraus verlangt die Rechtsordnung auch Unbeteiligten den Einbruch in ihre Privatsphäre ab. Dies gilt jedoch für Nutzer einer Telefonzelle nicht, in der in besonderem Maße gerade die Anonymität gegeben zu sein scheint. Darüber hinaus läßt sich für Nutzer von Telefonzellen die von der StPO vorgesehene Benachrichtigung über die erfolgte Überwachung (§ 101 Abs. 1) nicht realisieren. Ich habe deswegen die Löschung der Gespräche bzw. ihre Sperrung verlangt, sobald feststeht, daß sie in keinem Zusammenhang mit dem Strafverfahren stehen.

Dieselbe Forderung habe ich für Gespräche erhoben, die aufgrund der technischen Abläufe der Überwachung ohne Zusammenhang mit dem Fernmeldeverkehr aufgezeichnet werden (Aufzeichnung von Raumgesprächen ohne Zustandekommen einer Verbindung oder bei nicht korrekt aufgelegtem Telefonhörer). Die richterliche Anordnung ist auf die Überwachung des Fernmeldeverkehrs beschränkt, zu dem derartige Raumgespräche nicht gehören.

Zur Beanstandung führte die Aufzeichnung und Auswertung von Verteidigergesprächen entgegen der eindeutigen Bestimmung des § 148 Abs. 1 StPO, die unmittelbar aus der Verbürgung der freien Strafverteidigung durch das Grundgesetz resultiert. Jeder Eingriff in den Verkehr zwischen Beschuldigten und Verteidigung ist - liegen die auch dafür vorhandenen Ausnahmefälle nicht vor - verboten. Die Einhaltung dieses rechtsstaatlichen Gebots ist unverzüglich sicherzustellen. Die kurz vor Redaktionsschluß eingegangene Stellungnahme der zuständigen obersten Landesbehörde zu dieser Prüfung läßt den Willen dazu nicht erkennen.

31.5.2 Kontrolle der Zentralen Namenskartei einer Staatsanwaltschaft.

Im Zentrum der am Ende des Berichtszeitraums durchgeführten Prüfung einer Zentralen Namenskartei (ZNK) steht die Aktualität und Richtigkeit der Eintragungen. Die ZNK wird wie beim überwiegenden Teil der Staatsanwaltschaften Niedersachsens mit Unterstützung der EDV (SIJUS-STRAF)

geführt. Besondere Bedeutung gewinnen diese Dateien wegen der durch das Verbrechensbekämpfungsgesetz notwendig werdenden Meldung aller Verfahren an ein zentrales staatsanwaltliches Verfahrensregister beim BZR (vgl. 31.2). Über das Ergebnis der Prüfung kann hier noch nicht berichtet werden.

## 31.6 Schutz von Opfern und Zeugen im Strafverfahren

### 31.6.1 Akteneinsicht

Das Thema Akteneinsicht war auch in diesem Berichtszeitraum Gegenstand zahlreicher Petitionen (vgl. X 31.3). In einem Fall hatte der Verteidiger eines Jugendlichen die ihm durch Akteneinsicht bekanntgewordenen Daten der übrigen Verfahrensbeteiligten an die Mutter seines Mandanten weitergegeben mit dem Ziel, alle Mitangeklagten zu einem strafmildernden Täter-Opfer-Ausgleich (§ 45 Abs. 2 Satz 2 JGG) zu bewegen. Demselben Zweck diente die Weitergabe des Namens und der Anschrift der Zeugin eines Banküberfalls durch einen Verteidiger an seinen dieser Tat angeklagten Mandanten.

Jede Einsicht in eine Strafakte führt zu Eingriffen in das Recht auf informationelle Selbstbestimmung, weil damit Informationen über Personen zugänglich gemacht werden. Die Rechtsgrundlage für die Einsicht durch die Verteidigerin bzw. den Verteidiger enthält § 147 StPO. Die Verteidiger haben sich in beiden Fällen offensichtlich nicht auf die Einsicht beschränkt, sondern haben dabei gewonnene Daten an ihre Mandanten weitergegeben. Dies wird allgemein für zulässig gehalten; in der Regel wird sogar von einer Verpflichtung zur Weitergabe ausgegangen. Meines Erachtens kann sich dies jedoch nur auf solche Informationen beziehen, die für die Wahrnehmung der Verteidigung erforderlich sind. Ob dies in den beiden Fällen gegeben war, entzieht sich meiner Beurteilung. Die Gewährung der Akteneinsicht war jedenfalls nicht zu beanstanden.

In einem anderen Fall hatte ein Petent einen offensichtlich sachdienlichen Hinweis an die Polizei gegeben und wurde daraufhin von der Beschuldigten telefonisch drangsaliert. Auch sie hatte den Namen und die Anschrift des Petenten von ihrem Anwalt nach erfolgter Akteneinsicht erhalten. Hier ist die Akteneinsicht ebenfalls durch § 147 StPO gedeckt. Gleichwohl habe ich mich zunächst gegenüber dem Niedersächsischen Justizministerium dafür eingesetzt, daß Bürgerinnen und Bürger, die lediglich Ermittlungsansätze vermitteln, ohne als Zeugen in Betracht zu kommen, zunächst nicht in die Ermittlungsakte aufgenommen werden. Sie sollen nur im Tagebuch der Polizei notiert werden, damit man gegebenenfalls auf sie zu einer Zeugenaussage zurückkommen kann. Ob dies ein gangbarer Weg ist, wird der weiteren Prüfung vorbehalten bleiben.

Was die Weitergabe der Daten von Rechtsanwältinnen und Rechtsanwälten an ihre Mandanten betrifft, so sind mir datenschutzrechtlich die Hände gebunden, denn sie sind zwar Organe der Rechtspflege, aber sie üben einen "freien Beruf" aus (§§ 1, 2 Bundesrechtsanwaltsordnung). Sie sind datenschutzrechtlich als Private zu behandeln. Zwar nehme ich auch die Funktion der Aufsichtsbehörde nach § 38 BDSG wahr. Mir obliegt auch die Aufsicht über die Einhaltung der Datenschutzvorschriften von Privaten. Das BDSG regelt jedoch nur die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien (vgl. 34.2). Die Rechtsanwälte hatten jedoch in allen oben genannten Fällen keine Datenübermittlung aus einer Datei, sondern lediglich aus einer Akte vorgenommen. Das BDSG ist hierauf nicht anwendbar.

31.6.2 Einstellungsverfügung an den Anzeigeersttatter

Die Staatsanwaltschaft hat den Anzeigeerstatter gemäß § 171 StPO in einem Bescheid mit Gründen darüber zu unterrichten, wenn sie das von ihm beantragte Verfahren nicht eröffnet oder einstellt. Näheres regelt das Gesetz nicht. In einem solchen Bescheid kann die Staatsanwaltschaft daher sehr eingehende Angaben über Opfer und Zeugen aufnehmen, indem sie die Einstellungsverfügung ungekürzt an den Anzeigeerstatter weitergibt. Dabei ist zu berücksichtigen, daß der Anzeigeerstatter nicht selbst vom Verfahren betroffen sein muß, es kann sich um einfache interessierte Bürgerinnen oder Bürger handeln. Diese erhalten auf diese Weise u.U. intime Details über den Gesundheitszustand, die häuslichen Verhältnisse etc. von Opfern, Zeugen und Beschuldigten. Ich habe mich gegenüber dem Niedersächsischen Justizministerium dafür eingesetzt, daß durch eine Änderung der RiStBV die schutzwürdigen Interessen des betroffenen Personenkreises mit dem Informationsbedürfnis der Anzeigeerstattenden abgewogen werden müssen. Das Justizministerium hat zugesagt, diese Position in dem für die RiStBV zuständigen bundesweiten Ausschuß zu unterstützen.

31.6.3 Nennung von Zeugenanschriften im Strafbefehl

Im Zuge meiner Anfrage zum Verzicht der Wohnanschrift von Zeugen in den Strafbefehlsanträgen der Staatsanwaltschaften (vgl. XI 31.3) hat das Niedersächsische Justizministerium auf die erweiterten Schutzmöglichkeiten für die Vernehmung, die Ladung und die Anklageschrift (§§ 68 Abs. 2, 200 Abs. 1 Satz 2, 222 StPO) hingewiesen, die durch das OrgKG vom 15. Juli 1992 geschaffen worden sind. Danach ist es bei gefährdeten Zeugen generell möglich, statt des Wohnortes den Geschäfts- oder Dienstort oder eine andere ladungsfähige Anschrift anzugeben. Die Neuregelung sei in einer Dienstbesprechung mit den Staatsanwaltschaften dahingehend erörtert worden, daß auch im Strafbefehl bei gefährdeten Zeugen entsprechend verfahren werden solle. Ein genereller Verzicht auf die Angabe der Wohnanschrift von Zeugen in den Strafbefehlsanträgen der Staatsanwaltschaften werde jedoch nicht möglich sein, um den Beschuldigten die Prüfung zu ermöglichen, ob die Tat beweisbar oder ein Einspruch gegen den Strafbefehl aus-

sichtsreich ist. Das Justizministerium geht jedoch davon aus, daß zukünftig vermehrt auf die Angabe der Wohnanschriften von gefährdeten Zeugen verzichtet werde. Aus datenschutzrechtlicher Sicht wäre dies zu begrüßen.

31.7 Akteneinsicht für die Wahrnehmung privater Interessen

Akteneinsicht in strafprozessuale Akten wird nicht nur im Zusammenhang mit dem konkreten Verfahren gewährt. Ein Petent beschwerte sich darüber, daß im Rahmen eines Zivilrechtsstreits die Akte eines früher gegen ihn geführten Strafverfahrens vom Prozeßgegner vorgelegt wurde. Ich konnte den Beschwerdeführer bedauerlicherweise nur auf die Vorschriften der Nrn. 182 ff. - insbesondere Nr. 185 Abs. 3 - RiStBV verweisen, nach denen einem bevollmächtigten Rechtsanwalt oder Rechtsbeistand Akteneinsicht gewährt werden kann, wenn er ein berechtigtes Interesse (z.B. für die Prüfung bürgerlich-rechtlicher Ansprüche) darlegt und wenn sonst Bedenken nicht bestehen. Da die längst überfällige Novelle der StPO nach wie vor fehlt (siehe 31.3), werden hier weiterhin Datenübermittlungen auf eine Verwaltungsvorschrift und nicht auf ein Gesetz gestützt.

31.8 Datenübermittlungen bei Überweisung von Geldbußen an gemeinnützige Einrichtungen

Nach § 153a StPO besteht die Möglichkeit, Strafverfahren gegen die Zahlung einer Geldbuße einzustellen. Gemeinnützige Einrichtungen erfahren als Empfänger der Zahlungen durch die Überweisungen die persönlichen Daten der Betroffenen. Eine Rechtsgrundlage für diese Datenübermittlungen sollte m.E. auch nicht geschaffen; die Übermittlungen sollten vielmehr vermieden werden. Dies wäre durch die Gestaltung der Überweisungsformulare möglich, die zwar im Durchschreibeverfahren ausgefüllt werden, bei denen jedoch auf dem Beleg für den Empfänger nur das Aktenzeichen, und nicht der Name des Anweisenden und dessen Unterschrift durchgeschrieben werden. Der Zahlungseingang könnte dann durch das dem Empfänger mitgeteilte Aktenzeichen überwacht werden. Eine Antwort des Niedersächsischen Justizministeriums zu meinem Vorschlag steht noch aus.

31.9 Information der Angezeigten über die oder den Anzeigeerstattenden im Ordnungswidrigkeitenverfahren

Anlaß für eine Reihe von Petitionen war die Praxis in Ordnungswidrigkeitsverfahren, die Anhörung der Betroffenen in der Weise durchzuführen, daß ihnen eine Durchschrift der Anzeige mit allen darin enthaltenen Informationen zur Anzeigeerstatterin bzw. zum Anzeigeerstatter übersandt wird. Meine Bemühungen gegenüber dem Niedersächsischen Justizministerium, hier zu einer Veränderung zu kommen, waren bisher nicht erfolgreich. Die geschilderte Praxis ist durch keine Rechtsvorschrift gedeckt. Weder die Bestimmungen über die Anhörung (§ 55 OWiG) noch die über die Akteneinsicht (§ 46 Abs. 1 OwiG i.V.m. § 147 StPO) rechtfertigen die routinemäßige

Übermittlung der Anzeige. Auch der bereits über Gebühr strapazierte sog. "Übergangsbonus" vermag hier keine "Ersatzrechtsgrundlage" zu verschaffen, da die dargestellte Übung nicht erforderlich ist, sondern allein der Arbeitsersparnis dient. Für die Sachbearbeiterin bzw. den Sachbearbeiter entfällt so die eigene Darstellung des Sachverhalts in einem Anhörungsschreiben. Arbeitsökonomie ersetzt jedoch nicht die vom Bundesverfassungsgericht geforderte Rechtsgrundlage, wenn sie auch im Entwurf des StVÄG 94 entscheidendes Kriterium für eine Vielzahl von Datenübermittlungen wird.

31.10 Ehescheidungsverbundurteile

Ehescheidungsverfahren können gem. § 623 Abs. 1 ZPO zusammen mit Entscheidungen über die elterliche Sorge, Umgangsrechte und Unterhaltspflichten mit einem Verbundurteil abgeschlossen werden. Diese Urteile sind von den Beteiligten in vielfacher Weise bei Behörden wie z.B. dem Standesamt, Gerichtsvollziehern, u.U. auch dem Arbeitgeber vorzulegen (vgl. XI 31.14). Dabei ist nur die Vorlage einer Ausfertigung des Urteilstenors, nicht jedoch die Kenntnisnahme von den teilweise sehr sensiblen Daten der Entscheidungsgründe erforderlich. Die Erteilung derartiger beschränkter Ausfertigungen ist möglich. Leider weiß die nicht anwaltlich vertretene Partei oft nichts über diese Möglichkeit. Ein Hinweis darauf wird in Zukunft diejenigen erreichen, bei denen das Amtsgericht/Familiengericht bereits mit dem System SIJUS-FAM arbeitet, dessen flächendeckender Einsatz in Niedersachen Mitte 1994 begonnen hat.

31.11 Nettolohn und Unterhaltsberechtigte in Drittschuldnererklärungen

Eine Petition wandte sich dagegen, daß die Beschäftigungsbehörde des Petenten im Rahmen eines Zwangsvollstreckungsverfahrens in einer Drittschuldnererklärung Angaben zur Höhe seiner monatlichen Nettobezüge und der Anzahl der Unterhaltsberechtigten gemacht hatte. Diese Angabe wurde in einem von der Bezirksregierung verwandten Vordruck erfragt. Die Beschwerde war begründet. Rechtsgrundlage für die Erklärungen der Bezirksregierung als Drittschuldnerin war § 840 Abs. 1 ZPO. Danach ist eine Aussage weder zu den monatlichen Nettobezügen noch zu der Zahl der Unterhaltsberechtigten erforderlich. Der eindeutige Wortlaut dieser Bestimmung kann nicht mit wirtschaftlichen Überlegungen zugunsten des Gläubigers erweitert werden. Diese Auffassung vertritt auch das Niedersächsische Justizministerium.

Die Bezirksregierung hat zwischenzeitlich veranlaßt, daß der Vordruck, in dem die Angabe der Höhe des Nettogehalts und der Zahl der unterhaltsberechtigten Personen vorgesehen ist, entsprechend den datenschutzrechtlichen Erfordernissen korrigiert wird.

## 31.12 Gerichtsvollzieher

### 31.12.1 Ersatzzustellungen

Mir lag die Beschwerde des Datenschutzbeauftragten eines Instituts (GmbH) darüber vor, daß ein Gerichtsvollzieher dem Unternehmen mehrfach Lohnpfändungsbescheide offen zugestellt habe, indem er wahllos Bedienstete, die sich gerade an der Pforte des Instituts aufhielten, ansprach und diese um Unterschrift unter die Zustellungsurkunde mit dem Hinweis bat, er sei berechtigt, jedem angetroffenen Bediensteten den Vorgang auszuhändigen, auch wenn dadurch Einblick in die Daten der oder des Betroffenen genommen werden konnte. Gegen diese offene Aushändigung der Unterlagen wehrten sich die Mitarbeiterinnen und Mitarbeiter, da dies mit Peinlichkeiten verbunden war.

Bei Zustellung an Gesellschaften oder sonstige Personenmehrheiten (§ 184 ZPO) war bisher in § 35 Nr. 1 der Gerichtsvollziehergeschäftsanweisung (GVGA) eine offene Übergabe vorgesehen. Meine Bemühungen gegenüber dem Niedersächsischen Justizministerium um eine datenschutzgerechte Verfahrensweise hatten Erfolg. Vom 1. November 1994 an gelten Gerichtsvollziehervorschriften, die eine offene Übergabe auf den Fall beschränken, daß der Empfänger persönlich zur Abgabe der Drittschuldnererklärung befugt ist. Diese Regelung ist datenschutzrechtlich akzeptabel.

### 31.12.2 Zwangsvollstreckung in EDV-Hardware

Die Pfändung von Informationstechnik-Systemen (IT-Systeme) durch Gerichtsvollzieher ist datenschutzrechtlich nicht unproblematisch, wenn in den zur Pfändung anstehenden Geräten noch personenbezogene Daten gespeichert sind. Es stellte sich heraus, daß sich das Niedersächsische Justizministerium bereits Anfang 1993 mit diesem Problem befaßt hatte. Angesichts der geringen bisherigen Erfahrungen mit der Pfändung von EDV-Anlagen hielt das Ministerium allerdings eine Regelung noch für verfrüht. Der Meinungsaustausch zwischen den Justizverwaltungen ist noch nicht abgeschlossen. Ich werde die Entwicklung weiter verfolgen (vgl. 19.4).

## 31.13 Schuldnerverzeichnis

Nach jahrelangen Beratungen (vgl. IX und X 31.11) sind mit dem Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis vom 15. Juli 1994 (BGBl. I S. 1566) neue Rechtsgrundlagen geschaffen worden. Neben aus datenschutzrechtlicher Sicht begrüßenswerten Bestimmungen, wie z.B. Zweckbindungsvorschriften in § 915 Abs. 2 ZPO und Löschungsregelungen in § 915 a, § 915 b Abs. 2, § 915 g Abs. 2 ZPO, blieben wichtige datenschutzrechtliche Forderungen unberücksichtigt. Dies betrifft im wesentlichen die weite und kaum kontrollierbare Streuung der Abdrucke (§ 915 e) und Listen (§ 915 f ZPO). Eine gravierende Entscheidung dazu ist mit § 915 e

Abs. 1 Buchst. b getroffen worden: Abdrucke aus den Schuldnerverzeichnissen können zur Errichtung und Führung zentraler bundesweiter oder regionaler Schuldnerverzeichnisse erteilt werden. Die Einrichtung derartiger privater bundesweiter Schuldnerverzeichnisse ist damit erstmals möglich geworden. Ich teile die Auffassung mit anderen Beauftragten für den Datenschutz, daß die Auskunft und Pflege der zwangsweise den Bürgern abverlangten Daten unter staatlicher Obhut bleiben muß.

Die an mich herangetragene Beschwerde über die Veröffentlichung des Zusatzes "Sozialth. Anstalt" hinter der Adresse des Betroffenen in einem Schuldnerverzeichnis hielt ich für begründet. Durch diesen Zusatz werden Informationen über den Betroffenen ohne Zustimmung und Rechtsgrundlage offenbart. Neben dem zuständigen Amtsgericht habe ich mich auch an das Niedersächsische Justizministerium gewandt, um auf eine Klarstellung über den Wegfall derartiger Zusätze, wie er bereits im Zusammenhang mit Urteilsabfassungen erfolgt ist (vgl. XI 31.12.), hinzuwirken.

## 31.14 Grundbuch

### 31.14.1 Einsichtnahme

Beschwerden über Einsichtnahmen in das Grundbuch finden kein Ende. Ich teile den Anfragenden immer wieder mit, daß die Darlegung eines berechtigten Interesses für die Bewilligung der Einsichtnahme ausreicht. Nach einschlägiger Rechtsprechung ist ein berechtigtes Interesse schon gegeben, wenn die antragstellende Person ein verständiges, durch die Sachlage gerechtfertigtes Interesse verfolgt. Es genügt, daß sachliche Gründe vorgetragen werden, die die Verfolgung unbefugter Zwecke oder bloße Neugier ausschließen. Ein berechtigtes Interesse hat zunächst jeder, der im Zusammenhang mit dem Grundstück ein eigenes Recht geltend macht, unabhängig davon, ob er auch als berechtigt eingetragen ist. Auch ein tatsächliches, z.B. wirtschaftliches Interesse kann ausreichen. Daher kann eine Mieterin in das Grundbuch des Vermieters, z.B. bei einem Mieterhöhungsverlangen wegen gestiegener Kapitalkosten, insbesondere auch in die Abteilung 3 des Grundbuchs Einsicht nehmen.

Auch Mitglieder von Wohnungseigentümergemeinschaften können grundsätzlich ein berechtigtes Interesse daran geltend machen, in das Grundbuch der übrigen Miteigentümer Einsicht zu nehmen. Dazu gehört auch das Recht, Abschriften hieraus zu erhalten. Die Rechtsprechung der Oberlandesgerichte betont dabei den Publizitätsgrundsatz des Grundbuches, der einen Geheimnisschutz ausschließt. Insbesondere die Mitglieder einer Miteigentümergemeinschaft seien z.B. durch das Hausgeld und die Reparaturkostenumlage in so vielfältiger Weise miteinander verbunden, daß die Information über den wirtschaftlichen Status anderer Miteigentümer nicht als Ausdruck bloßer Neugier abqualifiziert werden könne.

Das berechtigte Interesse muß gegenüber dem Amtsgericht weder glaubhaft gemacht noch bewiesen werden. Es genügt die Darlegung, d.h. ein überzeugender Vortrag der Gründe. Die Einsichtnahme erstreckt sich dabei nicht nur auf den Einblick in das Grundbuch selbst, sondern kann auch auf die Grundakte mit den darin enthaltenen Urkunden wie Kaufvertrag, Testament u.ä. ausgedehnt werden.

Ein derartig weitgehendes Einsichtsrecht ist jedoch nicht in jedem Fall gegeben. Das Recht reicht nur so weit, als ein berechtigtes Interesse dargetan ist. Das Einsichtsrecht kann daher auf wenige Abteilungen des Grundbuchs beschränkt sein. Die Beschränkung ist durch die Bediensteten des Grundbuchamtes zu gewährleisten.

### 31.14.2 Protokollierung

Leider sind meine Möglichkeiten, die Rechtmäßigkeit der Einsichtnahme ins Grundbuch zu überprüfen, sehr beschränkt, da keine Pflicht besteht, die Einsichtnahmen zu protokollieren. Bei der Vielzahl von Einsichtnahmen vermag sich die zuständige Rechtspflegerin bzw. der Rechtspfleger nicht zu erinnern, was die einzelne antragstellende Person bei der Einsichtnahme als Grund vorgetragen hat. Ich habe mich im Zusammenwirken mit den anderen Datenschutzbeauftragten darum bemüht, durch eine Novellierung der einschlägigen Gesetzesvorschriften insofern Abhilfe zu schaffen. Leider ist dies bisher nicht gelungen. Das Registerverfahrensbeschleunigungsgesetz vom 20. Dezember 1993 (BGBl. I S. 2182) hat weder das Einsichtsrecht neu geregelt noch eine Protokollierungspflicht aufgenommen. Lediglich in Berlin und Schleswig-Holstein sind entsprechende Landesregelungen getroffen worden. Ich werde mich, da die Initiative auf Bundesebene gescheitert ist, um eine niedersächsische Lösung bemühen.

## 31.15 Datenschutz bei Notaren

### 31.15.1 Rechtsgrundlagen

Weder die Bundesnotarordnung noch das Beurkundungsgesetz enthalten ausreichende klare Befugnisnormen für die Verarbeitung personenbezogener Daten durch Notare. Die von den Notaren für ihre tägliche Arbeit herangezogene Dienstordnung für Notare ist eine Verwaltungsanordnung, der es an Rechtsnormqualität fehlt und die nach dem Volkszählungsurteil des BVerfG für Eingriffe in das Recht auf informationelle Selbstbestimmung nicht ausreicht. Darüber hinaus wurde die dringend erforderliche Überarbeitung wegen anderer Aufgaben zurückgestellt. Gesetzliche Vorschriften, die das Handeln der Notare beim Umgang mit personenbezogenen Daten regeln, finden sich verstreut z.B. im Grunderwerbsteuergesetz (§§ 18, 20), dem Baugesetzbuch (§§ 24, 25, 195) oder dem Erbschaftsteuer- und Schenkungsteuergesetz (§ 34). Im übrigen kann die Datenverarbeitung weitgehend

nur auf der Grundlage von Einwilligungserklärungen, vergleichbar der anwaltlichen Prozeßvollmacht, erfolgen.

