XIII. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Niedersachsen für die Jahre 1995 und 1996

1. Vorbemerkung

2. Zur Situation des Datenschutzes

2.1 Informationsgesellschaft und Datenschutz

2.2 Bundesrepublik Deutschland, Niedersachsen, Europa

2.3 Neue Tendenzen und Konzepte

3. Der Datenschutzbeauftragte

3.1 Status

3.2 Geschäftsstelle

3.3 Außenprüfungen und Beratungen

3.4 Dateibeschreibungen und das Dateienregister im öffentlichen Bereich

3.5 Öffentlichkeitsarbeit

3.6 Zusammenarbeit mit anderen Kontrollorganen

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

4.1 Die Informationsgesellschaft

4.1.1 Die rasante Fahrt auf der Datenautobahn

4.1.2 Multimedia in Niedersachsen

4.1.3 Regelungsbedarf

4.1.4 Technikgestaltung unterstützt Datenschutz

4.2 Internet - das Netz der Netze

4.2.1 Was ist das Internet?

4.2.2 Probleme und Risiken

4.2.3 Empfehlungen

4.3 Verschlüsselung: Wirksamer Impfstoff gegen unsichere Datenübertragung

4.3.1 Warum gerade ich?

4.3.2 Verschlüsselung ist günstiger als Sie denken

4.3.3 "Digitale Signatur" sichert die Echtheit von Daten

4.3.4 Recht auf Privatsphäre auch in Datennetzen

4.4 Normen, Standards und Empfehlungen

4.5 Grundschutz bei der automatisierten Datenverarbeitung

4.6 Technikfolgenabschätzung

4.6.1 Präventiver Datenschutz

4.6.2 Erste Erfahrungen

4.7 Chipkarten

4.7.1 Rechtliche Einordnung von Chipkarten

4.7.2 Anforderungen an die informationstechnische Sicherheit bei Chipkarten

4.8 Optische Speicher

4.8.1 Eine beachtenswerte neue Technologie

4.8.2 Datenschutzprobleme bei der optischen Datenspeicherung

4.8.3 Keine Löschung von Informationen bei CD-ROM bzw. WORM

4.8.4 Empfehlungen zum Einsatz optischer Datenspeicherung

4.9 Neue Datenschutz-Prüfkonzepte

4.9.1 Prüfkonzept Windows NT

4.9.2 Prüfkonzept für MVS/VM-Systeme

4.9.3 Prüfkonzept Mailboxen

4.10 Alle Jahre wieder - Pannen bei der Aktenvernichtung und beim Postversand

5. Europa, Ausland

5.1 EU-Datenschutzrichtlinie

5.2 BahnCard-Daten in den Staaten

5.3 Das VW-Haustelefonbuch gehört nicht in die USA

5. 4 Der elektronische Pranger im "Netz der Netze"

5.5 Chinesische Teppichwerbung

6. Datenschutzrecht - allgemein

6.1 Novelle des NDSG

6.2 Straftaten im Umgang mit Daten

7. Statistik

7.1 Dauerbrenner Mikrozensus

7.2 Novellierung des Bundesstatistik-Gesetzes

7.3 Sozialhilfestatistik

7.4 Einzelhandelsstatistik - Erhebung per Postkarte?

8. Neue Medien

8.1 Telekommunikation

8.1.1 Rechtsgrundlagen in Bewegung

8.1.2 Teledienstgesetz

8.1.3 Telekommunikationsdienstunternehmen-Datenschutzverordnung

8.1.4 Elektronische Telefonverzeichnisse auf CD-ROM

8.1.4.1 Die bisherige Rechtslage

8.1.4.2 Das neue Telekommunikationsrecht

8.1.4.3 Abwehrmöglichkeiten

8.1.4.4 ... und kein Ende ?!

8.2 Datenschutz und Medien

8.2.1 Die Medienlandschaft verändert sich

8.2.2 Der "gläserne" Fernsehzuschauer

8.2.3 Landesrundfunkgesetz

8.2.4 Staatsvertrag über Mediendienste

9. Personenstandsrecht: ungewollte amtliche Beihilfe zur Kindesentführung?

10. Ausweis- und Melderecht

10.1 Chancen für ein bürgerfreundlicheres Melderecht

10.2 Schöne neue Welt: Meldedaten auf CD-ROM und im Internet

10.3 Technische Mängel in Meldeämtern: Die Rechte der Betroffenen kommen zu kurz

11. Polizei

11.1 Eindrücke

11.2 Weniger Datenschutz wagen: Über den Abbau von Bürgerrechten im Gefahrenabwehrgesetz

11.3 EUROPOL: über uns nichts als blauer Himmel

11.3.1 EUROPOL-Konvention

11.3.2 Das BKA als nationale Verbindungsstelle

11.3.3 Ratifizierungsgesetz zur EUROPOL-Konvention

11.4 Statt einer Bilanz nur eine Sammlung spektakulärer Einzelfälle

11.5 Lauschangriff zur Gefahrenabwehr

11.6 Aus der Praxis der polizeilichen Arbeit

11.6.1 Die Angst des Staates vor seinem Bürger

11.6.2 Kinder werden wie Kriminelle behandelt

11.6.3 Wie aus friedfertigen Besuchern Gewalttäter wurden

11.7 Nachtrag zum XII. TB

11.7.1 Speicherungen über Suizidversuche neu geregelt

11.7.2 Hinweise auf Aids im Polizeicomputer

12. Ausländerangelegenheiten

12.1 Der Chip-Flüchtling

12.2 Deutsche Behörden als Informationsbeschaffer der

Heimatstaaten

12.2.1 Beschaffung von Paßersatzpapieren

12.2.2 Abschiebung von kurdischen Volkszugehörigen

12.3 Asylbewerberleistungsgesetz

12.4 Ausnahmslose ED-Behandlung von Bürgerkriegsflüchtlingen

13. Verfassungsschutz

13.1 Änderung des Niedersächsischen Verfassungsschutzgesetzes

13.2 Bundesverfassungsgericht bremst bei strategischer Rasterfahndung des BND

13.3 Unterstützungsunterschriften für Wahlvorschlag landen beim Verfassungsschutz

13.4 Sicherheitsüberprüfung

13.5 Zuverlässigkeitsüberprüfungen nach dem Atomgesetz

14. Personalangelegenheiten

14.1 Inhalt der Personalakte/Abgrenzung zur Sachakte

14.2 Inhalt der Personal(neben)akte

14.3 Hinweise in der Personalakte auf andere Bedienstete

14.4 Kriminalpolizeiliche Erkenntnisse in einer Personalnebenakte

14.5 Beschwerden und ungünstige Bewertungen in der Personalakte

14.6 Unbegründete Dienstaufsichtsbeschwerden

14.7 Übermittlung von Personaldaten an dritte Stellen

14.7.1 Mitteilungen an die Presse

14.7.2 Argloser Austausch zwischen öffentlichen Stellen

14.7.3 Personalnachrichten

14.7.4 Nur mit vollständiger Personalakte in den Ruhestand?

14.8 Akteneinsicht in Sachakten

14.9 Aufbewahrung von Bewerbungsunterlagen

14.10 Heftung, Paginierung von Personalakten

14.11 Abschottung von Personalakten

14.12 Probleme bei Organisationsuntersuchungen und Mitarbeiterbefragungen

14.13 Trennung von Beihilfe- und Personalsachbearbeitung

14.14 Wenn Ärzte mit Patientinnen telefonieren ...

14.15 Datenübermittlungen zwischen Personalrat, Stufenvertretung, Gesamtpersonalrat

14.16 Einsicht der Schwerbehindertenvertretung in Bewerbungsunterlagen und Teilnahme an Vorstellungsgesprächen

14.17 Öffentliche Bedienstete als Wahlhelfer

15. Kommunalverwaltung

15.1 Kommunalverfassungsrecht

15.2 Amtsverschwiegenheit

15.3 Weitergabe von Tonbandabschriften einer öffentlichen Ratssitzung

16. Ungeahnte Lesarten des Umweltinformationsgesetzes

17. Bau-, Wohnungs- und Vermessungswesen

17.1 Novellierung des Vermessungs- und Katastergesetzes

17.2 Mittagsruhestörung durch Veröffentlichung des

Baulückenverzeichnisses

17.3 Erforderlich? - Weitergabe von Daten einer bauaufsichtlichen Anordnung

17.4 Verteilerlisten für die Versendung von Planfeststellungsbeschlüssen an die Grundstückseigentümer

18. Finanzverwaltung

18.1 Wie gehabt: Abgabenordnung weiter ohne Datenschutzregelungen

18.2 Steuerdatenabrufverordnung - jetzt nur noch als Verwaltungsregelung?

18.3 Steuerberaterdaten für die Bundesversicherungsanstalt für Angestellte (BfA)

18.4 Anträge auf Wohnungsbauprämie - von wegen freiwillig!

19. Soziales

19.1 Berufliche Eingliederung von arbeitslosen Sozialhilfeempfängern

19.2 Datenübermittlung an Straßenverkehrsbehörden - rechtfertigender Notstand?

19.3 Sozialdaten auf Überweisungsträgern

19.4 Pauschale Einwilligungserklärung - ein Dauerbrenner

19.5 Aktenübermittlung an die Fachaufsichtsbehörde im Widerspruchsverfahren

19.6 Mitteilung der Anwesenheit von zur Fahndung ausgeschriebenen Sozialhilfeempfängern im Sozialamt an die Polizei

19.7 Haltet den Dieb!

19.8 Verschlüsselung von Diagnosen, ICD-10-Schlüssel

19.9 Übermittlung von Sozialdaten an Behörden der

Gefahrenabwehr

19.10 Fremdbefunde für gutachtliche Stellungnahme des Medizinischen Dienstes

19.11 Ärgerlich: Die sprechende Mitgliedsnummer der Ärzteversorgung

20. Gesundheit

20.1 Gesetzgebung

20.2 Einblick des Rechnungshofes in Patientenakten

20.3 Auswertung von Patientenunterlagen für "Verwaltungszwecke"

20.4 Übersendung ärztlicher Berichte an Aufnahmeeinrichtungen

20.5 Ungeklärt: Wie gelangte die Psychiatrieakte zur Zeitungsredaktion?

20.6 Tonträgerkontrolle bei Krankentransporten

21. Kinder- und Jugendhilfe

21.1 Kinder- und Jugendhilfedaten als Basis zur Berechnung von Sozialleistungen?

21.2 Und wie steht es mit vertraulichen Informationen?

21.3 Auskünfte an die Polizei

22. Forschung

23. Hochschulen

23.1 Telefon- und Vorlesungsverzeichnisse im Internet?

23.2 Warnung vor dem erfolglosen Doktoranden

23.3 "Akten mit Sexopfern in Unibibliothek"

24. Schulen

24.1 Novellierung des Niedersächsischen Schulgesetzes

24.2 Erfassungsbogen für Schulabgänger

24.3 Zusammenarbeit zwischen Jugendamt und Schule

25. Landwirtschaft und Forsten

25.1 Tierschutzgesetz

25.2 Zentrale Registratur Zirkus

26. Wirtschaft

26.1 Datenschutzrechtliche Regelungen in der Gewerbeordnung

26.2 Gewerbeanzeigenverwaltungsvorschrift - Beispiel für gute Zusammenarbeit

27. Verkehr

27.1 Zentrales Fahrerlaubnisregister

27.2 Ärztliche Zeugnisse für Bus- und Taxifahrer

27.3 Parksünderdateien ohne Rechtsgrundlage

28. Rechtspflege

28.1 Informationsverarbeitung im Strafverfahren

28.2 Justizmitteilungsgesetz - Never ending story ohne happy end

28.3 Errichtungsanordnung für ein länderübergreifendes staatsanwaltschaftliches Verfahrensregister

28.4 Justiz und Medien - zwei Welten treffen aufeinander

28.5 Die Einführung des großen Lauschangriffs ist nach wie vor abzulehnen

28.6 Eine Landtagsabgeordnete in der Telefonüberwachung

28.7 Informationen im OWi-Verfahren

28.8 Bewährungs- und Gerichtshilfe, Führungsaufsicht

28.9 Schuldnerverzeichnis

28.9.1 Auskünfte aus dem Schuldnerverzeichnis an Vermieter - auch über Ehegatten

28.9.2 Unterschiedliche Praxis bei Auskünften aus dem Schuldnerverzeichnis

28.9.3 Der laufende Bezug von Abdrucken aus dem Schuldnververzeichnis

28.10 Ehescheidungsverbundurteile

28.11 Datenschutz im Notariat

28.12 Kontrollen

28.12.1 Kontrolle von Telefonüberwachungsmaßnahmen

28.12.2 Kontrolle des staatsanwaltschaftlichen ADV-Systems SIJUS-STRAF

29. Strafvollzug

29.1 Novellierung des Strafvollzugsgesetzes - kalter Kaffee neu aufgewärmt

29.2 Anfertigung von Gefangenenlichtbildern

30. Religionsgesellschaften: Wie kirchlich ist der Unfallhilfe-Verein?

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

31. Grundsätzliches zum Datenschutz in der Wirtschaft

31.1 BDSG-Novellierungsbedarf

32. Kontrolltätigkeit: Zahlen, Fakten und Erfahrungen

32.1 Datenverarbeitung als Dienstleistung: Meldepflicht nach §

32 BDSG

32.2 Kontrolle vor Ort (Stand: 5.9.)

32.3 Abberufung eines Datenschutzbeauftragten

32.4 Streit um die Auskunftspflicht einer Bank: Viel Lärm um nichts?

33. Adressenhandel und Markt- und Meinungsforschung

33.1 Listbroking

33.2 Weshalb sollten "christliche Spender" gegen Abtreibung sein?

33.3 Die Crux mit den Widersprüchen und der Robinsonliste

33.4 Mit dem Berliner Bären auf Kundenjagd

33.5 Der Brief an den Weihnachtsmann

33.6 Das Geschäft mit der Not

34. Kundendaten und Werbung

34.1 Neue Zoo Card für Besucher des hannoverschen Zoos

34.2 Parteienwerbung

34.3 Die private Telefonnummer im Bankeinzugsverfahren

35. SCHUFA: viermal Klaus Müller, geb. am 4.4.1944

36. Auskunfteien

36.1 Datenklau durch Wirtschaftsauskunftei

36.2 Benachrichtigung nach § 33 BDSG als Wink mit dem Zaunpfahl

36.3 Auskunfteirecherche über mißliebigen Journalisten?

37. Finanzwirtschaft

37.1 Wertpapierhandel: Freiwillige Beratung oder Zwangsangaben?

37.2 Geldwäsche: Bisher fast nur weiße Westen!

37.3 Schüler hatte Zugriff an den Kontostand der Nachbarn

38. Versicherungen: Der Trick mit der Allfinanz-Klausel

39. Wohnungswirtschaft: Unzulässige (Sozial-) Hilfeleistung des Vermieters

40. Privates Gesundheitswesen: Arztdaten als Objekt eines Beziehungsclinchs

Anlagen Materialien zum Datenschutz

1. Vorbemerkung

Der vorliegende XIII. Tätigkeitsbericht betrifft gemäß § 22 Abs. 3 Satz 1 NDSG zwei Kalenderjahre: 1995 und 1996. Redaktionsschluß war der 21. November 1996. Der Bericht behält weitgehend die bewährte und vertraute Gliederung bei. Am Ende - Kapitel 31 bis 40 - findet sich wiederum der Bericht über den Datenschutz im nicht-öffentlichen Bereich (§ 22 Abs. 6 Satz 3 NDSG).

Aus Sparsamkeitsgründen ist die Seitenzahl im Vergleich zum letzten Tätigkeitsbericht reduziert worden. Ferner habe ich die Auflagenhöhe des Berichts, die seit Jahren bei 10.000 Exemplaren lag, auf 9.000 gesenkt. Dies ist vor allem deshalb vertretbar, weil ich den Tätigkeitsbericht gemeinsam mit anderen Datenschutzinformationen kostengünstig auch als Diskette anbiete (vgl. 3.5). Angemerkt sei, daß die früheren Tätigkeitsberichte entweder völlig oder fast vergriffen sind.

2. Zur Situation des Datenschutzes

2.1 Informationsgesellschaft und Datenschutz

Der Berichtszeitraum stellt eine wichtige Etappe im Übergang von der klassischen Industriegesellschaft zur Informationsgesellschaft dar. Diese Entwicklung ist unumkehrbar. Informationen werden für Staat, Wirtschaft und Private immer wichtiger. Neuartige Informations- und Kommunikationstechniken verändern unsere Lebensverhältnisse grundlegend. Insbesondere "Datenautobahn" und "Multimedia" sind Stichworte, ja Schlüsselbegriffe, die auf bahnbrechende Technikinnovationen hinweisen. Multimedia wurde 1995 nicht ohne Grund zum "Wort des Jahres" erkoren.

Durch die technischen Umwälzungen ergeben sich neue und besondere Auswirkungen auch beim Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger. Als Beispiel sei genannt, daß Firmen in einer weit größeren Dimension als früher Kundendaten sammeln, die zu Kundenprofilen verarbeitet werden können. Es stellen sich neue Fragen an den Datenschutz, die zu beantworten sind. Ich möchte aber klar herausstellen, daß sich der Datenschutz nicht gegen die moderne technische Entwicklung stellen darf. Datenschutz sollte nicht ein Stolper-, sondern ein Baustein der Informationsgesellschaft sein. Datenschutz ist eine Funktionsvoraussetzung der im wesentlichen marktwirtschaftlich organisierten Informationsgesellschaft, die demokratischen und bürgerrechtlichen Anforderungen genügen muß. Ich verweise näher auf meinen Aufsatz "Nochmals: Datenschutz in der Informationsgesellschaft" in ZRP 1996, 206.

Im letzten Tätigkeitsbericht (XII 2.1) hatte ich 1993 und 1994 - bundesweit gesehen - als schwierige Jahre für den Datenschutz bezeichnet. Diese Aussage trifft auch für den Berichtszeitraum zu. Aber zwei Momente sind neu und stimmen hoffnungsvoll: Es gibt Anzeichen, daß das Datenschutzbewußtsein der Bürgerinnen und Bürger gestiegen ist. So gab es z.B. erheblichen Unmut bei der Einführung der neuen BahnCard durch die Deutsche Bahn AG und die Citibank sowie bei der Unterrichtung, die die Deutsche Telekom AG hinsichtlich der Komfortauskunft und elektronischer Kundenverzeichnisse vornahm. Ferner scheint sich in der Wirtschaft die Erkenntnis zu verbreiten, daß Produkte Wettbewerbsvorteile haben, wenn sie datenschutzgerechter als andere sind. Das Beispiel Umwelttechnologie sollte in Deutschland als Anstoß und Chance begriffen werden, auch in der Datensicherheitstechnologie weltweit führend zu werden.

2.2 Bundesrepublik Deutschland, Niedersachsen, Europa

Was den Bund anbetrifft, gab es im Berichtszeitraum keine herausragenden Neuregelungen im Bereich des Datenschutzes. Einige datenschutzrechtliche Defizite, seit Jahren beklagt, bestehen nach wie vor; insbesondere stehen eine umfassende Überarbeitung der Strafprozeßordnung und eine Regelung des Arbeitnehmerdatenschutzes immer noch aus. Die im letzten Tätigkeitsbericht (XII 2.1) angesprochene Tendenz, unter dem Aspekt der Bekämpfung der Kriminalität und des Mißbrauchs sozialer Leistungen das Instrumentarium der Kontrolle und Überwachung der Bürgerinnen und Bürger auszuweiten, besteht weiterhin. Der markanteste Fall ist der erneute Versuch, den sogenannten großen Lauschangriff zu regeln. Das böse Schlagwort "Datenschutz ist Täterschutz" ist leider nicht aus der Welt. Es zeugt von verfassungsrechtlicher Ignoranz. Die Bürgerinnen und Bürger haben sowohl einen Anspruch darauf, daß sie sich vor Kriminalität sicherfühlen können, als auch darauf, daß ihre Privatsphäre nicht beeinträchtigt wird; beide Belange müssen miteinander in Einklang, in praktische Konkordanz, gebracht werden. Es ist erfreulich, wenn sich prominente Politiker gegen das Schlagwort "Datenschutz ist Täterschutz" wenden, so Bundesinnenminister Kanther auf einer bemerkenswerten Tagung "Informationsgesellschaft und innere Sicherheit" am 12. Februar 1996 in Stuttgart.

In der Gesetzgebung des Landes Niedersachsen gab es 1995 und 1996 kaum datenschutzrechtliche Fortschritte. Als größtes Defizit ist die immer noch ausstehende Verbesserung des Datenschutzes im Gesundheitswesen zu beklagen. Auf einigen Gebieten zeichnet sich leider ein datenschutzrechtliches Rollback, eine "Gegenreform" (Jürgen Seifert, Kritische Justiz 1996, 356, 357) ab. Den Anfang machte ein Gesetz vom 4. April 1995 (Nds. GVBl. S. 103), das das datenschutzfreundliche Niedersächsische Verfassungsschutzgesetz vom 3. November 1992 änderte. Das Gesetz zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes (NGefAG) vom 20. Mai 1996 (Nds. GVBl. S. 230) brachte in einem Punkt eine datenschutzrechtlich relevante Korrektur. Insbesondere mit dem Stichwort "Deregulierung" meint das Niedersächsische Innenministerium hinreichend Anlaß zu haben, ein Artikel-Gesetz mit einer Änderung des Niedersächsischen Datenschutzgesetzes (NDSG) und - erneut - des NGefAG folgen zu lassen.