31.15.2 Notar-Anderkonto

Die Führung eines Notar-Anderkontos führte zu einer Beanstandung. Der den Vertragsparteien übergebene Ausdruck enthielt eine detaillierte Aufstellung über die Geldbewegungen bei der Zahlung des Kaufpreises (Auflistung der Eingänge und Ausgänge und Angabe der Einzahler und Empfänger der Geldbeträge), ohne daß das Einverständnis hierzu erteilt worden wäre. Eine Rechtsgrundlage ist nicht erkennbar. Der Notar sah sich trotz mehrfacher Aufforderung nicht zu einer Stellungnahme veranlaßt. Dies habe ich gem. § 23 Abs. 1 NDSG beanstandet. Aus der nach mehrmaliger Mahnung eingetroffenen Stellungnahme des Justizministeriums ergibt sich, daß der betroffene Notar zwar nach wie vor die Offenlegung der Darlehnsablösungen für richtig hält, aber wohl in Zukunft darauf verzichten wird. Eine Begründung, warum er auf unsere Schreiben entgegen seiner Pflicht aus § 22 Abs. 4 Nr. 1 NDSG keine Auskunft erteilt hat, gab er nicht.

31.15.3 Geburtsdatum im Beglaubigungsvermerk

Im Rahmen meiner Prüfung der im dritten Absatz unter XI 31.17 geschilderten Angelegenheit sehe ich kein Erfordernis für die Aufnahme des Geburtsdatums in einem Beglaubigungsvermerk. Gleichwohl vermochte ich die Verfahrensweise des Notars datenschutzrechtlich nicht zu beanstanden. Nach den Kommentaren zum Beurkundungsgesetz hat der Notar für die Prüfung der Personenidentität einen Ermessensspielraum. Einen offensichtlichen Ermessensfehler konnte ich jedenfalls nicht feststellen. Ich habe den Fall zum Anlaß genommen, im Gespräch mit dem Niedersächsischen Justizministerium auf eine Präzisierung des § 10 Beurkundungsgesetz hinzuwirken.Der Fall zeigt, daß die Weitergabe vollständiger Beglaubigungsvermerke - bei fehlender normenklarer Rechtsgrundlage - problematisch ist. Aus datenschutzrechtlicher Sicht sollte der Umfang der zu erhebenden personenbezogenen Daten auf das zur Aufgabenerfüllung ausschließlich Erforderliche, d.h. Unerläßliche beschränkt werden.

31.15.4 Personalausweis in der Handakte

Ein Notar nahm im Zuge der Beurkundung von Verträgen Fotokopien der vorgelegten Personalausweise zu seinen Handakten. Dies begründete er mit gesetzlichen Vorschriften. Bei der Fertigung von Fotokopien der Ausweise (Datenerhebung) und ihrer Aufbewahrung in der Handakte (Datenspeicherung) handelt es sich um Eingriffe in das Recht auf informationelle Selbstbestimmung, für die bei der hier fehlenden Einwilligung eine Rechtsgrundlage erforderlich ist. Um sich Gewißheit über die Person gemäß § 10 Abs. 2 Beurkundungsgesetz zu verschaffen, reicht die Vorlage der Ausweise aus. Auch dieser Notar weigerte sich, seinen Pflichten aus § 22 NDSG nachzu-

kommen. Der Präsident des zuständigen Landgerichts, den ich um Unterstützung gebeten hatte, teilte mir mit, daß der Notar auf seine Rechtsanwaltszulassung verzichtet habe und damit zugleich aus seinem Notaramt ausgeschieden sei. Die Sache hat sich damit erledigt.

31.16 Presse- und Öffentlichkeitsarbeit der Justiz

Das Niedersächsische Justizministerium hat nunmehr nach meinem langjährigen Drängen (zuletzt XI 31.18) eine neue Presse-AV erlassen. Es ist zu begrüßen, daß dort Regelungen aufgenommen wurden, die die angemesse Berücksichtigung des allgemeinen Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung gegenüber dem Auskunftsanspruch der Medien sicherstellen sollen. So wird die Auskunft über Namen von beteiligten Personen, z.B. Beschuldigten, Opfern, Zeugen grundsätzlich von deren Zustimmung abhängig gemacht.

Meiner Anregung, schriftliche Auskunftserteilungen an die Presse ebenfalls den jeweils Betroffenen zur Kenntnis zu übersenden und diese über geplante Pressekonferenzen zu informieren, wurde gefolgt. Leider fehlt der von mir erbetene Hinweis auf ganz besondere Zurückhaltung im Falle von Jugendlichen, wie er in entsprechenden Regelungen im Polizeibereich (Nds. MBl. 1993 S. 204 f.) enthalten ist.

In Bezug auf Auskünfte der Staatsanwaltschaften hatte ich zu bedenken gegeben, ob bis zur Entscheidung über die Erhebung der öffentlichen Klage nicht eine Auskunftssperre in die AV aufgenommen werden sollte. Da jede, auch unberechtigte, Strafanzeige aufgenommen werden muß und so bei einer Pressenachfrage zur Bestätigung eines Ermittlungsverfahrens führt, halte ich eine solche Sperre für erwägenswert. Auch dies hat leider keinen Niederschlag in der AV gefunden.

31.17 Aufbewahrungsbestimmungen für das Schriftgut der ordentlichen Gerichtsbarkeit, Staatsanwaltschaften und Justizvollzugsbehörden

Die Aufbewahrung von Schriftgut der ordentlichen Gerichtsbarkeit sowie der öffentlich-rechtlichen Gerichtsbarkeiten, der Staatsanwaltschaften und der Justizvollzugsbehörden ist derzeit in einer Verwaltungsvorschrift geregelt (AV vom 28. August 1972, Nds. Rpfl. S. 207, zuletzt geändert durch AV vom 30. November 1993 - Nds. Rpfl. S. 348).

Die Aufbewahrung der Akten aus den oben genannten Bereichen greift tief in das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger ein, deren persönliche Daten darin gespeichert sind. Besondere Bedeutung gewinnen diese Regelungen vor dem Hintergrund, daß zunehmend auch im Bereich der Justiz automatisierte Datenverarbeitungssysteme eingeführt werden und regelmäßig für die Speicherungsdauer von Informationen in diesen Systemen auf die genannten Aufbewahrungsbestimmungen verwiesen wird. Ich halte es für erforderlich, solche Bestimmungen auf eine ge-

setzliche Grundlage zu stellen, die auf die unterschiedlichen Verfahren und die damit verbundenen Interessen sowohl hinsichtlich der Anknüpfungspunkte, als auch der Aufbewahrungs- bzw. Speicherungszeiträume eingeht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit dieser Problematik befaßt. Ein Beschluß hierzu ist in der ersten Sitzung des Jahres 1995 zu erwarten.

## 32. Strafvollzug

### 32.1 Strafvollzugsgesetz/Untersuchungshaftvollzugsgesetz

Das Strafvollzugsgesetz (StVollzG) ist wegen fehlender datenschutzrechtlicher Bestimmungen seit vielen Jahren Gegenstand der Kritik der Datenschutzbeauftragten des Bundes und der Länder. Unter XI 32.1 habe ich eingehend auf die datenschutzrechtlichen Defizite des Strafvollzuges bei der Erhebung, Speicherung, Übermittlung, Löschung personenbezogener Daten hingewiesen. Entsprechende Kritik hatte ich auch in bezug auf fehlende Datenschutzvorschriften im Untersuchungshaftvollzug erhoben, der sich lediglich auf die Verwaltungsvorschrift "Untersuchungshaftvollzugsordnung" (UVollzO) stützt. Weder im Hinblick auf das Strafvollzugsgesetz (Entwurf eines 4. Gesetzes zur Änderung des StVollzG von 1991) noch zum Arbeitsentwurf eines Untersuchungshaftvollzugsgesetzes (Stand: 24. Februar 1986) hat es Fortschritte gegeben. Die Berufung auf den Übergangsbonus ist, elf Jahre nach dem Volkszählungsurteil, aus rechtsstaatlichen Gründen immer weniger hinnehmbar.

### 32.2 Kontrollen

Im Berichtszeitraum habe ich das Postwesen in einer Justizvollzugsanstalt (JVA) für Langzeitinhaftierte geprüft. Das Verfassen und Empfangen von Post ist, insbesondere für Strafgefangene, die wie in der geprüften JVA zehn und mehr Jahre zu verbüßen haben, von eminenter Bedeutung. Bei der eingeschränkten Zahl von Besuchen ist der schriftliche Austausch mit anderen oft der einzige Weg nach draußen, der den Gefangenen jederzeit offensteht. Angesichts nur geringer anderer Beschäftigungsmöglichkeiten wird hiervon auch rege Gebrauch gemacht. Besondere Bedeutung gewinnt der Schriftwechsel gegen Ende der Haftzeit, wenn die Entscheidung über Haftlockerungen und vorzeitige Entlassung ansteht. Dann ist das Vorhandensein sozialer Beziehungen nach "draußen" u.U. entscheidend. Ohne ständigen Kontakt, auch und gerade durch die Post, sind diese bei Langzeitinhaftierten kaum aufrechtzuerhalten.

Gem. § 29 Abs. 3 StVollzG darf die Post der Strafgefangenen, mit Ausnahme einiger im Gesetz genannter Institutionen, aus Gründen der Behandlung oder der Sicherheit und Ordnung der Anstalt überwacht werden. Generell

gilt nach den internen Verwaltungsvorschriften eine Sichtkontrolle. Die Post wird optisch auf die Beifügung verbotenener Gegenstände hin untersucht. Dies soll in Gegenwart des Gefangenen geschehen. Die Inhaltskontrolle der Post ist grundsätzlich von einer entsprechenden Anordnung der Anstaltsleitung abhängig.

Bereits im Vorfeld der Prüfung wurde ich durch das Justizministerium darüber informiert, daß für die von mir zur Prüfung vorgesehene JVA eine generelle Anordnung der inhaltlichen Briefkontrolle Geltung habe. Dies sei aufgrund der besonderen Gefahrenlage der Anstalt erforderlich und rechtlich zulässig. Diese Ansicht halte ich für äußerst problematisch. Zwar findet sie sich in der Kommentarliteratur und der Rechtsprechung. Nach Gründen forscht man indessen vergebens. Es wird lediglich auf eine nur in einem nicht amtlichen Leitsatz veröffentlichte Entscheidung des BVerfG verwiesen. Hat man die Entscheidung nach Anforderung vor sich liegen, stellt man fest, daß es sich um eine zwei Absätze umfassende Einzelfallentscheidung des Zulassungsausschusses (vom 2. Juni 1981, Az. 2 BvR 1102/80) handelt. Ausführungen zur Frage, ob eine generelle Anordnung zur Inhaltskontrolle § 29 Abs. 3 StVollzG entspricht oder ob nicht bei jedem Gefangenen die Gefahr für die Behandlung oder die Sicherheit und Ordnung der Anstalt geprüft und bejaht werden muß, fehlen. Das Gericht hatte offensichtlich gar keine Veranlassung, sich mit diesem Problem auseinanderzusetzen. Dies mag jedoch an dieser Stelle offenbleiben.

Unzweifelhaft bedarf jedoch die Inhaltskontrolle durch den Vollzugsbediensteten und damit der dauernde, verhaltensunabhängige und daher von dem Strafgefangenen nicht zu beeinflussende Eingriff in das Briefgeheimnis einer Anordnung durch die Anstaltsleitung. Meine Prüfung hat ergeben, daß die Post aller Inhaftierten ohne eine solche Anordnung gelesen wird. Dies habe ich beanstandet. Nach der Stellungnahme des Niedersächsischen Justizministeriums soll sie in Kürze zusammen mit einer umfassenden Regelung des Postwesens ergehen.

Bei meiner Prüfung habe ich festgestellt, daß eine solche Verfügung bitter nötig ist. Bis auf wenige Weisungen in Einzelbereichen waren grundlegende Verfahrensweisen der Entscheidung der jeweiligen Bediensteten überlassen, die auch für die Weitergabe an Vertreter und/oder Nachfolger Sorge zu tragen hatten. Weiter wurden die Strafgefangenen nicht über ihre Rechte belehrt, z.B. hinsichtlich des Personenkreises, mit denen der Schriftwechsel ohne Inhaltskontrolle geführt werden kann.

Ebenfalls beanstandet wurde von mir die Aufnahme des Schriftverkehrs der Strafgefangenen in die Briefkartei. Derartige Karteien bestehen in fast allen Vollzugsanstalten. Eine Rechtsgrundlage für diese Datensammlung gibt es nicht. Auf den sog. "Übergangsbonus" könnte sie nur gestützt werden, wenn dies für die Fortführung des Strafvollzuges zwingend erforderlich wäre. Die Notwendigkeit wird teilweise mit der Dokumentation der sozialen Beziehungen des Strafgefangenen zur Beurteilung von Vollzugslockerungen, teilweise aber auch - so in der von mir geprüften Anstalt - mit der Dokumentation vom Ein- und Ausgang behördlicher Schreiben begründet. Auf keinen Fall

akzeptiert werden kann die vorgefundene Praxis, daß es offensichtlich der Einschätzung der jeweiligen Bediensteten überlassen bleibt, welche Eintragung erforderlich ist oder nicht. So fanden sich Eintragungen über den Schriftwechsel mit Versicherungen, Pfarrern, Abgeordneten und der Presse. Ich gehe davon aus, daß auch der Bereich der Briefkartei in die Anweisung der Anstaltsleitung zum Postwesen einbezogen und den Vorgaben des Übergangsbonus Rechnung tragen wird. Ob die angekündigte Anordnung den datenschutzrechtlichen Anforderungen genügt, bleibt im nächsten Tätigkeitsbericht nachzutragen.

## 32.3 Gefangenenpersonalakte

### 32.3.1 Einsichtnahme

Ähnlich wie bei der Polizei die Kriminalakten enthalten auch Gefangenenpersonalakten eine Vielzahl von personenbezogenen Daten. Eine (indirekte) Rechtsgrundlage findet die Gefangenenpersonalakte in den §§ 5 bis 7 St-VollzG, konkretisiert in Nrn. 58, 59 und 62 der Vollzugsgeschäftsordnung. Die Gefangenenpersonalakte enthält neben persönlichen Daten der Gefangenen auch das vollständige Urteil, das ebenfalls Daten über eine Vielzahl betroffener Dritter enthalten kann (vgl. 32.3.3). Die Akten werden nach Auskunft des Niedersächsischen Justizministeriums in Metallschränken verschlossen in der jeweiligen Vollzugsgeschäftsstelle aufbewahrt. Generelle Regelungen über Einsichtsrechte durch Bedienstete bestehen nicht.

Das Justizministerium vertritt dazu die Auffassung, daß viele Bedienstete Kenntnis vom Inhalt der Personalakten benötigten. Die verschiedenen Berufsgruppen müßten zusammenwirken, damit die Strafgefangenen das Vollzugsziel erreichen. Insbesondere die Bediensteten des allgemeinen Vollzugsdienstes benötigten das Hintergrundwissen über die Strafgefangenen, für die sie zuständig seien. Diese undifferenzierte Auffassung, die in dem Satz "Alle müssen alles wissen" zusammengefaßt werden könnte, ist datenschutzrechtlich nicht akzeptabel. Für die Einsichtnahme existieren weder eine gesetzliche Grundlage noch die Einwilligung. Unter der Geltung des mittlerweile sehr problematisch gewordenen Übergangsbonus ist ein strenger Erforderlichkeitsgrundsatz für die Datenübermittlung, die stets aus einer Einsichtnahme folgt, zu beachten. Sie ist daher auf die Mitarbeiterinnen und Mitarbeiter zu beschränken, die unmittelbar mit dem Strafgefangenen befaßt sind. Dies ist durch geeignete organisatorische Maßnahmen sicherzustellen.

### 32.3.2 Aufbewahrung von psychiatrischen und psychologischen Gutachten über Gefangene

Hinsichtlich der Einsichtnahme in Gefangenenpersonalakten, die psychiatrische Gutachten sowie die dazu erstellten psychologischen und neurologi-

schen Zusatzgutachten (vgl. XI 32.3) enthalten, ist es mir gelungen, auf organisatorische Regelungen hinzuwirken. Das Justizministerium hat verfügt, daß künftig Zugriffe von Vollzugsbediensteten auf Gefangenenpersonalakten, die psychologische Gutachten enthalten, zu dokumentieren sind, wenn die Bediensteten zum Zeitpunkt der Einsichtnahme weder mit dem Gefangenen selbst noch mit den - diesen Gefangenen betreffenden - Sicherheitsfragen befaßt sind. Hierbei sind Datum und Grund der Einsichtnahme sowie der Name des Bediensteten in einem gesonderten, der Gefangenenpersonalakte beizufügenden Vermerk festzuhalten.

### 32.3.3 Opferschutz im Knast, oder: wie bekomme ich das Urteil in die Tüte?

Mein Versuch, Einsichtnahmen in die bei der Akte befindlichen Strafurteile zu beschränken, hatte vorerst noch keinen Erfolg. Strafurteile enthalten viele personenbezogene Angaben, die nicht die Strafgefangenen, sondern Opfer und Zeugen betreffen. Zu deren Schutz sollte die Einsichtnahme in diese Dokumente nur dann erfolgen, wenn es wirklich für den Vollzug erforderlich ist. Insbesondere in Strafverfahren wegen Sexualdelikten müssen bei der Schilderung des Tatherganges intime Details in das Urteil aufgenommen werden. Die Rechtsordnung verlangt Opfern und Zeugen das Bekanntwerden derartiger Umstände ab. Um so wichtiger ist es dann aber, die Einsichtnahme auf das unumgänglich notwendige Maß zu beschränken. Deshalb habe ich vorgeschlagen, Urteile verschlossen in einem Umschlag zur Akte zu nehmen und jede Einsichtnahme durch einen Vermerk dokumentieren zu lassen, sobald die Aufnahmephase in der JVA, während der häufiger Einsicht in das Urteil genommen werden muß, um sich ein Bild von dem Strafgefangenen zu machen, abgeschlossen ist. Zu meinem Bedauern konnte das Justizministerium diesen Vorschlag nicht umsetzen, sondern besteht auf einem bundesweiten Abstimmungsverfahren. Regelungen, von welcher Rechtsqualität auch immer, die dem vorgeschlagenen Verfahren entgegenstehen, gibt es nicht. Derartige Inflexibilität muß befremden.

## 32.4 Falscher Registerauszug - falscher Vollzug

Die Frage, ob Gefangene ihre Haft im Regelvollzug oder im weniger belastenden Erstvollzug verbüßen, ist, wie die Begriffe schon zeigen, danach zu beurteilen, ob Vorverurteilungen bestehen. Diese Entscheidung wird anhand der Auskunft aus dem Bundeszentralregister getroffen. Für die Eintragungen in diesem Register gelten Tilgungsfristen, nach deren Ablauf Strafverfahren nicht mehr in die Auskunft aufgenommen werden dürfen.

Im Fall eines Petenten war dabei jedoch nicht beachtet worden, daß die Eintragungen zwischen Anklageerhebung - zu diesem Zeitpunkt war der Auszug angefordert worden - und Urteilsverkündung tilgungsreif geworden waren. Der nicht mehr zutreffende Auszug führte zur Aufnahme des Petenten in den Regelvollzug, später wurde dies aufgrund seiner Initiative korrigiert. Nicht korrigiert wurde jedoch die Speicherung der Vorverurteilungen. Im Vollzugsplan wurde unter der Rubrik "Vorstrafen" aufgenommen: "keine

(da verjährt)". Ich habe die Löschung bzw. Unkenntlichmachung dieses Zusatzes veranlaßt.

## 32.5 Gefangenenpost und Schriftverkehr

### 32.5.1 Briefkontrolle bei Untersuchungshaft

Bei der Briefkontrolle handelt es sich um eine Datenerhebung, die nur aufgrund eines Gesetzes zulässig ist. In der Untersuchungshaft wird sie allgemein auf § 119 Abs. 3 StPO gestützt. Danach dürfen Verhafteten jedoch nur solche Beschränkungen auferlegt werden, die der Zweck der Untersuchungshaft oder die Ordnung der Vollzugsanstalt erfordert. Diese Voraussetzungen sind für eine Kontrolle von Schreiben von Untersuchungsgefangenen an mich nicht gegeben. Durch die Nennung meiner Behörde als Adressat kann das Schreiben weder dem Zweck der Untersuchungshaft noch der Ordnung in der Vollzugsanstalt zuwiderlaufen. Aus diesen Gründen sind auch durch Nr. 30 Abs. 2 der Untersuchungshaftvollzugsordnung (UVollzO) Schreiben an in dieser Hinsicht vergleichbare Institutionen von der Überwachung ausdrücklich ausgenommen worden. Es stellt, trotz entgegenstehender Auffassung des Niedersächsischen Justizministeriums, keinen Eingriff in die richterliche Unabhängigkeit dar, wenn ich mit diesen Einrichtungen gleichgestellt werde. Das vorstehend aufgezeigte Problem wurde von einem Untersuchungsgefangenen an mich herangetragen, der sich dagegen wandte, daß seine Schreiben an mich der Briefkontrolle durch den zuständigen Richter unterworfen werden sollten.

Im Regelvollzug stellt sich die aufgezeigte Problematik nicht, weil Schreiben der Gefangenen an Behörden der Länder, und damit auch an mich, nach der Allgemeinen Verfügung (AV) des Justizministeriums vom 30. Mai 1994 (Nds. Rechtspflege S. 179) nicht der Überwachung unterliegen. Dies ist nicht zwingend, weil nach § 29 Abs. 3 StVollzG grundsätzlich auch die Überwachung des Schriftverkehrs mit Behörden, die nicht ausdrücklich in Abs. 2 genannt sind, gestattet ist. Nach § 119 Abs. 3 StPO ist dagegen eine solche Beschränkung unzulässig, wenn sie nicht dem Zweck der Untersuchungshaft oder der Ordnung in der Vollzugsanstalt dient.

Hinsichtlich meiner Schreiben an Untersuchungsgefangene halte ich daher dieselbe Handhabung für geboten, wie sie mit dem Justizministerium abgestimmt wurde (vgl. VIII 32.1). Diese Verfahrensweise hat sich in der Praxis bewährt und schließt es aus, daß der Schriftwechsel dem Zweck der Untersuchungshaft oder der Ordnung in der Vollzugsanstalt zuwiderläuft. Meine Bemühungen, die hier offenen Fragen mit dem Justizministerium zu klären, dauern an.

32.5.2 Telefax

Es erreichten mich Beschwerden von Gefangenen darüber, daß Telefaxnachrichten diesen lediglich als Kopien, nicht aber im Original und überdies verzögert und offen ausgehändigt wurden. Die Kopie wurde gemäß der Stellungnahme der Anstalt wegen Unlesbarkeit gefertigt und das unleserliche Original vernichtet. Die Justizvollzugsanstalt wird Telefaxschreiben für Gefangene künftig ausnahmslos im Original aushändigen. Da der offene Eingang telefax-typisch ist, kann Abhilfe insoweit nur dadurch geschaffen werden, daß der Empfänger des Telefaxes den Absender bittet, künftig von dieser Übersendungsform abzusehen.

32.5.3 Offene Zusendung dienstlicher Schreiben

Beschwerden von Gefangenen richteten sich gegen die offene Aushändigung behördlicher Schreiben.

Bei der Versendung dienstlicher Schreiben an Untersuchungs- und Strafgefangene, die von einer Justizbehörde durch das Verteilerfach einer JVA übermittelt werden, ist Vertraulichkeit zu wahren (Nr. 2.3 i.V.m. Nrn. 2.1 und 2.2 der AV des Justizministeriums vom 9. Juli 1992 - Vollziehung von Schriftstücken bei Justizbehörden -, Nds. Rechtspflege S. 190). Es sind geschlossene Umschläge zu verwenden, wenn bei Versendung durch die Post ebenfalls ein geschlossener Umschlag verwendet werden würde und dies nach dem Inhalt des Schreibens zur Wahrung der Vertraulichkeit erforderlich ist. Wie eine Petition zeigte, führt der Begriff "Vertraulichkeit" zu unterschiedlichen Interpretationen. Auf die Erfüllung dieses Kriteriums darf es jedoch nicht ankommen. Jede offene Versendung ist eine Datenübermittlung, für die es im Vollzugsbereich keine Rechtsgrundlage gibt.

Das Niedersächsische Justizministerium hält es nunmehr für geboten, eine Zustellung bzw. Aushändigung dienstlicher Schreiben im geschlossenen Umschlag vorzunehmen und hat deshalb das Niedersächsische Justizvollzugsamt gebeten, die Justizvollzugsanstalten anzuweisen, künftig entsprechend zu verfahren. Der Präsident des Landgerichts Hannover hat wegen der offensichtlichen Unklarheit darüber, ob ein geschlossener Umschlag zur Wahrung der Vertraulichkeit erforderlich ist, mit Hausverfügung vom 10. November 1992 angeordnet, daß Schriftstücke an Gefangene in allen Fällen in geschlossenen Umschlägen versandt werden.

32.5.4 Kontrolle post mortem - oder: wie werde ich die Post für meinen toten Bruder los?

Ein Gefangener rügte, daß er wiederholt Post für seinen vor mehreren Jahren aus der JVA entlassenen - mittlerweile verstorbenen - Bruder erhalte, die der Postkontrolle unterzogen worden sei. Er habe monatelang auf diesen Irrtum hingewiesen, gleichwohl habe sich an dem Verfahren nichts geändert.

Die von mir um Stellungnahme gebetene Anstalt teilte mit, der für die Postkontrolle zuständige Mitarbeiter könne sich an entsprechende Briefe nicht erinnern. Die Öffnung könne nur versehentlich erfolgt sein. Bevor sich der Petent an uns wende, solle er sich besser an den Bediensteten der JVA wenden. Angesichts des Umstandes, daß der Strafgefangene sich vor der Petition sowohl mit einer Dienstaufsichtsbeschwerde als auch - als diese erfolglos blieb - mit einer Strafanzeige gegen die weitere Postkontrolle der Schreiben an seinen Bruder gewandt hatte, war dieser Hinweis wenig sachdienlich.

Während der Aufklärung der Petition wurde dem Petenten erneut ein - geöffneter - Brief an seinen Bruder ausgehändigt. Die mir daraufhin zugegangene Stellungnahme der JVA lag noch weiter neben der Sache: Die Anstalt verwies auf § 2 StVollzG, nach dem die Gefangenen befähigt werden sollen, ein Leben in sozialer Verantwortung zu führen. Dazu gehöre auch die Nachlaßregelung für einen verstorbenen Bruder und die Benachrichtigung anderer Stellen und Privatpersonen über dessen Tod. Allerdings verabsäumte die JVA die Prüfung, ob der Petent zu derartigen Mitteilungen überhaupt befugt war. Weiter mußte ich sie darauf hinweisen, daß das Vollzugsziel des § 2 StVollzG die Anstalt nicht von ihrer Pflicht entbinden kann, für einen ordentlichen Postempfang Sorge zu tragen.

Nicht nur Befremden, sondern mein entschiedenes Dazwischentreten löste die durch die JVA angekündigte Konsequenz für den Petenten aus, er werde in Zukunft keine Post mehr erhalten, in deren Anschrift er nicht mit vollem Vornamen genannt sei. Hier drängte sich der Eindruck auf, der Petent solle entgegen § 19 Abs. 1 Satz 2 NDSG für meine Einschaltung bestraft werden. Ich habe darauf bestanden, daß an den Petenten gerichtete Post an ihn auszuhändigen ist, unabhängig davon, ob z.B. der Vorname ausgeschrieben ist oder nicht. Die rechtswidrig der Postkontrolle unterzogenen Briefe an den Bruder waren eindeutig adressiert und nicht an den Petenten gerichtet.

Das Niedersächsische Justizministerium hat mir abschließend mitgeteilt, der Briefstellenbeamte habe sich in seiner Stellungnahme für sein Versehen entschuldigt. Die Anregung, diese Entschuldigung in geeigneter Form auch gegenüber dem Gefangenen auszusprechen, unterstütze ich. Die von der JVA beabsichtigte Konsequenz, alle Briefsendungen an den Gefangenen ohne bzw. mit unklarer Vornamensnennung künftig mit dem Vermerk "Empfänger unbekannt" zurückzusenden, hält auch das Justizministerium nicht für sachgerecht. Seine weitere Anregung, Post für den Einsender vor Ausgabe auf der Station in Hinblick auf die Identität des Adressaten noch einmal zu überprüfen, ist aus datenschutzrechtlicher Sicht geboten. Der Fall zeigt einmal mehr, daß im sensiblen Bereich der Postkontrolle besondere Sorgfalt zu üben erforderlich ist (vgl. 32.2).

32.6 Dauerbrenner "Auskünfte von Justizvollzugsanstalten über Gefangene an private Dritte"

Das in XI 32.4 dargestellte Problem der Erteilung von Auskünften an Privatpersonen durch Justizvollzugsanstalten ist zum datenschutzrechtlichen Dauerbrenner geworden. Ich bin nach wie vor der Auffassung, daß für melderechtliche Auskünfte auch über die Anschrift Strafgefangener allein die Einwohnermeldeämter zuständig sind (§§ 2, 33 Abs. 1 NMG).

Eine Zuständigkeit von Justizvollzugsanstalten ergibt sich auch dann nicht, wenn gemäß § 17 Abs. 3 NMG eine Meldepflicht nicht besteht, weil der Strafgefangene im Geltungsbereich des Melderechtsrahmengesetzes für eine andere Wohnung gemeldet ist. Das Niedersächsische Justizministerium hingegen hält - in Abstimmung mit dem Niedersächsischen Innenministerium - eine Auskunftserteilung auf der Grundlage von § 13 Abs. 1 Nr. 2 NDSG für zulässig.

Bemühungen des Justizministeriums, anläßlich der Verabschiedung des Gesetzes zur Änderung des Niedersächsischen Meldegesetzes vom 10. Januar 1994 (Nds. GVBl. S. 1) in § 17 Abs. 3 NMG eine Regelung zu schaffen, nach der die Meldeämter zur Beantwortung der Anfragen zu Anschriften über sämtliche Gefangene, deren Aufenthalt die Dauer von zwei Monaten überschreitet, zuständig wären, haben nicht zum Erfolg geführt.

32.7 Kontoauszüge für Strafgefangene

Das unter XI 32.5 geschilderte Verfahren bei der Ausgabe von Kontoauszügen führt weiterhin zu einer nicht erforderlichen Übermittlung personenbezogener Daten, wie z.B. Kontonummer, Geburtsdatum, Haftart des Gefangenen an die aushändigenden Bediensteten. Wenngleich das Niedersächsische Justizministerium argumentiert, diesen seien die Daten der Gefangenen ohnehin bekannt, werde ich mich weiter dafür einsetzen, daß durch Programmsteuerung im ADV-System "BASIS-Buchungs- und Abrechnungssystem im Strafvollzug" künftig die Daten so ausgedruckt werden, daß nach dem Knicken und Klammern der Kontoauszüge nur noch der Name des Gefangenen sichtbar bleibt.

32.8 "Statistischer Erhebungsbogen" der Einweisungsabteilung Hannover

Der bereits unter II 5.8.4 erwähnte "Statistische Erhebungsbogen" befriedigt datenschutzrechtlich weiterhin nicht. Der Vordruck enthält zwar nunmehr die Erklärung "Ich fülle den Bogen mit meiner Zustimmung aus". Ich akzeptiere diesen Zusatz jedoch nicht als ausreichende Einwilligung. Die erforderliche Freiwilligkeit dieser Erklärung darf in Zweifel gezogen werden. Gemäß § 4 Abs. 2 Satz 3 NDSG sind die Betroffenen in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung auch über die Empfänger der Daten aufzuklären. Sie sind unter Darlegung der Rechtsfolgen darauf hin-

zuweisen, daß sie die Einwilligung verweigern oder mit Wirkung für die Zukunft widerrufen können. Hieran fehlt es. § 6 Abs. 1 und 2 StVollzG stellt keine normenklare gesetzliche Grundlage zur Erhebung statistischer Daten dar. § 3 Niedersächsisches Statistikgesetz fordert jedoch selbst für statistische Erhebungen ohne Auskunftspflicht eine Anordnung durch Rechtsvorschriften, in der Erhebungsmerkmale, Hilfsmerkmale, die Art der Erhebung, der Berichtszeitraum, der Berichtszeitpunkt, die zeitlichen Abstände wiederkehrender Erhebungen (Periodizität) und der Kreis der zu Befragenden zu bestimmen sind.

Die von mir angeschriebene Anstalt teilte meine Bedenken und hat mir mitgeteilt, sie werde auf die weitere Verwendung des Erhebungsbogens verzichten und diesen nicht mehr an die Gefangenen ausgeben.

### 32.9 Papierschnipsel mit personenbezogenen Daten neben der Mülltonne

Die Beschwerde eines Gefangenen, dem ein Mitgefangener Papierschnipsel eines ihn betreffenden Schreibens des Leiters der JVA an die Strafvollstreckungskammer übergeben hatte, veranlaßt mich, nochmals auf den sorgfältigen Umgang mit Entwürfen - um einen solchen handelte es sich bei dem Schriftstück - hinzuweisen. Die Schnipsel waren in der Abfallzelle der Untersuchungshaft neben der Mülltonne gefunden worden. Der Entwurf des Schreibens war offensichtlich für die Vernichtung bestimmt. Dazu ist es offenbar nicht gekommen. Seitens der JVA ließ sich nicht mehr aufklären, wer den in Papierstücke zerrissenen Entwurf in den Papierkorb geworfen hatte. In der Regel würden, so erklärte die Anstalt, die Bediensteten streng darauf achten, daß für Papiere mit personenbezogenen Daten von Gefangenen der Aktenvernichter genutzt wird. Eine weitere Aufklärung war nicht möglich, weil der Betroffene nicht bereit war, den Namen des Finders zu nennen.

So war nicht überprüfbar, ob die personenbezogenen Daten wirklich von einem Dritten zur Kenntnis genommen worden waren. Aus diesem Grunde habe ich gemäß § 23 Abs. 3 NDSG von einer förmlichen Beanstandung abgesehen.

## 33. Öffentlich-rechtliche Religionsgesellschaften: Neues Datenschutzrecht für die Kirchen

Der Datenschutz steht nun auch bei den großen Kirchen auf festeren Füßen. Im Berichtszeitraum haben die Evangelischen Landeskirchen und die Römisch-Katholische Kirche ihre Datenschutzvorschriften grundlegend überarbeitet. Für die Evangelische Kirche in Deutschland (EKD) hat deren Synode das Kirchengesetz über den Datenschutz der Evangelischen Kirchen in Deutschland (DSG-EKD) vom 12. November 1993 beschlossen, das am 1. Januar 1994 in Kraft getreten ist. Die einzelnen Gliedkirchen der EKD

haben dieses Gesetz übernommen; es gilt somit sowohl für die niedersächsische Evangelisch-Lutherische Kirche als auch für die Evangelisch-Reformierte Kirche. Für die Römisch-Katholische Kirche haben die Bischöfe von Hildesheim und Osnabrück für ihre Bistümer Anordnungen über den kirchlichen Datenschutz (KDO) erlassen, die ebenfalls zum 1. Januar 1994 in Kraft getreten sind. Damit verfügen die christlichen Kirchen über ein zeitgemäßes Datenschutzrecht, das sich insbesondere am Bundesdatenschutzgesetz orientiert.

Die neuen Rechtsvorschriften beantworten auch die Frage, wie die Datenverarbeitung von kirchlichen Einrichtungen zu beurteilen ist, die in privater Rechtsform betrieben werden (wie etwa das Diakonische Werk oder der Deutsche Caritasverband). Zwar ist von kirchlicher Seite hierzu schon in der Vergangenheit die Auffassung vertreten worden, auch diese Einrichtungen unterfielen dem kirchlichen Recht, weil auch ihre Tätigkeit zum Kernbereich kirchlichen Wirkens zu rechnen sei. Dem wird entgegengehalten, daß für solche Einrichtungen allerdings - ebenso wie für andere private Stellen - die Vorschriften des dritten Abschnitts des Bundesdatenschutzgesetzes gelten. Sowohl das DSG-EKD als auch die KDO erstrecken ihren Anwendungsbereich nunmehr ausdrücklich auf diese Einrichtungen.

Mit den kirchlichen Datenschutzbeauftragten bestand auch im Berichtszeitraum ein offener Gedankenaustausch.

## 34. Drei Jahre Aufsichtsbehörde - Datenschutzkontrolle bei Privaten

### 34.1 Kontrolle aus einer Hand

Als Landesbeauftragter für den Datenschutz bin ich im Lande Niedersachsen seit dem 1. Januar 1992 Aufsichtsbehörde für den Datenschutz bei nicht-öffentlichen Stellen nach § 38 BDSG. Damit wurde die Kontrolltätigkeit gegenüber Privaten in einer Stelle zentralisiert, die zugleich als Kontrollinstanz für den öffentlichen Bereich tätig ist (XI 34.1). Diese Aufgabenübertragung ist verfassungsrechtlich in Art. 62 Abs. 4 Satz 2 der neuen Nds. Verfassung vom 19.5.1993 sowie einfachgesetzlich in § 22 Abs. 6 NDSG abgesichert. Eine ähnliche Konstellation besteht außer in Niedersachen nur noch in Bremen und Hamburg. Im Saarland und schon früher in Schleswig-Holstein entzog man den dortigen Datenschutzbeauftragten die Zuständigkeit für den privaten Bereich, nachdem bei Novellierung des jeweiligen Datenschutzrechts deren Dienststellen organisatorisch dem Landtag zugeordnet worden sind.

Nach nahezu drei Jahren Doppelzuständigkeit kann in Niedersachsen eine fast durchgängig positive Bilanz gezogen werden. Es war schon vor dieser Organisationsänderung in der Öffentlichkeit schwer vermittelbar, weshalb ich z.B. für die Medizinische Hochschule Hannover zuständig sein soll, nicht aber für die private Spezialklinik, die im Kern dieselbe Arbeit verrich-

tet. Daher gingen auch schon vor 1992 bei mir ebenso wie bei den Dienststellen aller öffentlichen Datenschutzbeauftragten Eingaben aus dem privaten Bereich ein. Nunmehr werden Fälle einheitlich bearbeitet, wobei die Erfahrungen aus dem nicht-öffentlichen und dem öffentlichen Bereich für den jeweils anderen Sektor nutzbar gemacht werden können. Dies gilt für materiell-rechtliche, insbesondere aber für technisch-organisatorische Fragen, wo das Anlegen eines einheitlichen Maßstabes sowie umfassende EDV-Kenntnisse erforderlich sind. In meiner Dienststelle ist dieselbe Mitarbeiterin bzw. derselbe Mitarbeiter oft für den privaten wie den öffentlichen Datenschutz zuständig. Dies erlaubte durch Schwerpunktsetzung eine spürbare Verstärkung der Kontrolltätigkeit im privaten Bereich.

Die landesweite Zentralisierung hat einen weiteren positiven Effekt: Datenverarbeiter orientieren sich weder an Landes-, geschweige denn an Bezirksgrenzen. Die Datenverarbeitung der Filialen und Außenstellen konfrontiert die Datenschutzaufsicht immer wieder mit den gleichen Fragestellungen, die bei einer Zentralisierung nur einmal bearbeitet werden müssen. Betreibt z.B. eine bundesweite Handelsauskunftei ihren Betrieb nach einheitlichen Vertragsbedingungen über eine zentrale ADV-Anlage und haben alle regionalen rechtlich selbständigen Geschäftsstellen dieselbe Person als betrieblichen Datenschutzbeauftragten, so bestehen etwaige technische oder materiell-rechtliche Mängel zumeist bei allen Geschäftsstellen; eine festgestellte Unzuverlässigkeit eines betrieblichen Datenschutzbeauftragten trifft alle verarbeitenden Stellen. Zugleich ist die Kommunikation einer zentralen Landesbehörde mit den zentralen Stellen der anderen Länder, insbesondere über den "Düsseldorfer Kreis", ohne Reibungs- und Kommunikationsverluste möglich. Obwohl der LfD in Niedersachsen insofern nicht oberste Landesbehörde ist, so wurde mir vom Niedersächsischen Innenministerium doch die Möglichkeit zugestanden, an den Beratungen dieses bundesweiten Koordinierungsgremiums der Aufsichtsbehörden im nicht-öffentlichen Bereich teilzunehmen.

Ein weiterer Grund sprach für die Zusammenlegung der Datenschutzkompetenzen: Schon immer unterfallen öffentliche Stellen, die am Wettbewerb teilnehmen, materiell-rechtlich dem BDSG, während die Kontrolle bei den öffentlichen Datenschutzbeauftragten liegt (vgl. z.B. §§ 15, 18 NDSG a.F. v. 26.5.1978). Das hatte auch für Niedersachsen zur Folge, daß Unternehmen, die zueinander im Wettbewerb stehen, unterschiedlichen Kontrollinstanzen unterworfen waren. Dies wiederum kann zu unterschiedlichen Auslegungen des BDSG im Lande und damit zu Wettbewerbsverzerrungen führen - ein Effekt, der vermieden werden sollte.

Meine Doppelkompetenz erweist sich auch in der praktischen Tätigkeit und im Interesse effizienter Verwaltungstätigkeit als Vorteil: In der Vergangenheit waren die informationellen Beziehungen zwischen privaten und öffentlichen Stellen eher die Ausnahme. Inzwischen sind sie strukturell teilweise in Gesetzen angelegt und werden in der Praxis immer wichtiger. Zurückzuführen ist diese Strukturveränderung auf die Verlagerung von öffentlichen Aufgaben in private Hände sowie auf das verstärkte Zusammenwirken von Privaten mit öffentlichen Stellen. In diesen Fällen kommt es zwangsläufig

zu personenbezogenem Datenaustausch, z.B. zwecks Feststellung des Bedarfs an Kindergartenplätzen bei privaten Trägern, bei den Verdachtsmeldungen der Banken an die Polizei nach dem Geldwäschegesetz oder bei der systematischen Nutzung von Kfz-Produktionsdaten für die Strafverfolgung. Derartige einheitliche Lebensvorgänge sind rechtlich regelmäßig in eine Datenübermittlung durch eine private Stelle und in eine Datenerhebung durch die öffentliche Stelle aufzusplitten, wobei für die Kontrolle des ersten Teils die Aufsichtsbehörde, für die des zweiten Teils der Datenschutzbeauftragte für den öffentlichen Bereich zuständig ist. Zwischen den Kontrollorganen kann es dabei zu unterschiedlichen datenschutzrechtlichen Wertungen kommen. Diese Konstellation wäre problematisch, da die Rechtmäßigkeit der Datenerhebung und die Rechtmäßigkeit der Datenübermittlung voneinander abhängig sein können.

Mit der Doppelzuständigkeit können zudem Doppelermittlungen vermieden werden. Um insofern sofort Datenschutzeinwände zu zerstreuen: In § 22 Abs. 6 NDSG hat der Gesetzgeber zum Ausdruck gebracht, daß die Ermittlungsergebnisse aus dem öffentlichen und dem privaten Bereich für den jeweils anderen Bereich verwendet werden dürfen und daß insofern ein gemeinsamer Zweck verfolgt wird. Auch aus anderen Regelungen ist erkennbar, daß der Gesetzgeber die Einhaltung des jeweiligen Datenschutzgesetzes "und anderer Vorschriften über den Datenschutz" als einheitliche Aufgabe ansieht (vgl. z.B. § 24 Abs. 1 BDSG, § 22 Abs. 1 NDSG).

Der zentrale Einwand gegen die Doppelzuständigkeit ist, daß der an und für sich unabhängige Datenschutzbeauftragte im nicht-öffentlichen Bereich der Fachaufsicht unterliegt. Diese Konstellation ist sicher nicht unproblematisch, führte aber in Niedersachsen bisher nicht zu Konflikten. Wenn das zuständige Ministerium, in Niedersachsen das Innenministerium, und der Datenschutzbeauftragte ein entsprechendes Rollenverständnis haben und insofern gleiche, nämlich vorrangig Datenschutz-Interessen verfolgen, so ist der Rest vor allem eine Frage effektiver Arbeitsteilung und funktionierender Kommunikation. Ein Ministerium als oberste Aufsichtsbehörde ist nicht in der Lage und hat nicht die Aufgabe, die Vielzahl der auflaufenden Fälle aufzuarbeiten. Bei Grundsatzfragen ist ohnehin zumeist eine bundesweite Abstimmung nötig, so daß die Einschaltung der obersten Aufsichtsbehörde durch den LfD zum Zweck der Thematisierung im "Düsseldorfer Kreis" selbstverständlich ist.

## 34.2 Defizite beim Datenschutz im privaten Bereich

Die direkte Vergleichsmöglichkeit mit dem öffentlichen Bereich läßt die Mängel des Datenschutzes im privaten Sektor besonders deutlich hervortreten. Leider war in den letzten drei Jahren immer wieder festzustellen, daß Datenschutzverstöße und sonstige offenkundige Verletzungen des Persönlichkeitsrechts durch Private wegen der zu kurz greifenden materiellen und verfahrensrechtlichen Regelungen des BDSG nicht aufgeklärt und nicht geahndet werden konnten. Es dürfte zwar unstreitig sein, daß die bußgeldbewehrte Auskunftspflicht gegenüber der Aufsichtsbehörde nach § 38 Abs. 3

und 4 BDSG (vgl. § 44 Abs. 1 Nr. 6 BDSG) schon dann besteht, wenn hinreichende Anhaltspunkte für Datenschutzverstöße nach dem BDSG oder anderer Vorschriften bestehen. Dies gilt auch, wenn sich im nachhinein herausstellt, daß die Datenverarbeitung rechtmäßig war oder daß sie ausschließlich in Akten erfolgte. Das Ende der Fahnenstange für die Aufsichtsbehörde ist aber erreicht, wenn die verarbeitende Stelle nachvollziehbar begründet behauptet, die Verarbeitung sei nicht in oder aus Dateien erfolgt (vgl. § 27 BDSG). Wird dennoch zur Aufklärung eines "Akten"-Falls bei der verarbeitenden Stelle angefragt, so stößt man nicht nur auf Verständnis. So scheute sich z.B. ein Arzt, der ohne Begründung einem Patienten die Akteneinsicht verweigert hatte, nicht, in seiner Stellungnahme auf eine entsprechende Anfrage darum zu bitten, daß ihm seine Portokosten von 1 DM erstattet werden. Beim nächsten Mal solle der LfD einen Freiumschlag beilegen.

Die Grundannahme des Bundesgesetzgebers, die Datenverarbeitung in Akten sei weniger sensibel als solche in oder aus Dateien, erweist sich anhand der Eingaben in meiner Dienststelle immer wieder als falsch. Dies gilt natürlich zunächst für die Führung von Patientenakten in Krankenhäusern oder Personalakten bei Arbeitgebern, aber auch z.B. bei der Vertragsbearbeitung von Vermietern. Dabei entstehen, lagern und fließen Informationen, die für die Lebensplanung der Betroffenen existentiell sein können, unabhängig davon, ob mit Computer oder nur mit Papier, Telefax usw. (d.h. mit Akten) gearbeitet wird. Nicht geringer ist die Sensibilität von Daten zu bewerten, die von privaten Sicherheitsdiensten oder von Detektiven gesammelt werden, von religiösen Sekten (z.B. "Scientology Church") oder von Heiratsvermittlern. Inkassounternehmen und Banken führen in ihren Akten hochsensible Angaben über intime Bereiche ihrer Schuldner. Auch konventionell geführte Pressearchive enthalten oft vollständige Lebensläufe mit Details aus dem Privatleben. Ganz zu schweigen von der Vielzahl privater Beratungseinrichtungen, die in Eigeninitiative, oft aber auch im öffentlichen Auftrag, Beratungssuchenden helfen wollen. Sie sammeln dabei umfassend sensible Informationen in Akten, die dann potentiell für die Beantwortung von Anfragen zur Verfügung stehen. In keinem dieser Fälle kann den Petentinnen und Petenten klargemacht werden, weshalb hier eine Datenschutzkontrolle nicht stattfinden kann und der Aufsichtsbehörde nichts anderes übrig bleibt als ein freundlicher Appell.

Eine Quelle immer wieder auftretender Irritationen ist die Regelung des § 38 Abs. 1 BDSG, wonach die "Datenverarbeitung und Nutzung" als Kontrollgegenstand der Aufsichtsbehörde genannt wird. Daraus meinen einige den Schluß ziehen zu können, daß die Datenerhebung die Aufsichtsbehörden nichts angeht. Diese Ansicht ist zwar falsch. Der "soweit"-Satz in § 38 Abs. 1 BDSG bezieht sich nur auf die Ausführung "anderer Vorschriften über den Datenschutz". Nach dem Wortlaut überprüft die Aufsichtsbehörde bei hinreichenden Anhaltspunkten die Ausführung des BDSG unbeschränkt. Auch ist die Rechtmäßigkeit der Datenverarbeitung von der rechtmäßigen Datenerhebung abhängig. Doch hat es hier der Gesetzgeber an der nötigen Klarheit missen lassen - was in der Praxis immer wieder zu Klärungsbedarf gegenüber den Datenverarbeitern führt.