Was die Praxis im öffentlichen und nicht-öffentlichen Bereich in Niedersachsen anbetrifft, sind auch im Berichtszeitraum zahlreiche datenschutzrechtliche Verstöße zu verzeichnen; spätere Kapitel des Tätigkeitsberichts belegen dies. Auch meine Prüfungen im Schul- und im Polizeibereich haben erhebliche datenschutzrechtliche Defizite aufgezeigt. Gesetze werden häufig gar nicht gelesen. Es besteht kein Zweifel, daß die obersten Landesbehörden jeweils für ihren Geschäftsbereich die Ausführung des NDSG sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen haben (vgl. die Begründung zu § 8 des Entwurfs eines NDSG, LT-Drs. 12/3290, S. 38). Datenschutz ist nicht nur als Bestandteil der täglichen Praxis auf der Mitarbeiterebene zu verstehen, sondern auch als anspruchsvolle

Gestaltungs- und Führungsaufgabe. Datenschutz ist, wie der Vorstand der Kommunalen Gemeinschaftsstelle für Verwaltungsvereinfachung (KGSt) in einem Rundschreiben vom 10. März 1994 ausführte, Chefsache; Datenschutz - so heißt es dort weiter - enge nicht nur das Verwaltungshandeln ein, sondern biete die Chance, rechenbare Vorteile zu erzielen. Ich wiederhole meine Bitte aus dem letzten Tätigkeitsbericht (XII 2.2.1), der Aus- und Fortbildung in Fragen des Datenschutzes erheblich mehr Gewicht beizumessen.

Von großer Bedeutung für die Fortentwicklung des Datenschutzes ist das Inkrafttreten der Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Amtsblatt der Europäischen Gemeinschaften Nr. L 281/31). Die lange Kodifikationsarbeit hat sich gelohnt. Die EU-Datenschutzrichtlinie enthält zahlreiche Regelungen, die interessante und weiterführende Aspekte aus den Datenschutzgesetzen der anderen Mitgliedsstaaten der EU aufgreifen. Die Datenschutzgesetze des Bundes und der Länder sind in etlichen Punkten an die Richtlinie anzupassen. Die Frist für die Anpassung läuft drei Jahre, d.h. bis zum 24. Oktober 1998. Die Pflicht zur Anpassung des deutschen Rechts sollte als Chance genutzt werden, das Datenschutzrecht in der Bundesrepublik Deutschland von veralteten Regelungen zu befreien und den Erfordernissen der neuen informations- und kommunikationstechnischen Anwendungen gerecht zu werden. Dies kommt in der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 zur "Modernisierung und europäischen Harmonisierung des Datenschutzrechts" (vgl. unten Anlage 19) zum Ausdruck. Es darf nicht übersehen werden, daß nach Erwägungsgrund 9 der Richtlinie durch die Mitgliedsstaaten eine Verbesserung des Datenschutzes anzustreben ist.

Äußerungen aus dem Bundesministerium des Innern deuten darauf hin, daß sich der Bund bei der Novellierung des Bundesdatenschutzgesetzes (BDSG) auf das rechtlich zwingend Notwendige beschränken möchte. Diese Haltung sollten sich die Länder nicht zu eigen machen. So wünschenswert einheitliche Regelungen sind, so dringend ist es, daß das Recht auf die Herausforderungen der technischen Entwicklung adäquate Antworten auf einem hohen bürgerrechtlichen Niveau bereithält. Der Wettbewerb zwischen Bund und Ländern hat sich bei der Weiterentwicklung des Datenschutzrechts schon immer als äußerst produktiv erwiesen.

2.3 Neue Tendenzen und Konzepte

Das Konzept des Datenschutzes ist in Deutschland weitgehend als Reaktion auf die Datenverarbeitungsvorhaben einer expandierenden öffentlichen Verwaltung entstanden. Die Diskussion ist seit Jahren zu stark auf den Staat, den Leviathan, fixiert. Dies führte dazu, daß dem nicht-öffentlichen Bereich eine viel zu geringe Bedeutung beigemessen wurde. Dabei wurden und werden die privaten Datenbestände konsequent ausgebaut; heute liegt das Übergewicht bei der Verarbeitung personenbezogener Daten nicht mehr beim Staat, sondern bei nicht-öffentlichen Stellen. Daß die privaten Datenbestände auch das

Interesse des Staates wecken, sei nur angemerkt. Die Bürgerinnen und Bürger empfinden die Bedrohungen der informationellen Selbstbestimmung, die von der öffentlichen und der privaten Datenverarbeitung ausgehen können, zunehmend als gleich intensiv. Angesichts dieser Entwicklung ist es richtig gewesen, daß die Landesregierung mit Beschluß vom 17. Dezember 1991 (Nds. MBl. 1992, 230) die Datenschutzkontrolle für den nicht-öffentlichen Bereich dem Landesbeauftragten übertrug. Diese Kompetenzerweiterung gibt es außer in Bremen und Hamburg nun auch in Berlin. Konsequent wäre es ferner, den öffentlichen und den nicht-öffentlichen Bereich weitgehend einheitlichen Datenschutzregelungen zu unterwerfen; die EU-Datenschutzrichtlinie ist ein wichtiger Schritt dahin.

Die Verarbeitung personenbezogener Daten ist nie zuvor so umfangreich und so vielgestaltig gewesen. Das Datenschutzrecht der letzten 25 Jahre hat diese Entwicklung nicht aufhalten können. In seiner jetzigen Ausformung kann es die sich abzeichnende Entwicklung des PC zum Universalmedium nicht beeinflussen. Der Weg in eine um die virtuelle Präsenz konstruierte Lebenswelt zeichnet sich ab. Das ist ungemein interessant, ja verführerisch. Es muß aber auch der Preis dafür genannt werden, der hoch ist: eine immens gesteigerte Offenlegung personenbezogener Daten. So gibt es auf den derzeitigen Datenautobahnen nur gläserne Fahrerinnen und Fahrer. Wie immer die technische Entwicklung im einzelnen verlaufen mag: das Grundrecht auf informationelle Selbstbestimmung ist zu beachten. Das wird im wesentlichen nur dadurch möglich sein, daß eine Allianz von Datenschutz und Technologie angestrebt und verwirklicht wird. Insoweit verweise ich insbesondere auf einen Vortrag von Spiros Simitis zum Thema "Virtuelle Präsenz und Spurenlosigkeit - Ein neues Datenschutzkonzept" am 9. Juni 1995 in Wiesbaden (in: Hassemer/Müller, 25 Jahre Datenschutz, Baden-Baden 1996, S. 28 = Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft 1996, 99). Der herkömmlicherweise normativ ausgestaltete Datenschutz muß - so auch der Rat für Forschung, Technologie und Innovation in seinem Papier "Informationsgesellschaft - Chancen, Innovationen und Herausforderungen" vom Dezember 1995 (unter 2.5) - durch eine Datenschutztechnologie ergänzt werden, deren Aufgabe es ist, die informationelle Selbstbestimmung technikspezifisch und risikoadäquat zu gewährleisten. Es ist erforderlich, daß sich die Datenschutzbeauftragten stärker in die Technikgestaltung einmischen. Sie müssen nachdrücklicher denn je betonen (in Abwandlung des Titels eines Buches eines norddeutschen Schriftstellers): "Datenschutz ist not."

3. Der Datenschutzbeauftragte

3.1 Status

Berichtenswert ist folgender meinen Status tangierende Vorfall:

Zum 11. Juli 1996 lud ich Pressevertreter zu einem Gespräch ein; einer der drei Besprechungspunkte lautete "Abbau des Datenschutzes im Polizeirecht". In dem Gespräch ging ich kurz auf das Gesetz zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes vom 20. Mai 1996 (Nds. GVBl. S. 230) ein und sagte dann, die Arbeiten an der angekündigten zweiten Novelle seien im Niedersächsischen Innenministerium fortgeschritten. Das Ministerium hatte mir im Juni 1996 einen dort noch nicht abgestimmten Gesetzentwurf mit der Bitte übersandt, vorab Kenntnis zu nehmen. Dieser Entwurf war auch in Abgeordneten- und Journalistenkreisen vorhanden. Gleichwohl behandelte ich in dem Pressegespräch nicht den Entwurf als solchen, sondern nur einige bereits öffentlich bekannte Novellierungspunkte: Abbau von Richtervorbehalten (Minister Glogowski am 8. Mai 1996 im Niedersächsischen Landtag) und Streichung sowohl von speziell auf unbeteiligte Dritte zugeschnittenen Löschungsverpflichtungen als auch von bestimmten Unterrichtungen der Betroffenen über durchgeführte heimliche Ermittlungen (Aufsatz "NGefAG: Novelle kommt in zwei Schritten" in dem vom Niedersächsischen Innenministerium herausgegebenen Polizei-Extrablatt Nr. 3/1996). Ferner sprach ich die Anlegung von Kriminalakten über schuldunfähige Kinder an, ein Problem, das wegen einer datenschutzrechtlichen Prüfung bereits in der Öffentlichkeit bekannt war.

Das Gespräch fand in Presse, Rundfunk und Fernsehen ein großes Echo und wurde als nachdrückliche Wahrnehmung meiner verfassungsrechtlich verbürgten Wächterfunktion in Datenschutzangelegenheiten verstanden.

Zu meiner Überraschung warf mir der Staatssekretär des Niedersächsischen Innenministeriums mit Presseinformation Nr. 159/96 vom 12. Juli 1996 einen "eklatanten Vertrauensbruch" vor. Wörtlich heißt es weiter: "Hintergrund dieser Anschuldigung sind die Äußerungen Dronschs zu einem ersten internen Arbeitsentwurf eines Referenten des Niedersächsischen Innenministeriums zur Novellierung des Niedersächsischen Gefahrenabwehrgesetzes. ... Zwischen den niedersächsischen Behörden ist es üblich, Arbeitsentwürfe und Überlegungen zunächst intern zu beraten und zu diskutieren. Dies ist offensichtlich mit dem Datenschutzbeauftragten nicht mehr möglich. Er wird künftig keine Gelegenheit mehr erhalten, Rohentwürfe von Beamten zu finsteren Maßnahmen der Landesregierung aufzubauschen.

Herr Dronsch wird in Zukunft nur noch das bekommen, was ihm zusteht."

Bemerkenswert ist zunächst, daß gegen mich öffentlich Vorwürfe erhoben wurden, ohne mit mir vorher zu sprechen; ein solches Gespräch hätte die Haltlosigkeit der Vorwürfe ergeben. Das Innenministerium sah es nicht einmal als nötig an, mir seine Presseinformation Nr. 159/96 zukommen zu lassen. Es blieb mir nichts anderes übrig, als die Vorwürfe mit einer eigenen Presseinformation und in Medienauftritten zurückzuweisen.

Am 16. Juli 1996 erreichte mich ein Anruf des Staatssekretärs, der zur Beilegung des Konflikts führte.

Eine Kleine mündliche Anfrage der Abgeordneten Frau Stokar von Neuforn (Bündnis 90/Die Grünen) bereitete der Angelegenheit ein parlamentarisches Nachspiel (Frage Nr. 18 für die Fragestunde des Niedersächsischen Landtages am 6. September 1996, LT-Drs. 13/2149). Die Antwort des Niedersächsischen Innenministeriums auf diese Anfrage veranlaßt mich, die weitere Entwicklung der Zusammenarbeit mit diesem Ressort sorgfältig zu beobachten.

3.2 Geschäftsstelle

Die Stellenausstattung der Geschäftsstelle ist seit 1993 unverändert. Bereits im letzten Tätigkeitsbericht (unter Nr. 3.4) habe ich die Stellenausstattung als unzureichend bezeichnet. Die dort genannten Gründe für die Mehrbelastung gelten weiter; besonders verstärkt haben sie sich im nicht-öffentlichen Bereich, und zwar sowohl hinsichtlich der Umsetzung des materiellen Rechts als auch der Bewältigung der technischen Probleme. Die Stellenausstattung meiner Geschäftsstelle ist im Vergleich zu der in anderen Bundesländern sehr ins Hintertreffen geraten. Eine nachhaltige Wahrnehmung meiner Aufgaben ist beim derzeitigen Stellenbestand nicht möglich.

Die Informations- und Kommunikationsmöglichkeiten der Geschäftsstelle wurden im Vergleich zum letzten Berichtszeitraum ausgeweitet:

Zusätzlich zu dem bereits vorhandenen Bürokommunikationssystem ALIS habe ich in der Geschäftsstelle ein Windows NT-Testnetz mit 4 Arbeitsplätzen (Clients) installiert. Damit ist es mir möglich, eigene Erfahrungen im Umgang mit dem Netzwerkbetriebssystem Windows NT und darauf aufbauenden Anwendungsprogrammen zu sammeln. Durch die beabsichtigte stufenweise Erweiterung dieses Systems erhoffe ich mir einen nahtlosen Übergang vom System ALIS auf Windows NT.

Seit Mitte 1996 habe ich direkten Zugriff auf das Internet über einen Einzelplatz-PC. Die Geschäftsstelle ist nunmehr von jedermann aus aller Welt unter der Adresse "lfd@lfd-nds.rrzn-serv.de" zu erreichen. Auch durch die Einführung der elektronischen Post (Electronic-Mail nach

X.400) in der Landesverwaltung (vgl. Nds. MBl. 1996, S. 1258) wurde meine Erreichbarkeit verbessert; ich nutze diesen Dienst, um elektronische Dokumente zu empfangen und sicher zu versenden. Jede Mitarbeiterin und jeder Mitarbeiter der Geschäftsstelle kann auf diesen Dienst direkt vom Arbeitsplatz aus zugreifen. Für die interne Kommunikation mit den übrigen Landesbeauftragten sowie dem Bundesbeauftragten für den Datenschutz nutze ich die vom Bundesbeauftragten eingerichtete Mailbox.

3.3 Außenprüfungen und Beratungen

Im Berichtszeitraum habe ich ein weit gefächertes Prüfungs- und Beratungsprogramm durchgeführt.

Der Schwerpunkt materiell-rechtlicher Prüfungen im öffentlichen Bereich lag bei der Polizei (z.B. Führung von Kriminalakten in Polizeiinspektionen) und bei der Schulaufsicht (Führung von Personalakten und Nebenakten); im nicht-öffentlichen Bereich waren Adressenhandel und Auskunfteien zentrale Prüfungspunkte. Technisch-organisatorische Kontrollen führte ich bei zahlreichen Städten und Gemeinden, der Medizinischen Hochschule Hannover und dem Landesamt für Ökologie sowie im nicht-öffentlichen Bereich vor allem bei Mailbox-Betreibern und Aktenvernichtern durch.

Schließlich wurde auch eine Reihe von Kontrollen durchgeführt, bei denen sowohl materiell-rechtliche als auch technisch-organisatorische Punkte untersucht wurden. Hierzu gehörten das staatsanwaltschaftliche Verfahren SIJUS-Straf, die Meldeverfahren in drei niedersächsischen Meldeämtern und das Verfahren bei Telefonüberwachungen im Mobilfunkbereich.

Durch diese Prüfungen konnten zwar viele Mängel aufgedeckt und erhebliche Überzeugungsarbeit geleistet werden; insgesamt ist die Zahl der Prüfungen aber niedriger als in den Vorjahren. Die weiter steigenden Belastungen durch die rasante Fahrt in die Informationsgesellschaft ließen - bei dem jetzigen Personalbestand - einen größeren Einsatz für Außenprüfungen nicht zu.

Im Berichtszeitraum ist die Zahl der Beratungsgespräche erneut gestiegen. Insbesondere aus der Privatwirtschaft werde ich zunehmend mit Beratungsersuchen konfrontiert. Ich bin gerne bereit, den Firmen im Rahmen meiner begrenzten Möglichkeiten hilfreich zu sein. Dies kann aber nicht dazu führen, daß ich für Unternehmen Datenschutzkonzepte entwerfe oder Vorschläge ausarbeite, wie Unternehmensziele datenschutzgerecht erreicht werden können. Wer im Geschäftsleben mit personenbezogenen Daten arbeitet und dabei Geld verdient, muß auch bereit sein, die Datenschutz-Folgekosten aufzubringen und die notwendige Expertise zu bezahlen. Meine Aufgaben nach § 38 BDSG zielen auf hoheitliche Überprüfungs-, nicht auf geldwerte Beratungstätigkeit. Dies soll Unternehmer nicht daran hindern, mich um Rat zu bitten, wenn nach Beteiligung des betrieblichen Datenschutzbeauftragten und sonstiger Experten Zweifel nicht beseitigt

werden konnten. Ich kann dann darlegen, wie ich im Fall einer Prüfung eine spezielle Datenschutzfrage beantworten bzw. behandeln würde. Verwehrt ist es mir dagegen, bestimmten Verfahren ihre datenschutzrechtliche Unbedenklichkeit zu bescheinigen.

3.4 Dateibeschreibungen und das Dateienregister im öffentlichen Bereich

Die Dateibeschreibungen nach § 8 Abs. 1 NDSG und das Dateienregister nach § 22 Abs. 5 NDSG sollen die Verarbeitung personenbezogener Daten der öffentlichen Verwaltung für jedermann transparent machen. Leider sind viele öffentliche Stellen der gesetzlichen Vorlagepflicht bisher nicht nachgekommen. Auswertungen des Dateienregisters, das ich zu führen habe, weisen aus, daß z. B. von insgesamt 38 niedersächsischen Landkreisen bisher nur 16 (rd. 42 %) Dateibeschreibungen vorgelegt haben. Ähnlich sieht die Situation in der Landesverwaltung, z. B. bei den Ministerien aus. Von 10 Ressorts haben mir erst 6 Dateibeschreibungen zugeleitet. Positives ist vom Schulbereich zu vermelden; dank einer guten und umfassenden Information durch das Niedersächsische Kultusministerium sind zwischenzeitlich sehr viele Schulen ins Dateienregister aufgenommen worden.

Die Pflicht zur Dateibeschreibung besteht seit mehreren Jahren. Es ist mir nur schwer verständlich, warum öffentliche Stellen das mit der Dateibeschreibung verfolgte Ziel, Angaben über die Datenverarbeitung für sich selbst und für auskunftsuchende Betroffene durch einen einfachen, strukturierten und damit schnellen Zugriff verfügbar zu haben, derart vernachlässigen. Vom Zweckverband Kommunale Datenverarbeitung Oldenburg (KDO) wurde mit meiner Unterstützung ein automatisiertes Verfahren - "Datenschutzregister" - entwickelt, mit dessen Hilfe sowohl Dateibeschreibungen als auch ein Geräteverzeichnis gemäß § 8 Abs. 2 NDSG elektronisch unter einer Windows-Oberfläche erstellt werden können. Allen Landesbehörden steht das Verfahren "Datenschutzregister" über das Nieders. Landesverwaltungsamt kostenlos zur Verfügung. Ob die schleppende Bestellung des behördlichen Datenschutzbeauftragten mitverantwortlich für die "Verweigerungshaltung" vieler öffentlicher Stellen ist, vermag ich nicht abschließend zu beurteilen.

3.5 Öffentlichkeitsarbeit

Gute Öffentlichkeitsarbeit ist für die Datenschutzbeauftragten eine Voraussetzung für die Realisierung ihres Auftrages. Mein Interesse ist nicht darauf gerichtet, mit Datenschutzskandalen in Presse, Funk und Fernsehen zu erscheinen. Mir ist vielmehr vorrangig daran gelegen, von vornherein Verstöße zu vermeiden.

Auch 1995 und 1996 waren Angehörige meiner Geschäftsstelle und ich an zahlreichen Vortrags- und Diskussionsveranstaltungen beteiligt. Es ging dabei um neue datenschutzrechtliche Regelungen (wie z.B. das NGefAG), um datenschutzrechtliche Einzelthemen oder um

Grundsatzprobleme des Datenschutzes.

Im Berichtszeitraum habe ich wiederum etliche Broschüren und Merkblätter herausgegeben: "Datenschutz und Forschung - Hilfen zur Auslegung der Forschungsklausel nach § 25 NDSG -", "Handels- und Wirtschaftsauskunfteien" (gemeinsam mit den Kollegen in Berlin, Bremen und Hamburg), "Die Gesundheits-Chipkarte: Alles auf eine Karte setzen?" (gemeinsam mit anderen Landesbeauftragten, mit Verbraucherzentralen und mit Patientenstellen), "Datenschutz bei elektronischen Mitteilungssystemen", "Schutzstufenkonzept", "Zugangskontrollmaßnahmen", "Datenschutz beim Anschluß an Multimedia-Dienste", "Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung", "Datensicherung beim Einsatz von Chipkarten" und "Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet". Dieses Material kann, ebenso wie älteres Informationsmaterial, bei mir bestellt werden.

Die Liste der von mir angebotenen Informationen wird bereichert durch "LfD Niedersachsen Info 1.0". Angeregt durch eine vergleichbare Diskette des Landesbeauftragten für den Datenschutz Schleswig-Holstein, habe ich mit Hilfe der Software "MS Help Compiler" und "Profi Install" sowie unter Nutzung der bei mir bereits vorhandenen Software "MS Windows 3.11" und "MS Word für Windows 6.0" eine Informationsdiskette mit folgendem Inhalt erstellt: EU-Datenschutzrichtlinie, Bundesdatenschutzgesetz, Niedersächsisches Datenschutzgesetz, Verwaltungsvorschriften zum NDSG, 20 Orientierungshilfen zum Datenschutz und zur Datensicherheit (z.B. Paßwortgestaltung und -verwendung, Multimedia und Datenschutz, Anschluß an das Internet, Prüfkonzepte für UNIX bzw. Novell-Netzwerke, Einsatz optischer Speicher, Aufgaben und Stellung von Datenschutzbeauftragten). Die Installation sowie die Bedienung des Programmes sind sehr einfach. Dank der aus der "Windows Hilfe"-Funktion bereits vielfältig bekannten Hyperlink-Technik (vergleichbar mit der HTML-Technik bei Web-Browsern im Internet) ist es einfach und zugleich komfortabel möglich, zwischen verschiedenen Informationen bzw. Informationsteilbereichen hin und her zu springen. Die "LfD Niedersachsen Info 1.0" steht seit Mitte 1996 allen Interessierten kostenlos zur Verfügung. Ich habe bewußt darauf verzichtet, ein Copyright geltend zu machen, weil mir daran gelegen ist, einer möglichst großen Anzahl von Interessierten die Nutzung zu gestatten. Dies gilt sowohl für den öffentlichen als auch für den privaten Bereich. Nachdem bereits über 500 Exemplare abgefordert worden sind, bezeugen die erhaltenen Rückäußerungen ein hohes Interesse an dem Angebot. Die erstmalige Zusammenstellung vieler datenschutzrelevanter Informationen in digitalisierter Form scheint eine "Marktlücke" zu füllen. Das positive Echo bestätigt mich in meinem Bemühen, einer breiten Öffentlichkeit einen modernen Zugang zum Datenschutzrecht anzubieten. Gleichzeitig läßt sich damit eine Senkung der Gesamtkosten für die Publikationen erzielen.