Probleme entstehen auch oft bei der Kontrolle von privaten Großdatenverarbeitern wie Banken, Versicherungen, Bausparkassen usw., da diese nach der bisherigen Praxis als Stellen angesehen wurden, die Datenverarbeitung für eigene Zwecke betreiben und daher nicht der anlaßunabhängigen Kontrolle unterliegen. Ob diese Praxis nach der aktuellen Rechtslage aufrecht erhalten werden muß und darf, ist Gegenstand gemeinsamer Überlegungen mit dem Niedersächsischen Innenministerium. In jedem Fall unglücklich ist es, daß nach § 38 Abs. 1 BDSG nur Einzelfallüberprüfungen durchgeführt werden können. Insbesondere im Finanzsektor sind Umfang und Sensibilität der Datenverarbeitung nicht geringer einzuschätzen als bei Adressenhändlern, Auskunfteien oder Rechenzentren, gegenüber denen Spontankontrollen nach § 38 Abs. 2 BDSG möglich sind. Es ist nicht einzusehen, daß erst ein konkreter Anlaß nötig sein soll, der zu einem Einzelfall führt, über den generell problematische Formen der Datenverarbeitung überprüft werden können.

Unzureichend sind auch die Sanktionsmöglichkeiten der Aufsichtsbehörde. Während bei Verstößen gegen die Datensicherheit Anordnungen zur Beseitigung der technisch-organisatorischen Mängel getroffen werden können (§ 38 Abs. 5 BDSG), bleibt die Aufsichtsbehörde zahnlos, wenn sie evtl. gar vorsätzlich begangene materiell-rechtliche Verstöße feststellt. Das Gesetz erlaubt ihr nicht einmal ausdrücklich, das Vorliegen eines Rechtsverstoßes festzustellen. Dies läßt sich nur indirekt aus dem Prüfauftrag nach § 38 Abs. 1 BDSG ableiten. Nach entsprechenden Feststellungen müssen die Betroffenen selbst zivilrechtlich oder per Strafanzeige aktiv werden. Daß die als Antragsdelikt ausgestaltete Strafnorm des § 43 BDSG ungeeignet ist, um repressiv, aber vor allem präventiv die Einhaltung des Datenschutzes zu bewirken, versteht sich fast von selbst. Die Hindernisse, die bis zu einer Verurteilung nach § 43 BDSG überwunden werden müssen, sind nur selten zu bewältigen. Ähnliches gilt übrigens für die zweite grundlegende Datenschutz-Strafnorm, den § 203 StGB.

## 34.3 Ausblick

Während für den Datenschutz im öffentlichen Bereich eine hohe Regelungsdichte und auch eine relativ hohe Kontrolldichte bestehen, so kann dies für den privaten Bereich sicherlich nicht gesagt werden. Datenschutz droht hier zur Alibiveranstaltung zu werden. Diese schon gesetzlich angelegte Tendenz wird dadurch verstärkt, daß die personelle und materielle Ausstattung der Aufsichtsbehörden keinesfalls als optimal bezeichnet werden kann. Daß dies im Hinblick auf die rasante Entwicklung der Informations- und Kommunikationstechnik und auf die verstärkte Verlagerung von öffentlichen Aufgaben in den privaten Bereich immer weniger zu verantworten ist, ist in der Öffentlichkeit leider viel zu wenig bewußt. Hier ist Öffentlichkeitsarbeit angesagt. Die öffentlichen Datenschutzbeauftragten erreichen insbesondere mit ihren Tätigkeitsberichten eine große Leserschaft und wirken so meinungsbildend. Die Berichte von Hamburg, Bremen und Niedersachen enthalten immer auch einen ausführlichen Teil zum Datenschutz in der Wirt-

schaft (hier die Kapitel 34 bis 43, vgl. § 22 Abs. 6 Satz 3 NDSG). Vergleichbare Berichte der obersten Aufsichtsbehörden anderer Länder sind bisher leider nicht so öffentlichkeitswirksam gewesen. Den Aufsichtsbehörden ist es grundsätzlich unbenommen, ähnlich der Konferenz der Datenschutzbeauftragten, nach außen zu treten. Eine breite öffentliche Diskussion über den Datenschutz in der Wirtschaft tut Not. Die kommende EU-Datenschutzrichtlinie, die den Datenschutz im öffentlichen und im privaten Bereich gemeinsam regelt, sollte zu einer solchen Diskussion anregen.

## 35. Kontrolltätigkeit: Zahlen und Fakten

### 35.1 Datenverarbeitung als Dienstleistung: 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. In XI 35.1 habe ich darauf hingewiesen, daß vermutlich viele Unternehmen ihrer Meldepflicht nicht nachkommen. In den letzten zwei Jahren habe ich darauf hingewirkt, diese Dunkelziffer zu verringern.

Am 1. Dezember 1994 waren insgesamt 270 Firmen nach § 32 BDSG zum Register gemeldet. Dies entspricht einer Zunahme gegenüber Ende 1992 von ca. 25 %; damals waren 214 Firmen registriert. In den zwei Jahren gab es 68 Neuanmeldungen und 12 Löschungen. Von den insgesamt gemeldeten 270 Firmen

- speichern 32 Firmen personenbezogene Daten zum Zweck der Übermittlung (3 Adreßverlage und 29 Auskunfteien),
- beschäftigen sich 2 Firmen mit der Markt- und Meinungsforschung bzw. speichern personenbezogene Daten zum Zweck der anonymisierten Übermittlung,
- verarbeiten 236 Firmen personenbezogene Daten im Auftrag als Dienstleistungsunternehmen.

Die genaue Aufteilung nach Berufssparten und deren Veränderung gegenüber 1992 zeigt Abb. 1. Es lassen sich Erfolge aber auch Defizite bei der Verringerung der Dunkelziffer ablesen. Ein besonders starker Anstieg an registrierten Unternehmen ist bei den Datenträger- und Aktenvernichtungsbetrieben erkennbar. Diese lassen sich leicht aufgrund ihrer Werbeaktionen ausfindig machen. Ähnliches gilt für Erfassungsbetriebe, für Mikroverfilmungsbetriebe oder für Service-Rechenzentren. Problematisch ist die Reduzierung der Dunkelziffer bei Unternehmen, die in erster Linie Datenverarbeitung für eigene Zwecke betreiben. Solche Unternehmen treten zumeist nicht durch Werbung o.ä. für ihr Dienstleistungsangebot in Erscheinung. Die systematische Suche nach solchen Firmen ist daher sehr schwierig und zeitaufwendig. In diesem Zusammenhang möchte ich noch einmal darauf hin-

weisen, daß eine Pflicht zur selbständigen Meldung besteht und daß das Unterbleiben der Meldung oder eine unkorrekte Meldung eine Ordnungswidrigkeit darstellt, die mit einem Bußgeld geahndet werden kann.

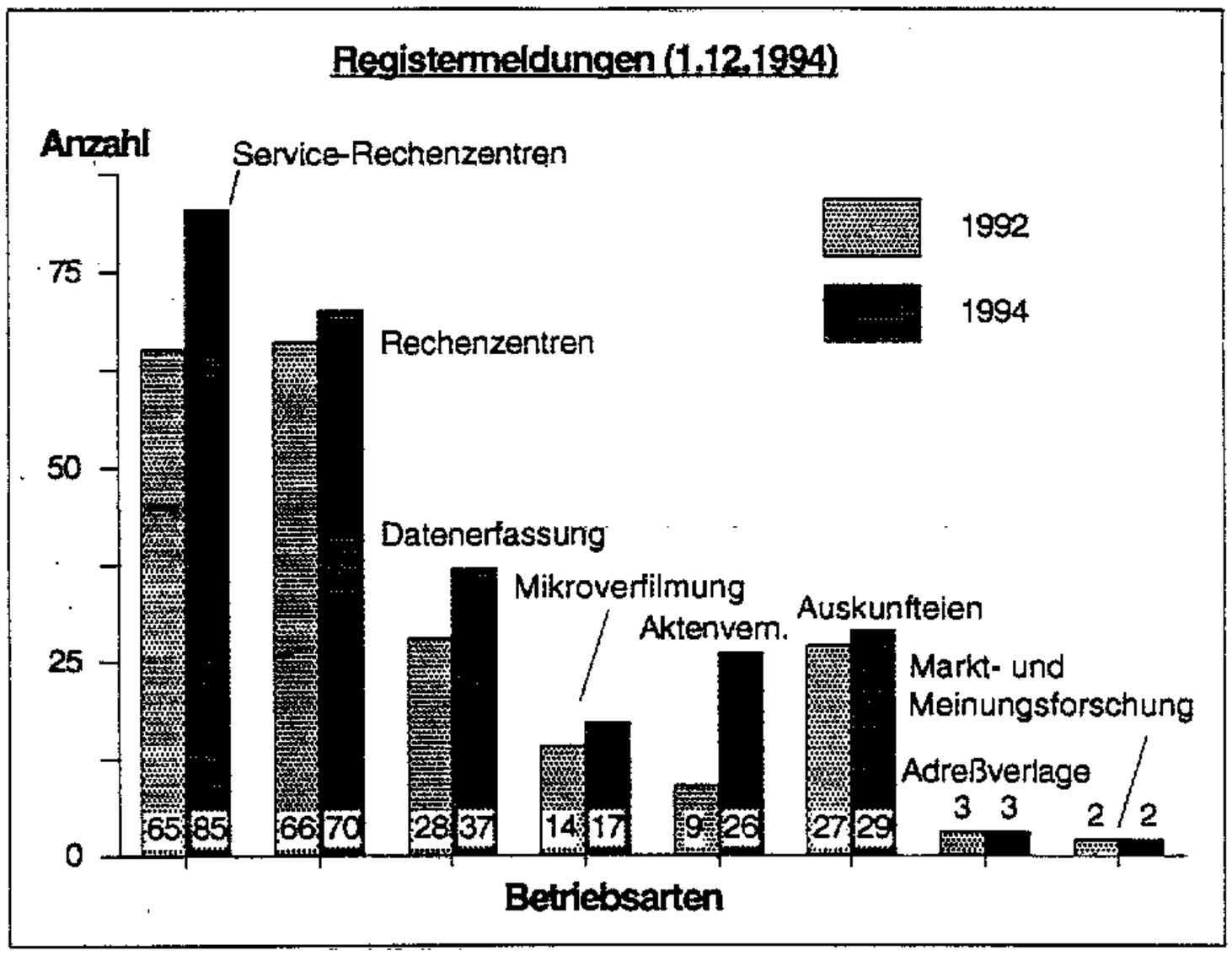


Abb. 1 Aufteilung der gemeldeten Firmen nach Betriebsarten für Ende 1992 und 1994 (Service-Rechenzentren: überwiegend Aufragsdatenverarbeitung; Rechenzentren: überwiegend Datenverarbeitung für eigene Zwecke).

Im Rahmen von Überprüfungen vor Ort hat sich gezeigt, daß Registermeldungen häufig nicht in allen Punkten korrekt waren. Soweit es sich um unerhebliche Mängel handelte, habe ich bislang auf die Einleitung von Ordnungswidrigkeitenverfahren verzichtet. Ein Beispiel sei hier aber angeführt, bei dem die unkorrekten Registereintragungen als besonders mangelhaft bezeichnet werden müssen. Im Frühjahr 1994 war von mir eine Prüfung bei einer Firma vorgesehen, die laut Registermeldung aus dem Jahre 1991 in einem Ort bei Hannover ansässig war. Ein Anschreiben, das über den Prüfungstermin informieren sollte, wurde von der Post mit der Mitteilung "unbekannt verzogen" zurückgeschickt. Die Prüfung wurde daraufhin abgesagt. Genauere Recherchen haben dann ans Licht gebracht, daß die Firma durchaus noch existiert, daß sie aber in einer andere Stadt gezogen ist und eine Korrektur der Registermeldung nicht vorgenommen hat. In diesem Fall entstand durch die unkorrekte Registereintragung ein unnötig hoher Verwaltungsaufwand. Auch das weitere Verhalten der Firma legte die Vermutung nahe, daß sich die Verantwortlichen entweder bewußt der Datenschutzaufsicht entziehen wollten oder daß sie den Datenschutz für absolut nachrangig betrachten. In einem solchen Fall kommt die Verhängung eines Bußgeldes in Betracht.

35.2 Kontrolle vor Ort

Auch in den Jahren 1993 und 1994 habe ich im Rahmen meiner Aufsichtstätigkeit nach § 38 BDSG Prüfungen bei niedersächsichen Firmen vorgenommen. Insgesamt wurden von mir 34 Prüfungen durchgeführt, also im Schnitt 17 pro Jahr. Vier der 34 Prüfungen waren "Anlaßprüfungen" von nicht meldepflichtigen Firmen nach § 38 Abs. 1 BDSG, der Rest gehörte zu "Routineprüfungen" nach § 38 Abs. 2 BDSG.

Schwerpunktmäßig habe ich in den letzten zwei Jahren Unternehmen geprüft, die ein UNIX-Betriebssystem einsetzen. Eine entsprechende Auswahl von Firmen war mir aufgrund der Angaben im Register nach § 32 BDSG möglich. Bei diesen Unternehmen bin ich mit Hilfe eines Prüfkatalogs detailliert auf Datensicherungsaspekte der Betriebssystemebene eingegangen. Ergebnisse dieser Prüfungen sind in 4.5 dargestellt. Ein neuer Prüfungsschwerpunkt sind Stellen, die das Betriebssystem Novell NetWare 3.11 oder 3.12 einsetzen (vgl. 4.4.3). Außerdem habe ich verstärkt Vernichtungsunternehmen geprüft, die sich zum großen Teil neu zum Register nach § 32 BDSG gemeldet haben und damit überwiegend ungeprüft sind (vgl. 4.9).

Bei den Prüfungen wurden zahlreiche Mängel festgestellt. Aus den am häufigsten kritisierten Punkten habe ich eine "Top-Ten- Liste der Mängel" zusammengestellt:

1. Der Zugriffsschutz auf Rechnern mit Hilfe von Paßwortverfahren war nicht ausreichend sicher (weniger als 6 Stellen, keine Paßwort-Alterung usw.).
2. Es bestanden keine oder unzureichende schriftliche Arbeitsanweisungen.
3. Auftragsverhältnisse waren nicht ausreichend durch geeignete Verträge festgelegt.
4. Der Zugang zu Rechnern und Datenbeständen war nicht genügend abgesichert (z.B. nicht ausreichend sichere Türen).
5. Der Umgang mit der Systemverwalter-Kennung war nicht datenschutzgerecht (zuviele kannten das Systemverwalter-Paßwort, keine Anzeige des letzten Login usw.).
6. Die Sicherheit der Netzinfrastruktur in lokalen Netzwerken befand sich auf sehr niedrigem Niveau (Netzstruktur mit Bustopologie usw.).
7. Der Datenschutzbeauftragte besaß nicht die notwendige Zuverlässigkeit oder Fachkunde.
8. Datenfernübertragungen waren risikobehaftet, weil keine Verschlüsselung vorgenommen wurde.
9. Die Protokollierung wurde nicht korrekt durchgeführt (zu geringer Umfang, keine Kontrolle, keine Löschung der Protokolle).
10. Es existierten keine gesicherten Pausenfunktionen, die die Rechner bis zur Eingabe des Paßwortes sperren.

Um die immer wieder auftretenden Mängel der Paßwortverfahren abzubauen, habe ich ein Merkblatt zur Paßwort-Gestaltung und -Verwendung erstellt, das ich kostenlos versende. Ich hoffe, daß das Merkblatt zur Beendi-

gung der traurigen Spitzenreiterrolle dieses Punktes in den "Top Ten" beiträgt. Zu weiteren Punkten der Hitliste sind in anderen Bereichen dieses Tätigkeitsberichtes Anmerkungen zu finden (Auftragsverhältnis: 4.9; Arbeitsanweisung, Systemverwalter-Kennung, Verschlüsselung, Protokollierung und Netzinfrastruktur: 4.5, Datenschutzbeauftragter: 4.10; Pausenfunktion: 4.4.1).

## 36. Adressenhandel und Markt- und Meinungsforschung

### 36.1 Wer wirbt wen - wer verantwortet was?

Von der Datenschutzaufsichtsbehörde eines anderen Bundeslandes wurde ich darauf hingewiesen, daß eine in meinem Zuständigkeitsbereich arbeitende Direct-Marketing-Firma auf sog. "Datenkarten" Adressen anbietet, deren Vermittlung datenschutzrechtlich zweifelhaft sei. Dabei tritt die Firma im sog. Listbroking-Verfahren nur als Adress-Mittler auf. Die anbietende Firma stellt ihre Kundenadressen einer anderen Firma für Werbezwecke zur Verfügung.

Bei mehreren Datenkarten wurden zwei oder mehrere Selektionskriterien angeboten, die nicht im Katalog des § 28 Abs. 2 Nr. 1b BDSG aufgeführt sind. So werden regelmäßig die Adressen von weiblichen Kundinnen und männlichen Kunden gesondert aufgeführt. Auch gab es Differenzierungen danach, wann die Betroffenen bei der Firma ein Kundenkonto eingerichtet und wann sie Ware bestellt hatten. Bei einer Besprechung der rechtlichen Fragen mit Vertretern der Firma sowie von Verbänden der Werbewirtschaft wurde mir mitgeteilt, daß sich der Adressenhandel praktisch nur noch selten auf den § 28 Abs. 2 Nr. 1b BDSG beruft, der gerade für diese Branche die listenmäßige Datennutzung erleichtert, sondern auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist eine Datennutzung zur Wahrung berechtigter Interessen zulässig, wenn kein Grund zur Annahme besteht, daß schutzwürdige Betroffeneninteressen überwiegen. Obwohl ich den Rückgriff auf diese Generalklausel aus Betroffenensicht für sehr problematisch halte, so mußte ich konzedieren, daß der Gesetzgeber die Heranziehung dieser Norm nicht ausgeschlossen hat. Bei einigen der Adressenangeboten auf den "Datenkarten" drängte sich jedoch für mich die Annahme eines schutzwürdigen Interesses geradezu auf. So dürfte es "Mitgliedern eines exklusiven Clubs" regelmäßig nicht lieb sein, als solche beworben zu werden. Ähnliches dürfte für die Kunden und Interessenten eines Sexartikelversandes gelten oder, so ein anderes Angebot, für "junge Mütter". Unbestreitbar wurde die Grenze zur Unzulässigkeit bei der Vermietung von Adressen von "schüchternen und gehemmten" Menschen überschritten. Dabei handelt es sich um Personen, die Interesse für Kurse und Bücher zeigten, bei denen es um "emotionale Enthemmung", "Gedächtnisschulung" und "Erfolgsliteratur" ging. Ich kam mit der Direct-Marketing-Firma und den Vertretern der Wirtschaftsverbände überein, daß ein Kriterienkatalog erarbeitet werden soll, der für die Beurtei-

lung der Unzulässigkeit von Direktwerbemethoden herangezogen werden kann.

Kontrovers war zunächst auch, ob die Adressenhändler als Listbroker verpflichtet sind, ihren Auftraggebern, also den Firmen, für die sie Kundenadressen vermitteln, mitzuteilen, daß sie bestimmte Adressenangebote für unzulässig halten. Nach § 11 Abs. 3 Satz 2 BDSG ist der Auftragnehmer nämlich verpflichtet, den Auftraggeber unverzüglich darauf hinzuweisen, daß er bestimmte Aufträge für unzulässig hält. Von seiten der Vertreter der Werbewirtschaft wurde die These vertreten, daß mit der Regelung keine Verpflichtung zu einer rechtlichen Prüfung der Aufträge verbunden sei. Gemeint sein könnten nur die Fälle, bei denen der Datenschutzverstoß offenkundig sei, dem Auftrag "auf der Stirn geschrieben steht". Dem konnte ich so nicht beipflichten. Zwar kann vom Auftragnehmer nicht in jedem Fall eine detaillierte rechtliche Prüfung verlangt werden. Wohl aber entsteht eine Prüf- und gegebenenfalls eine Hinweispflicht, wenn er von der Aufsichtsbehörde auf die datenschutzrechtliche Problematik hingewiesen worden ist. Dem Auftragnehmer kommt wegen seiner besseren Branchen- und Datenschutzkenntnisse eine Beratungsaufgabe zu, die in § 11 Abs. 3 BDSG ihren Niederschlag gefunden hat.

## 36.2 Von der Baby-Windel bis zum ungewollten Urinverlust

Gleich von mehreren Seiten wurde ich über einen "Fragebogen für Familien mit Kleinkindern" einer "Studiengruppe für Haushaltsforschung" unterrichtet. Die Studiengruppe, die sich selbst als unabhängiges Marktforschungsinstitut bezeichnete, wollte allzuviel von jungen Müttern wissen. Gefragt wurden zunächst Name und Adresse der Mutter sowie Name, Geschlecht und Geburtsdatum des Kindes. Die "Unabhängigkeit" der Haushaltsforschung wurde dadurch unterstrichen, daß die Mütter mit dem Ausfüllen des Fragebogens auch automatisch im Kleingedruckten ihr Interesse für die Zusendung von Werbeinformationen und Mustern erklärten. Das ist aber noch lange nicht alles. Die Studiengruppe wollte weitere intime Informationen erhalten: Nicht nur Angaben über verwendete Windeln, Lernhöschen, Babytücher, Damenhygieneprodukte, Binden, Slipeinlagen sowie über die aufgesuchten Geschäfte wurden erbeten, sondern auch Angaben über das Alter aller im Haushalt lebenden Personen, über erlernte Kinderheilberufe, über das Gewicht der Kinder, ob diese "sauber" sind, und ob die Mütter Erfahrungen "mit ungewolltem Urinverlust" gemacht hätten. Wollte die Studiengruppe, die eine Postfachadresse angab, einerseits über die Kundinnen viel Intimes wissen, so war andererseits dem Fragebogen nichts über Auftraggeber, über die Wahrung der Anonymität und über die Freiwilligkeit der Angaben zu entnehmen. Dubios erschien mir das ganze auch, weil die Studiengruppe als Marktforschungsinstitut nicht nach § 32 BDSG bei mir im Dateienregister gemeldet war.

Zwei Monate nach meiner Aufforderung zur Stellungnahme hatte ich immer noch keine Antwort von der Studiengruppe erhalten. Nach meiner Mahnung kam Erstaunliches zutage: Bei der "Studiengruppe" handelte es sich um

nichts anderes als um ein "Pseudonym" eines großen Direct-Marketing-Unternehmens. Dieses Unternehmen wurde tätig im Auftrag eines großen Konzerns. Dieser Konzern hatte die Adressen der Mütter über Werbeaktionen erhalten, die direkt nach der Geburt unter so wohlklingenden Namen wie "Bambino" und "Felicitas" durchgeführt worden waren. Dabei erhob der Konzern nicht nur die Adressen der Mütter, sondern auch Geschlecht, Name und Geburtsdatum der Kinder. Als nun angeschriebene Mütter sich nicht nur bei mir, sondern über das Postfach auch bei der "Studiengruppe" beschwerten, stellte das Direct-Marketing-Unternehmen fest, daß die Aktion nicht nur gegen das Datenschutzrecht, sondern auch gegen das Gesetz gegen unlauteren Wettbewerb verstieß. Statt nun die Angeschriebenen über den Fehler zu unterrichten und um Entschuldigung zu bitten, ergriff man die Flucht nach vorn: Die Rückläufe wurden ungeöffnet unter Verschluß genommen und "unter notarieller Aufsicht" bei einem Entsorgungsunternehmen durch Reißwolf vernichtet. Dieses Schicksal dürfte aber nicht nur die Rückläufe der angeschriebenen Mütter ereilt haben, sondern auch meine schriftliche Anfrage in dieser Angelegenheit.

Daß die Markt- und Meinungsforschung bestimmten Datenschutzanforderungen genügen muß, war von den beteiligten Firmen nicht erkannt worden. Ich wies sie darauf hin, daß nicht nur eine Meldepflicht gemäß § 32 Abs. 1 Nr. 2 besteht, sondern daß § 30 BDSG Anforderungen an die Anonymität und Zweckbindung von Marktforschungsaktivitäten stellt. Zwar enthält § 30 BDSG keine materiellen Kriterien für die Datenerhebung. Dies entbindet die Unternehmen aber nicht von der Pflicht, Daten nach Treu und Glauben und auf rechtmäßige Weise zu erheben (vgl. § 28 Abs. 1 Satz 2 BDSG). Nicht nur, daß der Fragebogen wenig schamhaft war, er forderte auch Daten ab, die Dritte betreffen und über die die Mütter nicht ohne weiteres verfügen konnten. Die beteiligten Firmen zeigten sich einsichtig. Zwar plant das Direct-Marketing-Unternehmen, weiterhin im Auftrag von Firmen Daten zum Zweck der Markt- und Meinungsforschung zu erheben. Dies soll aber nicht mehr unter einem Pseudonym erfolgen; der Auftraggeber soll eindeutig genannt werden. Die datenschutzrechtliche Hauptverantwortung soll nach § 11 BDSG also künftig beim Auftraggeber liegen, der auch die Auswertung der Unterlagen vornimmt.

Der geschilderte Fall ist ein Beleg dafür, daß es sich Menschen zweimal überlegen sollten, ob sie an Markt- und Meinungsforschungsaktionen teilnehmen wollen. Der gesamte Text des Fragebogens wie der Erläuterungen sollte zuvor gelesen, offene Fragen sollten zuvor beantwortet werden. Jede und jeder sollte sich darüber im klaren sein, daß keine Auskunftspflicht besteht und daß Fragen unbeantwortet bleiben können. Und niemand sollte sich wegen des vorherigen Erhalts von kleinen "Präsenten" der Marktforschenden bei der Beantwortung unter einen moralischen Druck gesetzt fühlen. Erscheint Betroffenen ein Marktforschungsprojekt fragwürdig, so können sie sich jederzeit an mich als Aufsichtsbehörde wenden.

## 37. Kundendaten und Werbung

### 37.1 Wie kommt mein Name in die Kundenzeitschrift?

Mehrere Bausparerinnen und Bausparer beschwerten sich bei mir darüber, daß in Werbeanzeigen von verschiedenen Firmen in ihrem Exemplar einer Kundenzeitschrift einer Bausparkasse deren Name abgedruckt war. Mit der namentlichen Nennung sollten die Kundinnen und Kunden besonders individuell angesprochen werden. Diese Werbemaßnahme ging, zumindest teilweise, nach hinten los: Bei vielen Betroffenen entstand der Eindruck, die Bausparkasse habe die Adreßdaten an das werbende Unternehmen weitergegeben.

Das Unternehmen teilte mir mit, daß es seine Kundenzeitschrift bei einer Fremddruckerei drucken läßt. Diese hat auch den Auftrag, die Zeitschriften zu versenden. Für die Adressierung werden der Druckerei die Anschriften der Kundinnen und Kunden zweckgebunden auf einer Diskette zur Verfügung gestellt. Die Druckerei ist mit ihrer modernen Technik in der Lage, die Anschrift oder den Namen einer Kundin bzw. eines Kunden auch noch an anderen Stellen der Kundenzeitschrift, z.B. in Anzeigen, abzudrucken. Diese Technik führt dazu, daß die besonders persönlich gestalteten Anzeigen mit der Anschrift ausschließlich im persönlichen Exemplar der Zeitschrift erschien. Jedes dem Kunden zugestellte Heft ist gewissermaßen ein Unikat. Mit der Druckerei ist seitens des Unternehmens ein Vertrag zur Auftragsdatenverarbeitung abgeschlossen worden. Dieser beinhaltet, daß eine Weitergabe der Daten an die werbenden Unternehmen oder an Dritte nicht erfolgt. Von daher hat das Unternehmen das Seine getan, um Verstößen gegen die Vorschriften des Bundesdatenschutzgesetzes vorzubeugen.

Das dargestellte Verfahren war aus datenschutzrechtlicher Sicht nicht zu beanstanden. Gleichwohl habe ich das Unternehmen auf die Irritationen in seiner Kundschaft hingewiesen. Dort will man künftig auf diese Werbemaßnahme verzichten.

### 37.2 Datenschatten beim bargeldlosen Einkauf im Kaufhaus

Daß die Möglichkeit des "problemlosen" Einkaufs ohne Bargeld und darüber hinaus ohne Ausstellen eines über den Rechnungsbetrag belaufenden Schecks zu Datenschutzproblemen führen kann, zeigt folgender Fall: Der Kunde eines Bekleidungskaufhauses hatte die Möglichkeit genutzt, lediglich mit Vorzeigen seiner Scheckkarte zu bezahlen. Dabei hatte er seine Adresse bekanntgegeben. Als er ein Jahr später erneut mit seiner EC-Karte bezahlen wollte, mußte er feststellen, daß seine komplette Adresse einschließlich seiner Bankverbindung automatisch auf dem Kaufbeleg ausgedruckt wurde. Der Petent beschwerte sich darüber, daß ohne sein Einverständnis seine Adresse über ein Jahr lang im Computer des Kaufhauses gespeichert wurde. Nach seiner Auffassung hätten seine Daten nach Abwicklung der Lastschrift über sein Kreditunternehmen von der Firma wieder gelöscht werden

müssen. Auch habe er seinerzeit mit dem von ihm unterschriebenen Beleg keine Ermächtigung zur Speicherung seiner Daten abgegeben.

Das Unternehmen teilte mir mit, daß für das Bankabbuchungsverfahren folgende Daten im hauseigenen System gespeichert werden: Bankleitzahl der Bank des Kunden, Kontonummer des Kunden und Name des Kunden bzw. der Kundin. Auf die Angabe der Anschrift werde seit Januar 1993 verzichtet. Die verarbeiteten Kundendaten würden "bis auf weiteres" gespeichert. Die Notwendigkeit begründet das Unternehmen damit, daß bei Nichteinlösung der Lastschrift das Kundenkonto sofort gesperrt wird, um weiteren Mißbrauch mit der EC-Karte in diesem Haus auszuschließen.

Ich habe Verständnis dafür, daß sich das Kaufhaus gegen wirtschaftlichen Schaden schützen will. Eine unbefristete Speicherung von Kundendaten in den Fällen, in denen das Abbuchungsverfahren erfolgreich und damit der Ausgleich des Kundenkontos herbeigeführt wurde, ist aber unnötig und nach den Vorschriften des Bundesdatenschutzgesetzes nicht zulässig. Hier besteht ein Löschungsanspruch nach § 35 Abs. 2 Nr. 3 des Gesetzes. Ich habe das Unternehmen aufgefordert, seine diesbezügliche Praxis zu ändern. Dem Petenten habe ich vorgeschlagen, seinen Auskunftsanspruch nach § 34 BDSG geltend zu machen und, sofern noch Daten unzulässigerweise gespeichert sein sollten, die Löschung der Daten einzufordern.

## 37.3 Naturgesetzpartei erhält Kursteilnehmerdaten

Der Hamburgische Datenschutzbeauftragte hat mich im August 1993 davon in Kenntnis gesetzt, daß Bürgerinnen und Bürger der Hansestadt anläßlich der bevorstehenden Bürgerschaftswahl einen Wahlbrief von der Naturgesetzpartei - Landesverband Hamburg - erhalten haben. Die Betroffenen waren nicht Mitglieder dieser Partei. Sie hatten jeweils an Kursen der Transzendentalen Meditation teilgenommen, die von einer privaten Gesellschaft mit beschränkter Haftung (GmbH) veranstaltet wurden. Es drängte sich ihnen der Verdacht auf, daß das Unternehmen Teilnehmerdaten an die Naturgesetzpartei weitergegeben hatte.

Die GmbH teilte mir zunächst auf Anfrage mit, daß sie Daten von Kursteilnehmern nicht an den Landesverband der Naturgesetzpartei weitergegeben habe. Diese Aussage mußte von mir zunächst so hingenommen werden. Anläßlich der Landtagswahl in Niedersachsen erhielt ich dann aber Kenntnis von einem Wahl-Werbeschreiben der Naturgesetzpartei - Landesverband Niedersachsen. Darin wurde eingangs darauf verwiesen, daß die Partei die Adresse der Angeschriebenen von der GmbH erhalten habe mit der Bitte, "sie über die Neuigkeiten im Zusammenhang mit der Naturgesetzpartei zu informieren". Einzelne angeschriebene Bürgerinnen und Bürger wiesen jedoch darauf hin, eine derartige Neugierde nicht gezeigt bzw. bisher weder Kontakt zur GmbH noch zur Naturgesetzpartei gehabt zu haben.

Die GmbH hat nunmehr eingeräumt, dem Landesverband Niedersachsen der Naturgesetzpartei Kundenadressen übermittelt zu haben. Einige der Kundin-

nen und Kunden hätten ihr Interesse an dieser Partei bekundet. Das Vorgehen wurde damit begründet, daß ein berechtigtes Interesse des Unternehmens bestand, seinen Kundenkreis über die Naturgesetzpartei zu informieren.

Dies sehe ich völlig anders. § 28 BDSG erlaubt eine Datenübermittlung von einem Meditationskurs an die Naturgesetzpartei nicht. Die Tatsache der Teilnahme einer Person an einem Grundkurs Transzendentale Meditation ist ein sehr sensibles Datum. Die Übermittlung von Teilnehmerdaten an die Naturgesetzpartei lag auch nicht im Rahmen der Zweckbestimmung des zwischen der GmbH und Kursteilnehmern geschlossenen Vertrages (vgl. § 28 Abs. 1 Satz 1 Nr. 1 BDSG). Soweit einige ein spezielles Interesse an Informationen über die Naturgesetzpartei geäußert haben, hätte man diesen Material aufgrund einer schriftlichen Einwilligung zusenden können. Ich habe die Gesellschaft gebeten, künftig nur noch entsprechend zu verfahren und mir dies schriftlich zu bestätigen.

Nach mehrmaliger telefonischer und schriftlicher Erinnerung hat mir die GmbH mitteilen lassen, daß sie nach dem Zeitpunkt meiner Feststellung ihres rechtswidrigen Vorgehens keine Daten mehr an Dritte herausgegeben habe. Dies sei auch in Zukunft nicht beabsichtigt. Ich habe daher die Hoffnung, daß das Unternehmen künftig das Datenschutzrecht beachten wird.

## 38. SCHUFA

Zwar ist vielen Menschen die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) ein Begriff. Die Vielzahl der wieder bei mir eingegangenen Petitionen zu diesem Register zeigt, daß immer noch über dessen Arbeitsweise und die Rechtsgrundlagen wenig bekannt ist. Ich verweise insofern auf XI 36.3, wo ich die Funktionsweise der SCHUFA im Überblick darstellte. Die Empörung der Betroffenen über bestimmte Auskunftspraktiken der SCHUFA ist zwar individuell oft nachvollziehbar, erwies sich jedoch zumeist aus datenschutzrechtlicher Sicht als unbegründet.

Es ist z.B. einfach so, daß die SCHUFA gemäß § 34 Abs. 5 BDSG für eine Selbstauskunft dann ein Entgelt verlangen darf, wenn diese gegenüber Dritten zu wirtschaftlichen Zwecken genutzt werden kann. Bei einer schriftlichen SCHUFA-Auskunft besteht zweifellos grundsätzlich eine solche Nutzungsmöglichkeit. Nur selten dürfte insofern eine Ausnahme gegeben sein. Ich kann daher Petentinnen und Petenten, die kostenlos ihre bei der SCHUFA gespeicherten Daten erfahren wollen, zumeist nur darauf verweisen, sich gebührenfrei direkt bei den SCHUFA-Geschäftsstellen eine mündliche Auskunft einzuholen. Auf Unverständnis stößt auch immer wieder, daß frühere Wohnadressen bei der SCHUFA gespeichert bleiben. Doch auch dies ist zumeist nicht zu beanstanden, da die einzelnen Personen zum Zweck der Auskunftserteilung eindeutig identifiziert werden müssen, was

bei zeitlich zurückliegenden Sachverhalten oft nur über führere Adressen möglich ist.

38.1 Auskunftserteilung bei den SCHUFA-Vertragspartnern

In Nr. 1.4.4 der SCHUFA-Vertragsbedingungen wird den Vertragspartnern der SCHUFA (z.B. den Kreditinstituten) untersagt, gegenüber Betroffenen eine datenschutzrechtliche Auskunft zu erteilen. Diese Vertragsregelung hielt ich zunächst wegen des Widerspruchs zu § 34 BDSG für unzulässig. Die Bundes-SCHUFA stellte daraufhin klar, daß nach den SCHUFA-Vertragsbestimmungen lediglich die Aushändigung von Formularen mit eingetragenen Merkmalen an Dritte untersagt ist. Damit solle verhindert werden, daß die auf dem Formular enthaltene Kennziffer des Vertragspartners bekannt wird. Dies sei auch kein personenbezogenes Datum. Nr. 1.4.4 verbiete dagegen keineswegs die Weitergabe des Inhaltes von SCHUFA-Auskünften, soweit es sich um personenbezogene Daten handele. Dem kann ich beipflichten. Ich empfahl bei einer Überarbeitung der Vertragsbedingungen eine eindeutige, § 34 BDSG berücksichtigende Formulierung zu verwenden.

Weiterhin meinte die Bundes-SCHUFA, die aktenmäßige Speicherung der SCHUFA-Auskunft sei nicht zur Übermittlung bestimmt (§ 1 Abs. 3 Nr. 2 BDSG). Daher gälten nur die §§ 5, 9, 39 und 40 BDSG, nicht aber die Regelung über die Auskunftspflicht (§ 34 BDSG). Dies halte ich nicht für richtig. Da die Angaben offensichtlich aus einer automatisierten Datei entnommen sind, ist das gesamte BDSG anzuwenden (§ 27 BDSG).

38.2 Die Telefonauskunft - ein delikater Fall

Leider werden die Möglichkeiten des SCHUFA-Verfahrens nicht nur zu Zwecken der Kreditsicherung verwendet, sondern auch, um mit erlangten Daten unzulässigerweise private Auseinandersetzungen zu betreiben. So meldete sich bei mir ein Bürger, der sich in einer Testamentsvollstreckung mit seinem Onkel auseinandersetzen muß. Im Rahmen dieses Verfahrens teilte der Onkel dem Gericht mit, ihm seien aus SCHUFA-Auskünften negative Merkmale über den Neffen bekannt. Dieser habe auf einer Bank-Warnliste ("Schwarze Liste") gestanden. Nach wie vor sei ein nicht erledigter Haftbefehl gespeichert.

Bei meinen Ermittlungen stellte sich schnell heraus, daß der Onkel keine SCHUFA-Abfrageberechtigung hat. Weiterhin ergab sich, daß der Onkel sein Wissen nur aus einer SCHUFA-Auskunft erlangt haben konnte, die von einer Bankfiliale in der Stadt H. "zum Girokonto" getätigt worden ist. Nur, daß der Petent bei dieser Bank gar kein Girokonto unterhielt. Die weiteren Ermittlungen erwiesen sich als äußerst schwierig. Eine Anfrage beim Onkel wurde von diesem schroff abgewiesen; Datenschutzverletzungen müßten ihm erst einmal nachgewiesen werden. Die den Petenten vertretenden Anwältinnen überzog er mit Strafanzeigen. Auch bei der Bankfiliale wurde mir die Aufklärung nicht gerade leicht gemacht. Es stellte sich später

heraus, daß der Onkel vor Jahren selbst Mitleiter einer anderen Filiale derselben Bank gewesen ist.

Die SCHUFA bestätigte die telefonische Anfrage bei ihr unter Verwendung der nur intern bekannten SCHUFA-Kennziffer der Filiale und des Paßwortes. Die telefonische Anfrage sei, wie üblich, nachträglich schriftlich bestätigt worden.

Von seiten der Bankfiliale wurde versichert, die fragliche Auskunft nicht eingeholt zu haben. Alle Abfrageberechtigten hätten auf mündliche Anfrage "nachdrücklich" beteuert, eine entsprechende telefonische Auskunft nicht vorgenommen zu haben. Bedingt durch Mitarbeiterwechsel und nicht vorliegender Unterlagen sei der Urheber der Anfrage aber nicht mehr feststellbar. Aus "Gründen des Datenschutzes" sah sich die Bank gehindert, die Namen der abrageberechtigten Personen mitzuteilen. Es zeigte sich, daß die Bank seit Jahren das für telefonische SCHUFA-Anfragen verwendete Paßwort nicht geändert hatte, so daß dieses im Laufe der Zeit einer kaum übersehbaren Vielzahl von Personen bekannt wurde. Außerdem teilte mir die Bank mit, daß die schriftlichen SCHUFA-Auskunftsbestätigungen über Nichtkunden im Einzelfall als "Irrläufer" sofort vernichtet werden.

So geht es nun auch nicht. Äußerst unbefriedigend war, daß wegen der Vernichtung der schriftlichen Bestätigungen die Anfrage nicht mehr nachvollzogen werden konnte. Die Bank führte auch kein Protokoll über die erfolgten telefonischen SCHUFA-Anfragen. Daher ordnete ich gegenüber der Bank gemäß § 38 Abs. 5 BDSG an, bei telefonischen Auskünften die erforderlichen Datenschutzmaßnahmen zu ergreifen. Erforderlich erschien mir zunächst die sofortige Änderung des Paßwortes. Außerdem meine ich, daß durch eine Protokollierung der telefonischen Anfragen und durch Überprüfung und Dokumentation der schriftlichen Bestätigungen der telefonischen SCHUFA-Auskünfte verhindert werden sollte, daß unter "falscher Flagge" Auskünfte eingeholt werden.

Hinsichtlich des Tatbeitrages des Onkels hatte ich keine weiteren Aufklärungsmöglichkeiten. Hier ermittelt nun die Staatsanwaltschaft.

## 39. Auskunfteien: Wer ist speichernde Stelle?

Diese Frage ist nicht nur rein akademischer Natur. Sie ist insbesondere für die betroffenen Bürgerinnen und Bürger relevant, da diese ihre Auskunfts-, Löschungs- oder Schadensersatzansprüche nur gegenüber der speichernden Stelle geltend machen können. Anläßlich einer Vorortprüfung bei einer regionalen Auskunftei, die Mitglied einer bundesweiten Auskunfts-Gesellschaft ist, bat ich um die schriftlichen Unterlagen über die Rechtsverhältnisse zwischen den beteiligten Rechtspersonen. Vorgelegt werden konnte mir nur ein - nicht mehr aktueller - Gesellschaftsvertrag. Wer im datenschutzrechtlichen Sinne "speichernde Stelle" (§ 3 Abs. 8 BDSG) sei, konn-

te mir nicht eindeutig mitgeteilt werden. Hierfür in Frage kamen die BGB-Gesellschaft der Auskunfteien, die als GmbH geführte Zentralverwaltung oder die regionalen Auskunfteien. Beteiligt an der Datenverarbeitung sind außerdem noch eine Wirtschaftsinformationsgesellschaft sowie eine Rechenzentrumsgesellschaft.

Nachdem mir die derzeit gültige Version des Gesellschaftsvertrages vorgelegt worden war, war das juristische Chaos perfekt: Zwar wurde auf der einen Seite die rechtliche Selbstständigkeit der regionalen Auskunfteien behauptet, doch waren diese in ein starkes Abhängigkeitsverhältnis zur zentralen GmbH eingebunden: Das gesamte regional erarbeitete Archivmaterial sollte von Anfang an Eigentum der GmbH werden, die in gewissen Fällen selbst auskunftsberechtigt sein sollte. Außerdem werden der Zentrale Anordnungs-, Kündigungs- und Bestrafungsrechte zugestanden. Die gesamte elektronische Datenverarbeitung erfolgt über ein Rechenzentrum, mit dem die Auskunfteien nur entsprechend den Anweisungen der Zentrale zu verkehren haben. Nachdem ich auf die Unklarheiten hingewiesen hatte, legte sich der betriebliche Datenschutzbeauftragte darauf fest, daß allein die regionalen Auskunfteien speichernde Stellen seien. Der Umstand, daß sich die Auskunfteien vertraglich stark gebunden hätten, ändere hieran nichts. Auch aus dem Umstand, daß das gesamte Archivmaterial privatrechtlich als Eigentum der GmbH behandelt wird, ergäbe sich datenschutzrechtlich nichts anderes. Zugegeben wurde, daß die gesetzlich geforderte Schriftform der Auftragsverhältnisse fehlt (§ 11 BDSG). Man sei jedoch bemüht, diesen Mangel zu beheben.

Wieweit es mit der Selbständigkeit der regionalen Auskunfteien als speichernden Stellen her ist, konnte ich aufgrund einer Mitteilung eines früheren Betreibers einer regionalen Auskunftei erahnen. Daraus entnahm ich, daß angeblich noch vor rechtsförmlicher Beendigung von dessen Mitgliedschaft in der Auskunfts-Gesellschaft Mitarbeiter der Zentrale in einer Nachtaktion aus den Räumen der regionalen Auskunftei die gesamten Archivunterlagen entwendet hatten. Es handelte sich ja um Eigentum der Zentrale!

Das rechtliche Chaos bei der genannten Auskunftei-Gesellschaft ist damit noch nicht komplett: Diese meinte nämlich, den Anforderungen des § 10 BDSG, der das automatisierte Abrufverfahren regelt, nicht entsprechen zu müssen, weil die zentrale elektronische Datenverarbeitung für die regionalen Auskunfteien bei einem Auftragnehmer (der Rechenzentrums- bzw. der Wirtschaftsinformationsgesellschaft) erfolge. Läge ein automatisiertes Abrufverfahren zwischen Auftragnehmer und Auftraggeber vor, so käme nicht § 10 BDSG, sondern nur die Regelung des § 11 BDSG, der die Datenverarbeitung im Auftrag regelt, zur Anwendung. § 10 BDSG verlangt mehr als § 11 BDSG. Er läßt ein automatisiertes Abrufverfahren nur nach angemessener Berücksichtigung der Betroffeneninteressen und nach genauer schriftlicher Festlegung des Übermittlungsverfahrens zu. Außerdem muß durch ein Stichprobenverfahren eine Kontrolle möglich sein. All das sollte für die automatisierten Abfragen durch die regionalen Auskunfteien beim gemeinsamen Rechenzentrum nicht gelten.

Ich stellte gegenüber dem für alle regionalen Auskunfteien zuständigen betrieblichen Datenschutzbeauftragten klar, daß § 10 BDSG anwendbar ist. Fragt die Auskunftei A automatisiert aus dem eigenen beim Auftragnehmer gespeicherten Bestand Daten ab, so gilt dies nicht als Abruf nach § 10 BDSG. Etwas anderes gilt jedoch, wenn eine andere regionale Auskunftei B beim gleichen (gemeinsamen) Auftragnehmer einen Abruf aus dem Datenbestand der Auskunftei A vornimmt. Und genau dies passiert laufend bei der genannten Auskunftei-Gesellschaft.

## 40. Finanzwirtschaft

### 40.1 Der gescheiterte Versuch einer datenschutzrechtlichen Ermittlung

Als ich Anfang 1994 eine Beschwerde der Stadt Langenhagen erhielt, daß Angaben aus einer vertraulichen Ratsdrucksache von einer Bank zu Versendung von Werbeschreiben benutzt worden seien, handelte es sich um eine Eingabe wie viele andere auch. Daß hieraus ein Konflikt entstehen würde, der letztlich die Justiz beschäftigen würde, war ihr nicht anzusehen.

In der vertraulichen Ratsdrucksache waren Bewerber für Baugrundstücke in einem neuen Wohngebiet aufgeführt. Die Bank schrieb diese mit dem Angebot für einen Beratungstermin zur Finanzierung von Wohneigentum an. Sieben der angeschriebenen Personen wandten sich empört an die Stadt und wollten wissen, wie die Information über ihre Grundstücksbewerbung an die Bank gelangt sei. Die Stadt erkundigte sich bei der Bank. Diese teilte der Stadt mit, die Namen der Bauwilligen stammten "von einem seriösen Partner". Es habe "keine Anzeichen für ein unseriöses Zustandekomen" der Liste gegeben. Über das Telefonbuch habe man den Namen Adressen zugeordnet, wodurch es in einem Fall zum Anschreiben eines Nicht-Bauinteressierten gekommen sei. In anderen Fällen sei es zu Gesprächsvereinbarungen gekommen, was den "beträchtlichen Informationsbedarf in puncto Eigenheim bestätigt" habe. Den Informanten wollte die Bank jedoch nicht nennen.

Aufklärungsversuche, auch in Form eines unangemeldeten Kontrollbesuchs, waren unergiebig. Meine Fragen und Bitten um Akteneinsicht blieben ohne Wirkung. Ich mußte daher ein Bußgeldverfahren wegen der Behinderung meiner Kontrolltätigkeit nach § 44 Abs. 1 Nr. 6 i.V.m. § 38 Abs. 3 und 4 BDSG einleiten. Im Rahmen des Bußgeldverfahrens erhielt ich erstmals eine einigermaßen substantiierte Darstellung des Vorganges:

"Ein(e) ehemalige(r) Mitarbeiter(in)" habe dem Vorstandsmitglied beiläufig eine Liste von Bauinteressenten angeboten. Wer die Quelle ist, wird bis heute verschwiegen. Die Liste, allerdings ohne Vornamen und Anschriften, sei in der Marketing-Abteilung über das Telefonbuch mit Adressen versehen worden. Die Adressen seien, nachdem die Briefe mit einer elektronischen Schreibmaschine geschrieben worden waren, sofort wieder gelöscht wor-

den. Die Schreibvorlage und die Briefkopien seien nach kurzer Zeit vernichtet worden, so daß es zu diesem Vorgang auch keinen Aktenrückhalt mehr gebe.