Mit der Herausgabe dieses Tätigkeitsberichtes wird gleichzeitig eine neue Version als "LfD Niedersachsen Info 2.0" zur Verfügung gestellt.

Die Version 2.0 wird erstmals neben den bisherigen Informationen auch diesen Tätigkeitsbericht enthalten. Möglich werden damit strukturierte Auswertungen des Berichtes, die gezielte Weitergabe von interessanten Beiträgen oder die Weiterverwendung einzelner Ausführungen in anderen Medien. Für Anregungen und Kritik bin ich dankbar.

3.6 Zusammenarbeit mit anderen Kontrollorganen

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

Gemeinsam mit dem Niedersächsischen Innenministerium nehme ich an den Beratungen des "Düsseldorfer Kreises", des bundesweiten Zusammenschlusses der obersten Aufsichtsbehörden für den nicht-öffentlichen Bereich, teil. Verstärkt wurde die Zusammenarbeit mit den Aufsichtsbehörden für den nicht-öffentlichen Bereich. Gemeinsam mit dem Landesbeauftragten für den Datenschutz Bremen und dem Hamburgischen Datenschutzbeauftragten führte ich zwei bundesweite Workshops für die Aufsichtsbehörden durch, um Erfahrungen auszutauschen und Kenntnisse weiterzugeben. Beide Veranstaltungen - 1995 in Hamburg und 1996 in Hannover - waren sehr erfolgreich.

Mit den kirchlichen Datenschutzbeauftragten fand ein häufiger Gedankenaustausch statt.

An Datenschutzkonferenzen auf europäischer und internationaler Ebene habe ich aus Kostengründen bislang nicht teilgenommen.

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

4.1 Die Informationsgesellschaft

4.1.1 Die rasante Fahrt auf der Datenautobahn

In geradezu dramatischer Fahrt steuern wir in die Informationsgesellschaft. Durch einen gewaltigen Sprung der Computertechnologie sind Informations- und Kommunikationsmethoden entstanden, die noch vor kurzem unvorstellbar schienen. Datenverarbeitung, Telekommunikation und Rundfunk sind nicht mehr getrennt, sondern technisch miteinander verbunden und gehen ineinander über. Selbst die Tagesschau der ARD weist mit "http://www.tagesschau. de" ihr Millionenpublikum darauf hin, daß sie im Internet präsent ist. Die Entwicklung ist für niemanden übersehbar; wir bewegen uns mit rasanter Geschwindigkeit in die vernetzte Gesellschaft. Das "World-Wide-Web" im Internet verwandelt den Personalcomputer in ein Universalmedium. Dieser ist nicht - wie eine alte IBM-Prognose vorhersagte - Spezialisten vorbehalten geblieben, sondern längst zum Alltag in Büros und Wohnungen geworden.

Goldgräber-Zeiten stehen bevor, will man den Schlagzeilen zu Multimedia - dem "Wort des Jahres" 1995 - Glauben schenken. Bill Gates spricht von einem Phänomen, das die Welt verändern wird. Der Unternehmensberater Roland Berger meint gar: "Multimedia läßt keinen Stein auf dem anderen". Im Niedersächsischen Landtag war die Rede von der Revolution einer Informationsgesellschaft, "für die sich nicht mehr die Frage stellt, ob sie gewollt ist, sondern wie sie gestaltet und beeinflußt wird".

Die technische Revolution wird durch folgende Aspekte geprägt:

1. Text, Sprache, Ton, Bild und Film werden digitalisiert, in zentralen oder dezentralen Computern gespeichert und können von jedermann elektronisch abgerufen, ausgewertet und mit anderen Informationen verknüpft werden.

2. Unterschiedliche multimediale Dienste können über ein einziges Gerät genutzt werden; dieses kann das Radio, das Fernsehgerät, die Stereoanlage, die Schreibmaschine, das Bücherregal, ja den Einkaufszettel ersetzen.

3. Weltweit werden bisher getrennte Rechnernetze und Telekommunikationsdienste über Hochgeschwindigkeitsleitungen zusammengeführt.

4. Aus den bisher passiven Konsumentinnen und Konsumenten der Medien werden aktive Sender und Empfänger. Multimedia wird benutzerfreundlich gestaltet und ermöglicht es, auf einfache Weise in weltweiten Informationsnetzen zu "surfen".

Dies alles klingt interessant und verspricht Nutzen für jedermann. Der private Briefwechsel verläßt das Zeitalter der Postkutsche. Elektronisches Zeitunglesen wird zeitnäher, zielgerichteter und schneller. Mit Telearbeit ersparen sich Arbeitnehmerinnen und Arbeitnehmer den Weg ins Büro und bekommen so die Chance, ihre Arbeitszeit flexibel zu gestalten. Kundinnen und Kunden führen ihre Geschäfte vom Sofa aus. Auch der Behördengang kann durch Online-Dialog mit dem Amtscomputer ersetzt werden. Längst haben Unternehmen der Wirtschaft das weltweite Internet als billiges Informations-, Marketing- und Vertriebsmedium entdeckt. Der Standort des Unternehmens und seiner Betriebsstätten spielt keine Rolle mehr und kann schnell verändert werden. Die Vernetzung ganzer Unternehmen wird in der vorhandenen Internet-Infrastruktur als geschlossene Benutzergruppe mit gleicher Technik und Software als "Intranet" verwirklicht. Für den Vertrieb über Internet werden Unternehmen mit dem Argument geworben, das neue Medium liefere viele neue, kostenlose Kundendaten und lasse so zielgruppenspezifische Planungen zu.

Auch die öffentliche Verwaltung ist dabei, sich dieser neuen technischen Möglichkeiten zu bedienen. Der Zwang zur "Verschlankung" des Staates mit dem Ziel der Kosteneinsparung führt dazu, daß sich die Landes- und Kommunalverwaltungen mit moderner Informations- und Kommunikationstechnik ausstatten. Es wird eine schnelle und kostengünstige Vernetzung ganzer Verwaltungszweige gesucht. Die Landesregierung hat eine Landesinitiative zur Unterstützung der niedersächsischen Informations- und Kommunikationswirtschaft gestartet (vgl. 4.4). Das Land Bayern ist dabei, ein öffentliches Netz, das "BAYERNNETZ" aufzubauen, das vorrangig von bayerischen Hochschulen und staatlichen Behörden zum Datenverkehr benutzt werden soll, aber auch für Multimedia-Pilotversuche und für die Sprachkommunikation in "corporate networks" bereitsteht. Allen Bürgerinnen und Bürgern wird darüber hinaus ein kostenloser Internet-Zugang angeboten. Das Land Sachsen-Anhalt plant, das Landesverwaltungsnetz als Intranet-Lösung zu realisieren.

4.1.2 Multimedia in Niedersachsen

Das Niedersächsische Ministerium für Wirtschaft, Technologie und Verkehr hat 1995 in Zusammenarbeit mit der Unternehmensberatung Roland Berger & Partner GmbH ein Konzept zur Unterstützung der Informations- und Kommunikationswirtschaft entwickelt. Die Landesregierung hat dieses Konzept als Landesinitiative im September

1995 beschlossen. Das Konzept besteht aus drei Kernelementen:

1. Entwicklung und Demonstration von Multimedia-Anwendungen in sechs für Niedersachsen repräsentativen Anwendungsbereichen,

2. Sicherstellung einer breitbandigen Telekommunikationsinfrastruktur zu kostengünstigen Tarifen und

3. Initiierung von strukturpolitischen Entwicklungen, z.B. Unterstützung von Multimedia-Unternehmens-Gründungen.

Für die verschiedenen Anwendungsfelder wurden sieben Projektgruppen gebildet. Besonders gespannt bin ich auf das Projekt "Multimed", mit dem ein interaktives medizinisches Fachinformations- und Kommunikationssystem für Krankenhäuser, niedergelassene Ärzte und Patienten geschaffen werden soll. Das gleiche gilt für das Projekt "Telearbeit", mit dem in strukturschwachen Regionen Arbeitsplätze bei den Arbeitnehmerinnen und Arbeitnehmern zu Hause geschaffen werden sollen. Beides sind Projekte, bei denen dem Datenschutz besondere Bedeutung zukommt. Leider wurde ich bisher nur unzureichend über die Landesinitiative für die Informations- und Kommunikationswirtschaft unterrichtet. Erst am 5. Februar 1996 erfuhr ich im Rahmen der öffentlichen Veranstaltung "4. Niedersachsen-Dialog" von dem beschlossenen Konzept.

Der Niedersächsische Landtag führte - initiiert durch einen Entschließungsantrag der CDU-Fraktion (LT-Drs. 13/1326) - im Februar 1996 eine öffentliche Anhörung "Multimedia-Strategie-2000 - Aktionsplan für eine offensive Nutzung neuer Informationstechniken" durch. Ich habe die Gelegenheit für eine datenschutzrechtliche Bewertung des Aktionsplans genutzt und erläuterte den Landtagsausschüssen die Datenschutz-Probleme und die Regelungsnotwendigkeiten für Multimedia-Anwendungen. Auf zwei Gebieten sehe ich noch Untersuchungs- und Erprobungsbedarf:

- Technikfolgenabschätzung

Für alle Teilprojekte sollte eine Technikfolgenabschätzung durchgeführt werden - gleich ob die Verarbeitung öffentliche Stellen oder Unternehmen der Wirtschaft betrifft.Dies fordern § 7 Abs. 3 NDSG und Art. 20 der EU-Datenschutzrichtlinie, wenn bei der Verarbeitung personenbezogener Daten spezifische Risiken für die Rechte und Freiheiten von betroffenen Personen entstehen können.

- Sicherungstechnologie

Für die niedersächsischen Initiativen ist ein Grundschutzstandard zu entwickeln und zu erproben, der Kryptoverfahren zum Schutz der Vertraulichkeit und Integrität von Dokumenten und eine digitale Signatur zur Kontrolle der Authentizität und Urheberschaft umfassen sollte (vgl. 4.3).

Die Landtags-Entschließung "Multimedia-Strategie-2000" (LT-Drs. 13/2322) spricht die Erwartung aus, "daß auf dem niedersächsischen Weg zur Informationsgesellschaft digitale Schlüsselprojekte gezielt gefördert werden". Sie enthält von mir geforderte Aussagen zum Datenschutz. Ich habe dem Niedersächsischen Wirtschaftsministerium mein Gutachten "Multimedia und Datenschutz" zur Verfügung gestellt und meine Unterstützung beim Erarbeiten der Technikfolgenabschätzung und des Datensicherungskonzepts angeboten. Beides wurde bisher nicht in Anspruch genommen. Ich weiß daher nicht, ob die gesetzlichen Voraussetzungen des § 7 Abs. 3 NDSG, vor der Entscheidung über den Einsatz von automatisierten Verfahren derartige Gefahrenabschätzungen vorzunehmen und Sicherungskonzepte zu erstellen, beachtet werden.

4.1.3 Regelungsbedarf

Die öffentliche Diskussion um Probleme im Internet und bei Multimedia vermittelt manchmal den Eindruck, als spielten sich alle Aktivitäten auf der Datenautobahn im rechtsfreien Raum ab. Der "Information-Super-Highway" gehöre niemandem; jeder könne tun, was er wolle. Ähnlich wie beim grenzüberschreitenden Satellitenfernsehen scheinen auch bei Multimedia nationale Gesetze ausgehebelt zu sein. Dieser Eindruck trügt: Der im Grundgesetz verankerte Schutz personenbezogener Daten gilt, ganz gleich ob die Daten in Akten verwaltet, in Dateien gespeichert oder über das Internet verbreitet werden.

Datenschutz wird angesichts der Risiken der modernen Informationsgesellschaft zu einer wichtigen rechtlichen und politischen Aufgabe. Die Empfehlung des Rates für Forschung, Technologie und Innovation an die Bundesregierung sagt dazu im Gutachten "Informationsgesellschaft - Rechtliche Rahmenbedingungen": "Ein konsequenter Datenschutz zählt zu den zentralen Akzeptanzvoraussetzungen der Informationsgesellschaft". Dafür muß ein einheitlicher Ordnungsrahmen geschaffen werden, der eindeutige Kriterien für die Abgrenzung der neuen Medien- und Telekommunikationsdienste und präzise einheitliche Regelungen zum Datenschutz und zur Datensicherheit enthält. In der öffentlichen Anhörung "Multimedia-Strategie-2000" habe ich den Landtagsausschüssen folgende Grundsätze dargelegt:

- Es muß sichergestellt werden, daß Multimedia-Nutzende nur dann ihre personenbezogenen Daten offenbaren müssen, wenn dies zur Erbringung des gewählten Dienstes erforderlich ist.

- Die Zwecke, für die personenbezogene Daten gespeichert, genutzt und weitergegeben werden dürfen, sind restriktiv festzulegen. Auch die interne Nutzung der Daten durch den Diensteanbieter ist zu regeln, damit keine Verhaltensprofile der Nutzerinnen und Nutzer erstellt werden.

- Diensteanbieter haben grundsätzlich Anonymität und Vertraulichkeit

zu garantieren. Die anonyme Bezahlung (z.B. mit vorausbezahlter Karte, prepaid) sollte den Diensteanbietern als anzubietende Option vorgeschrieben werden.

- Der bisher an formellen Kriterien anknüpfende Rundfunkbegriff muß entsprechend Art. 9 EU-Datenschutzrichtlinie durch einen materiellen Rundfunkbegriff abgelöst werden.

- Die Vorschriften zur Datensicherheit sind den sich weiterentwickelnden Anforderungen der modernen Informations- und Kommunikationstechnik anzupassen. Empfohlen wird die Festschreibung eines Grundschutzstandards. Zu den erforderlichen technischen Sicherheitsmaßnahmen zählt insbesondere der Einsatz von Verschlüsselungsverfahren. Dafür ist in offenen Netzen eine Sicherheitsinfrastruktur, z.B. unter Einbeziehung durch Trust-Center, zu schaffen. Anforderungen und Zulassung sind gesetzlich zu regeln.

- Die Befugnis staatlicher Stellen zur Entschlüsselung von Dokumenten darf nur in einem engen Rahmen erteilt werden. Die Kriterien hierfür sind präzise und eindeutig zu regeln.

- Kommerzielle Diensteanbieter außerhalb der EU sind zu verpflichten, innerhalb der EU einen datenschutzrechtlich zur Verantwortung zu ziehenden Vertreter zu benennen, um Datenschutzverstöße im internationalen Netz wirksam ahnden zu können.

- Für Multimedia ist eine Datenschutzkontrolle zu schaffen, die die grenzüberschreitenden Multimedia-Dienste und die weltweite Vernetzung effektiv kontrollieren kann. Hierfür ist wohl eine dezentrale, aber vernetzte Kontrollinfrastruktur am besten geeignet. Die Kontrollinstanzen sollten getrennt sein von der Gewerbe- bzw. der Rundfunkaufsicht. Sie müssen mit ausreichenden materiellen und personellen Ressourcen sowie mit wirksamen Kontroll- und Sanktionsrechten ausgestattet werden.

Diese Grundsätze konnten bei den Entwurfsarbeiten zur Neuregelung des Informationstechnikrechts zumindest teilweise umgesetzt werden. Bund und Länder sind dabei, einen einheitlichen Ordnungsrahmen für das Telekommunikations- und Medienrecht zu definieren. Die insofern relevanten Gesetze sollen aufeinander abgestimmt werden. Auch die Novellierung des BDSG und der Länderdatenschutzgesetze aufgrund der EU-Datenschutzrichtlinie sollte genutzt werden, um aufeinander abgestimmte Datenschutzregelungen zu schaffen. Angesichts der stürmischen Entwicklung der Technik und angesichts der ungebremsten Expansion des Technikeinsatzes muß schnell gehandelt werden. Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis müssen für alle Nutzerinnen und Nutzer gegenüber allen Netzbetreibern und Diensteanbietern ungeachtet ihrer Rechtsformen, ihrer Kundenstruktur und ihres Firmensitzes auf einem hohen Niveau gesichert werden. Beim Internet, bei Online-Diensten, bei interaktiven Verteil- und Videodiensten oder beim digitalen Fernsehen handelt es sich allerdings um weltweite Kommunikationsmittel, die nicht

allein durch nationales Recht gesteuert werden können. Zur Gewährleistung des Datenschutzes und der Sicherheit in der Informationstechnik bedarf es daher einer internationalen Zusammenarbeit mit dem Ziel der Rechtsvereinheitlichung auf hohem Datenschutzniveau. Die gegenwärtige Entwicklung im Telekommunikations- und Medienrecht wird in Kapitel 8. beschrieben.

4.1.4 Technikgestaltung unterstützt Datenschutz

Die Erfahrungen der Vergangenheit zeigen, daß normative Vorgaben durch Technik gefördert werden müssen. In Befragungen über Hindernisse bei der Einführung von Multimedia wird nicht nur von Bürgerinnen und Bürgern, sondern auch von Unternehmen der interessierten Wirtschaft an erster Stelle fehlende Datensicherheit genannt. Es sollte jede Chance genutzt werden, durch effiziente Technikgestaltung das informationelle Selbstbestimmungsrecht und die vertrauliche Kommunikation zu schützen. Nur durch eine hinreichende technische Infrastruktur wird es gelingen, weltweit einen angemessenen Datenschutzstandard durchzusetzen sowie Vertrauen und Akzeptanz für Multimedia zu schaffen. Sicherungstechnik muß zum integralen Bestandteil der Informations- und Kommunikationstechnologie werden. Multimedia-Dienste und -Einrichtungen sind so zu gestalten, daß keine oder möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden. Den Nutzerinnen und Nutzern sind grundsätzlich wahlweise auch anonyme Nutzungs- und Zahlungsformen anzubieten. Soweit eine anonyme Mediennutzung nicht realisiert werden kann, sollte durch andere Verfahren, z.B. durch die Verwendung von Pseudonymen, ein unmittelbarer Personenbezug vermieden werden. Zum Grundschutz in Multimedia sollten zudem Verschlüsselungsverfahren zählen, um die Vertraulichkeit und Integrität der übertragenen Daten sowie eine sichere Identifizierung und Authentifizierung zwischen Teilnehmern und Anbietern zu gewährleisten (vgl. 4.3 und Anlage 16). Wir stehen noch am Anfang der Multimedia-Entwicklung und sollten jetzt die Weichen richtig stellen. Eine so gestaltete Sicherungstechnologie kann manches rechtliche Verbot überflüssig machen.

4.2 Internet - das Netz der Netze

4.2.1 Was ist das Internet?

Das Internet ist das größte Datennetz der Welt und verbindet heute über 6 Millionen Rechner in mehr als 140 Ländern. Die Zahl der Internet-Nutzerinnen und -Nutzer wird auf über 50 Millionen geschätzt, im Jahr 1999 sollen es 200 Millionen Menschen sein. Über das Internet wird eine unvorstellbar große Informationsfülle erschlossen. Der Datenumsatz pro Monat wird mit 1,5 Tera-Bytes angegeben. Die Datenwachstumsrate in Deutschland soll zur Zeit 23% pro Monat betragen. Das Internet ist inzwischen mit seinem World-Wide-Web multimedial geworden, d.h. es lassen sich nicht nur Daten, sondern auch Bild- und Toninformationen übertragen, in naher Zukunft selbst Bewegtbilder in guter Qualität. Die Kommunikation erfolgt nach dem einheitlichen Übertragungsstandard TCP/IP (Transmission Control Protocol/Internet Protocol). Jeder Rechner

im Internet erhält eine eindeutige numerische Adresse, die IP-Adresse. Die zu übertragenden Daten werden in "Pakete" zerlegt, die mit der Absender- und der Empfänger-IP-Adresse versehen werden. Den Weg einer Nachricht sucht sich das System selbst; er ist nicht vorherbestimmbar, sondern allenfalls nachvollziehbar. An jedem an einem Kommunikationsvorgang beteiligten Knotenrechner werden sowohl die Verbindungsdaten als auch der Kommunikationsinhalt zwischengespeichert.

Die ursprünglich militärische und wissenschaftliche Nutzung wird zunehmend durch die gewerbliche Nutzung für Handel, Werbung und Unterhaltung verdrängt. Banken versuchen das Internet-Banking "informationsgesellschaftsfähig" zu machen; sie versprechen Sicherheiten, ohne allerdings Garantien übernehmen zu wollen. Auf der Elektronik-Ausstellung "CeBIT-Home" in Hannover stellte sich 1996 erstmalig die Landesregierung im Internet vor. Der Niedersächsische Landtag will in Kürze folgen. Aber auch politischer Extremismus, Gewalt und Pornographie haben sich Zugang zum Netz der Netze verschafft; das Internet wird - wie jedes andere technische Vehikel - zur Begehung von Straftaten genutzt.

Die wichtigsten Internet-Dienste sind:

E-Mail Electronic Mail ermöglicht das Verschicken von "elektronischen Briefen" zwischen mehreren Computerbenutzern. Die Nachrichten können aus Texten, Programmen, Grafiken oder Tönen bestehen. Sender und Empfänger müssen jeweils eine eindeutige E-Mail-Adresse besitzen, die einer postalischen Anschrift ähnelt (Form: Name@Anschrift).

Usenet-News Öffentliche Nachrichten werden im Internet in thematisch gegliederten Diskussionsforen (Newsgroups) ausgetauscht. Ein Usenet (Kurzform für User's Network) gleicht einer riesigen Zeitung mit Fachartikeln, Leserbriefen und Kleinanzeigen. Zur Zeit gibt es etwa 16000 verschiedene Newsgroups, in denen rund 4 Millionen Artikel pro Monat geschrieben werden.

Telnet Mit Telnet ist es möglich, auf einem entfernten Rechner eine Terminalsitzung aufzubauen (Remote Login). Damit kann man z.B. Informationssysteme wie Spezial-Datenbanken und Bibliotheksregister nutzen. Auch Fernwartung von Kundenrechnern wird so durchgeführt.

WWW World-Wide-Web ist ein neues Verfahren im Internet, das Texte, Sprache, Töne, Bilder und Filme erschließt. Die Benutzerin bzw. der Benutzer bewegt sich per Mausklick durch die weltweiten Angebote. Dabei wird er automatisch einem Rechner zum nächsten verbunden, ohne selbst Steuerbefehle geben zu müssen (sog. Hypertext-Mechanismus).

Finger Finger ist ein Werkzeug zur Suche von Informationen über Personen und Rechner, die an der Kommunikation im Internet beteiligt sind. Darüber können z.B. personenbezogene Daten (Name, E-Mail-

Adresse, Telefonnummer, Arbeitszeit, öffentliche Schlüssel usw.) oder sicherheitsrelevante Informationen über angeschlossene Rechner ermittelt werden.

Die Auffahrt zur "Datenautobahn" Internet bieten Netzbetreiber, Online-Dienste-Anbieter, spezielle Anschlußanbieter (sog. Internet-Provider) und auch die größeren Mailbox-Betreiber. Für private Nutzerinnen und Nutzer fallen neben einer monatlichen Anschluß-Gebühr meist nur noch die Telefonkosten für die Anrufe zum Rechner des Internet-Providers im Ortstarif an.

4.2.2 Probleme und Risiken

Mit Problemen und Risiken im Internet beschäftige ich mich seit einem Jahr intensiv. Im Mai 1996 habe ich in meiner Geschäftsstelle einen Internet-Anschluß eingerichtet, mit dem ich Risiken für den Datenschutz im Internet untersuche und mit dem ich Bürgerbeschwerden über Internet-Verstöße nachgehe.

Eine anonyme Nutzung ist dem Internet bis heute fremd. Jeder Tastendruck hinterläßt Spuren. Daraus lassen sich Nutzungs- und Kommunikationsprofile erstellen. So kann z.B. der Internet-Provider feststellen, wer wann welche Information abgerufen hat und wer mit wem elektronische Nachrichten ausgetauscht hat. Auch ein noch so hoher Schutz am eigenen Endgerät bleibt wirkungslos, weil Kommunikationsdaten auf ihrem Weg durch die Medienwelt beliebig ausgespäht werden können. Die Gefahr des Ausspähens gilt selbst für einen Kommunikationsvorgang zwischen zwei Teilnehmern der gleichen Stadt. Ein solcher Vorgang kann im Internet über Rechner im Ausland (z.B. USA oder Japan) geführt werden. Weitere Gefahren erwachsen aus der völlig unsicheren Netzinfrastruktur des Internet. Schwächen finden sich z.B. bei den Protokollen für die Datenübertragung, bei der Implementierung und Installation der Programme für die Internet-Dienste sowie bei den Betriebssystemen der angeschlossenen Rechner. Potentielle Angreifer kennen bestehende Sicherheitslücken und verfügen über große Rechnerkapazitäten sowie über die Zeit, um am Internet angeschlossene Rechner auszuforschen und zu bedrohen. Viele der schon heute an das Internet angeschlossenen Rechnersysteme weisen Schwachstellen auf, wie erfolgreiche Eindringversuche von Hackern belegen. Diese verschaffen sich oft mit wenig Aufwand unberechtigten Zugang zu fremden Rechnern, spähen Daten aus und manipulieren oder löschen diese.

Bei der Diskussion über die gesellschaftlichen Risiken des Internets wird bisher viel über die Verbreitung von Kinderpornographie, von Mord- und Gewaltdarstellungen sowie über rechtsradikale Inhalte geredet. Zu wenig Aufmerksamkeit finden dagegen die Gefahren, die das Internet für den Schutz des Persönlichkeitsrechts darstellt. Internet-Nutzer greifen, ohne sich Gedanken über mögliche Datenspuren zu machen, auf die verschiedenen Dienste zu; sie senden unbekümmert persönliche und intime Dokumente. Selbst Kreditkartennummern werden unverschlüsselt ins Netz gespeist. Im Internet entstehen auf diese

Weise vielfältige Konsumentendaten, die - durch kostenfreie Software unterstützt - zu sensitiven Datensammlungen zusammengeführt werden können.

Mitglieder der neuen Informationsgesellschaft sollten grundsätzlich von einer unsicheren Infrastruktur ausgehen, der sie ihre Informationen anvertrauen. Aber auch unbeteiligte Dritte können in die Netze des Internet geraten, wie einige Beispiele aus meiner Prüfpraxis beweisen:

- Mit Suchprogrammen wie "deja news" lassen sich Autorenprofile aller in Newsgroups eingestellten Nachrichten erstellen. Auf diese Weise werden Hobbies und intime Neigungen für jedermann sichtbar.

- Das in Washington ansässige "Center of democracy and technology" beweist in Sekundenschnelle, daß jeder Internet-PC "gläsern" ist. Eine Abfrage dort wird mit den Eingangssatz beantwortet: "Hallo, hier ist das, war wir über Dich wissen." Dann wird einem das eigene benutzte Betriebssystem, der Internet-Browser und der Zwischenspeicher des Internet-Anbieters angegeben.

- Zu digitalen Brandzeichen können "cookies" werden, die im Internet angewählte Rechner gern auf der Festplatte von Internet-Surfern hinterlassen. Damit werden die Rechnereinstellungen gespeichert, die bei der nächsten Einwahl automatisch wieder aufgerufen werden können. Die netten "cookies" werden ungefragt hinterlegt und meist für sehr lange Zeit gespeichert (Ende 1999). Sie verraten detaillierte Informationen über Netzgewohnheiten des PC-Nutzers auch an interessierte Dritte.

- Internetdienste finanzieren sich immer stärker aus Werbeanzeigen. Deshalb überrascht es nicht, daß z.B. auf eine Suchanfrage bei "lycos" zuerst eine gezielte Werbung folgt, ehe die gestellte Suchanfrage beantwortet wird.

- Ein Hochschulangehöriger beobachtete über das Universitätsnetz den Bildschirm einer Kollegin, um sie über elektronische Nachrichten oder nach Arbeitsschluß zu belästigen. Mit den UNIX-Funktionen "finger", "who" und "last" gelangte er an die Anwesenheitsdaten.

- Mehrere niedersächsische Hochschulen wollten das Verzeichnis aller Mitarbeiter und das komplette Vorlesungsverzeichnis über Internet verfügbar machen. Was als Abdruck in einem Vorlesungsverzeichnis sinnvoll sein kann, ist elektronisch aufbereitet und weltweit verfügbar ein Risiko für das Persönlichkeitsrecht. Voraussetzung für dieses Verfahren ist die schriftliche Einwilligung der Betroffenen.

- In einer "c-box" finden sich Kunstschaffende unter der Überschrift "Kreativ-Teams", z.B. Maler und Grafiker, mit Name, Adresse, Telefon- und Fax-Nr. sowie Art der Beschäftigung, ohne vorher gefragt worden zu sein. Die Folge: Ein Bombardement mit Werbung, teilweise aus fernen Ländern. Werden solche Listen im Ausland gespeichert, gibt es

keinerlei Handhabe gegen solche Belästigungen.

- Die "Food and Drug Administration" (FDA), eine US-Behörde, listet in einer Art behördlichem Pranger vollständig die Versendung von Medikamenten, die in den USA nicht zugelassen sind, im Internet mit genauer Angabe des versendenden Apothekers und des Datums auf (vgl. 5.4).

Das weltweite Internet ist bisher ein System ohne organisierte Verantwortlichkeit und ohne Kontrolle. Versuche von Online-Diensten, nationale Zugänge zu sperren, ließen sich ohne weiteres umgehen; auch noch so gute nationale Regelungen haben nur sehr begrenzte Wirkung. Auch die deutschen Datenschutzbeauftragten und die Aufsichtsbehörden für den nicht-öffentlichen Bereich haben nur wenig Möglichkeiten zur Einflußnahme. Uns bleibt häufig genug nur die Aufklärung über bestehende Gefahren und Risiken.

4.2.3 Empfehlungen

Jedem, der vor der Entscheidung steht, ob er das Internet nutzen möchte, empfehle ich, sich vorher eingehend damit zu befassen, Inhalt und Nutzen des Internet zu prüfen und sich beraten zu lassen, welche Absicherungsmöglichkeiten für den eigenen Rechneranschluß vorhanden sind. Öffentliche Stellen Niedersachsens sind grundsätzlich verpflichtet, vor der Entscheidung über den Internet-Anschluß einen Erforderlichkeitsnachweis zu führen und eine Technikfolgenabschätzung zu erstellen (§ 7 Abs. 3 NDSG). Hierfür ist der Kommunikationsbedarf zu beschreiben, die Gefahren sind zu analysieren, Sicherungen zu konzipieren und die Restrisiken abzuschätzen. Es muß geprüft und nachgewiesen werden, daß der Anschluß zwingend erforderlich ist. Dabei sollte wegen der besonderen Gefahrenlage im Internet ein strenger Maßstab angelegt werden. Kommunikationsmöglichkeiten haben sich am Kommunikationsbedarf zu orientieren. Auf Grund der ermittelten Anforderungen und der erforderlichen Dienste sind die unterschiedlichen Anschlußmöglichkeiten - zentraler Zugang oder Anschluß einzelner Rechner - zu untersuchen.

Für diese Untersuchungen biete ich die "Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet" an, die ich zusammen mit den Datenschutzbeauftragten des Bundes und der Länder erarbeitet habe. Auch unterstütze ich im Rahmen meiner begrenzten Kapazitäten die Erarbeitung von Technikfolgenabschätzungen. Zwar wendet sich die Orientierungshilfe primär an die öffentlichen Stellen Niedersachsens, doch enthält sie auch wichtige Informationen für die Internet-Entscheidung von Bürgerinnen und Bürgern. Sie wird an jeden Interessierten kostenfrei abgegeben. Darüber hinaus empfehle ich dem privaten Internet-Surfer folgendes "Kochrezept":

- Informieren Sie sich gründlich über die Risiken des Netzes.

- Wählen Sie Verfahren zur anonymen Internet-Nutzung (z.B.

Verwendung von Proxy-Servern, "anonymous remailer").

- Halten Sie sich bei der Vernetzung sensitiver Anwendungen zurück.

- Wenn Sie Ihr Rechnernetz ans Internet anschließen wollen, schützen Sie dies durch Firewall. Auch hier gilt die Lebensweisheit "Doppelt hält besser".

- Verwenden Sie Verschlüsselungsverfahren zur Wahrung der Vertraulichkeit und der Integrität der übermittelten Informationen (z.B. Pretty Good Privacy; das Programm ist unter "ftp://ftp.cert.dfn.de/pub/pgp/" für alle gängigen Rechnertypen kostenfrei erhältlich).

- Verwenden Sie Einmal-Paßwörter als Schutz gegen Ausforschungsversuche.

- Benutzen Sie die Option "Network: Preferences: Protocols" gegen "cookie"-Protokolle.

- Benutzen Sie die Funktion "x-no-archive: yes" als Schutz gegen die Erstellung von Autorenprofilen.

- Prüfen Sie Daten aus dem Netz grundsätzlich auf Virenbefall.

- Beachten Sie die Anstandsregeln im Internet ("Netiquette"). Diese sorgen für ein wenig Netzkultur, auch wenn sie nicht umfassend und nicht durchsetzbar sind.

4.3 Verschlüsselung: Wirksamer Impfstoff gegen unsichere Datenübertragung

4.3.1 Warum gerade ich?

Heutzutage werden Unmengen von personenbezogenen Daten über Kabel oder per Satellit hin- und hergeschickt. "Auf der Datenautobahn gibt es zur Zeit nur gläserne Fahrer". Dies ist das Ergebnis einer Untersuchung: Die bloße E-Mail-Adresse genügte, um 150 Angaben über einen Internet-Nutzer zusammenzutragen. Weder Absender noch Empfänger haben Einfluß darauf, welchen Weg die Daten während der Übertragung nehmen und wer sie zu sehen bekommt. Auch nach vertraglichen Absicherungen mit den Netzbetreibern oder den Service-Providern, bei Einrichtung von geschlossenen Benutzergruppen oder bei Schaltung von Standleitungen bleibt ein hohes Risiko bestehen, so daß Verbindungs- und Inhaltsdaten Unbefugten "in den Schoß fallen" können. Auch die bisherigen Telekommunikationsmethoden wie Telefon, Telefax oder Funk sind Lauschgefahren ausgesetzt. Telefongespräche oder Datenübertragungen über ISDN können abgehört werden, wenn

man über entsprechende Geräte verfügt, die frei zu kaufen sind. Allein die Telekom soll hiervon 12.000 Testgeräte - sicherlich mit anderer Zweckbestimmung - besitzen. Sprechfunkverkehr von Sicherheitsdiensten oder das mobile Haustelefon sind oft mit einfachsten Mitteln abhörbar. Faxsendungen mit sensiblen Inhalten - etwa Anzeigen nach dem Geldwäschegesetz - werden versehentlich an Unbeteiligte gefaxt.

Diesen Risiken kann nur mit einem Mittel wirklich wirkungsvoll begegnet werden: mit der Kommunikationsverschlüsselung während der Übertragung. Werden z.B. Daten vor der Übertragung mit einem sicheren Verfahren - z.B. RSA, IDEA oder DES, besser Triple-DES - verschlüsselt und erst nach der Übertragung in sicherer Umgebung entschlüsselt, so wird eine sehr hohe Übertragungssicherheit erreicht - mehr Sicherheit, als sie bei der herkömmlichen Briefpost möglich wäre. Die Datenschutzbeauftragten fordern daher in zwei Entschließungen die Einführung sicherer kryptografischer Verfahren bei der Übertragung von personenbezogenen Daten (Anlagen 3 und 21).

4.3.2 Verschlüsselung ist günstiger als Sie denken

Als Argument gegen die Einführung einer Verschlüsselung werden mir bei Kontrollen oft die hohen Anschaffungs- und Personalkosten entgegengehalten. Es wird häufig behauptet, daß die Rechner durch die Verschlüsselung stark belastet würden und hohe Leistungsverluste zu erwarten wären. Erfahrungen zeigen aber, daß bei den heutigen Rechnerleistungen und den verfügbaren Verschlüsselungsprogrammen diese Verluste fast immer vernachlässigbar sind; den Engpaß bilden ohnehin meist die teuren Übertragungsleitungen, die durch eine Verschlüsselung praktisch nicht stärker belastet werden.

Verschlüsselungssoftware gibt es oft zum Nulltarif. So wird z.B. das Verschlüsselungsprogramm PGP (pretty good privacy) im Internet kostenlos angeboten (vgl. 4.2.3). Andere Programme, wie WISO-CRYPT oder für die öffentliche Verwaltung MIC vom Bundesamt für die Sicherheit in der Informationstechnik (BSI), sind ebenfalls kostenlos erhältlich. In anderen Fällen enthalten Anwendungsprogramme bereits Verschlüsselungsmöglichkeiten. Hardwarebasierte Verschlüsselungswerkzeuge, etwa transparent zuschaltbare Kryptoboxen oder chipkartenunterstützte Systeme, gibt es natürlich nicht umsonst. Sie bieten dafür aber besonders komfortable Lösungen oder zahlreiche zusätzliche Nutzungsmöglichkeiten. Chipkartensysteme sind wegen des Kostensturzes bei Kartenlesern sehr günstig geworden.

Auch die Personalkosten werden überschätzt. Sicherlich ist für die Schlüsselverwaltung Zeit und Arbeitsaufwand erforderlich. Es ist aber im allgemeinen nicht notwendig, Trust Center mit einem größeren Mitarbeiterstab einzurichten. Schlüssel können direkt zwischen den Nutzern ausgetauscht werden. Auch wenn die Verschlüsselung für die Nutzer völlig transparent und damit sehr komfortabel ablaufen soll, ist ein Schlüsselmanagement nicht zwingend erforderlich. Übertragungsprotokolle können so gestaltet werden, daß sie bei einem

Verbindungsaufbau den öffentlichen Schlüssel vom Empfänger erfragen und hiermit verschlüsseln. Nur der Empfänger kann dann mit seinem privaten Schlüssel die Nachricht entschlüsseln. Dieses Verfahren funktioniert mit den geeigneten Zusatzgeräten sogar beim ISDN-Sprachdienst. Aber auch eine zentrale Schlüsselverwaltung kann weitgehend automatisch arbeiten; die Personalkosten können gering gehalten werden.

4.3.3 "Digitale Signatur" sichert die Echtheit von Daten

Verschlüsselung kann nicht nur zur Wahrung der Vertraulichkeit eingesetzt werden, sondern dient mit Verfahren zur digitalen Signatur auch der Sicherstellung von Integrität und Authentizität. Hierzu wird vom elektronischen Dokument eine Art Quersumme, die "Hash-Funktion", gebildet, verschlüsselt und an das Dokument angehängt. Der Empfänger bildet dann selbst von dem empfangenen Dokument die Hash-Funktion und vergleicht diese mit der an das Dokument angehängten Hash-Funktion, die er vorher mit dem öffentlichen Schlüssel des Absenders entschlüsselt hat. Das Verfahren ist so eingerichtet, daß der öffentliche Schlüssel nur zum Entschlüsseln, nicht aber zum Verschlüsseln verwendet werden kann. Sind beide Hash-Funktionen gleich, weiß der Empfänger nicht nur, daß das Dokument während der Übertragung unverändert geblieben ist (Integrität), er ist auch sicher, daß das Dokument vom angegebenen Absender stammt (Authentizität). Das Dokument enthält also eine digitale Signatur oder - anders ausgedrückt - eine elektronische Unterschrift.

Da elektronische Dokumente viel leichter als schriftliche Dokumente zu manipulieren sind, ist die Einführung rechtlich anerkannter Verfahren zur digitalen Signatur äußerst wichtig für das Funktionieren der vernetzten Gesellschaft. Der Bund bereitet daher ein Gesetz zur "elektronischen Unterschrift" vor, das regeln soll, welche Voraussetzungen für die Anerkennung einer Rechtsverbindlichkeit geschaffen werden müssen.

Aus Datenschutzsicht sind anerkannte digitale Signaturverfahren zu begrüßen, denn Integrität und Authentizität müssen neben der Vertraulichkeit zur Wahrung der Datensicherheit gewährleistet werden.

4.3.4 Recht auf Privatsphäre auch in Datennetzen

Die hohe Sicherheit, die Verschlüsselungstechniken bieten, läßt sich sehr eindrucksvoll an den Reaktionen von Sicherheitsbehörden zu diesem Thema ablesen. Sie sehen eine Gefahr darin, daß bei zunehmender verschlüsselter Datenübertragung ihre Möglichkeiten des heimlichen Mitlesens oder Mithörens verringert werden. Insbesondere in den USA wird seit Jahren heiß und sehr kontrovers diskutiert, inwieweit der Einsatz von Verschlüsselungstechniken reglementiert oder sogar verboten werden soll. In der Diskussion ist, eine Verschlüsselung nur dann zuzulassen, wenn der Schlüssel für die Sicherheitsbehörden jederzeit an zentraler Stelle zugänglich hinterlegt wird. Auch in Deutschland gibt es Diskussionen zu diesem Thema.

Zusammen mit Landesbeauftragten anderer Länder habe ich mich intensiv mit diesem Thema beschäftigt und das Für und Wider abgewogen. Das Ergebnis ist eindeutig: Die staatliche Reglementierung des Einsatzes von Verschlüsselungsverfahren hätte nur geringe Erfolgsaussichten, weil sie z.B. durch "Steganographie" oder "Überschlüsselung" leicht umgangen werden könnte und kaum kontrollierbar wäre. Es entstünden erhebliche Kosten bei der Überwachung der Regelungen. Festgestellte Verstöße könnten eventuell geahndet werden, verschlüsselte Verbrechensabsprachen blieben aber weiter unentdeckt. Andererseits würden solche Regelungen nicht nur das informationelle Selbstbestimmungsrecht, die Privatsphäre jeder Nutzerin und jedes Nutzers der Datennetze, einschränken, sondern auch anderen staatlichen und wirtschaftlichen Interessen an der Sicherung von Daten zuwiderlaufen (vgl. Anlagen 21 und 25).

4.4 Normen, Standards und Empfehlungen

Das Niedersächsische Innenministerium hat im März 1996 eine neue Fassung der "Normen, Standards und Empfehlungen für den Einsatz der IuK-Technik in der Landesverwaltung" herausgegeben; sie wurde gründlich überarbeitet und dem neuesten Stand der Technik angepaßt. Wie das Vorwort der "Normen und Standards" ausweist, sind die technischen und organisatorischen Maßnahmen zum Datenschutz im Kapitel "Datenschutz und Datensicherung" als verbindlich anzusehen. Zentraler Punkt dieses Kapitels ist die Auflistung wichtiger Grundschutzmaßnahmen. Zusätzlich muß für jedes System geprüft werden, ob weitere Maßnahmen erforderlich sind. Dies gilt vor allem für sensitive Daten, zu deren Sicherung in den Normen und Standards zusätzliche Maßnahmen beispielhaft genannt werden.

Als Hilfe für die Einschätzung der Sensitivität personenbezogener Daten ist das von mir bereits seit langem verwendete Schutzstufenkonzept aufgenommen worden. Außerdem werden Aussagen zur Durchführung von Technikfolgenabschätzungen nach § 7 Abs. 3 NDSG (vgl. 4.6), zum Virenschutz und zu Einsatzvoraussetzungen für Applikationen aus Standard-Software getroffen. An den "Normen und Standards" habe ich mitgearbeitet. Dabei gelang es in den meisten Fällen, schnell Konsens zu finden. Nur wenige Punkte, z.B. die verpflichtende Einführung von Verschlüsselungsverfahren zur sicheren Datenübertragung, waren aus Kostengründen nicht durchsetzbar.