Die rechtliche Argumentation der Bank zur Abwehr meiner Aufklärungsversuche, die Liste mit der Überschrift "Bauinteressenten" enthalte mangels näherer Präzisierung der Personen keine personenbezogenen Daten, war abwegig. Für die Anwendung des Datenschutzesrechtes genügt, daß ein Personenbezug herstellbar ist, auch wenn dies einen gewissen Aufwand erfordert. Die Herstellung dieses Personenbezugs ist der Bank ja auch, abgesehen von einer Ausnahme, gelungen. Unergiebig war auch die Behauptung, die Bewerberliste habe unsensible Daten enthalten, da die Ratsdrucksache nicht als "geheim" eingestuft worden ist. Der Datenschutz ist unabhängig von derartigen Einstufungen zu beachten. Sollten die wegen der Aktenvernichtung nicht mehr überprüfbaren Angaben der Bank richtig sein, daß nämlich die beworbenen Adressen nicht automatisch, sondern manuell eingefügt wurden, so hat keine dateimäßige Datenverarbeitung vorgelegen. Um dies aber feststellen zu können, mußte mir die Bank nach § 38 Abs. 3 und 4 BDSG Auskunft erteilen. Hinreichenden Anhaltspunkte für einen Datenschutzverstoß lagen vor: Offensichtlich rechtswidrig war die auch bei der Stadt Langenhagen nicht mehr aufklärbare Übermittlung der Liste an die Bank. Daraus ergab sich der Verdacht, daß auch die Beschaffung der Daten durch die Bank sowie die spätere Speicherung und Nutzung rechtswidrig waren.

Nach § 38 Abs. 3 BDSG haben die meiner Prüfung unterliegenden Stellen auf Verlangen die zur Erfüllung meiner Aufgaben erforderlichen Auskünfte "unverzüglich" zu erteilen. Dieser Pflicht kann man sich nicht dadurch entziehen, daß unsubstantiiert behauptet wird, ich sei für die Datenschutzkontrolle gar nicht zuständig. Die Bank hat gegen den Bußgeldbescheid Einspruch eingelegt. Auch wenn dieses Verfahren einmal abgeschlossen sein wird: Meine Hoffnung, die undichte Stelle bei der Stadt Langenhagen sowie die Rechtmäßigkeit der Verarbeitung bei der Bank festzustellen, dürfte weiterhin vergeblich bleiben.

## 40.2 Inkassounternehmen

Wie beschränkt die Möglichkeiten der Datenschutzkontrolle sind, zeigte sich auch anläßlich einer Eingabe, in der sich ein Bürger über die Art und Weise beschwerte, wie eine als Inkassobüro tätige Rechtsanwaltskanzlei versuchte, Ausforschungen vorzunehmen. Zunächst wandte sich das Anwaltsbüro an die örtliche Postdienststelle mit der Anfrage nach der Richtigkeit der Adresse des betroffenen Bürgers, versehen mit dem Zusatz: "Wir bitten höflichst um Angabe des Vornamens der Ehefrau". Nach § 4 der Postdienst-Datenschutzverordnung darf die Bundespost einem Dritten auf Verlangen "zum Zweck des Postverkehrs" Auskunft darüber erteilen, ob die angegebene Postanschrift richtig ist. Eine Abfrage des Vornamens der Ehefrau ist von dieser Vorschrift nicht abgedeckt. Die Post verweigerte daher die Auskunft. Nach dieser gescheiterten Ausforschung wurde der Petent, so seine Angabe, von einem "Katholischen Bildungswerk Münsterland" angerufen

und um Auskünfte gebeten. Da er einen fingierten Anruf des Anwalts vermutete, rief er in dessen Büro zurück: "... und siehe da: dieselbe Stimme".

Auf diesen Sachverhalt angesprochen, meinte ein Anwalt der beteiligten Kanzlei: "Wenn ein Verstoß gegen den Datenschutz vorliegt, so ist dieser bei der Bundespost erfolgt, die meine entsprechende Anfrage nicht hätte beantworten dürfen". Die telefonische Ausforschung wurde vom Anwalt bestritten bzw. er teilte mit, er habe nicht feststellen können, wer die Anfrage durchgeführt haben soll. So ärgerlich diese Anwort auch war, für mich gab es keine weiteren Möglichkeiten, in dieser Angelegenheit etwas zu unternehmen.

## 41. Versicherungen

### 41.1 Das Ende des Gebäudeversicherungsmonopols

Im Rahmen der EG-Harmonisierung haben die öffentlichen Gebäudefeuerversicherungen ihr bisher bestehendes Monopol verloren und stehen ab 1. Juli 1994 im freien Wettbewerb in Konkurrenz zu anderen Anbietern. Schon ein Jahr vor diesem Termin gingen die Monopolversicherungen daran, durch Werbemaßnahmen ihren Kundenstamm zu sichern, indem mit den bisherigen Kundinnen und Kunden Vorverträge für die Zeit nach dem 1. Juli 1994 abgeschlossen wurden. Dabei wurden Außendienstvertreter eingesetzt, die auch für andere private Versicherungsverhältnisse warben. Um den Brandversicherungsschutz zu erhalten, mußten die Gebäudeeigentümer bisher umfangreiche und detaillierte Angaben über versicherte Grundstücke, Häuser und Wohnungen machen. Auf diese Weise erhielten die Brandkassen Kenntnis über den Wert des Anwesens sowie über die Wohnverhältnisse der einzelnen Bewohner, z.B. über die Ausstattung der Wohnungen. Die Eigentümer konnten sich darauf verlassen, daß diese sensitiven Daten nur zu dem angegebenen Zweck verwendet werden.

Es gibt keine ausdrückliche datenschutzrechtliche Regelung zu der Frage, inwieweit hoheitlich erlangte Daten weitergenutzt werden dürfen, wenn die verarbeitende Stelle ihre rechtlich gesicherte Monopolstellung verloren hat und mit anderen Unternehmen im Wettbewerb steht. Der Entwurf eines Gesetzes über die öffentlich-rechtlichen Versicherungsunternehmen in Niedersachsen (NöVersG) enthielt zwar hierzu Aussagen. Danach werden die Versicherungsverhältnisse, die in den jeweiligen Monopolbereichen begründet wurden, fortgesetzt. Die Monopolversicherungen sollten befugt sein, mit Wirkung vom 1. Juli 1994 an neue Versicherungsverträge abzuschließen. Dieses Gesetz war aber zur Zeit der Werbemaßnahmen noch nicht in Kraft. Da Gesetzentwürfe keine rechtliche Wirkung entfalten können, war der Entwurf für meine datenschutzrechtliche Bewertung ohne Bedeutung.

Im Hinblick auf diese rechtliche Lage hielt ich es für erforderlich, die Regelungen zur Übermittlung vom öffentlichen in den privaten Bereich entspre-

chend anzuwenden. Entsprechend § 13 Abs. 1 NDSG n.F. hielt ich danach eine Nutzung der Monopolversicherungsdaten zum Abschluß von Brandversicherungs-Folgeverträgen bzw. zur Fortführung der bisherigen Verträge unter Wettbewerbsbedingungen für zulässig, da die Brandkassen insofern zumindest ein berechtigtes Interesse an der Weiternutzung der Daten geltend machen können. Ich stellte jedoch klar, daß die Nutzung der genannten Daten für andere Zwecke, z.B. zur Anbahnung anderer Versicherungsverhältnisse oder zur Übermittlung an andere Unternehmen der eigenen Versicherungsgruppe unzulässig wäre.

Problematisch bleibt aber, daß Außendienstvertreter bei ihren Vertragsverhandlungen hinsichtlich anderer Versicherungsverhältnisse gar nicht umhin können, zumindest unbewußt ihre aus der Monopolversicherung bestehenden Kenntnisse für die Abschlüsse anderer privater Versicherungen zu nutzen. Da sich dieser Effekt in der Praxis kaum vermeiden läßt und mir offensichtliche zweckwidrige Verwendungen nicht vorgetragen wurden, sah ich keinen konkreten Anlaß für eine datenschutzrechtliche Beanstandung. Inzwischen ist das NöVersG in Kraft getreten (Nds. GVBl. 1994, S. 5 ff.).

## 41.2 Datenflüsse zwischen Versicherungen

Mir sind eine Reihe von Eingaben zugegangen, mit denen sich Versicherungsnehmer darüber beschwerten, daß Versichertendaten ohne ausdrückliche Einwilligung an eine andere Versicherung der Versicherungsgruppe weitergegeben wurden bzw. mehrere Versicherungen einen Zugriff auf die Daten hatten. Vielfach wurde als Begründung seitens der Versicherungsunternehmen angegeben, daß die Betreuung der Versicherten durch Versicherungsvertreter oder Außendienstmitarbeiter erfolgt, die für mehrere Versicherungen gleichzeitig tätig sind.

So wurde mir mitgeteilt, daß eine Landesbrandkasse Daten an eine öffentliche Versicherung übermittelt habe. Diese wiederum hätte die Daten einem selbständigen Handelsvertreter zur Verfügung gestellt. Die Landesbrandkasse hat dazu festgestellt, daß die Versichertendaten nicht an die andere Versicherungsgesellschaft (öffentliche Versicherung), sondern direkt an den Versicherungsvertreter übermittelt wurden. Voraussetzung für diese Übermittlung sei der Abschluß eines Vertretervertrages zwischen der Landesbrandkasse und dem Versicherungsvertreter. Dieser sei auf das Datengeheimnis verpflichtet worden.

Da das neue NDSG noch nicht in Kraft war, mußte ich die Rechtmäßigkeit der Übermittlung auf der Grundlage von § 15 Abs. 4 NDSG a.F. prüfen. Die Übermittlung war zulässig. Durch die Übermittlung sollte ermöglicht werden, den Versicherungsschutz im Bereich der Feuerversicherung zu prüfen und ggf. zu erweitern. Auch hatte die Versicherungsagentur ein berechtigtes Interesse an der Kenntnis der Daten. Schutzwürdige Belange des Betroffenen waren nicht beeinträchtigt. Der Petent war von der Landesbrandkasse über das Betreuungsverhältnis schriftlich informiert worden. Unter den ab 1. Juli 1994 geltenden Voraussetzungen war eine Übermittlung ausschließ-

lich auf der Grundlage des § 28 BDSG zu prüfen. Die Übermittlung war nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG "im Rahmen der Zweckbestimmung eines Vertragsverhältnisses" zulässig. Unabhängig davon hat die Landesbrandkasse gegenüber dem Betroffenen zugestanden, falls gewünscht, die Vertreterbetreuung bei seiner Feuerversicherung aufzuheben.

In einem anderen Fall hatte ein Versicherungsunternehmen die Versichertendaten an eine Tochtergesellschaft weitergegeben. Auf Anfrage hat das betroffenen Versicherungsunternehmen einen individuellen Bearbeitungsfehler eingestanden. Mir wurde mitgeteilt, daß künftig dafür Sorge getragen wird, daß derartige Datenschutzverstöße nicht mehr erfolgen. Zweifel an dem Bemühen um einen datenschutzgerechten Umgang mit Versichertendaten durch das Unternehmen konnte ich nicht äußern, zumal in einem detaillierten Merkblatt zur Datenverarbeitung eine ausführliche Kundeninformation erfolgte.

## 41.3 Ärger mit den Sachverständigen

Ein Wasserschaden im Eigenheim verursachte für die betroffenen Wohnungsbesitzer einige Probleme mit der zuständigen Hausrats- und Wohngebäudeversicherung. Diese hatte nämlich zur Begutachtung des entstandenen Versicherungsschadens einen öffentlich bestellten und vereidigten Sachverständigen eingeschaltet. Dieser wiederum hatte, da er sich aus terminlichen Gründen selbst zur Begutachtung nicht in der Lage sah, als Untergutachter eine Sanierungsfirma beauftragt. Diese führte die "Begutachtung" durch. Nach den Angaben der betroffenen Eheleute ging der Untergutachter wie selbstverständlich davon aus, daß er die Sanierung auch vornehmen werde. Außerdem schien ihnen die Höhe des durch die Sanierungsfirma veranschlagten Schadens völlig überzogen. Dies war aber nicht der Grund, weshalb sie sich an mich wandten. Sie beschwerten sich darüber, daß das Versicherungsunternehmen ihre Daten an die Sanierungsfirma übermittelt hatte.

So dubios der mir geschilderte Sachverhalt war, so wenig erhellend war zunächst die erste Stellungnahme der Versicherung. Es war von einer Unterlassungs- und Widerrufserklärung des Ehegatten die Rede. Anhand der mir schließlich vorgelegten Versicherungsbedingungen konnte ich feststellen, daß diese zumindest die Beauftragung des vereidigten Sachverständigen abdeckten. Es bedurfte keiner gesonderten Einwilligung durch die Versicherungsnehmer. Hinsichtlich der im Streit stehenden Unterbeauftragung mußte ich den Eheleuten mitteilen, daß ich insofern zur Aufklärung nicht ermächtigt bin, da sich meine Befugnisse als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich auf die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien beschränken (vgl. 34.2). Ich konnte die Petenten nur darauf hingeweisen, daß sie die Möglichkeit haben, die Rechtmäßigkeit der Unterbeauftragung von der für sie regional zuständigen Industrie- und Handelskammer überprüfen zu lassen. Die in diesem Zusammenhang maßgebliche Rechtsvorschrift ist die Sachverständigenordnung.

## 42. Vereine - Nichtmitglieder im Mitgliederverzeichnis

Aus dem Landesverband Niedersachsen einer bundesweiten Landsmannschaft wurde bei mir angefragt, ob es datenschutzrechtlich zulässig ist, die Mitgliederdaten an den Bundesverband zur Erstellung eines bundesweiten Mitgliederverzeichnisses zu übermitteln.

Die jüngst verabschiedete Benutzerordnung der Landsmannschaft, von der die zuvor eingetretenen Mitglieder teilweise keine Kenntnis hatten, regelt Umfang und Nutzung des Mitgliederverzeichnisses. Da Neuaufnahmen im Verband die Ausnahme sind, wissen daher nur wenige hierüber Bescheid. Meines Erachtens lagen die Voraussetzungen des § 28 BDSG für die Übermittlung hier nicht vor. Ich habe daher vorgeschlagen, die Einwilligung der betroffenen Mitglieder einzuholen.

Die Benutzerordnung der Vereinigung sah auch vor, daß Daten von deutschstämmigen Landsleuten gespeichert werden, die nicht Mitglied in der Landsmannschaft sind. Dies halte ich nicht für zulässig. Da die Landsmannschaft auf Bundesebene ihren Vereinssitz nicht in meinem Zuständigkeitsbereich hat, habe ich die zuständige Aufsichtsbehörde von dem vorstehenden Sachverhalt in Kenntnis gesetzt.

## 43. Privates Gesundheitswesen

### 43.1 Veräußerung der Arztpraxis - Verbleib der Patientenunterlagen

Der Bundesgerichtshof (BGH) hat mit Urteil vom 11. Dezember 1991 folgende Entscheidung getroffen (NJW 1992, 737):

> "Eine Bestimmung in einem Vertrag über die Veräußerung einer Arztpraxis, die den Veräußerer auch ohne Einwilligung der betroffenen Patienten verpflichtet, die Patienten- und Beratungskartei zu übergeben, verletzt das informationelle Selbstbestimmungsrecht der Patienten und die ärztliche
> Schweigepflicht (Art. 2 Abs. 1 GG, § 203 StGB)...".

In der Entscheidung hat das oberste deutsche Zivilgericht außerdem festgestellt, daß Hinweise auf einen möglichen Arztwechsel in den Wartezimmern sowie Anzeigen in der örtlichen Presse dem Einwilligungserfordernis nicht genügen. Erst ein eindeutiges schlüssiges Verhalten, z.B. durch Aufsuchen der Sprechstunde des Praxisübernehmers könne als Einverständnis angesehen werden, daß sich der Praxisübernehmer die Unterlagen vom Vorgänger beschafft. Bis zur Behandlung durch den Nachfolger muß die Patientenkartei grundsätzlich beim früheren Praxisinhaber verbleiben.Praktische Schwierigkeiten könnten dadurch vermieden werden, daß die Praxisüberge-

ber oder die ärztliche Standesorganisation Vorsorge für die leicht erreichbare Aufbewahrung solcher Unterlagen treffen.

Bei einer Praxisauflösung hat der Arzt bzw. dessen Erbe die Patientenunterlagen "in gehörige Obhut" (§ 11 Abs. 4 der Berufsordnung der Ärztekammer Niedersachsen) - etwa bei der Ärztekammer - zu geben. Die Ärztekammer Niedersachsen hat nun dem Urteil des BGH insofern Rechnung getragen, als sie ihre Berufsordnung durch folgende Regelung ergänzt hat: "Der Arzt, dem bei einer Praxisaufgabe oder Praxisübergabe ärztliche Aufzeichnungen über Patienten in Obhut gegeben werden, muß diese Aufzeichnungen unter Verschluß halten und darf sie nur mit Einwilligung des Patienten einsehen oder weitergeben."

Demgegenüber hat mir die Zahnärztekammer Niedersachsen mitgeteilt, daß dort kein entsprechender Beschluß geplant ist. Man sehe erhebliche praktische Probleme z.B. bei Tod oder Konkurs des Zahnarztes bzw. der Zahnärztin. Die Verwahrung der ärztlichen Unterlagen in den Diensträumen der Kammer entspreche nicht unbedingt den Patienteninteressen. So werde z.B. das spätere Auffinden von Unterlagen erschwert. Auch der Zahnärztekammer ist jedoch bewußt, daß die Nutzung von Patientenunterlagen nur nach vorheriger Einwilligung erfolgen darf. Sie will daher streng zwischen Verwahrung der Unterlagen und Verwertung der Unterlagen unterscheiden. Ich gehe, solange ich nichts Gegenteiliges feststelle, davon aus, daß auch in der Zahnärzteschaft die Rechtsprechung des BGH beachtet wird.

43.2 Keine Benachrichtigung der Notärzte

Aus den Reihen der Notärzteschaft wurde bei mir angefragt, ob es zulässig ist, ihnen die Kopien der Entlassungsberichte der per Notfall in Kliniken eingelieferten Patientinnen und Patienten zur Verfügung zu stellen. Den Notärztinnen und Notärzten soll damit die Möglichkeit gegeben werden, ihren Notfalleinsatz zu überprüfen und sich fortzubilden. In Einzelfällen könnten die Informationen hilfreich sein, um bei einem späteren Notfall der gleichen Person eine adäquate Behandlung durchzuführen. Ich mußte dem anfragenden Arzt mitteilen, daß eine Unterrichtung vorbehandelnder Ärztinnen und Ärzte unproblematisch ist, wenn diese von der Patientin bzw. dem Patienten frei gewählt worden sind. Auch § 2 Abs. 6 der Berufsordnung der Ärztekammer Niedersachsen geht hier von einer konkludenten Einwilligung aus, wenn kein ausdrücklicher Widerspruch erklärt wurde. Bei Notärztinnen und Notärzten liegt der Fall jedoch anders. Da der Patientin bzw. dem Patienten hier keine freie Arztwahl möglich war, bedarf es zur Übermittlung der Entlassungsberichte der Einwilligung. Denkbar ist, daß im Aufnahmevertrag mit der Klinik eine Einwilligungserklärung aufgenommen wird. Den Betroffenen muß jedoch im Aufnahmevertrag die Wahlmöglichkeit eingeräumt werden, ob eine Übermittlung an die Notärztin bzw. den Notarzt gewollt wird oder nicht.

## Anlagen

## Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

### Anlage 1

### Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. Februar 1993 zur Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (30/313/EWG)

Im Interesse eines wirksamen Umweltschutzes hat der Ministerrat der Europäischen Gemeinschaft die Umweltinformationsrichtlinie erlassen, die jedem Bürger ein Recht auf Zugang zu den bei Behörden vorhandenen Informationen über die Umwelt gewährt. Da es nicht gelungen ist, die Richtlinie innerhalb der vorgegebenen Frist bis Ende 1992 in deutsches Recht umzusetzen, herrscht gegenwärtig Rechtsunsicherheit bei Bürgern und Behörden über den Zugang zu Umweltinformationen.

Die Konferenz der Datenschutzbeauftragten sieht in der Gewährleistung eines freien Zugangs zu Umweltinformationen einen wesentlichen Beitrag zu größerer Transparenz des Verwaltungshandelns. Informationsfreiheit und Datenschutz bilden dabei keinen unlösbaren Gegensatz. Die Konferenz hält es für geboten, die Arbeit am Entwurf des Umweltinformationsgesetzes (UIG) zügig zum Abschluß zu bringen. Sie begrüßt entsprechende Initiativen auf Landesebene.

In den Gesetzen sind folgende datenschutzrechtliche Grundsätze zu berücksichtigen:

Soweit Umweltinformationen auf Personen beziehbar sind, ist das Grundrecht auf informationelle Selbstbestimmung zu beachten. Deshalb sind Informationen grundsätzlich in anonymisierter oder aggregierter Form zu geben. Wenn damit das Informationsinteresse nicht erfüllt werden kann, sind Eingriffe in das Persönlichkeitsrecht nur unter klaren gesetzlichen Voraussetzungen zulässig, welche die Rechte, insbesondere die Verfahrensrechte, der Betroffenen wahren.

### Anlage 2

### Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 15. April 1993 zum Entwurf eines Gesetzes zur Umsetzung des Föderalen Konsolidierungsprogramms - FKPG - (Bundesrats-Drucksache 121/93 vom 5. März 1993)

Der Gesetzentwurf sieht Regelungen vor, die eine mißbräuchliche Inanspruchnahme von Sozialleistungen verhindern sollen und von erheblicher datenschutzrechtlicher Bedeutung sind.

Über die bisher gesetzlich vorgesehene Einzelfallprüfung hinaus würde durch den Gesetzentwurf ermöglicht, daß insbesondere die Daten aller Sozialhilfeempfänger, also auch derjenigen, bei denen kein Anhaltspunkt für falsche Angaben oder Verletzungen von Mitteilungspflichten besteht, ohne weiteres pauschal mit den Datenbeständen der Renten- und der Arbeitslosenversicherung abgeglichen werden. Darüber hinaus soll nach dem Regierungsentwurf der Online-Abruf von Daten aus einer unbegrenzten Vielzahl von Dateien anderer Verwaltungsbereiche ohne Rücksicht auf die jeweilige Sensibilität dieser Daten möglich sein.

Im Bereich der Arbeitslosenversicherung soll die erst zum 1. Januar 1993 in Kraft getretene, datenschutzgerechte Vorschrift über die Erhebung von Daten bei Außenprüfungen ohne erkennbaren sachlichen Grund durch eine Vorschrift ersetzt werden, die wichtige Grundsätze des Persönlichkeitsschutzes nicht berücksichtigt.

Im einzelnen weisen die Datenschutzbeauftragten - unter Einbeziehung der Empfehlungen der Ausschüsse des Bundesrats vom 8. April 1993, Drs. 121/2/93 - auf folgendes hin:

Artikel 9 Nr. 29 (§ 117 Bundessozialhilfegesetz - BSHG -)

1. § 117 Abs. 1 BSHG
   Nach der Begründung zu § 117 Abs. 1 BSHG (Regierungsentwurf) - allerdings nicht nach dem Wortlaut der Vorschrift - soll der Leistungsmißbrauch über einen Datenabgleich mit der Bundesanstalt für Arbeit (BA) und der gesetzlichen Rentenversicherung aufgedeckt werden. Irgendein Anlaß für diesen Datenabgleich muß nicht gegeben sein. Ein solches, die Glaubwürdigkeit aller Sozialhilfeempfänger in Zweifel ziehendes Vorgehen ist allenfalls dann verhältnismäßig und damit vertretbar, wenn verifizierbare Erkenntnisse darüber vorliegen, daß ein erheblicher Anteil der Sozialhilfeempfänger der schon jetzt bestehenden Verpflichtung, den Sozialhilfeträgern Leistungen der BA und das Eingehen von Beschäftigungsverhältnissen mitzuteilen, nicht nachkommt. Der Gesetzesbegründung lassen sich solche Feststellungen nicht entnehmen.