4.5 Grundschutz bei der automatisierten Datenverarbeitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat bereits die zweite Version des "IT-Grundschutzhandbuches" herausgegeben. Ziel des Handbuches ist eine umfassende, konkrete Auflistung von Datensicherungsmaßnahmen in den verschiedensten Bereichen der Informations- und Kommunikationstechnik mit niedrigem und mittlerem Schutzbedarf. Das Handbuch berücksichtigt Bereiche wie Organisation, Personal, Infrastruktur und geht konkret auf EDV-Technik, z.B. Personal Computer, Unix-Systeme oder TK-Anlagen ein. Es ist

modular aufgebaut und enthält für die einzelnen Bereiche Gefährdungs- und Maßnahmelisten. Es gibt eine gute Übersicht über erforderliche technische und organisatorische Maßnahmen zur Datensicherheit. Die Empfehlungen sind als Mindeststandard zu verstehen, also als eine Liste der Maßnahmen, die mindestens in einem IuK-System zu treffen sind. Es muß überprüft werden, ob weitere, spezielle Maßnahmen erforderlich sind.

Ich begrüße diese bundesweite Standardisierung technischer und organisatorischer Datensicherungsmaßnahmen. Da die Maßnahmen auch unter dem Aspekt der Vermeidung finanzieller Verluste ausgewählt wurden, sind sie gelegentlich aus Sicht des Datenschutzes korrekturbedürftig. Eine Arbeitsgruppe der Datenschutzbeauftragten, an der auch ich beteiligt bin, erarbeitet zur Zeit in Zusammenarbeit mit dem BSI entsprechende Änderungsvorschläge .

Der Preis für das IT-Grundschutzhandbuch beträgt 98 DM. Da es dem Stand der Technik anzupassen ist, kommen auf den Dauernutzer nicht unerhebliche Kosten zu. Der Inhalt des Buches sollte kostengünstiger verfügbar sein. Meine erfragten Erfahrungen zeigen, daß der Umfang des Buches häufig vom Lesen abschreckt. Ich stelle mir die Anwendung des Handbuches in Niedersachsen in der Weise vor, daß öffentliche Stellen gezielt auf relevante Punkte im IT-Grundschutzhandbuch durch Auszug hingewiesen werden. Hierfür wäre eine Software-Version des Handbuches, etwa auf CD-ROM, sehr hilfreich. Eine solche CD-ROM ist beim BSI in Vorbereitung und soll 1997 erscheinen.

4.6 Technikfolgenabschätzung

4.6.1 Präventiver Datenschutz

In Niedersachsen haben öffentliche Stellen 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 (§ 7 Abs. 3 NDSG). Diese gesetzliche Pflicht scheint weitgehend unbekannt zu sein, denn bisher liegen mir erst zwei Dokumentationen über durchgeführte Untersuchungen vor.

Dabei hat schon das BVerfG im sog. Volkszählungsurteil 1983 gefordert, daß wegen der Undurchsichtigkeit der Speicherung und Verwendung von personenbezogenen Daten unter den Bedingungen der automatisierten Datenverarbeitung im Interesse eines "vorgezogenen Rechtsschutzes" rechtzeitig Vorkehrungen getroffen werden müßten, um einen effektiven Schutz des Grundrechts auf informationelle Selbstbestimmung zu gewährleisten. Die Methodik der Technikfolgenabschätzung gibt hierzu eine Chance. Damit lassen sich die Sicherheitsrisiken von geplanten automatisierten Verfahren frühzeitig erkennen, die besonderen Gefahren für die Rechte der Betroffenen bewerten und die Technik so gestalten, daß diese Gefahren

vermieden oder beherrscht werden können. Die Technikfolgenabschätzung sollte daher nicht auf eine reine Gefahrenanalyse beschränkt werden, sondern den Nutzen der angestrebten automatisierten Datenverarbeitung und Verfahrensalternativen zur Vermeidung der Erhebung von personenbezogenen Daten aufzeigen. Rechtzeitig durchgeführt und in der geeigneten Form erstellt, sind Technikfolgenabschätzungen nicht nur für die Sicherstellung des Datenschutzes hilfreich, sie führen auch zu erhöhter Wirtschaftlichkeit. Durch die frühzeitige Planung und Einführung der notwendigen Sicherungsmaßnahmen können aufwendige Nachrüstungen vermieden werden.

4.6.2 Erste Erfahrungen

"Learning by doing" war meine Empfehlung zum Thema Technikfolgenabschätzung vor zwei Jahren (XII 4.2.2). Die bisherigen Versuche "X.400" und "KOMNET" können sich sehen lassen, auch wenn sie schüchtern begonnen wurden. Ziel der ersten Technikfolgenabschätzung war es, neben der eigentlichen Untersuchung auch den richtigen und angemessenen Weg für diese Methode zu finden. Hierzu wurde eine Projektgruppe mit Vertretern dreier Ministerien, des Niedersächsischen Landesverwaltungsamtes, der Arbeitsgemeinschaft der Hauptpersonalräte und der Arbeitsgemeinschaft der Personalräte der obersten Landesbehörden gebildet. Mir wurde Gelegenheit zur Mitarbeit gegeben. Die Projektarbeit wurde wissenschaftlich begleitet.

Die Projektgruppe empfiehlt, daß Technikfolgenabschätzungen folgende Untersuchungsfelder umfassen sollten:

- Ist-Zustand vor der Technikeinführung,

- Geplante Nutzung der IuK-Technik,

- Gefahrenanalyse des einzusetzenden Systems (Auflistung der Gefahren),

- Risikoanalyse (Bewertung von Häufigkeit und Ausmaß von Schäden),

- Geplante technische und organisatorische Maßnahmen,

- Darstellung und Bewertung des Restrisikos,

- Betrachtung alternativer Lösungen.

Beide Projekte wurden nach diesen Gestaltungsvorgaben untersucht und dokumentiert. Insbesondere bei der Gefahrenanalyse der Technikfolgenabschätzung X.400 hat die Projektgruppe mit viel Sachverstand und Fleiß gearbeitet. Bei zukünftigen Technikfolgenabschätzungen sollte es möglich sein, mit weniger

Aufwand das angestrebte Ziel zu erreichen. Um hierbei Hilfestellung zu geben, erstelle ich zur Zeit eine Muster-Technikfolgenabschätzung, die ich Interessierten gerne zur Verfügung stelle.

Die beiden Technikfolgenabschätzungen "X.400" und "KOMNET" wurden auch veröffentlicht. Von der Veröffentlichung der Untersuchungsergebnisse verspreche ich mir zum einen Anteilnahme und Engagement von Politikern und der interessierten Öffentlichkeit. Die Veröffentlichung soll zugleich auch Stellen, die ähnliche Projekte planen, in die Lage versetzen, sich frühzeitig über Gefahren, Risiken und Verfahrenslösungen zu informieren. Damit kann mehrfacher Untersuchungsaufwand für vergleichbare Projekte vermieden werden.

4.7 Chipkarten

Chipkarten sind im Kommen. Sie sind "handlich, billig, intelligent, effektiv". Sie versprechen hohe Rationalisierungseffekte und eine massive Verbesserung der "Datenlage" bei Wirtschaft und Verwaltung. Die Menschen, die als Kartenträger fungieren und deren Daten auf den Karten gespeichert sind, werden zunächst nicht gefragt. Es ist kein Wunder, daß insofern erst einmal Skepsis herrscht: Dem mit menschlichen Sinnen wahrnehmbaren Äußeren einer Chipkarte ist nicht zu entnehmen, was in ihr steckt. Dies zu beurteilen bedarf es vertrauenswürdiger Spezialisten. Daher werden die Datenschutzkontrollinstanzen von den Kartenanwendern vorher gefragt und haben die Chance der Einflußnahme schon bei der Gestaltung des jeweiligen informationstechnischen Systems. Der aus wirtschaftlichem Interesse bei den Kartenanbietern vorhandene datenschutzrechtliche "Absegnungsdruck" verschafft dem informationellen Selbstbestimmungsrecht vor allem bzgl. der Sicherheit bei Chipkarten eine hohe Akzeptanz.

Es gibt fast keinen gesellschaftlichen Bereich mehr, in dem nicht Chipkarten eingesetzt oder zumindest geplant sind: Gesundheitskarten, elektronische Geldbörsen, Nahverkehrsausweise, Betriebs- und Mitgliederausweise, Kunden- und Kreditkarten, Telefonkarten, Verschlüsselungskarten usw. Nach der Einführung vieler Einzellösungen scheint nun die multifunktionale Karte zum Renner werden zu wollen. Mit ihr soll dem Kartenwirrwarr in der Brieftasche ein Ende bereitet werden. Die Datenverarbeitung wird standardisiert und vereinfacht. Beispiele für geplante multifunktionale Karten sind die Asylcard (vgl. 12.1) oder eine standardisierte Hochschulkarte (UniversCard). Letztere soll nicht nur als Studentenausweis dienen, sondern auch der Zutrittskontrolle, als Berechtigungsnachweis oder als Zahlungsmittel. Der Geldkarte sollen alle möglichen weiteren Funktionen aufgesattelt werden.

Teilweise wird die Behauptung aufgestellt, Chipkarten wären für die informationelle Selbstbestimmung förderlich, weil die Betroffenen ihre eigenen Daten selbst bei sich trügen. Dies ist hinsichtlich fast aller Anwendungen Unsinn: Die Betroffenen haben regelmäßig weder die technische Möglichkeit noch das Recht, die auf dem Chip gespeicherten

Daten zu verändern. Mangels Lesegerät fehlt ihnen derzeit zumeist auch die Kenntnis, welche auf sie bezogenen Daten sie mit sich herumtragen und durch Hingabe der Karte offenbaren. Hinzu kommt: Die personenbezogene Datenspeicherung erfolgt oft nicht auf der Karte, sondern im Peripheriesystem mit den Schreib- und Leseterminals als Schnittstellen. Daher muß bei der datenschutzrechtlichen Bewertung einer Chipkarte nicht nur diese selbst geprüft werden, sondern das gesamte informationstechnische System, in dem die Karte lediglich ein Bestandteil ist. Sicherlich können Chipkarten zur Förderung des Datenschutzes eingesetzt werden, z.B. als Nachweis der Zugangsberechtigung zu einem EDV-System, als Hilfsmittel zur Verschlüsselung oder zur Erbringung einer elektronischen Unterschrift. Chipkarten erlauben anonym bargeldloses Einkaufen oder den Nachweis einer Berechtigung (sog. White Cards). Ungleich größer sind aber die von diesem Medium ausgehenden Gefahren: Nutzungs-, Bewegungs-, Kommunikations- oder Tätigkeitsprofile können erstellt werden. Daten können langfristig aus den verschiedensten Lebensbereichen zusammengeführt werden, so daß Persönlichkeitsbilder erstellt werden können. Der Umfang erhobener Daten sowie der Zugang zu diesen werden massiv ausgeweitet. Jeder Chipkarten-Schnittstellen-Kontakt hinterläßt eine über den Besitzer der Karte aussagekräftige elektronische Spur.

4.7.1 Rechtliche Einordnung von Chipkarten

Wegen der elektronischen Auswertbarkeit der mit einer Chipkarte gespeicherten personenbezogenen Daten ist durchgängig der Dateibegriff erfüllt; das Datenschutzrecht ist anwendbar. Daß die gespeicherten Daten sich nur auf die Person des Kartenbesitzers beziehen, ist dafür nicht schädlich. Der Besitzer ist nicht verarbeitende Stelle, da er die gespeicherten Daten selbst nicht verändern kann. Als verarbeitende Stelle ist vielmehr die Stelle anzusehen, die die Herrschaft über den Verarbeitungsvorgang hat. Dies können mehrere Stellen sein, z.B. bei der UniversCard mit Zahlungsfunktion, Mensaberechtigung und Immatrikulationssektor: eine Bank, das Studentenwerk und die Universitätsverwaltung. Verwendet ein Besitzer seine Karte, so kann hierin eine Datenerhebung, eine Datenspeicherung oder auch eine Datenübermittlung liegen, ohne daß die verarbeitenden Stellen örtlich anwesend sind. Gibt z.B. ein Patient seine Gesundheitschipkarte mit medizinischen Daten einem Arzt, so erfolgt damit eine Datenübermittlung von Arzt zu Arzt. Der Patient ist nur Bote.

Selbstverständlich stehen den Betroffenen ihre datenschutzrechtlichen Ansprüche auf Auskunft, Berichtigung, Löschung, Sperrung und Schadensersatz auch bei Chipkartenanwendungen zu. Das Auskunftsrecht kann z.B. dadurch realisiert werden, daß den Betroffenen der Zugang zu Leseterminals eröffnet wird. Äußerst schwierig werden datenschutzrechtliche Zuordnungen, wenn mehrere Stellen bzgl. des gleichen Kartensegments schreib- und leseberechtigt sind. Nicht geringer sind die Probleme, wenn Datenspeicherungen aus unterschiedlichen Kartensegmenten sich gegenseitig beeinflussen. Hier kann man evtl. auf die Erfahrungen bei Verbunddateien zurückgreifen. Bei anderen Fragen ist man mit dem aktuellen Datenschutzrecht am

Ende des Lateins: Es ist völlig ungeklärt, wie die Betroffenen vor einer unbefugten Offenbarung oder einer Beschlagnahme bei Daten bewahrt werden, die einer beruflichen Schweigepflicht unterliegen (§ 203 StGB). Wer ist verantwortlich für die Datensicherheit? Wie ist zu verhindern, daß sich Dritte, z.B. Vermieter, Arbeitgeber oder Versicherungen, die Karte von Betroffenen mißbräuchlich vorlegen lassen? Wer kontrolliert die Chipkarte bei auf einer Karte integrierten öffentlichen und privaten Anwendungen? Es gibt derzeit mehr rechtliche Fragen als Antworten.

Spezialgesetzlich geregelt ist bisher nur eine einzige Chipkarte, die Krankenversichertenkarte nach § 291 SGB V. Es stellt sich daher die Frage, inwieweit darüber hinausgehend heute schon Chipkarten zulässig sind. Dies ist zweifellos der Fall, wenn die Betroffenen in die Nutzung der Chipkarte eingewilligt haben. Eine wirksame Einwilligung ist aber nur bei wirklicher Freiwilligkeit anzunehmen. Davon kann z.B. keine Rede mehr sein, wenn bestimmte grundlegende Leistungen nur noch unter Nutzung einer Chipkarte zu erhalten sind. Die Betroffenen müssen eine Wahlmöglichkeit haben zwischen einer personenbezogenen Chipkartennutzung und anderen Verfahren. Auch bei faktischen Abhängigkeitsverhältnissen, z.B. bei Vertragsverhältnissen zu Arbeit, Wohnung, Versicherung und Kredit oder bei bestehenden Vertrauensverhältnissen zu einem Arzt oder einem Psychologen darf eine Leistung nicht von der Einwilligung zu einer Chipkartennutzung abhängig gemacht werden. Von Freiwilligkeit kann gesprochen werden, wenn die Erklärung ohne größere Nachteile widerrufen werden kann. Außerdem kann eine Einwilligung nur dann wirksam sein, wenn die Betroffenen hinreichend über Art, Umfang, Zweck und Beteiligte der Datenverarbeitung informiert sind. Die Betroffenen müssen also noch überblicken können, was mit ihren Daten geschieht. Bei multifunktionalen Karten dürfte ab einer bestimmten Komplexität eine Grenze erreicht sein, bei der eine wirksame Einwilligung nicht mehr eingeholt werden kann.

Es drängt sich die Frage auf: Ist die Chipkarte nichts anderes als ein etwas schneller zu überprüfender Papierausweis, und wann bedarf es für die Nutzung von Chipkarten eines speziellen Gesetzes? Auch bei anderen EDV-Systemen holt sich die verarbeitende Stelle keine besondere Legitimation für die Wahl des elektronischen Verarbeitungsmediums. Mit der Chipkarte erfolgt jedoch dort ein qualitativer Sprung, wo der Inhalt und der Speicherumfang für den Betroffenen nicht direkt erkennbar sind. Davon muß bei Prozessorchipkarten mit veränderbarem Speicherinhalt grundsätzlich ausgegangen werden. Werden die Betroffenen aus rechtlichen oder faktischen Gründen zur Chipkartennutzung gezwungen, so ist nach der verfassungsrechtlichen Wesentlichkeitstheorie dafür eine gesetzliche Grundlage erforderlich.

4.7.2 Anforderungen an die informationstechnische Sicherheit bei Chipkarten

Wenn auch noch erhebliche datenschutzrechtliche Unwägbarkeiten im Zusammenhang mit dem Einsatz und der Nutzung von Chipkarten mit personenbezogenen Daten zu beklagen gibt, so gibt es für die

Datenschutzbeauftragten des Bundes und der Länder doch schon erfolgversprechende Ergebnisse auf technisch-organisatorischem Gebiet. Eine Arbeitsgruppe, in der Mitarbeiter des BfD und der Landesbeauftragten von Berlin, Brandenburg, Hamburg, Hessen, Schleswig-Holstein und Niedersachsen mitgewirkt haben, hat ein Anforderungsprofil für Entwickler, Hersteller und Betreiber von Chipkarten zusammengestellt. Die Ausarbeitung entspricht zwar dem Wissenstand von Mitte 1995. Daraus lassen sich aber bereits vielfältige Anforderungen an die informationstechnische Sicherheit bei Chipkarten ableiten.

Für den datenschutzgerechten Einsatz von Chipkarten ist eine konsequente und überzeugende Sicherungstechnologie erforderlich. Datensicherungsmaßnahmen müssen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Mißbrauch gewährleisten. Vor der Entscheidung über den Einsatz von Chipkarten sollte daher eine Technikfolgenabschätzung durchgeführt werden, so wie dies Art. 20 der EU-Datenschutzrichtlinie als Vorabkontrolle fordert. Zur Auswahl geeigneter und angemessener Sicherungsmaßnahmen ist eine systematische Einschätzung der Gefahren für das informationelle Selbstbestimmungsrecht vorzunehmen. Lösungsvorschläge für eine Sicherungstechnologie sind zu erarbeiten.

Die Auseinandersetzung mit dem Phänomen "Chipkarte" zwingt zur Differenzierung zwischen den technischen Systemen und den Applikationen, die sich dieser Systeme bedienen, und der Chipkarte selbst. Genausowenig wie es "die" Chipkarte gibt, genausowenig kann man von "der" Chipkartenanwendung sprechen. Würde man datenschutzrechtliche und sicherheitstechnische Schlußfolgerungen ausschließlich aus einer der vielen Kombinationsmöglichkeiten ziehen, wäre eine Allgemeinverbindlichkeit der Aussagen bzw. Anforderungen nicht zu erreichen. Konkrete Rechtsprobleme und Risiken lassen sich nur mit einem Bezug zu bestimmten inhaltlichen und technischen Rahmenbedingungen aufzeigen. Die erweist sich z.B. bei den geplanten Gesundheits- und Patientenchipkartensystemen.

Künftige neue Anwendungen werden sich tendenziell der Prozessorchipkartentechnologie bedienen. Prozessorchipkarten sind miniaturisierte Computer, die allerdings nicht über eigene "Mensch-Maschine-Schnittstellen" verfügen. Diese werden über Kartenterminals realisiert. Datenschutzrechtliche Anforderungen erstrecken sich hier neben den Kartenterminals auch auf die Rahmenbedingungen bei der Herstellung, bei der Initialisierung, beim Versand und bei der Ersatzbeschaffung in Fällen des Verlustes oder der Zerstörung einschließlich des "Ungültigkeitsmanagements". Mehrere Hersteller bieten derartige spezielle Chipkarten bereits heute an. Deren Leistungsfähigkeit und Funktionsweise sind zum Teil noch sehr unterschiedlich. Eine Standardisierung wäre auch aus datenschutzrechtlicher Sicht in diesem Bereich dringend zu empfehlen.

Das Sicherungskonzept für Chipkarten sollte folgende Mindestanforderungen erfüllen:

1. Grundschutzmaßnahmen

- Ausstattung des Kartenkörpers mit fälschungssicheren Authentifizierungsmerkmalen wie z.B. Unterschrift, Foto, Hologramme.

- Sicherung unterschiedlicher Chipkartenanwendungen auf multifunktionalen Chipkarten durch gegenseitige Abschottung.

- Sicherung der Kommunikation zwischen der Chipkarte, dem Kartenterminal und dem ggf. im Hintergrund wirkenden System durch kryptographische Maßnahmen, wobei eine Übertragung des (geheimen) kryptographischen Schlüssels der Chipkarte zum Kommunikationsgerät ausgeschlossen sein muß bzw. im Ausnahmefall nur verschlüsselt erfolgen darf. Das Einlesen bzw. Ändern des kryptographischen Schlüssels muß durch ein Authentifikationsverfahren abgesichert sein.

- Benutzung allgemein anerkannter, veröffentlichter Algorithmen für Verschlüsselungs- und Signaturfunktionen sowie zur Generierung von Zufallszahlen.

- Realisierung aktiver und passiver Sicherheitsmechanismen gegen eine unbefugte Analyse der Chip-Inhalte sowie der chipintegrierten Sicherheitsfunktionen.

- Steuerung der Zugriffs- und Nutzungsberechtigungen durch die Chipkarte selbst.

- Sicherung der gegenseitigen Authentifizierung von Chipkarte und Kartenterminal mit dem "Challenge-Response-Verfahren".

2. Erweiterte Sicherungsmaßnahmen

- Realisierung weiterer "aktiver" Sicherheitsfunktionen des Betriebssystems wie "Secure Messaging", I/O-Kontrolle aller Schnittstellen, Interferenzfreiheit der einzelnen Anwendungen, Verzicht auf Trace- und Debug-Funktionen und dergleichen.

- Auslagerung von Teilen der Sicherheitsfunktionen des Betriebssystems in dynamisch zuladbare Tabellen, damit der Chipkartenhersteller nicht über ein "Gesamtwissen" verfügt.

3. Grundsätzlich sollte bei Chipkartenbenutzung Anonymität gewahrt bleiben. Wenn dies nicht möglich ist, sollten Wahlmöglichkeiten anonymer Alternativen geschaffen werden.

4. Der Chipkarteninhaber bzw. die Betroffenen sollten die Möglichkeit erhalten, auf neutralen, zertifizierten Systemumgebungen die Dateninhalte und Funktionalitäten ihrer Chipkarten einzusehen (Gebot der Transparenz).

5. Die gesamte Infrastruktur ist zu dokumentieren, und die Produktion, die Initialisierung und der Versand der Chipkarten sind zu überwachen.

6. Für die gesamte Infrastruktur ist ein Mindestschutzniveau vorzuschreiben, dessen Unterschreitung strafbewährt sein sollte.

7. Alle Systemkomponenten sind auf der Basis der Grundsätze ordnungsgemäßer Datenverarbeitung zu evaluieren.

8. Für die Informationsstrukturen sind zu Echtheits- und Gültigkeitsüberprüfungen (z.B. Abgleich gegen Sperr- und Gültigkeitsdateien) Kontrollmöglichkeiten zu schaffen.

4.8 Optische Speicher

4.8.1 Eine beachtenswerte neue Technologie

Die optische Datenspeicherung entwickelt sich zunehmend zu einer Alternative für herkömmliche Datenträger- und Speichermedien wie Magnetplatte, Diskette und Magnetband. Der Begriff der optischen Datenspeicherung ist abgeleitet vom zugrundeliegenden Aufzeichnungsverfahren mit Hilfe eines Laserstrahls. Auch hierbei können ähnlich wie bei der Mikroverfilmung - dem ältesten optischen Aufzeichnungsverfahren - Papierdokumente, Bilder und Graphiken optisch erfaßt, gespeichert und durch automatisierte Verfahren ausgewertet werden. Es kann daher nicht überraschen, daß für die optische Datenspeicherung Anwendungsmöglichkeiten einer papierlosen Datenverarbeitung und einer aktenlosen Verwaltung überlegt und erprobt werden.

4.8.2 Datenschutzprobleme bei der optischen Datenspeicherung

Bei der Verarbeitung personenbezogener Daten sind die verfassungsrechtlichen Grundsätze der Verhältnismäßigkeit, der Zweckbindung und der informationellen Gewaltenteilung zu beachten, unabhängig davon, auf welche Weise (Akte, Datei, Groß-EDV, Mehrplatzsystem, PC usw.) die Datenverarbeitung geschieht. Beim Einsatz moderner Informations- und Kommunikations-Technologie sind insbesondere die Zweck- und Aufbewahrungsbestimmungen der Datenverarbeitung durch technische Maßnahmen zu gewährleisten. Auch die Betroffenenrechte, z.B. die Ansprüche auf Akteneinsicht, Auskunft, Berichtigung und Löschung, müssen zu jeder Zeit erfüllbar sein.

Während bei mehrfach beschreibbaren, magnetisch-optischen Systemen die technischen Möglichkeiten mit denen der herkömmlichen Magnetplatten bzw. Disketten weitgehend übereinstimmen, ist das Löschen von Daten bei CD-ROM- bzw. WORM-Datenträgern nicht ohne weiteres realisierbar. Das Bundesdatenschutzgesetz und die meisten Landesdatenschutzgesetze definieren das Löschen als das

Unkenntlichmachen gespeicherter Daten (die entsprechende Formulierung im Berliner Datenschutzgesetz lautet: Beseitigen). Personenbezogene Daten werden dann als unkenntlich angesehen, wenn die Informationen nicht länger aus den ursprünglich gespeicherten Daten gewonnen werden können. Insbesondere die Löschungspflicht der Datenschutzgesetze kann daher einer optischen Datenspeicherung entgegenstehen.

Ein weiteres Datenschutzproblem kann bei der optischen Datenspeicherung dann auftauchen, wenn auf die Aufbewahrung von Originaldokumenten in Verfahrensakten verzichtet und an deren Stelle ausschließlich eine digitale Aktenführung treten soll. Es stellt sich die Frage, ob die Reproduktionen von Akten gerichtsverwertbar sind. Gesetze, die bei optischer Datenspeicherung den Verzicht auf einen Aktennachweis erlauben, fehlen weitestgehend. Der Verzicht auf Papieraktenrückhalt muß meines Erachtens differenziert für jedes einzelne Fachgebiet untersucht und begründet werden.

4.8.3 Keine Löschung von Informationen bei CD-ROM bzw. WORM

Bei CD-ROM- bzw. WORM-Systemen können Daten aufgrund der technischen Spezifikationen nicht direkt gelöscht werden. In separat betriebenen, den Zugriff steuernden EDV-Systemen ist lediglich der Zugriff auf die CD-ROM bzw. WORM durch Löschen der Verweisdaten zu unterbinden. In der aktuellen Indexdatei bzw. Datenbank sind dann die alten Verweise auf die zu löschende Information nicht mehr enthalten, obwohl die Nutzdaten auf dem optischen Speichersystem noch physikalisch und im Volltext vorhanden sind. Zwar sind ohne die Kenntnis dieser Verweisdaten die auf CD-ROM bzw. WORM (gestreut) abgelegten Nutzinformationen nicht gezielt verwertbar. Da aber der Zugriff auf die Verweisdaten nur durch Software, die geändert werden kann, unterbunden ist, ist es denkbar, daß der Anbieter der CD-ROM- bzw. WORM-Platte und des Laufwerks über das Wissen und die Möglichkeit verfügt, auf eigentlich gelöschte Daten zuzugreifen.

In einigen Archivierungssystemen werden diese Verweisdaten in der jeweils aktuellen Form für eventuelle Notfall-Restaurierungen ebenfalls auf dem optischen Datenträger abgelegt, so daß mit Hilfe älterer Verweisdaten die nur scheinbar gelöschten Nutzdaten für einen potentiellen Angreifer lesbar sind.

Das Sperren von Einzeldaten oder Datensätzen kann durch das Setzen und Abfragen von entsprechenden Kennzeichen in den separat geführten Verweisdaten vorgenommen werden.

Die gesetzlichen Berichtigungs- und Löschungsansprüche von Betroffenen können bei CD-ROM- bzw. WORM-Speicherung dadurch realisiert werden, daß unverzüglich ein neuer Datenträger aus dem alten erzeugt wird, wobei nur noch die gültigen Daten übernommen und die Daten auf dem ursprünglichen Datenträger gelöscht werden. Eine vollständige Löschung der auf CD-ROM- bzw. WORM-Platten

enthaltenen Informationen ist derzeit nur möglich durch Zerstörung der Speicherfläche (Ätzen, Zerkratzen) oder durch physikalische Vernichtung des gesamten Datenträgers (Einschmelzen, Verbrennen, Schreddern); analog der Behandlung von Magnetdatenträgern und Mikrofilmen. Bei der Anwendung der Grundsätze der DIN 32757 (Vernichtung von Informationsträgern) muß beachtet werden, daß diese Speichermedien bisher unübliche, hochkapazitäre Datenablagen bieten (ca. 1.000 Seiten pro Quadratzentimeter, ca. 300.000 Schreibmaschinenseiten bei einer WORM mit 5 1/4 Zoll). Es besteht also die Gefahr der Erzeugung bzw. Wiedergewinnung von höchst umfangreichen und sensiblen Datenbeständen. Eine Rekonstruktion kann erfolgen - wenn auch mit sehr hohem Aufwand.

4.8.4 Empfehlungen zum Einsatz optischer Datenspeicherung

Die Datenschutzbeauftragten des Bundes und der Länder haben eine Orientierungshilfe "Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung" erarbeitet, die kostenlos bei mir angefordert werden kann. Sie enthält eine ausführliche Technikbeschreibung sowie datenschutzrechtliche Hinweise und Empfehlungen.

Beim Einsatz optischer Datenspeicher ist zu unterscheiden zwischen Datenträgern, die nur einmal beschreibbar, aber beliebig oft lesbar sind (z.B. CD-ROM, WORM, MO als WORM), und anderen Datenträgern, die mehrfach beschreibbar und lesbar sind (z.B. MO). Aufgrund der fehlenden Löschbarkeit von Daten bei den nur einmal beschreibbaren optischen Datenträgern und unter Berücksichtigung der Löschungs-, Sperrungs- und Berichtigungsvorschriften der Datenschutzgesetze des Bundes und der Länder empfehle ich, nach folgenden Regeln zu verfahren:

1. Grundsätzlich sind wiederbeschreibbare, optische Datenträger einzusetzen. Diese können wie Magnetplatten behandelt werden.

2. Es können nur einmal beschreibbare optische Datenträger lediglich verwendet werden, wenn die gesetzlichen Regelungen, insbesondere die zur Löschung, dies zulassen. Gesperrte Daten sind besonders zu kennzeichnen. Spätestens nach dem vollständigen Beschreiben des Datenträgers sind die Datenbestände durch Umkopieren auf einen neuen Datenträger zu bereinigen. Der Ursprungsdatenträger ist unverzüglich und vollständig zu löschen, wozu der Datenträger vernichtet werden muß.

3. Werden Daten gesichert oder langfristig archiviert, können ebenfalls optische Datenträger verwandt werden, die nur einmal beschreibbar sind. Dabei sollten möglichst nur Daten mit gleichen Löschungsfristen auf dem gleichen Datenträger abgelegt werden.

4. Sind Daten auf einem nur einmal beschreibbaren Datenträger zu löschen oder zu berichtigen, muß unter Verwendung des alten Datenträgers ein neuer Datenträger beschrieben werden, der die zu

löschenden Daten nicht mehr enthält. Der ursprüngliche Datenträger ist unverzüglich und vollständig zu löschen, wozu der Datenträger vernichtet werden muß.

5. Das vollständige Löschen von Daten auf einem nur einmal beschreibbaren optischen Datenträger (d. h. dessen Vernichtung) ist mit angemessenen technisch-organisatorischen Maßnahmen unter Beachtung der DIN 32757 vorzunehmen. Dazu sind Verfahren wie Ätzen, Einschmelzen, Verbrennen, Zerkratzen oder Schreddern unter Berücksichtigung von Sicherheits- und Umweltverträglichkeitsaspekten anzuwenden.

4.9 Neue Datenschutz-Prüfkonzepte

Zur Zeit erstelle ich Prüfkonzepte zu den Bereichen Mailbox, MVS/VM und Windows NT. Die Prüfkonzepte schließen an die bereits von mir erstellten Konzepte für Unix-Systeme und Novell Netware - Systeme an und sind in ähnlicher Weise aufgebaut. Sie enthalten jeweils eine umfangreiche Checkliste zur Realisierung einer möglichst datenschutzgerechten Konfiguration und sind sowohl für die Unterstützung meiner Prüftätigkeit als auch zur Eigenkontrolle geeignet.

Das Mailbox-Prüfkonzept steht kurz vor der Fertigstellung, die beiden anderen Konzepte sollen 1997 fertiggestellt werden. Interessierten, die die jetzigen Entwürfe bereits kennenlernen möchten und bereit sind, durch Anregungen an der Weiterentwicklung mitzuarbeiten, sende ich gerne bereits jetzt Exemplare zu.

4.9.1 Prüfkonzept Windows NT

Windows NT messe ich wegen der kontinuierlich steigenden Zahl von Installationen in der Privatwirtschaft wie auch in der öffentlichen Verwaltung zukünftig eine beachtliche Bedeutung zu. In das Prüfkonzept sind Erfahrungen eingeflossen, die ich durch den Aufbau und Betrieb eines Testnetzes in meiner Geschäftsstelle (vgl. 3.4) gewonnen habe.

Windows NT bietet eine Reihe von Funktionen, die für den Datenschutz und die Datensicherheit sowohl auf dem Server selbst als auch auf den angeschlossenen Arbeitsplätzen genutzt werden können. Eine vom Betriebssystem bereits angebotene Zugriffs- bzw. Benutzerkontrolle läßt Berechtigungsvergaben gegenüber gespeicherten Informationen bis auf Dateiebene zu. Dabei ist es unerheblich, ob die Daten auf den Arbeitsplatzrechnern (unter Windows NT Workstation) oder auf dem Server (unter Windows NT Server) abgelegt sind.

Für die Sicherheit des gesamten Netzes ist ein Konzept erforderlich, das die Sicherheit auf dem NT Server und den angeschlossenen Arbeitsplätzen unter dem jeweiligen lokalen Betriebssystem berücksichtigt. Insbesondere in Netzwerken kann die Sicherheit von

Einzelkomponenten des eingesetzten Systems nicht isoliert betrachtet werden. Ein Netzwerk ist nur so sicher wie die schwächste Einzelkomponente. Außerdem ergeben sich aus der Kombination an sich sicherer Einzelkomponenten häufig neue Gefahren für das Gesamtsystem.

Im folgenden werden einige wichtige Punkte des Prüfkonzeptes stichwortartig wiedergegeben:

- Domänen- bzw. Arbeitsgruppenmodell (einschl. Trust Relationships),

- Systemverwaltung, Administrator, Benutzerklassen,

- Anmeldung an Windows NT,

- Dateiverwaltung, Vergabe von Berechtigungen,

- Verschlüsselung (durch Zusatzsoftware),

- Protokollierung von System-, Anwendungs- und Benutzeraktivitäten,

- Zugriff über Remote Access Service,

- Backup-Konzept,

- Einsatz der von Windows NT zur Verfügung gestellten Security-Möglichkeiten,

- Registrierung von Windows NT.

4.9.2 Prüfkonzept für MVS/VM-Systeme

Dezentrale Rechnersysteme mit PC- oder Unix-Rechnern sind zwar weiter auf dem Vormarsch, dennoch sind die oft als Dinosaurier bezeichneten Großrechner noch lange nicht ausgestorben. Gerade bei eingeschliffenen Verfahren mit großen Mengen von personenbezogenen Daten werden diese Systeme noch über viele Jahre ihren Dienst versehen. Ich erarbeite daher zur Zeit ein Prüfkonzept, das für Datenschutz-Prüfungen im Großrechnerbereich, insbesondere bei Großrechnern mit den Betriebssystemen MVS und VM, konzipiert ist. Es berücksichtigt vor allem Großrechner mit der Datensicherungssoftware RACF. Kernbereiche des Konzeptes sind die Benutzerverwaltung, die Ressourcenverwaltung und die RACF-Administration.

4.9.3 Prüfkonzept Mailboxen

Mailboxen haben in den letzten Jahren eine starke Wandlung erfahren. Dominierten noch vor einigen Jahren isolierte Systeme oder kleine, abgeschlossene Netze, so ist es inzwischen zu einer starken Vernetzung

der Mailboxsysteme sowohl untereinander als auch mit dem Internet gekommen. Aus fast allen Mailboxen kann elektronische Post aus dem Internet empfangen und dahin verschickt werden. Während die weitere Verbreitung bei Amateursystemen noch ungebrochen ist, so ist bei vielen kommerziellen Mailboxbetreibern bereits eine immer deutlichere Ausrichtung an das Internet zu erkennen. Diese neuen Internet-Provider haben weiter ihre klassischen Mailboxdienste wie E-Mail und Netnews im Programm. Aus dem "stand-alone"-PC mit einem Modem und dem selbst zusammengestellten Mailboxprogramm ist ein vernetztes Rechnersystem geworden, das neben dem Internet-Gateway auch die Aufgaben einer Mailbox übernimmt.

Da die meisten Mailboxbetreiber als Techniker in rechtlichen Fragen nicht bewandert sind, habe ich meinem Mailbox-Prüfkonzept einen materiell-rechtlichen Bereich vorangestellt. Hier wird die Registrierungspflicht, das Datengeheimnis und die Pflicht zur Bestellung von Datenschutzbeauftragten angesprochen. Der Schwerpunkt des Prüfkonzepts liegt bei den technisch-organisatorischen Maßnahmen, der Absicherung der personenbezogenen Daten gegenüber Hackerangriffen, der Aufnahme der Bestandsdaten eines neuen Nutzers, dem Schutz der Inhaltsdaten, in der Gestaltung der Paßwörter und insbesondere in der Sicherung der elektronischen Post der Kundinnen und Kunden.

Das Prüfkonzept wird an Interessierte auch in elektronischer Form abgegeben werden. Es darf in Mailboxen und ftp-Servern zum kostenlosen Download bereitgehalten und weitergegeben werden, solange der Inhalt nicht verändert wird. Im folgenden möchte ich einige interessante Erfahrungen weitergeben, die sich aus meiner Mailbox-Prüftätigkeit mit diesem Konzept ergeben haben:

- Mailboxen, die in Niedersachsen geschäftsmäßig betrieben werden, müssen sich bei mir registrieren lassen. Bei vielen Mailboxbetreibern herrscht Unkenntnis über diese Rechtslage (vgl. 32.1).

- Der Schutz der Inhaltsdaten, insbesondere der elektronischen Post, existiert kaum. Systemverwalter können Einsicht in elektronische Post nehmen, und einige tun dies auch. Wie im Internet hat elektronische Post die Datenschutzqualität einer Postkarte.

- Nutzer und Systemverwalter verwenden leicht zu erratende Paßwörter, die zudem selten oder nie geändert werden. Bei einigen Mailboxprogrammen werden Paßwörter unverschlüsselt auf der Festplatte abgelegt.

- Viele Mailboxen werden als Hobby betrieben; der räumliche Zugangsschutz dieser "Service-Rechenzentren" ist in aller Regel unzureichend.

Auch wenn es sich bei vielen Mailboxen um relativ kleine Anlagen und einen amateurhaften Betrieb handelt, kann es durch die Vernetzung der Mailboxen zu der regelmäßigen Zustellung elektronischer Post an viele tausend Nutzer kommen. Diese wird für den Systembetreiber offen

lesbar in der jeweiligen Mailbox bis zum Weitertransport zwischengespeichert. Kopien können problemlos gezogen werden. Abhilfe kann hier nur eine Ende-zu-Ende-Verschlüsselung bieten, wie sie z.B. das Programm Pretty Good Privacy (PGP) bietet (vgl. 4.2.3 und 4.3.2).

4.10 Alle Jahre wieder - Pannen bei der Aktenvernichtung und beim Postversand

Was nützen die besten edv-technischen Sicherungsmaßnahmen, wenn bei der Vernichtung von personenbezogenen Unterlagen "geschludert" wird? Auch Staatsanwaltschaft und Polizei leisten sich gelegentlich grobe Schnitzer, wie Beispiele aus der jüngsten Vergangenheit beweisen. So wurden Entwürfe von Verfügungen und Untersuchungsberichten sowie Beschlüsse in Ermittlungsverfahren gegen Betroffene aus einer Staatsanwaltschaft unzerkleinert in Müllsäcken auf einem Privatgrundstück gefunden. In einem anderen Fall habe ich in einem Altpapiercontainer, der neben dem Dienstgebäude einer Polizeiinspektion für jedermann zugänglich aufgestellt war, aktuelle Einsatzpläne mit Namen, Tarnbezeichnungen, Telefonnummern und Kfz-Kennzeichen sowie Untersuchungsberichte entdeckt. Die Dienststellen zeigten sich sehr betroffen. Durch geeignete Maßnahmen sollen künftige Verstöße vermieden werden.

Ähnlich spektakulär war der Fund von vollständigen Altakten über "Fürsorgezöglinge" auf einer Deponie. Die Nachforschungen der zuständigen Bezirksregierung verliefen leider im Sande. Eine abschließende Klärung, ob ein datenschutzrechtlicher Verstoß der Bezirksregierung oder der mit der Aktenvernichtung beauftragten Firma vorlag, konnte nicht erbracht werden. Der Vorfall wurde allerdings zum Anlaß genommen, mögliche Schwachpunkte der Verfahrensabläufe bis hin zur Aktenvernichtung zu beseitigen.

Beschwerden über den Ausdruck von Geburtsdaten im Anschriftenfeld von Fensterbriefumschlägen und auf Postzustellungsaufträgen, "sprechende" Stempelaufdrucke auf Briefumschlägen, der Versand von sensibler Post in offenen Briefumschlägen - die Liste der Nachlässigkeiten von Behörden in diesem Bereich ist lang. Kurz gefaßt möchte ich nochmals an alle Verantwortlichen appellieren, auch im Umgang mit Papierdokumenten und beim konventionellen Postversand datenschutzgerecht zu denken und zu handeln. Notwendige organisatorischen Maßnahmen erfordern keinen zusätzlichen personellen oder finanziellen Aufwand.

5. Europa, Ausland

5.1 EU-Datenschutzrichtlinie

Für den internationalen Datenschutz war der 24.7.1995 ein wichtiges Datum: Der Rat der Europäischen Union (EU) verabschiedete die "Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (ABl. Nr. L 281/31). Diese EU-Datenschutzrichtlinie wird in den nächsten Jahren Richtschnur und Orientierungshilfe bei der Novellierung des nationalen Datenschutzrechtes sowie beim Umgang mit grenzüberschreitendem Datenschutz sein. Es ist zu hoffen, daß von ihr eine Wirkung über den räumlichen Bereich der EU hinaus ausgeht. Osteuropäische Staaten, die ein Interesse am Beitritt zur EU haben, scheinen sich beim erstmaligen Erlaß von nationalen Datenschutzvorschriften am EU-Standard orientieren zu wollen. Daß internationale Datenschutzstandards dringend erforderlich sind, zeigt sich bei meiner Prüfpraxis immer wieder.