   Die Zwecktauglichkeit dieses Abgleichs erscheint zudem zweifelhaft, da etwa Nebeneinkünfte von Sozialhilfeempfängern, für die keine Sozialabgaben entrichtet werden, auch der Sozialversicherung nicht bekannt sind.

   Die Ausschüsse des Bundesrates haben nunmehr empfohlen, von dem pauschalen Datenabgleich abzusehen sowie eine Zweckbindungs- und eine Löschungsregelung einzuführen. Die Datenschutzbeauftragten begrüßen diese Empfehlung.

2. § 117 Abs. 2 BSHG
   Die Bundesratsausschüsse haben empfohlen, § 117 Abs. 2 BSHG des Regierungsentwurfs, insbesondere wegen der Unklarheiten des Gesetzestextes, zu streichen. In der Begründung verweisen sie auf die Regelungen

von Datenübermittlungen aus anderen Verwaltungsbereichen in den jeweiligen bereichsspezifischen Vorschriften.

Die Datenschutzbeauftragten begrüßen die Empfehlungen der Bundesratsausschüsse schon wegen der fehlenden Normenklarheit des Regierungsentwurfs.

Artikel 13 Nr. 20 (§§ 150 a und 150 b Arbeitsförderungsgesetz - AFG -)

a) Es ist unverständlich, daß die Neuregelung der §§ 19 a und 132 a Abs. 1 a AFG, die erst am 1. Januar 1993 in Kraft getreten sind, schon wenige Monate danach wieder aufgehoben und durch neue Regelungen ersetzt werden sollen. Gegen eine solche Notwendigkeit spricht auch die einschlägige Presseinformation der BA vom 18. März 1993, in der betont wird,
"... die von Jahr zu Jahr zunehmende Zahl der aufgedeckten Verstöße zeige, daß das rechtliche und administrative Instrumentarium immer besser greife."

b) Entgegen der in den §§ 19 a und132 a Abs. 1 a AFG enthaltenen Regelungen sieht § 150 a AFG keinen Datenkatalog dahingehend mehr vor, welche Daten im Rahmen der Prüfungen zulässigerweise erhoben werden können. Weil in den in § 150 a AFG zu regelnden Fällen Unverdächtige in den Datenabgleich einbezogen werden, ist es erforderlich, den Eingriff auf das unbedingt notwendige Maß zu beschränken. Dazu ist weiterhin erforderlich, daß im ersten Schritt nur die hierfür unbedingt notwendigen Daten abgeglichen werden. Der Datenkatalog ist umso dringender, als die neue Vorschrift über Außenprüfungen nach § 150 a AFG eine Erweiterung gegenüber den bisherigen Vorschriften bringt.

c) Es ist ferner unerläßlich, daß die erhobenen Daten auch weiterhin der derzeit in § 132 a Abs. 1 a Satz 3 AFG normierten Zweckbindung unterliegen.

d) § 150 a Abs. 5 AFG erweitert die nach dem geltenden Recht bestehende Auskunftspflicht von Arbeitgeber und Arbeitnehmer auf jedermann. Dies erscheint überzogen, nachdem im Bereich der Datenerhebung für Steuerzwecke eine Auskunftspflicht Dritter nur besteht, "wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht" (§ 93 Abs. 1 AO).

Anlage 3

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ)**

- gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens -

Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung aus folgenden Gründen ab:

Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. Über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.

Anlage 4

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zum Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste**

Im Zuge der sogenannten Postreform II soll die Deutsche Bundespost Telekom - nach der dafür notwendigen Änderung des Grundgesetzes - in Form einer Aktiengesellschaft privatisiert werden. Zugleich hat der Ministerrat der Europäischen Gemeinschaften in seiner Entschließung vom 22. Juli 1993 (Amtsblatt der EG Nr. C 213 vom 06.08.1993) seine Entschlossenheit

bekräftigt, die Monopole im öffentlichen Sprachtelefondienst (Festnetz) der Mitgliedstaaten bis zum 1. Januar 1998 zu beseitigen.

In absehbarer Zeit werden daher in Deutschland neben der "Telekom AG" auch im Telefondienst andere private Unternehmen Telekommunikationsdienstleistungen anbieten. Diese Privatisierung hat Konsequenzen für den Datenschutz, der bisher für die Deutsche Bundespost Telekom auf einem vergleichsweise hohen Niveau geregelt ist. Insbesondere das grundgesetzlich garantierte Fernmeldegeheimnis würde für private Netzbetreiber und Diensteanbieter jedenfalls nicht mehr unmittelbar gelten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für unabdingbar, daß durch die Privatisierung und Liberalisierung der Schutz der Bürger insbesondere in solchen Bereichen nicht verringert wird, die - wie der Telefondienst - der Daseinsvorsorge zuzurechnen sind. So wie bisher die konkurrierenden privaten Betreiber der Mobilfunknetze einen gleichmäßig hohen Datenschutzstandard gewährleisten müssen, hat dies auch zu gelten, wenn in Zukunft private Unternehmen im Wettbewerb miteinander stationäre Telefonnetze betreiben und entsprechende Dienste anbieten. Die Einhaltung von datenschutzrechtlichen Bestimmungen bei Telekommunikationsnetzen und -diensten muß zukünftig von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien und von Amts wegen kontrolliert werden können.

Da der Wettbewerb zwischen privaten Netzbetreibern und Diensteanbietern nicht nur national begrenzt, sondern im europäischen Binnenmarkt stattfinden wird, sind auch Rechtsvorschriften der Europäischen Gemeinschaften erforderlich, die einen möglichst hohen, einheitlichen Datenschutzstandard in der Telekommunikation gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

**Anlage 5**

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zur Gewährleistung des Datenschutzes bei Mobilkommunikation**

Die Verbreitung mobiler Sprach- und Datenübertragungsdienste hat in jüngster Vergangenheit stark zugenommen. So gibt es bereits jetzt in Deutschland mehr als eine Million Teilnehmer der Funktelefonnetze C und D; mit der Aufnahme des Regelbetriebs von MODACOM ist seit Juni dieses Jahres auch ein öffentlicher mobiler Datenübertragungsdienst in Deutschland verfügbar. Es ist zu erwarten, daß sich die Teilnehmerzahl mobiler Kommunikationsdienste in Zukunft weiter vergrößern wird.

Die mit der Nutzung von Mobilfunkdiensten verbundenen Vorteile gehen mit Gefährdungen für den Datenschutz einher. Neben den auch bei anderen Te-

lekommunikationsdiensten gespeicherten Angaben, wer wann mit wem in Verbindung war, wird bei der Mobilkommunikation auch erhoben, wo sich der mobile Teilnehmer jeweils aufhält. Die Speicherung dieser Daten ermöglicht die Bildung von problematischen Bewegungsprofilen.

Darüber hinaus ist vielfach auch die Vertraulichkeit der Kommunikationsinhalte gefährdet, insbesondere dann, wenn Daten unverschlüsselt per Funk übertragen werden. Dies gilt sowohl für die analogen Funktelefon-Netze B und C als auch für den von der Deutschen Bundespost Telekom betriebenen mobilen Datenübertragungsdienst MODACOM. Bei satellitengestützten Diensten ist es sogar möglich, die übertragenen Daten im gesamten, teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich des Satelliten unbemerkt abzuhören und aufzuzeichnen.

Von den Herstellern und Betreibern mobiler Kommunikationsdienste ist zu fordern, daß sie diesen Gefahren für das Fernmeldegeheimnis und für den Datenschutz durch eine entsprechende Gestaltung entgegenwirken und technische Vorkehrungen für eine sichere Kommunikation treffen.

Die Teilnehmer mobiler Kommunikationsdienste müssen von den Anbietern, Herstellern und Betreibern über die mit der Nutzung verbundenen Risiken und das erreichte Sicherheitsniveau aufgeklärt werden. Sofern bei bestimmten Diensten Sicherheitsmerkmale realisiert sind - wie z.B. in den digitalen D-Netzen -, muß die Sicherheit für die Aufsichts- und Kontrollorgane auch nachprüfbar sein. Falls durch den Dienstbetreiber nicht die erforderliche Sicherheit gewährleistet werden kann, ist eine Übertragung personenbezogener oder sonstiger sensibler Daten mit dem jeweiligen Dienst nur dann vertretbar, wenn der Benutzer zusätzliche Sicherheitsvorkehrungen trifft, also z.B. die übertragenen Daten anwendungsseitig verschlüsselt.

Zusätzlich kompliziert wird die Datenschutzproblematik bei der Mobilkommunikation dadurch, daß unter Umständen bei verschiedenen Dienst- und Netzbetreibern, aber auch bei anderen Unternehmen - den sogenannten Service-Providern, die lediglich Dienste vermarkten -, personenbezogene Daten gespeichert werden.

Hier muß im Zuge der anstehenden Überarbeitung des Telekommunikationsrechts dafür Sorge getragen werden, daß sich die Verarbeitung der Kommunikationsdaten auf das wirklich erforderliche Maß beschränkt und daß die Nutzer darüber aufgeklärt werden, bei welcher Stelle welche personenbezogenen Daten gespeichert oder sonst verarbeitet werden.

Besonders problematisch ist es, wenn bei der internationalen Mobilkommunikation auch in solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen das Fernmeldegeheimnis nicht sichergestellt wird. Deshalb ist es erforderlich, auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei mobilen Kommunikationsdiensten gewährleisten.

Die Konferenz unterstreicht aus diesem Grunde ihre Forderung, die Arbeiten an der EG-Richtlinie über Datenschutz im ISDN und in öffentlichen digitalen Mobilfunknetzen zu einem datenschutzrechtlich befriedigenden Abschluß zu bringen. Auch für den noch gänzlich datenschutzrechtlich ungeregelten Bereich der Satellitenkommunikation müssen endlich völkerrechtlich verbindliche Regelungen getroffen werden.

**Anlage 6**

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zur Gefährdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten**

Durch die Aufhebung der bisher gültigen Beschränkungen der zulässigen Empfangsbereiche für Rundfunkempfänger zum 30. Juni 1992 werden zunehmend Empfangsgeräte betrieben, die das Abhören des Funkverkehrs ermöglichen. Dies stellt eine erhebliche Bedrohnung des Fernmeldegeheimnisses dar.

Die Datenschutzbeauftragten des Bundes und der Länder beobachten die damit verbundene Gefährdung der Vertraulichkeit der Funkkommunikation von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) mit Sorge. Sie erkennen die Bemühungen der Polizeiverwaltungen der Länder an, durch zusätzliche technische Maßnahmen die Sicherheit des Sprechfunkverkehrs zu erhöhen. Sie stellen jedoch fest, daß die erforderliche Vertraulichkeit bisher nicht gewährleistet werden konnte. Auch Sprachverschleierungssysteme erreichen diese nicht hinreichend.

Daher begrüßt die Konferenz die im Rahmen des Schengener Abkommens getroffene grundsätzliche Entscheidung, im BOS-Bereich eine europäische Normierung zu erarbeiten, die die Digitalisierung und eine Verschlüsselung des BOS-Funkverkehrs vorsieht.

Die Konferenz hält es für erforderlich, daß das Normierungsverfahren so zügig wie möglich durchgeführt wird und auch schon vor der Umsetzung dieser Norm alle Möglichkeiten für einen effektiven Schutz der Vertraulichkeit des BOS-Funkverkehrs entsprechend dem jeweiligen Stand der Technik genutzt werden.

Die Konferenz weist weiter darauf hin, daß nicht nur bei den Behörden der Polizei, sondern auch in anderen BOS-Bereichen, wie z.B. dem Rettungswesen, eine Vertraulichkeit des Funkverkehrs zu gewährleisten ist. Daher sind auch in den übrigen BOS-Bereichen frühestmöglich entsprechende Absicherungen zur Vertraulichkeit des Funkverkehrs gefordert.

**Anlage 7**

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zu kartengestützten Zahlungssystemen im öffentlichen Nahverkehr**

Mit der Weiterentwicklung von Chipkarten werden kartengestützte Zahlungssysteme zunehmend auch im Verkehrsbereich eingesetzt. Damit besteht die Gefahr, daß sehr detaillierte Bewegungsprofile entstehen, die den persönlichen Bereich jedes einzelnen einschränken und z.B. auch für Strafverfolgungsbehörden, Finanzämter und für die Werbewirtschaft von Interesse sein könnten. Da sämtliche Fahrten für einen gewissen Zeitraum aufgelistet werden können, hat jeder Kontoinhaber die Möglichkeit, Fahrten sämtlicher Familienmitglieder jederzeit nachzuvollziehen.

So sind im öffentlichen Nahverkehr zahlreiche sogenannte Postpaid-Verfahren in Erprobung, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden. Diese Zahlungsweise erfordert die Speicherung umfangreicher personenbezogener Daten: Neben der Konto-Nr. und Bankleitzahl des Fahrgastes werden sowohl Datum und Uhrzeit des Fahrscheinkaufs bzw. des Fahrantritts als auch Automatennummer und Preisstufe der jeweiligen Fahrt erhoben.

Ein solche Vorgehensweise ist um so problematischer, als technische Alternativen existieren, die weitaus datenschutzfreundlicher sind. Im öffentlichen Nahverkehr können - wie skandinavische und auch deutsche Projekte aufzeigen - Wertkartensysteme eingesetzt werden, bei denen im voraus bezahlt wird und die daher gänzlich ohne personenbezogene Daten auskommen.

Die Datenschutzbeauftragten halten es daher für dringend erforderlich, daß mehr als bisher bei der Einführung kartengestützter Zahlungssysteme darauf geachtet wird, die "datenfreie Fahrt" zu ermöglichen. Im öffentlichen Nahverkehr sollte weiterhin auch die datenschutzfreundlichste Lösung angeboten werden: Der Kauf einer Fahrkarte am Automaten mit Bargeld.

Die Konferenz fordert weiter, daß noch vor der Pilotierung der dargestellten Technikvorhaben im Verkehrsbereich eine Untersuchung möglicher Alternativen, eine Analayse der von ihnen ausgehenden Gefahren für das informationelle Selbstbestimmungsrecht und eine Darstellung der technischen und organisatorischen Möglichkeiten zur Gewährleistung des Persönlichkeitsschutzes zu erstellen ist (Technikfolgen-Abschätzung). Nur Verfahren mit dem geringsten Eingriff in das allgemeine Persönlichkeitsrecht sollten eine Chance zur Erprobung erhalten.

**Anlage 8**

## Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zum Integrierten Verwaltungs- und Kontrollsystem (InVeKoS) (Verordnungen der EWG Nrn. 3508/92 und 3887/92)

Die vom Ministerrat der EG 1992 beschlossene Reform der gemeinsamen Agrarpolitik sieht die Angleichung der gemeinschaftlichen Preise für bestimmte Kulturpflanzen an den Weltmarkt vor und gewährt auf Antrag als Ausgleich für die dadurch bedingten Einkommenseinbußen flächen- und tierbezogene Zuwendungen an die Erzeuger. Zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln hat die EG die Mitgliedsstaaten dabei zur Einführung eines "Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)" verpflichtet. Diese haben danach integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder hat die EG mit dem "Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, widersprechen kann. Insbesondere legt das EG-Recht für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenzen fest.

Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte fordern daher die Datenschutzbeauftragten des Bundes und der Länder:

- ortsunabhängige Überwachungsmöglichkeiten (Fernerkundung mittels Satellit oder Flugzeug) nicht für eine flächendeckende Totalüberwachung einzusetzen, sondern auf den von der EG geforderten Stichprobenumfang zu beschränken;

- bei der Nutzung des Kontrollsystems InVeKoS und der darin gespeicherten personenbezogenen Daten den Grundsatz der Verhältnismäßigkeit und insbesondere der Zweckbindung zu beachten;

- nur dezentrale Datenbanken in den einzelnen Bundesländern einzurichten (keine Euro- oder Zentraldatenbank über Landwirte!) und an zentrale Datenbanken keine personenbezogenen Daten zu übermitteln;

- zu beachten, daß die EG-Verordnungen zu InVeKoS keine Rechtsgrundlage für eine Erweiterung der Nutzungen enthalten (z.B. zu Kontrollzwecken bei anderen landwirtschaftlichen Förderungsmaßnahmen oder außerhalb des landwirtschaftlichen Bereichs, z.B. zur Besteuerung).

**Anlage 9**

**Konferenz vom 9./10. März1994 in Potsdam**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat - bei Stimmenthaltung Bayerns und in Abwesenheit Baden-Württembergs - die folgende Bestandsaufnahme über die Situation des Datenschutzes "10 Jahre nach dem Volkszählungsurteil" zustimmend zur Kenntnis genommen.

Nach Ablauf von über 10 Jahren seit der Verkündung des Urteils des Bundesverfassungsgerichtes zum Volkszählungsgesetz am 15. Dezember 1983 sieht sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder veranlaßt, eine Bestandsaufnahme der Situation vorzulegen, in der sich der Datenschutz derzeit befindet.

Entwicklung nach dem Volkszählungsurteil:

Bereits unmittelbar nach Inkrafttreten der Datenschutzgesetze in Bund und Ländern war die Frage heftig diskutiert worden, welchen Rang der Datenschutz gegenüber anderen Rechtsgütern habe. Befürwortern der Auffassung, dem Datenschutz komme Grundrechtsqualität zu, standen zurückhaltendere Stimmen gegenüber, die die Subsidiarität des Datenschutzes betonten.

Das Volkszählungsurteil hat den Datenschutz zu einer elementaren Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens erklärt und den Grundrechtscharakter der informationellen Selbstbestimmung festgeschrieben. Dieses Grundrecht gewährleistet die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Damit wurde klargestellt, daß der Datenschutz unter den Bedingungen der modernen Datenverarbeitung das zentrale Mittel zur Gestaltung der Informationsbeziehungen zwischen den einzelnen und den Institutionen in Staat und Gesellschaft ist. Das Bundesverfassungsgericht hat seine Grundposition in der Zwischenzeit in einer Reihe weiterer Urteile eindrucksvoll bestätigt.

Danach ist von dem verfassungsrechtlichen Grundsatz auszugehen, daß die Entscheidung über die Preisgabe und Verwendung personenbezogener Daten zuallererst beim Betroffenen selbst liegt. Einschränkungen der individuellen Dispositionsfreiheit sind für die Rechts- und Gesellschaftsordnung von so wesentlicher Bedeutung, daß sie nur auf einer gesetzlichen Grundlage zulässig sind. Wie mit personenbezogenen Daten umzugehen ist, darf weder administrativer Zweckmäßigkeit noch dem Markt überlassen bleiben, sondern ist im Gesetzgebungsverfahren, d.h. vor den Augen der Öffentlichkeit zu entscheiden.

Bei der Regelung des Informationsumgangs ist von den individuellen Freiheitsrechten auszugehen; doch darf und muß der Gesetzgeber selbstverständlich berücksichtigen, daß der einzelne in vielfältiger Weise auf den

Schutz und die Hilfe des Staates angewiesen ist und daß die Tätigkeit des Staates kontrollierbar sein muß. In gesetzlich klar vorgegebenen Fällen ist daher die Verwendung personenbezogener Daten auch ohne selbstbestimmte Mitwirkung des Betroffenen erforderlich.

Das Grundrechtsverständnis mit der Selbstbestimmung des Bürgers als Regelfall und ihre Einschränkung als Ausnahme ist allerdings keineswegs von allen Seiten als Selbstverständlichkeit akzeptiert worden: Nach 10 Jahren ist eine positive, aber auch eine kritische Bilanz zu ziehen.

Nach der Entscheidung des Bundesverfassungsgerichts sind, wenn auch in vielen Fällen in langwierigen Verfahren, viele gesetzgeberische Aktivitäten entfaltet worden. Dabei mußte mancher datenschutzrechtliche Fortschritt hart umkämpft werden.

Neben einer grundlegenden Novellierung der Datenschutzgesetze in Bund und Ländern wurden Spezialbestimmungen in zahlreichen Sondermaterien geschaffen. Auf der Ebene des Bundes zählen dazu:

- einzelne Bücher des Sozialgesetzbuches,
- das Personalaktenrecht für Beamte,
- das Straßenverkehrsrecht,
- die Gesetze über die Nachrichtendienste des Bundes,
- das Telekommunikationsrecht.

Besonderer Handlungsbedarf für die Verwirklichung der informationellen Selbstbestimmung entstand durch die deutsche Einigung. Dabei stellt die Aufarbeitung der Hinterlassenschaft des Staatssicherheitsdienstes der ehemaligen DDR auch für den Datenschutz eine besondere Herausforderung dar.

Noch weitergehend ist der Umfang der datenschutzrechtlichen Neuregelungen in den Ländern, in denen die Vorgaben des Bundesverfassungsgerichtes teilweise konsequenter umgesetzt wurden als im Bund.

Diese Verrechtlichungswelle hat auch Kritik hervorgerufen:

In Dutzenden von Gesetzen ist nunmehr das "Kleingedruckte" des Rechts auf informationelle Selbstbestimmung bereichsspezifisch geregelt. Das so entstandene Normengeflecht ist engmaschig und kompliziert. Dies steht der Intention des Verfassungsgerichtes, der Bürger solle bereits aus normenklaren Gründen erkennen können, mit welcher Verarbeitung seiner Daten er zu rechnen hat, gelegentlich bereits entgegen. Eine weitergehende Kritik stellt in Frage, ob diese Normenflut mit ihren perfektionistischen und detaillistischen Regelungen der Verwirklichung des Grundsatzes der Verhältnismäßigkeit dient und notwendig war. Geäußert wurde auch die Annahme, daß die Effizienz der staatlichen Verwaltung bei der Bewältigung ihrer Aufgaben unter der Last perfektionistischer detaillistischer Regelungen gelitten habe und daß die Kreativität der Gesellschaft und ihre Fähigkeit zur Anpas-

sung und Bewältigung der gegenwärtigen Herausforderungen durch enge, starre Gesetze behindert würden.

Dem muß allerdings entgegen gehalten werden, daß die Fülle und Kompliziertheit der Datenverarbeitung in den verschiedensten Verwaltungsbereichen für die Regelungsdichte verantwortlich ist. Sie ist eine Konsequenz des Umstands, daß in allen Verwaltungsbereichen der - zunehmend automatisierten - Informationsverarbeitung immer mehr Bedeutung zukommt: Eine notwendige Folge der Entwicklung hin zur "Informationsgesellschaft".

Ein weiterer Grund für die Komplexität der Gesetzgebung liegt darin, daß die Gesetze häufig nicht darauf abzielen, die Rechtsposition des Bürgers zu stärken, sondern vielmehr Verarbeitung personenbezogener Daten zu ermöglichen, oft über das Maß hinaus, das bislang zulässig war. Viele Vorschriften sind so derart allgemein und umfassend zugunsten der Eingrifffsseite formuliert, daß es schwerfällt, sie als "Datenschutzgesetze" im eigentlichen Sinn zu verstehen. Wann immer Verwaltungen sich durch den Datenschutz behindert glaubten, ertönte der Ruf nach dem Gesetzgeber, der - zugunsten der Verwaltung - korrigierend eingreifen soll.

Trotz alledem blieb der Datenschutz in wesentlichen Bereichen ungeregelt. Auf Bundesebene gibt es z.B. bis heute keine hinreichenden datenschutzrechtlichen Vorschriften auf den Gebieten des Arbeitnehmerdatenschutzes, der Justizmitteilungen und der Zwangsvollstreckung, des Abgabenrechts, des Mieterschutzes, der Arbeit von Auskunfteien, Detekteien und privaten Sicherheitsdiensten, der Bundespolizeibehörden, des Ausländerzentralregisters oder - am gravierendsten - des gesamten Strafverfahrens.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, diese Lücken umgehend und im Sinne der informationellen Selbstbestimmung zu schließen.

Zur aktuellen Situation:

Die derzeitige Situation des Datenschutzes wird von den beiden großen Themenbereichen geprägt, die die Innenpolitik beherrschen: Die innere Sicherheit und der Zustand unserer Wirtschafts- und Sozialordnung. Diese Felder ängstigen die Menschen und stärken die Kontrollbedürfnisse des Staates. Auf beiden Gebieten wird die vermeintliche Lösung darin gesucht, daß die gesetzlichen Möglichkeiten zur Verarbeitung personenbezogener Daten erheblich ausgeweitet und auf der anderen Seite die Rechte der Bürger entsprechend eingeschränkt werden.

Auf dem Gebiet der Strafverfolgung haben sich bisher die Ermittlungen auf den Beschuldigten konzentriert und die prozessuale Aufklärung geschah im wesentlichen offen.

Jetzt setzt man auf Heimlichkeit und interessiert sich für Unbeteiligte. Ermittlungsverfahren ist nicht mehr Aufklärung eines konkreten Tatverdachts, sondern flächendeckende Sammlung personenbezogener Daten. Der Staat

hält sich nicht mehr an die Grenzen der Ausforschung, die selbstverständlich waren, und er trifft dabei auf breite öffentliche Zustimmung.