Die Richtlinie nimmt Anleihen im Datenschutzrecht verschiedener Mitgliedsstaaten. Es ist jedoch nicht zu verkennen, daß insbesondere das französische und das deutsche System bei der Formulierung Pate standen. Daher zwingt die Richtlinie auch nicht zur völligen Überarbeitung des deutschen Rechtssystems. Dessenungeachtet enthält die Richtlinie Regelungen, die dem deutschen Recht unbekannt sind und deren Umsetzung eine Verbesserung des Datenschutzniveaus bei uns zur Folge haben wird. So fordert Art. 8 Abs. 1 den verstärkten Schutz sensibler Daten, d.h. von Daten über rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben. Damit stellt die Richtlinie nicht auf ein besonderes berufliches Vertrauensverhältnis (z.B. Arztgeheimnis), die verarbeitende Stelle oder einen bestimmten Zweck (z.B. Sozialgeheimnis) ab, sondern auf das Risiko für die Betroffenen. Die Gesetzgebung wird nicht umhinkommen, den entsprechenden Schutz bereichsspezifisch neu zu regeln, z.B. durch ein Arbeitnehmerdatenschutzgesetz oder durch Gesundheitsdatenschutzgesetze. Neu ist auch ein allgemeines Widerspruchsrecht (Art. 14). Dieses Widerspruchsrecht eröffnet den Betroffenen die Möglichkeit, eine Prüfung der Rechtmäßigkeit und der Zweckmäßigkeit von Speicherungen durch die verarbeitende Stelle zu veranlassen. Der dem französischen Recht entnommene Art. 15 verbietet belastende Entscheidungen gegen Personen, die ausschließlich auf automatisierten Vorgängen basieren. Damit soll nicht die sinnvolle Automation bestimmter Massenvorgänge verhindert werden. Vielmehr soll ausgeschlossen werden, daß Menschen auf ein Informationsmuster reduziert und von Maschinen gelenkt werden. Im Mittelpunkt jeder

Datenverarbeitung muß - sei es als Anwender oder als Betroffener - der Mensch stehen. Bestehen bei einer Datenverarbeitung spezifische Risiken, so schreibt Art. 20 eine Vorabkontrolle vor, die der in § 7 Abs. 3 NDSG geregelten Technikfolgenabschätzung entspricht. Der aus der niederländischen Rechtspraxis stammende Gedanke, Verhaltensregeln, sog. Codes of Conduct, von berufsständischen Organisationen erarbeiten zu lassen und diese für verbindlich zu erklären, fand in Art. 27 Eingang. Diese Regelung wird hoffentlich die Eigenverantwortlichkeit für den Datenschutz insbesondere im privaten Bereich durch Aktivitäten der Wirtschaftsverbände stärken. Schließlich gibt Art. 28 der Richtlinie Anlaß, die Organisation und die Befugnisse der Kontrollinstanzen zu überdenken. Insbesondere im privaten Bereich müssen durch Ausweitung der Kontroll- und der Einwirkungskompetenzen Verbesserungen erfolgen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat aufgelistet, welche Änderungen des allgemeinen Datenschutzrechts von der Datenschutzrichtlinie gefordert und welche Verbesserungen wünschenswert sind (Anlage 19). Der sich im nicht-öffentlichen Bereich ergebende Änderungsbedarf ist unter 31.1 dargestellt.

5.2 BahnCard-Daten in den Staaten

Als die Deutsche Bahn AG im Juli 1995 bei der BahnCard die Citibank mit ins Schlepptau nahm, standen in meiner Dienststelle die Telefone nicht mehr still. Laufend beschwerten sich Kundinnen und Kunden der Bahn über die Formulargestaltung des BahnCard-Antrags, über übermäßige Datenerhebungen vor allem bei Beantragung der BahnCard ohne Zahlungsfunktion (BahnCard-pur), über die Zusendung falscher BahnCards, die ungesicherte Mitteilung der PIN, über Anschreiben aus Holland, über die Verarbeitung der Antragsdaten in den USA u.s.w. Die Bearbeitung dieser Beschwerden war zunächst dadurch erschwert, daß relevante Verträge zwischen Bahn, Citibank und weiteren beteiligten Unternehmen noch gar nicht ausgehandelt waren und die Beantwortung meiner an die Citibank gerichteten Anfragen zu wünschen übrig ließ. Inzwischen ist die Zahl der Eingaben geringer geworden; die Verträge liegen vor. Unter Federführung des für die Deutsche Bahn AG zuständigen Berliner Datenschutzbeauftragten wurden mit den Beteiligten Verhandlungen geführt, die zu einer datenschutzgerechteren Formulargestaltung führten. Verfahrensmängel wurden beseitigt. Ich war und bin an den Diskussionen beteiligt, weil zwei der Citibank-Töchter, u.a. die Citicorp Card Operations GmbH, ihren Sitz in Niedersachsen haben. Die gesamte Datenschutzproblematik des Verfahrens darzustellen, würde den Umfang dieses Tätigkeitsberichtes sprengen.

Eingegangen werden soll jedoch auf die grundsätzliche Problematik der Datenverarbeitung in den USA: Bahnkundinnen und -kunden, die eine BahnCard-pur haben wollen, müssen die "Einwilligung" dazu erteilen, daß ihre Daten in einem Rechenzentrum "in den USA auf einem dem Bundesdatenschutzgesetz vergleichbar hohen Schutzniveau" verarbeitet werden. Die Gründe für dieses "Outsourcing", diese Auslagerung der Datenverarbeitung in die USA: "Rationalisierung und Zentralisierung".

Das nunmehr verabredete und von den Datenschutzbehörden akzeptierte Verfahren sollte aus folgenden Gründen für andere Anwendungen kein Vorbild sein: Voraussetzung jeder Einwilligung ist deren Freiwilligkeit. Von Freiwilligkeit kann aber keine Rede sein, wenn diejenigen, die verbilligt mit der Bahn reisen wollen, zu einer entsprechenden Erklärung gezwungen sind. Die Verarbeitung der Antragsdaten sowie der Abrechnungsdaten erfolgt bei der Citibank South Dakota. Die Herstellung und Erneuerung aller drei BahnCard-Kartenvarianten erfolgt bei der Citibank Nevada. Rechtliche Grundlage für die Übermittlung von Antragsdaten nach South Dakota und Nevada in den USA kann eigentlich nur § 28 Abs. 1 Satz 1 Nr. 1 BDSG sein. Die Verarbeitung bewegt sich im Rahmen der Zweckerfüllung des BahnCard-Vertrages. Problematisch ist aber, daß die Kundinnen und Kunden der Bahn einem faktischen Zwang zum Vertragsabschluß unterliegen. Von Vertragsfreiheit kann insofern wohl kaum noch gesprochen werden. Außerdem erreicht das Datenschutzniveau in den USA nicht den deutschen Standard.

Um diesen Mängeln abzuhelfen, hat man sich einer Notlösung bedient: Die deutschen und die amerikanischen Citibank-Unternehmen schlossen eine "Vereinbarung zum gebietsübergreifenden Datenschutz" zugunsten Dritter. Danach ist die Weitergabe der Daten in den USA für Werbezwecke verboten. Die Kartenkundinnen und -kunden können ihre Rechte auf Auskunft, Berichtigung, Sperrung, Löschung und Schadensersatz gegenüber dem deutschen Kartenunternehmen oder der Deutschen Bahn AG auch mit Wirkung auf die USA wahrnehmen. Schließlich wurde verabredet, daß der Berliner Datenschutzbeauftragte in den USA vor Ort selbst Datenschutzprüfungen vornehmen oder durch einen Beauftragten vornehmen lassen kann. Im Ergebnis dürfte damit ein ausreichendes Datenschutzniveau erreicht worden sein (vgl. die Kriterien des Düsseldorfer Kreises in Anlage 1). Damit ist nicht ausgeschlossen, daß im Rahmen des Verfahrens neue Probleme auftauchen. Unbefriedigend bleiben die nicht erforderliche Verarbeitung in den USA und die dies legitimierende rechtliche Konstruktion.

5.3 Das VW-Haustelefonbuch gehört nicht in die USA

Im letzten Tätigkeitsbericht (XII 5.3) stellte ich dar, wie ein Kläger im Rahmen eines Schadensersatzverfahrens in Texas/USA die Volkswagen AG dazu verpflichten wollte, ihr Konzern-Telefonbuch zu Beweisermittlungszwecken herauszugeben. Trotz meiner Intervention sowie der anderer Datenschützer bzw. öffentlicher Stellen bestätigte das Berufungsgericht die erstinstanzliche Entscheidung des Einzelrichters, daß die VW AG das aktuelle Telefonbuch herausgeben müsse. Es führte aus, die Vorlage des Telefonbuchs würde nicht die Rechte der Beklagten, also von VW, beeinträchtigen, sondern nur die Datenschutzinteressen ihrer deutschen Bediensteten. Zwar verstoße die Herausgabe gegen ein deutsches Gesetz. Das texanische Zivilprozeßrecht kenne aber keine generelle Privilegierung ausländischen Rechts. Aus "Rücksicht und Respekt" vor fremden Gesetzen seien diese im Rahmen der Abwägung zu berücksichtigen. Im konkreten Fall wurden jedoch "die Interessen dieses Staates sowie der Vereinigten Staaten" für gewichtiger angesehen als die deutschen

Datenschutzbelange. Auf die hiergegen von VW eingelegte Revision hob der Supreme Court of Texas Ende 1995 die beiden vorangegangenen Entscheidungen auf (DuD 1996, 500 f.). Bei der Beschaffung von Beweismitteln im Ausland seien fünf Kriterien zu prüfen: die Bestimmtheit des Beweisantrages, die ausländische Herkunft des Beweismittels, das Fehlen alternativer Beweismöglichkeiten, die Abwägung gegenüberstehender staatlicher Interessen sowie letztendlich eine Abwägung der Parteiinteressen. Das Fehlen dieser Abwägung und die Unterschlagung des deutschen Datenschutzrechts sowie der damit verbundenen staatlichen und parteilichen Interessen führte letztendlich dazu, daß das Telefonbuch doch nicht herausgegeben werden mußte. Diese Entscheidung ist im Hinblick auf die EU-Datenschutzrichtlinie von Bedeutung, da ihr der Gedanke zugrundeliegt, daß bei der Anwendung nationalen Rechtes in den USA das Datenschutzrecht des Herkunftslandes zumindest im Rahmen einer Abwägung berücksichtigt wird. Dies wiederum kann ausschlaggebend für die Zulässigkeit von Datenübermittlungen aus der EU in die USA sein, da nach Art. 25 EU-Datenschutzrichtlinie im Empfängerland "ein angemessenes Schutzniveau gewährleistet" sein muß.

5. 4 Der elektronische Pranger im "Netz der Netze"

Am Ende meiner Handlungsmöglichkeiten bin ich regelmäßig, wenn Daten vom Ausland aus ins Internet eingestellt werden, da es keinerlei weltweite gemeinsame Datenschutzstandards gibt. Hierzu ein markanter Fall: Ein Apotheker berichtete mir, daß seine Medikamentenversendung in die USA über Internet abrufbar wäre. Bei meiner Suche im Internet wurde ich sofort fündig: Die Food and Drug Administration (FDA), eine US-Behörde, listet vollständig die Versendung von Medikamenten, die in den USA nicht zugelassen sind und deshalb gestoppt wurden, mit Nennung des Datums und genauer Angabe des jeweiligen versendenden Apothekers in ihrer Homepage auf. Die Befürchtung des Apothekers, daß auch die Patientennamen im Internet genannt würden, konnte ich zerstreuen. Über einen Arzt, der hier in Deutschland auch viele Patientinnen und Patienten aus den USA behandelt und zur Nachbehandlung Medikamente dorthin versenden läßt, enthält das Internet gar einen mehrseitigen detaillierten Steckbrief. Nach Angaben dieses Arztes ist die Versendung nichtzugelassener Medikamente in die USA erlaubt, wenn durch Nennung eines Arztes die dortige medizinische Betreuung der medikamentösen Nachbehandlung sichergestellt ist. Der behördliche "Internet-Pranger" der FDA zeigte Folgen: Bei den auf der Internet-Liste aufgeführten Apothekern meldete sich jemand aus Holland, der diesen anbot, ihre Medikamentenversendung illegal an der FDA vorbei zu übernehmen. Nach deutschem Datenschutzrecht wäre die Veröffentlichung derartiger "schwarzer Listen" eindeutig unzulässig. Auch wenn diese Informationen Personen in Deutschland betreffen und die Angaben in Deutschland abfragbar sind, sind mir rechtlich die Hände gebunden. Weitere Ausführungen zum Internet sind unter 4.2 zu finden.

5.5 Chinesische Teppichwerbung

Baß erstaunt war ein niedersächsischer Bürger, als er aus China, genauer gesagt aus Peking, die Einladung zu einer in heimischen

Landen stattfindenden Möbel-Verkaufsausstellung erhielt - garniert mit vielen schönen chinesischen Schriftzeichen. Meine Anfrage, wie die chinesische Firma an die deutschen Kundendaten gekommen war, richtete ich nicht an Peking, sondern an das niedersächsische Möbelhaus. Dieses teilte mir lapidar mit, bei dem Anschreiben habe es sich um eine "übliche Werbeaktion" gehandelt. Da derartige Antworten mich nie zufriedenstellen können, hakte ich nach und erfuhr, daß Kundenadressen des Möbelgeschäftes in Deutschland als Selbstklebeetiketten ausgedruckt worden waren, die dann von einem Agenten nach China mitgenommen worden sind. In China wurden die Etiketten dann auf chinesische Briefumschläge geklebt und einzeln als Luftpost wieder nach Deutschland gesandt. Auch wenn ich gegen diese Erklärung keine datenschutzrechtlichen Einwände erheben konnte, so bleibt ein solches Verfahren dennoch ärgerlich: Die Befürchtung, daß im Ausland - und im konkreten Fall in einem Land, das es offensichtlich mit Bürgerrechten nicht genau nimmt - mit Daten gehandelt wird, war auf den ersten Blick nicht unbegründet. Der "Werbegag" kommt einer Täuschung nah und war nicht gerade ein Vorbild für Transparenz und Kundenfreundlichkeit im Bereich der Datenverarbeitung im Direktmarketing.

6. Datenschutzrecht - allgemein

6.1 Novelle des NDSG

Im Zuge der Überlegungen zur Verwaltungsreform wurde die Frage aufgeworfen, ob durch Änderungen des NDSG eine Entlastung der Verwaltung erreicht werden kann. Ich halte es aus grundsätzlichen Erwägungen für problematisch, ein Gesetz, das erst vor drei Jahren - in Teilen sogar noch später - in Kraft getreten ist, bereits zu einer Zeit zu novellieren, zu der hinreichende praktische Erfahrungen damit noch nicht gewonnen werden konnten. Nach meinem Eindruck ist in den Verwaltungen das geltende Recht noch immer nicht hinreichend bekannt (vgl. z.B. 15.1), in der Praxis wird grundlegenden datenschutzrechtlichen Forderungen vielfach immer noch mit Unverständnis begegnet, z.T. wurden und werden Verpflichtungen des NDSG - etwa zur Bestellung von Datenschutzbeauftragten - nur zögerlich umgesetzt. Vor diesem Hintergrund ist zu befürchten, daß eine Novellierung zum jetzigen Zeitpunkt die in der Praxis z.T. vorhandene Skepsis gegenüber dem Datenschutzrecht verstärkt. Hinzu kommt, daß die EU-Datenschutzrichtlinie bis 1998 eine weitere Änderungen des NDSG notwendig macht (vgl. 5.1, Anlage 19). Je kürzer das Verfalldatum gerade auch grundlegender Rechtsvorschriften für die Verwaltung ist, desto größer dürften auch die in der Praxis zu beobachtenden Umsetzungsdefizite sein. Schließlich wird nach meiner Einschätzung der Einspareffekt, der mit einer Deregulierung datenschutzrechtlicher Vorschriften erzielt werden kann, weit überschätzt. Ungeachtet dieser grundsätzlichen Vorbehalte gegen eine Rechtsänderung zum derzeitigen Zeitpunkt, werde ich mich sachlich vertretbaren Änderungen des NDSG, die auf eine Verminderung des Verwaltungsaufwandes abzielen, ohne den gebotenen Schutz des Rechts auf informationelle Selbstbestimmung abzubauen, nicht verschließen.

Mit dem Niedersächsischen Innenministerium sind in diesem Zusammenhang folgende Rechtsänderungen erörtert worden:

1. In § 7 NDSG soll verdeutlicht werden, daß die von den speichernden Stellen zu treffenden technischen und organisatorischen Maßnahmen unter Berücksichtigung des Standes der Technik und der hierfür entstehenden Kosten ein Schutzniveau zu gewährleisten haben, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

Ich habe dieser Rechtsänderung nicht grundsätzlich widersprochen, halte sie aber für entbehrlich. Sie ändert an der bisherigen Rechtslage im Ergebnis nichts. Schon in den Gesetzesberatungen zur geltenden Rechtsvorschrift bestand Einvernehmen, daß technische Maßnahmen

zur Sicherstellung des Datenschutzes nur im Rahmen der Verhältnismäßigkeit gefordert werden können. Praktische Probleme beim Vollzug der Vorschrift sind überdies nicht bekannt geworden.

2. Die gesetzlichen Verpflichtungen, auch für nicht-automatisierte Dateien Dateibeschreibungen zu fertigen und bei automatisierter Datenverarbeitung ein Geräteverzeichnis zu führen (§ 8 Abs. 1 und 2 NDSG), sollen entfallen.

Diese Änderung befürworte ich, da sie unnötigen Verwaltungsaufwand vermeidet. Die Verwaltungspraxis hat im übrigen nach meinen Prüfungserfahrungen zumindest die Verpflichtung zur Anfertigung von Dateibeschreibungen für nicht-automatisierte Dateien weitgehend unbeachtet gelassen.

3. Die Zahl der Bildschirmarbeitsplätze, die die Bestellung von Datenschutzbeauftragten erforderlich macht (§ 8 Abs. 3 NDSG), soll erhöht werden, um insbesondere die Kommunen zu entlasten.

Diesem Vorschlag stehe ich skeptisch gegenüber. Meine Kontakte zu behördeninternen Datenschutzbeauftragten zeigen, daß diesen gerade auch im kommunalen Bereich erhebliche Bedeutung für die Sicherstellung des Datenschutzes zukommt. Eine maßvolle gesetzliche Anhebung der Zahl der Beschäftigten, die regelmäßig mit automatisierter Datenverarbeitung betraut sind, würde im übrigen angesichts des zunehmenden EDV-Einsatzes nur geringfügige Einsparungen mit sich bringen. Schließlich sieht auch die EU-Datenschutzrichtlinie - sofern nicht umfassende Meldungen an eine Kontrollstelle erfolgen - eine Bestellung solcher Datenschutzbeauftragter vor (Art. 18). Meine abschließende Bewertung des Vorschlages wird von der Beschäftigtenzahl abhängen, an die die Pflicht zur Bestellung eines Datenschutzbeauftragten anknüpft.

4. Das grundsätzliche Erfordernis einer Verordnung für regelmäßige Datenübermittlungen soll nach dem Wunsch des Innenministeriums gestrichen werden. Es wird geprüft, ob künftig besondere Regelungen nur noch für die regelmäßige Übermittlung oder die Aktualisierung kompletter Datenbestände gelten sollen. Für automatisierte Abrufe soll es dagegen bei der derzeitigen Regelung bleiben.

Auch diesem Änderungsvorschlag stimme ich im Ansatz zu. Der Begriff der regelmäßigen Datenübermittlung ist unklar; nach den in den Verwaltungsvorschriften zum NDSG gegebenen Erläuterungen erstreckt sich das Verordnungserfordernis auch auf Fälle, in denen besondere Regelungen zur Sicherstellung des Datenschutzes nach meiner Einschätzung nicht notwendig sind. Entscheidend wird jedoch auch hier die Ausgestaltung der Änderung im einzelnen sein.

5. Auf meinen Vorschlag hin soll die Möglichkeit, daß oberste Landesbehörden unter bestimmten Voraussetzungen eine datenschutzrechtliche Prüfung durch den Landesbeauftragten für den Datenschutz persönlich verlangen können (§ 22 Abs. 4 NDSG),

entfallen. Diese Forderung hatte ich bereits im Gesetzgebungsverfahren zum geltenden NDSG erhoben.

6. Das Register der automatisierten Dateien beim LfD und die hierfür bestehende Berichtspflicht der speichernden Stellen soll auf Meldungen aus besonders sensiblen Bereichen begrenzt werden (§ 22 Abs. 5 NDSG).

Gegen eine Beschränkung der Berichtspflicht habe ich keine grundsätzlichen Einwände. Besonders bei Massenverfahren, in denen weitgehend identische Datenverarbeitungen stattfinden, ist eine Vorlage von Dateibeschreibungen entbehrlich.

7. Anstelle der grundsätzlichen Rechtsverpflichtung des Landesbeauftragten für den Datenschutz, einen datenschutzrechtlichen Verstoß zu beanstanden (§ 23 Abs. 1 NDSG), habe ich vorgeschlagen, mir in dieser Frage einen Ermessensspielraum einzuräumen, wie ihn auch andere Datenschutzgesetze vorsehen. Auf Datenschutzverstöße kann damit differenzierter und angemessener reagiert werden.

Das Innenministerium beabsichtigt, die angesprochenen Rechtsänderungen zusammen mit Änderungen des NGefAG in einem Gesetzentwurf zusammenzufassen.

6.2 Straftaten im Umgang mit Daten

Mehrfach hatte ich mich im Berichtszeitraum mit der datenschutzrechtlichen Strafvorschrift des § 28 NDSG zu befassen.

Einmal beschwerte sich ein Petent über das Vorgehen der Polizei, die angeblich Daten seiner Vorstrafen an einen Privatmann weitergegeben hatte. Deswegen hatte er Strafanzeige erstattet. Bei Einsichtnahme in die staatsanwaltschaftlichen Akten ergab sich, daß jene Polizeidienststelle mit den Ermittlungen beauftragt wurde, deren Beamte angeblich die Daten weitergegeben hatten - ein zumindest unglücklich wirkendes Vorgehen. Die Staatsanwaltschaft hat das Verfahren wegen Verstoßes gegen § 28 NDSG wegen geringer Schuld eingestellt. Derjenige, dem die Daten mitgeteilt worden sind, habe ja jedenfalls über einen Anwalt im Rahmen eines Strafverfahrens Einsicht nehmen und damit dieselben Kenntnisse erlangen können. Dies habe ich nicht ohne Verwunderung zur Kenntnis genommen. Eine spätere Möglichkeit der Akteneinsicht eines Verteidigers macht eine unzulässige Datenübermittlung nicht zur Bagatelle.