Im Bereich der Wirtschafts- und Sozialordnung wird auf besonders drastische Weise versucht, durch die Einführung neuer Überwachungsverfahren eine Kostenminderung zu erreichen. Die Daten werden einerseits genutzt, durch Plafondierungen und Wirtschaftlichkeitsuntersuchungen eine Kostendämpfung zu erreichen (so etwa bei der Intensivierung der Kontrolle der Ärzte im Gesundheitsstrukturgesetz) oder eine angeblich mißbräuchliche Inanspruchnahme von Sozialleistungen aufzudecken (insbesondere durch regelmäßige Datenabgleiche bei Sozialhilfe und Arbeitsförderung).

Auf den Datenschutz wirkt sich dabei die Tendenz aus, weg von einer angeblichen egozentrischen Selbstbestimmung hin zu einer stärker betonten Gemeinschaftsverantwortung zu kommen. Individualrechte werden vielfach ohne zwingende Gründe zugunsten staatlicher Eingriffsrechte zurückgedrängt. Mehr und mehr begegnet der Staat dem einzelnen Bürger mit Mißtrauen und schafft ein immer dichteres Kontrollnetz. Es ist fraglich, ob dieses Menschenbild dem des Grundgesetzes entspricht.

Hinzu kommt, daß das reine Verwaltungsinteresse, das Bestreben nach größtmöglicher Perfektion und Einzelfallgerechtigkeit ein immer größeres Gewicht erhält. Je mehr Perfektion die Verwaltung anstrebt, desto mehr Daten muß sie erheben, nutzen, abgleichen oder sonst verarbeiten. Das Gespür für den "Mut zur Lücke" geht verloren. Kennzeichnend für den demokratischen Rechtsstaat ist aber nicht seine Allwissenheit, sondern die bewußte Beschränkung seiner Informationsherrschaft.

Besonders gern wird zur Intensivierung der Kontrolle die Wunderwaffe des Datenabgleichs genutzt. Perfektion und Korrektheit lassen sich dadurch auf bequeme Weise erreichen: Auf Knopfdruck lassen sich die verschiedensten Kontrollmechanismen in Gang bringen, ohne daß sich die Behörde unmittelbar mit dem einzelnen Bürger auseinandersetzen muß. Mühelos ist die Prüfung von Zehntausenden in kürzester Frist möglich.

Wird der Weg zu intensiverer Kontrolle und Überwachung, insbesondere zum Abgleich der verschiedensten Datenbestände, ungebremst fortgesetzt, könnte sich aus einer Unsumme von automatisierten Dateien und aus einem Netz von Datenabgleichen, das schließlich alle Bürger und fast alle ihre Lebensbereiche erfaßt, der "gläserne Bürger" ergeben. Selbst wenn jeder einzelne Abgleich und Kontrollvorgang für sich eine gewissen Berechtigung haben sollte, trägt er bei zu einem umfassenden Netz von Überwachungs- und Überprüfungsmöglichkeiten. Der Bürger wird dabei potentiell zum Verdächtigen, dessen korrektes Verhalten es zu überprüfen gilt. Damit ändert sich das Verhältnis des Bürgers zum Staat auf grundlegende Weise.

Wie dem begegnen?

Zwar ist die verfassungsrechtliche Dimension des Datenschutzes unbestritten. Gleichwohl fehlt der informationellen Selbstbestimmung das Funda-

ment im Grundgesetz. Eine grundlegende Verbesserung könnte erreicht werden, wenn 10 Jahre nach der Anerkennung des Grundrechts auf Datenschutz durch das Bundesverfassungsgericht dieses Grundrecht auch ausdrücklich in das Grundgesetz aufgenommen würde. Daß die erforderliche Mehrheit in Bundesrat und Bundestag hierfür bisher nicht erreicht werden konnte, bedauert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausdrücklich.

Die verfassungsrechtliche Verbesserung bei einer derartigen Grundgesetzänderung bestünde auch darin, daß bei jedem Gesetzentwurf von Anfang an die Berücksichtigung des Grundrechts auf Datenschutz zu prüfen wäre. Eine Einschränkung des Grundrechts müßte künftig durch ausdrückliche Erwähnung im Gesetz unter Angabe des neuen Grundgesetzartikels kenntlich gemacht werden (sog. Zitiergebot nach Art. 19 GG); anderenfalls wäre das Gesetz nichtig. Dies wäre ein erheblicher "Mehrwert" zu Gunsten der Bürger.

Für die weitere Ausgestaltung des einfachen Datenschutzrechts sollten folgende Erwägungen zugrunde gelegt werden:

In der Informationsgesellschaft ist der effektive Schutz der personenbezogenen Daten die Voraussetzung für eine breite Teilnahme der Bürger an der Gesellschaft. Nur wenn der Bürger sicher sein kann, daß seine dem Staat und der Wirtschaft überlassenen Daten soweit wie möglich geschützt werden, nimmt er aktiv am Gemeinschaftsleben teil. Der Bürger kann seine Freiheit zur Kommunikation (und umgekehrt ebenso seine Entscheidung zur Freiheit von Kommunikation) nur verwirklichen, wenn der Staat seine Schutzpflichten für die Daten der Bürger ernst nimmt.

Die wichtigste Folge dieser Einsicht ist, daß Datenschutzvorschriften nicht nur Rechtssicherheit, sondern auch materielle Freiheitsräume garantieren müssen. Dies bedeutet, daß bei der Frage, ob der einzelne einer Auskunftspflicht unterworfen werden soll, ob seine Daten außer für den Erhebungszweck auch für andere Zwecke freigegeben werden sollen, wie lange belastende Daten aufbewahrt werden dürfen und welche Datenverarbeitungsvorgänge dem Betroffenen verborgen bleiben dürfen, jeweils strenge Maßstäbe angelegt werden müssen. Hierfür ist eine neue Grenzziehung für Eingriffe in das Recht auf informationelle Selbstbestimmung erforderlich:

Der Begriff des "überwiegenden Allgemeininteresses", der alleine einen Eingriff in die informationelle Selbstbestimmung rechtfertigt, ist inhaltlich mehr aufzufüllen und mehr als bisher im Lichte der informationellen Selbstbestimmung zu interpretieren. In konkreten Konfliktfällen darf die Freiheitssicherung der Bürger gegenüber effektiver Staatstätigkeit nicht ins Hintertreffen geraten.

Für das Bundesverfassungsgericht ist die Beteiligung unabhängiger Datenschutzbeauftragter wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten im Interesse eines vorgezogenen Rechtsschutzes von erheblicher Bedeutung für einen effektiven

Schutz des Rechts auf informationelle Selbstbestimmung. Dies gilt insbesondere in den Bereichen, in denen ein Auskunfts- oder Einsichtsanspruch des Bürgers nicht oder nur unvollständig besteht. Daraus folgt, daß Rolle und Kompetenzen der Datenschutzbeauftragten auch im Hinblick auf effektivere Eingriffsmöglichkeiten gestärkt werden müssen. Versuchen, die Kontrollmöglichkeiten der Datenschutzbeauftragten zu beschränken, muß schärfstens widersprochen werden.

Datenschutzrechtliche Verstöße gehen meist auf Unkenntnis und mangelndes Problembewußtsein seitens der öffentlichen Stellen zurück. Aus- und Fortbildung in Fragen des Datenschutzes muß daher erheblich mehr Gewicht beigemessen werden als bisher. Insbesondere sind Bemühungen zu fördern, den Datenschutz in den einschlägigen Ausbildungsplänen (Informatikunterricht in der Schule, Rechts- und Informatikstudium an den Hochschulen) sowie den Fortbildungsveranstaltungen in der öffentlichen Verwaltung als obligatorisches Fach zu verankern.

Die Datenverarbeitungstechniken haben sich gegenüber der Zeit des Volkszählungsurteils geradezu revolutionär verändert. Der Umsetzung des Volkszählungsurteils durch die Schaffung der eigenen Rechtsgrundlagen muß daher verstärkt die Entwicklung geeigneter technisch-organisatorischer Maßnahmen zur Seite gestellt werden. Der Blick des Datenschutzes muß sich stärker auf die Technik des Verarbeitungsprozesses selbst richten. Dies bedeutet nicht nur die Entwicklung spezifischer Datenschutzvorkehrungen für neue informationstechnische Entwicklungen (Miniaturisierung der Rechner, Chipkarten, neue Vernetzungstechniken), sondern auch neuer komplexer Anwendungsformen (z.B. im Bereich des Zahlungsverkehrs, der Straßenbenutzung oder der Textverarbeitung).

Die Europäische Union wird zunehmend zur Informations- und Datengemeinschaft. Dies macht einen europäischen Datenschutz erforderlich. Die Konferenz teilt mit den europäischen Nachbarn nicht nur die Überzeugung, daß der Datenschutz in Europa harmonisiert werden muß, sondern auch, daß die Rechte der Gemeinschaftsbürger auf einem hohen Niveau gesichert werden müssen, damit die Öffnung der Grenzen für Güter, Kapital und Dienstleistungen - und damit auch für persönliche Daten - nicht zu Nachteilen für den einzelnen führt.

Innerhalb von Deutschland wirft die Integration der neuen und der alten Bundesländer nach wie vor Probleme auf. Nach wie vor besteht die Neigung, über Bürger aus den neuen Bundesländern erheblich mehr Daten zu erheben und unter erleichterten Bedingungen Daten zu verarbeiten, als dies in den alten Ländern der Fall wäre.

Die Notwendigkeit für Übergangsregelungen in den neuen Bundesländern wird nicht bestritten; die Eingriffe in Persönlichkeitsrechte müssen aber dennoch verhältnismäßig, erforderlich und darüber hinaus zeitbefristet sein. Aus dem Einigungsprozeß herrührende Sonderregelungen und Verwaltungsvorschriften sind nicht festzuschreiben, sondern auch im Sinne der informationellen Selbstbestimmung schrittweise abzubauen.

**Anlage 10**

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zu Chipkarten im Gesundheitswesen**

Die Datenschutzbeauftragten von Bund und Ländern verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern und
- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte "Gesundheitskarten", etwa "Service-Karten" von Krankenversicherungen und privaten Anbietern, "Notfall-Karten", "Apo(theken)-Cards" und "Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen "Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkarten-Technik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkarten-Technik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller - etwa ein Krankenversicherungsunternehmen oder

eine Krankenkasse - mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z.B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karten-Inhabern vorbehält bzw. erleichtert.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die "Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten - wie den Medizinern - und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest - vorbehaltlich weiterer Punkte - die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.

- Die freiwillige Gesundheitskarte darf nicht - etwa durch Integration auf einem Chip - die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.

- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.

- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung - z.B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung - entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.

- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.

- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

**Anlage 11**

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zur Informationsverarbeitung im Strafverfahren**

- bei Stimmenthaltung Bayerns -

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben.

Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiter verarbeitet werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4 §§ 474 ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz - BT-Drucksache 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittlungsakten enthalten eine Vielzahl höchst sensibler Daten, insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren - auch mit Zwangsmitteln - erhobenen Daten nicht entsprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten. Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend normenklar festzulegen.

1.1 Insgesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.

1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftser-

teilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen.

2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z.B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z.B. Spurendokumentations- und Recherchesysteme).

2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden, wenn dies zur Vorgangsverwaltung zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen.

In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrt wird. Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegriffen werden muß.

Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrundeliegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z.B. bei Fahrlässigkeitstaten der Fall sein. Bei laufenden Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach § 154 StPO oder die Gesamtstrafenbildung gegeben sein.

2.3 Für einen Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Daten der jeweils anderen Behörden ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei abstrakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß.

Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§§ 152 Abs. 2, 160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden - also auch von anderen Staatsanwaltschaften - Auskunft verlangen (§ 161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit - ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens - von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktabrufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu begründen sein. Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften. Auf § 78 SGB X ist in diesem Zusammenhang hinzuweisen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.

2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert.

Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./29. September 1981 zu "Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften", vom 24./25. November 1986 "Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" und vom 5./6. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 3. November 1988).

**Anlage 12**

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zum Abbau des Sozialdatenschutzes**

- gegen die Stimme Bayerns -

Der Gesetzgeber hat in den vergangenen Monaten die Möglichkeit der Überprüfung von Sozialleistungsempfängern ohne deren vorherige Befragung oder Kenntnis in drastischem Umfang vermehrt. Insbesondere durch das seit dem 1. Juli 1993 geltende Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms ist das Kontrollinstrumentarium von Sozial- und Arbeitsämtern noch einmal erheblich erweitert worden. Ohne Rücksicht auf konkrete Anhaltspunkte für einen unberechtigten Leistungsbezug im Einzelfall sind künftig automatisierte Datenabgleiche zwischen Sozialhilfeträgern sowie zwischen diesen und der Arbeitsverwaltung bzw. der Kranken-, Unfall- und Rentenversicherung gestattet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist sehr besorgt über diese Entwicklung, die zu einem immer dichteren Datenverbundsystem im Sozialleistungsbereich und zu immer nachhaltigeren Eingriffen in das Recht auf informationelle Selbstbestimmung aller Betroffenen, d.h. auch und gerade der großen Mehrheit rechtstreuer Antragsteller und Leistungsbezieher, führt.

Mit Nachdruck wenden sich die Datenschutzbeauftragten gegen Versuche von Sozialverwaltungen, bei der Umsetzung der neuen Kontrollregelungen durch extensive Interpretation über den gesetzlich vorgegebenen Rahmen hinauszugehen. So erlaubt beispielsweise der neu gefaßte § 117 Abs. 3 des Bundessozialhilfegesetzes entgegen der Handhabung einzelner Kommunen keinen automatisierten Datenabgleich zwischen Sozialhilfedatei und Kraftfahrzeug-Register, sondern nur den Vergleich von Angaben in Verdachtsfällen.

Die dargestellte Entwicklung macht es erneut notwendig, auf die verfassungsrechtliche Qualität des Grundsatzes der Datenerhebung beim Betroffenen hinzuweisen. An dem Prinzip, daß bei der Überprüfung der Leistungsberechtigung und der Nachweise Auskünfte zunächst beim Antragsteller anzufordern sind und nur aufgrund konkreter Verdachtsmomente Nachfragen bei dritten Stellen oder Datenabgleiche erfolgen dürfen, muß für den Regelfall festgehalten werden, soll der einzelne mündiger Bürger bleiben und nicht zum bloßen Objekt staatlicher Verhaltenskontrolle werden.

Sorge äußert die Konferenz auch über die hartnäckigen Bestrebungen, Datenbestände der Sozialverwaltung für immer neue Zwecke und Adressaten zu öffnen. Beispiele dafür sind die im Gesetzgebungsverfahren zum 2. SGB-Änderungsgesetz im letzten Augenblick gescheiterten Anträge, Polizei und Staatsschutz in unvertretbarem Umfang Zugriff auf Daten Arbeitsloser und sonstiger Sozialleistungsempfänger zu geben. Das Sozialgeheimnis muß ein wirksamer Sonderschutz für die besonders sensiblen Daten in

der Sozialverwaltung bleiben. Nur dies entspricht der Abhängigkeit des einzelnen von staatlichen Leistungen und der sich daraus ergebenden speziellen Verletzlichkeit seines Rechts auf informationelle Selbstbestimmung.

**Anlage 13**

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zum Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz - PTNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718) und der dafür erforderlichen Änderung des Grundgesetzes (BR-Drs. 114/94 = BT-Drs. 12/6717)**

I.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.

II.

Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom 25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten.

Die Datenschutzbeauftragten halten insbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:

a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.

b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.

c) Das Post- und Telekommunikationswesen muß auf Dauer - auch nach dem Wegfall der Monopole - einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kriterien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.

d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.

e) Die vorgesehene Vorschrift zum Einzelentgeltnachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen, wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufen bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.

f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des § 14 a Fernmeldeanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.

III.

Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des § 12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (BR-Drs. 416/91).

**Anlage 14**

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zum Ausländerzentralregistergesetz**

- gegen die Stimme Bayerns -

Das Ausländerzentralregister beim Bundesverwaltungsamt in Köln existiert seit 40 Jahren ohne gesetzliche Grundlage. Derzeit stehen den verschiedenen Benutzern des Registers Daten zu mindestens 8 Millionen Ausländern, die sich in der Bundesrepublik aufhalten oder aufgehalten haben, zur Verfügung. Gespeichert sind neben Daten zur Identifizierung und weiteren Beschreibung der Person insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern

gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 2. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragteen wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienten, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.

Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehen, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern - worauf die Entwurfsbegründung hinweist - der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen, unter denen u.a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen - wenn auch reduzierten - Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

**Anlage 15**

**Tendenzpapier des von den Datenschutzbeauftragten auf ihrer Konferenz vom 26./27. Oktober 1993 beauftragten Gesprächskreises zur Problematik der rechtlichen Einordnung von Wartung und Fernwartung**

Fernwartung
Die Voraussetzungen, unter denen die Weitergabe personenbezogener Daten im Rahmen von Wartung und Fernwartung zulässig ist, sind in den Daten-

schutzgesetzen des Bundes und der Länder bislang nicht eindeutig geregelt. Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb entsprechende normenklare gesetzliche Regelungen.

Im Rahmen der bestehenden Gesetze ist die datenschutzrechtliche Einordnung von Wartung, Fernwartung und Systembetreuung nach ganz überwiegender Ansicht der Datenschutzbeauftragten als Datenverarbeitung im Auftrag am ehesten geeignet, umfassende technische und organisatorische Sicherungsmaßnahmen durchzusetzen. Dagegen vertritt der LfD Nordrhein-Westfalen die Auffassung, daß die personenbezogenen Daten im Rahmen der Wartung und Fernwartung besser geschützt sind, wenn ihre Weitergabe den Vorschriften der Übermittlung unterworfen wird. Die im 15. Tätigkeitsbericht des LfD Bremen (S. 12, Ziff. 1-9) im Bereich der Fernwartung dargestellten Einwirkungsmöglichkeiten sollten beachtet werden.

Grenzen der Datenverarbeitung im Auftrag
Einschränkungen der Zulässigkeit der Verarbeitung personenbezogener Daten im Auftrag durch nicht-öffentliche Stellen können sich insbesondere ergeben aus

- verfassungsrechtlichen Hindernissen (z.B. gänzliche Übertragung eines Landesverwaltungsnetzes),
- entgegenstehenden spezialgesetzlichen Vorgaben (z.B. Krankenhausgesetz),
- Vorliegen von Berufsgeheimnissen (z.B. § 203 Abs. 1 StGB).

Die vorstehenden Gesichtspunkte können im Einzelfall auch einer Verarbeitung personenbezogener Daten im Auftrag durch öffentliche Stellen entgegenstehen.

Länderübergreifende Datenverarbeitung im Auftrag
Es wird für richtig gehalten, eine länderübergreifende Kontrolle von öffentlichen Stellen als Auftragnehmer im Wege der Amtshilfe durchzuführen. Anderslautende Absprachen sind möglich. Die Beteiligung der Aufsichtsbehörden bei der Kontrolle nicht-öffentlicher Stellen wird nicht für erforderlich gehalten; es sei denn, die Unterrichtung der Aufsichtsbehörde ist landesgesetzlich vorgeschrieben. Der Sonderfall des Sitzlandprinzips bei den Rundfunkanstalten ist zu berücksichtigen.

**Anlage 16**

**Entschließung der Datenschutzbeauftragten des Bundes und der Länder zu dem Entwurf der NADIS-Richtlinien vom 2. Mai 1994**

- beschlossen im Umlaufverfahren, bei Stimmenthaltung der Landesbeauftragten Thüringens und Bayerns -

Das von den Verfassungsschutzbehörden des Bundes und der Länder betriebene Verbundsystem NADIS-PZD (Nachrichtendienstliches Informationssystem/Personenzentraldatei) ist nach den Vorgaben der in Überarbeitung befindlichen NADIS-Richtlinien und der nunmehr erstellten Dateianordnung als Aktenhinweissystem zu qualifizieren. Die NADIS-Richtlinien

und die Dateianordnung haben sich hinsichtlich ihres Regelungsgehaltes an den Bestimmungen der Verfassungsschutzgesetze zu orientieren.

Die Datenschutzbeauftragten des Bundes und der Länder halten den Entwurf der NADIS-Richtlinien und der Dateianordnung für die Personenzentraldatei für zu weitgehend und fordern deshalb:

- Die in der Personenzentraldatei gespeicherten personenbezogenen Daten sind auf das unerläßlich notwendige Maß zu reduzieren. Eine solche automatisierte Datei darf nach den bindenden Vorgaben des Bundesverfassungsschutzgesetzes nur die Daten enthalten, die für das Auffinden der Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Eine Erweiterung für andere Identifizierungszwecke scheidet somit aus.
  Die Dateianordnung enthält darüber hinaus Arten von Daten, die über den Zweck einer Aktenhinweisdatei hinausgehen.

- Alle Rechtsvorschriften, die für die an dem zu übermittelnden Datensatz beteiligten Verfassungsschutzbehörden maßgeblich sind, sind zu beachten. Die in dem Entwurf der NADIS-Richtlinien enthaltenen Regelungen für die Übermittlung personenbezogener Daten sehen hingegen vor, daß hierfür ausschließlich das Recht der übermittelnden Stelle gelten soll.

- Die Dauer der Speicherung von Protokolldatenbeständen ist einheitlich zu regeln. Eine Differenzierung, ob die ursprünglich in der Personenzentraldatei erfaßte Information infolge Fristablaufs oder aufgrund einer Einzelfallentscheidung gelöscht wurde, erscheint nicht sachgerecht. Außerdem muß sichergestellt sein, daß Protokolldaten, so wie es die Verfassungsschutzgesetze vorsehen, nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage verwendet werden.

- Die Datenschutzbeauftragten sind im Rahmen der Durchführung und Fortentwicklung des Nachrichtendienstlichen Informationssystems frühzeitig zu unterrichten und zu beteiligen. Dies muß insbesondere bei der Vorbereitung von datenschutzrechtlichen Regelungen gelten.

**Anlage 17**

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. August 1994 zum Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik - EG-Statistikverordnung - (KOM(94) 78 endg.; Ratsdok. 5615/94 = BR-Drs. 283/94)**

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings darauf hin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs. 283/94 - Beschluß -).

Gegen den vorgelegten Vorschlag einer Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:

1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen - insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung - bei dieser Stelle bereits aufgrund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.

   Zugleich sollte EUROSTAT zumindestens einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotenen Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht wie in Art. 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik).

Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nicht-vertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff "statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 - allerdings mit einem anderen Begriffsinhalt - definiert wird. Der Begriff "statistische Geheimhaltung" sollte an einer Stelle in der Verordnung so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3b EG-Vertrag.

6. Gemäß dem Grundsatz der Subsidiarität sollte - ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) - auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.

7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3b EG-Vertrag. Dieser gebietet hier, daß - jedenfalls grundsätzlich - die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.

   Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z.B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nicht-Gemeinschaftsstatistiken zuständigen Stel-

len vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen. Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

**Anlage 18**

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994**
**Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen**

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und

Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sog. Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, d.h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

**Anlage 19**

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zu fehlenden bereichsspezifischen gesetzlichen Regelungen bei der Justiz**

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als 10 Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Statt dessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang er-

forderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z.B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz),
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sog. Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. 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 in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts des Bürgers entgegenwirken.

**Anlage 20**

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zu den datenschutzrechtlichen Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (Europol)**

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

- Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die materielle Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleiben die Zuständigkeiten und die dazugehörigen Befugnisse des BKA als nationale Stelle für den Informationsverkehr mit EUROPOL unberührt.

- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Be-

fugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, zum Beispiel durch eine Protokollerklärung zum EUROPOL-Übereinkommen, trifft.

**Anlage 21**

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zu Art. 12 Verbrechensbekämpfungsgesetz und zur Trennung von Polizei und Nachrichtendiensten**

Geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse müsen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Dies betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.

- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtsprechung des Bundesverfassungsgerichts sicherzustellen.

**Anlage 22**

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zum geänderten Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994 (KOM (94) 128 endg. - COD 288)**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen

Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedsstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht priviligiert werden.

2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei "berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.

3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.

4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte - wie im ursprünglichen Richtlinienentwurf vorgesehen - untersagt werden.

5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte - wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah - auf Unionsebene garantiert werden.

6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinie aufgenommen werden, z.B. indem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.

7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z.B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedsstaaten, diese Anregungen zu unterstützen.

Vom Abdruck der Rede von Prof. Spiros Simitis (Anlage 23) und des Stichwortverzeichnisses in der Landtagsdrucksache wird abgesehen.