In einem anderen Fall hatte sich eine Staatsanwaltschaft an mich gewandt und um Hilfe bei der Auslegung von § 28 NDSG gebeten. In einem Strafverfahren war fraglich, ob unter Schädigungsabsicht nur der Wille, einen Vermögensschaden zuzufügen, oder auch die Absicht, einen Rufschaden herbeizuführen, zur Erfüllung des strafrechtlichen Tatbestandes ausreicht. Die Formulierung im NDSG lehnt sich an andere Datenschutzgesetze an, die wiederum auf das Strafgesetzbuch

zurückgehen. Die dortige Formulierung hat Vorbilder im Wirtschaftsstrafrecht. Hinsichtlich all dieser Gesetze ist in der juristischen Fachliteratur geklärt, daß auch die Absicht, einen immateriellen Schaden herbeizuführen, zur Verwirklichung der Straftat ausreicht. Dies ergibt sich aus Formulierung und Sinn des Gesetzestextes. Weiter hat sich in dem Strafverfahren die Frage ergeben, ob in der Weitergabe von Daten eine "Nutzung" im Sinne von § 28 NDSG liegt. Dies ist, wie sich aus dem Rückgriff auf das BDSG, andere Landesdatenschutzgesetze und die Gesetzesmaterialien zum NDSG ergibt, zu bejahen. Dieser Fall zeigt eine gute Zusammenarbeit mit der Staatsanwaltschaft, die sich im Rahmen meiner Beratungsfunktion gemäß § 22 Abs. 1 Satz 2 NDSG an mich wandte.

7. Statistik

7.1 Dauerbrenner Mikrozensus

Beschwerden über die Auskunftspflicht zum Mikrozensus gehen bei mir schon seit Jahren ein. Beanstandungen waren von mir nie auszusprechen. Statistiker und Datenschutzbeauftragte bemühen sich um ausreichende Aufklärung der Bürgerinnen und Bürger. Am Entwurf der 96er-Erhebungsbogen kritisierten die Datenschutzbeauftragten, daß Pflicht- und freiwillige Angaben vermischt worden waren. Die Unterscheidung war optisch kaum erkennbar. Diese Bedenken aufgreifend, wurden die freiwilligen Angaben durch den Aufdruck "freiwillig", eine andere Farbgestaltung der Zeile und durch die zusätzliche Zeile "Keine Angabe" eindeutig kenntlich gemacht. Unterstützend wird in den Interviewer-Schulungen sowie im Interviewer-Handbuch besonderer Wert auf die Erläuterung zur Freiwilligkeit der Auskunftserteilung gelegt.

7.2 Novellierung des Bundesstatistik-Gesetzes

Im Zusammenhang mit dem neuen Mikrozensusgesetz wurde auch das Bundesstatistikgesetz geändert. Nunmehr gibt es im § 11a Bestimmungen über den Einsatz von computergestützten statistischen Erhebungsmethoden. Auch telefonische Erhebungen sind neuerdings zulässig. Diese sind datenschutzrechtlich problematisch, weil öffentliche Übertragungsleitungen relativ leicht abgehört werden können. Das Niedersächsische Landesamt für Statistik hat mir auf Anfrage mitgeteilt, daß z.Zt. von der Möglichkeit computerunterstützter Erhebungsverfahren kein Gebrauch gemacht wird.

7.3 Sozialhilfestatistik

Unter XII 7.4 stellte ich die Diskussion über die Erhebung von Daten auf freiwilliger Basis nur für Zwecke einer Sekundärstatistik dar. Während das Niedersächsische Innenministerium meiner Auffassung beitrat, es sei rechtswidrig, Datenlücken in einer Sekundärstatistik mit Hilfe von hierfür nachträglich erhobenen Daten zu schließen, vertrat das Niedersächsische Sozialministerium die Ansicht, die Daten seien leistungs- und entscheidungsrelevant und damit erforderlich. Sozialministerien in anderen Ländern sehen dies anders. So hat z.B. das Ministerium für Arbeit, Gesundheit und Soziales in Nordrhein-Westfalen auf Empfehlung des dortigen Landesbeauftragten für den Datenschutz per Erlaß die dortigen Sozialhilfeträger darauf hingewiesen, daß eine

Datenerhebung nur zum Zwecke der Sozialhilfestatistik durch die Vorschriften des BSHG nicht gedeckt sei. In Rheinland-Pfalz wurde die Rechtsauffassung des Landesbeauftragten für den Datenschutz durch den Städte- und Gemeindebund veröffentlicht und den Mitgliedern bekanntgemacht.

7.4 Einzelhandelsstatistik - Erhebung per Postkarte?

Per Postkarte sollten an der Einzelhandelsstatistik teilnehmende Unternehmen ihre Umsätze und die Anzahl der tätigen Personen zu den jeweiligen Berichtsmonaten an das Landesamt für Statistik melden. Wenn auch der Name des Unternehmens nicht direkt auf der Postkarte erscheint - nur eine Kenn-Nummer ist ausgedruckt - so ist doch nicht auszuschließen, daß z.B. durch das Namenszeichen des für die Richtigkeit der Angaben Zeichnenden Rückschlüsse auf das Unternehmen bzw. den Unternehmer gezogen werden können. Das Landesamt für Statistik hat meine Empfehlung aufgegriffen und weist nunmehr die angeschriebenen Unternehmen ausdrücklich auf die Möglichkeit der Rücksendung in geschlossenem Briefumschlag hin.

8. Neue Medien

8.1 Telekommunikation

8.1.1 Rechtsgrundlagen in Bewegung

Die Weichen für eine globale Informations- und Kommunikationsinfrastruktur des 21. Jahrhunderts sind gestellt. Der Bundestag hat mit Zustimmung des Bundesrates das Telekommunikationsgesetz (TKG) verabschiedet und am 1. August 1996 in Kraft gesetzt (BGBl. I, 1120). Die Postreform III zur Liberalisierung der Telekommunikation ist damit weitestgehend abgeschlossen; die letzten Monopole des Staates in der Sprachkommunikation fallen am 1. Januar 1998. Das TKG gilt allerdings nur für den "technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten mittels Telekommunikationsanlagen", nicht dagegen für die Telekommunikationsdienste und schon gar nicht für Mediendienste.

Die Datenschutzbeauftragten können mit dem Ergebnis des Telekommunikationsgesetzes trotz einiger Teilerfolge nicht zufrieden sein. Zum Positiven zählt, daß das Fernmeldegeheimnis gesetzlich neu bestimmt wurde. Es gilt für jeden am Telekommunikationsvorgang Beteiligten, gleichgültig ob er geschäftsmäßig Telekommunikationsdienste erbringt oder nur daran mitwirkt. Bedauerlicherweise enthält das TKG aber keine allgemeine Strafbewehrung von Verstößen gegen das Fernmeldegeheimnis. Dagegen wurde das unbefugte Abhören von Funkdiensten aller Art nun endlich verboten und unter Strafe gestellt. Positiv am TKG sind auch die Wahlmöglichkeiten der Betroffenen beim Eintrag in gedruckte oder elektronische Teilnehmerverzeichnisse; diese wurden deutlich verbessert (vgl. 8.1.4.2). Die Datenschutzbeauftragten hatten ein gesetzliches Gebot zur Datensparsamkeit eingefordert, so wie es die Bundesregierung in ihrem Bericht "Info 2000 - Deutschlands Weg in die Informationsgesellschaft" selbst formuliert hat. Eine Option zu anonymen Zugangs- und Nutzungsformen zur Wahrung des "Rechts auf unbeobachtete Kommunikation" fehlt im TKG.

Mit großer Sorge sehen die Datenschutzbeauftragten, daß die Telekommunikationssysteme zunehmend für Sicherungsfunktionen der Polizei, des Verfassungsschutzes und anderer staatlicher Dienste zweckentfremdet werden. So enthält § 90 TKG die Pflicht, ein automatisiertes Abrufverfahren für die aktuellen Kundendateien aller Telekommunikations-Diensteanbieter einzurichten, über das die zu schaffende Regulierungsbehörde Auskünfte jederzeit und unentgeltlich an folgende Stellen zu geben hat: Gerichte, Staatsanwaltschaften und andere Justizbehörden sowie sonstige Strafverfolgungsbehörden,

Polizeien des Bundes und der Länder für Zwecke der Gefahrenabwehr, Zollfahndungsämter für Zwecke eines Strafverfahrens, Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach dem Außenwirtschaftsgesetz, Verfassungsschutzbehörden des Bundes und der Länder, Militärischer Abschirmdienst und Bundesnachrichtendienst. Dies erfolgt ohne Kenntnis des Telekommunikationsanbieters, also hinter seinem Rücken. Mit dem Aufbau des automatisierten Abrufs wurde eine Infrastruktur-Plattform geschaffen, die jederzeit Erweiterungen des Zugriffs technisch möglich und - nach einfacher gesetzlicher Änderung - auch zulässig macht. Die Telekommunikationsnetze sollen der freien Kommunikation dienen, die nur ausnahmsweise beschränkt werden darf (Art. 5, 10 GG). Der Grenzbereich der Ausnahmen wird mehr ausgeweitet. Darauf immer wieder hinzuweisen, ist die Pflicht der Datenschutzbeauftragten.

Zu den Mängeln des TKG gehört auch die Regelung der Datenschutzkontrolle in § 91. In gemeinsamer Anstrengung der Datenschutzbeauftragten des Bundes und der Länder wurde die Datenschutzaufsicht im Telekommunikationsbereich statt der ursprünglich vorgesehenen Regulierungsbehörde dem Bundesbeauftragten für den Datenschutz (BfD) übertragen. Der Vorschlag der Länder, die Kontrollaufgabe für regionale Anbieter von der zuständigen Länderbehörde wahrnehmen zu lassen, wurde jedoch nicht berücksichtigt. Die jetzt festgeschriebene zentrale Kontrollösung ist aus meiner Sicht nicht praktikabel. Die Länder verfügen über funktionierende Aufsichtsbehörden und haben fast zwei Jahrzehnte Erfahrung in der Koordination von Aufsichtsfällen bundesweit tätiger Unternehmen.

8.1.2 Teledienstegesetz

Die Entwicklung der neuen Informations- und Kommunikationsdienste erfordert über das Telekommunikationsgesetz hinaus einheitliche rechtliche Rahmenbedingungen für die neuen Dienste. Der Bund beabsichtigt, hierfür innerhalb seiner Kompetenzen einen bundesgesetzlichen Ordnungsrahmen in einem Teledienstegesetz (TDG) zu schaffen. Im Mai 1996 gab er dazu datenschutzrechtlich beachtenswerte Vorgaben bekannt, so z.B. den Grundsatz der Datenvermeidung, Verhaltenspflichten, die Festlegung der Verantwortlichkeit der Beteiligten sowie die Verpflichtung der Anbieter zur Einführung von Sicherheitsfunktionen "Identifikation/Authentisierung" und "Zugriffskontrolle".

Wie nicht anders zu erwarten, war die Frage der Regelungskompetenz zwischen Bund und Ländern zunächst heftig umstritten. In einem "Friedensgespräch" im Bundeskanzleramt wurde ein Kompromiß gefunden. Danach unterfallen der Bundeskompetenz "alle elektronischen Informations- und Kommunikationsdienste, die eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne ermöglichen und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste)". Als reine Individualkommunikation werden einvernehmlich angesehen:

Elektronische Post, Telebanking, Telearbeit, Telemedizin, Videokonferenzen, Telelearning in geschlossenen Benutzergruppen, Elektronische Buchungsdienste, Datendienste und Telespiele.

Es wurde vereinbart, die Datenschutzregelungen bei Tele- und bei Mediendiensten zu harmonisieren und zu synchronisieren. Für die Teledienste sollen sie in einem eigenständigen Teledienstedatenschutzgesetz (TDDSG) normiert werden.

Dissens besteht allerdings hinsichtlich der Überwachungsforderungen des Bundes, "Bestandsdaten auf Ersuchen im Einzelfall an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich ist". Medienrechtler und Datenschutzbeauftragte lehnen eine solche Regelung entschieden ab, auch wenn sie "nur" Bestandsdaten betrifft. Das geltende gesetzlichen Grundlagen enthalten für die Sicherheitsbehörden bereits ausreichende Befugnisse im Bereich der Multimedia- und Postdienste (z.B. zur Beschlagnahme und Zeugenvernehmung). Die Pläne würden zu einer weitergehenden Überwachung auch von Unverdächtigen führen. Die gesetzgebenden Körperschaften sollten dem nicht zustimmen.

Kontrovers ist auch, ob es eine Höchstfrist für die Speicherung von Abrechnungsdaten geben soll. Die gerade in Kraft getretene Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) sieht eine Löschungspflicht spätestens 80 Tage nach Versendung der Entgeltrechnung verbunden mit einer Beweislastumkehr vor. Diese Frage soll nun unter dem Gesichtspunkt des Verbraucherschutzes geprüft werden. Auch in der Frage der Datenschutzkontrolle gibt es noch Abstimmungsbedarf. Während die Entwurfsfassung die Kontrolle der nach Landesrecht zuständigen Aufsichtsbehörde zuordnet, versucht der Bund einer zentralen Kontrolle das Wort zu reden. Die Länder haben inzwischen auch für Multimedia im privaten Bereich einen Arbeitskreis zur Gewährleistung des Datenschutzes gegründet, so daß die notwendige Koordination bei länderübergreifenden Kontrollen erfolgen kann.

Leider ist die Idee, für besonders gelungene Sicherungslösungen der Diensteanbieter einen "Datenschutz-Engel" zu vergeben, wieder aufgegeben worden. Zur Verbesserung von Datenschutz und Datensicherheit sollten danach Diensteanbieter ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen. Dieses Datenschutz-Audit könnte zu realen Wettbewerbsvorteilen für Anbieter mit guten Datenschutzlösungen führen.

8.1.3 Telekommunikationsdienstunternehmen-Datenschutzverordnung

An dieses "Unwort" müssen wir uns wohl oder übel gewöhnen, wenn wir nicht die Abkürzung TDSV verwenden wollen. Noch vor Verkündung des neuen Telekommunikationsgesetzes wurde eine neue Datenschutzverordnung in Kraft gesetzt. Der Bund regelt darin, was Netzbetreiber und Anbieter von Telekommunikationsdienstleistungen zum Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten zukünftig zu beachten haben. Der Bundesrat hat sich seine Zustimmung zur Verordnung nur schwer abringen lassen, allerdings nicht in erster Linie wegen Datenschutzproblemen. Die Verordnung wurde auf § 10 Abs. 1 des Gesetzes über die Regulierung der Telekommunikation und des Postwesens vom 14. September 1994 (Postreform) gestützt. Damit erfaßt sie z.Zt. nur Unternehmen, die Telekommunikationsdienstleistungen für die "Öffentlichkeit" erbringen oder daran mitwirken, nicht jedoch geschlossene Benutzergruppen (Corporate Networks).

Zusammen mit meinen Länderkollegen habe ich mich für eine Zustimmung des Bundesrates zur schnellen Verabschiedung der TDSV eingesetzt, weil andernfalls die verfassungsrechtlich unzulänglichen Regelungen der bisherigen TDSV und UDSV noch länger gegolten hätten. Die im ursprünglichen Verordnungsentwurf enthaltenen Btx-Vorschriften wurden auf Betreiben der Länder wieder gestrichen. Die Länder haben insofern auf die fehlende Gesetzgebungskompetenz des Bundes verwiesen und angekündigt, daß der gesamte Bereich der Online-Dienste als Überarbeitung des Bildschirmtext-Staatsvertrags unter neuem Namen von ihnen geregelt werde. Für die notwendige Anpassung der TDSV an das TKG und insbesondere an die Datenschutzanforderungen in § 89 TKG will sich der Bund noch bis 1997 Zeit lassen, um praktische Erfahrungen mit den neuen Rechtsgrundlagen zu sammeln.

8.1.4 Elektronische Telefonverzeichnisse auf CD-ROM

Seit Anfang der 90er Jahre werden Telefonbücher als auf CD-ROM gespeicherte elektronische Verzeichnisse vertrieben. Herausgeber sind nicht nur die Telekom bzw. die von ihr beauftragte Tochter DeTeMedien, sondern auch Hersteller, die Telefonbuch-Angaben kopieren, einscannen oder abschreiben lassen. Diese CD-ROM kosteten bisher mehrere hundert Mark. Ein qualitativer und quantitativer Sprung ergab sich durch die Herausgabe einer neuen bundesweiten Telefonbuch-CD-ROM für knapp 50 DM im Sommer 1995. Das Dumping-Angebot führte zu einem rapiden Preisverfall der Konkurrenzprodukte sowie zu gewaltigen Verkaufszahlen. Inzwischen sind derartige CD-ROM in Deutschland millionenfach im Umlauf. Sie sind teilweise nach allen gespeicherten Merkmalen auswertbar. Bei einigen ist auch die Invert-Suche möglich, d.h. der Schluß von der Telefon- bzw. Fax-Nummer auf Name und Adresse der Anschlußinhaberin bzw. des Anschlußinhabers. Dies führt dazu, daß über die Rufnummernanzeige auf einem Display sofort der Standort eines anrufenden Telefons lokalisiert werden kann. Die Telefonnummer, z.B. anonym verwendet in Kontakt- oder Verkaufsanzeigen, wird zur eindeutig und problemlos einer Person zuordnenbaren Personenkennziffer. Natürlich lassen sich mit den CDs

auch noch beliebige weitere Auswertungen vornehmen, an denen insbesondere Direktvermarkter ein großes Interesse haben. Da CD-ROM auch von Herstellern aus Niedersachsen stammen, erhielt ich zur Problematik eine Vielzahl von Anfragen und Eingaben.

8.1.4.1 Die bisherige Rechtslage

Obwohl dies zunächst äußerst umstritten war, vertrat ich von Anfang an die Ansicht, daß die Herausgabe von CD-ROM durch andere als die jeweiligen Telekommunikationsunternehmen gegen Datenschutzrecht verstößt. Der Verkauf von personenbezogenen CD-ROM ist eine Datenverarbeitung zum Zweck der Übermittlung, die gegen § 29 BDSG verstößt. Lediglich die Telekommunikationsdienstleister selbst konnten sich bisher auf eine Ermächtigung zur elektronischen Veröffentlichung ihrer Kundendaten berufen. Zwar lassen sich Telefonbuchdaten aus allgemein zugänglichen Quellen entnehmen, einer bundesweiten multifunktionalen Auswertung stehen jedoch offensichtlich schutzwürdige Betroffeneninteressen entgegen. Eine Glaubhaftmachung des berechtigten Empfängerinteresses wird überhaupt nicht geprüft. Erschwerend kommt hinzu, daß Korrekturansprüche (Löschung, Berichtigung, Sperrung) auf der CD-ROM schon aus technischen bzw. faktischen Gründen nicht durchgesetzt werden können. Widersprüche nach § 28 Abs. 3 BDSG gegen die Nutzung für Werbung bzw. Markt- und Meinungsforschung laufen leer. Da die auf der CD-ROM geführten Personen nach § 33 BDSG benachrichtigt werden müßten, was jedoch einen allzu großen Aufwand darstellen würde und nicht passiert, liegt ein weiterer Datenschutzverstoß vor. Die CD-ROM-Herausgeber können sich auch nicht auf die Privilegierung nach § 28 Abs. 2 Nr. 1 Buchst. b BDSG berufen, da die Telefonnummer nicht zu den privilegierten Daten gehört.

Inzwischen scheint sich sowohl in der Fachliteratur wie in der Rechtsprechung die auch von mir vertretene kritische Position durchzusetzen. Ungeachtet dieser Rechtslage werden die CD-ROM weiter herausgegeben. Ein Anbieter aus Baden-Württemberg sah sich selbst nach einer aufsichtsrechtlichen Verfügung nicht veranlaßt, sein datenschutzwidriges Treiben einzustellen, sondern präsentierte mit aggressivster Werbung neue Auflagen jeweils in Höhe von mehreren 100.000. Als das Landgericht Mannheim (CR 1996, 413 ff.) die Datenschutzwidrigkeit feststellte, lag schon die neue Auflage ausgeliefert in den Kaufhausregalen. Ein weiterer Trick war, formal als Herausgeber jeweils eine andere Firma zu benennen, so daß rechtliche Verfügungen an frühere Herausgeber nicht so einfach übertragbar waren.

8.1.4.2 Das neue Telekommunikationsrecht

Die neue TDSV und das TKG lassen den Telefonkunden verbesserte Wahlmöglichkeiten für den Eintrag in Teilnehmerverzeichnissen. Auf Verlangen muß die Eintragung in elektronischen oder allgemein in gedruckten öffentlichen Kundenverzeichnissen ganz oder teilweise kostenfrei unterbleiben. Diese Eintragungen sind gesondert zu

kennzeichnen (§ 10 Abs. 3 TDSV). Es ist möglich, im Papier-Telefonbuch mit vollem Namen eingetragen zu sein und die Veröffentlichung in elektronischen Verzeichnissen auszuschließen. § 89 Abs. 8 TKG setzt bei Neukunden sogar einen ausdrücklichen Antrag beim Eintrag in gedruckte oder elektronische Verzeichnisse voraus. Ich habe mich in einer Presseerklärung um Aufklärung über die Wahlmöglichkeiten und Widerspruchsrechte der Telefonkunden bemüht, nachdem die in der TDSV vorgeschriebene Unterrichtung der Telekom über die neuen Kundenrechte gründlich mißlungen war.

8.1.4.3 Abwehrmöglichkeiten

Aufsichtsbehörden haben gegen das CD-ROM-Unwesen nur wenig Handhabe. Ein rechtliches Verbot kann nicht durchgesetzt werden, da die Kompetenzen der Datenschutzaufsicht in § 38 Abs. 5 BDSG kein umfassendes Verarbeitungsverbot vorsehen. Nur "Maßnahmen zur Beseitigung technischer und organisatorischer Mängel" können erzwungen werden. Möglich ist außerdem die Verhängung eines Bußgeldes wegen des Verstoßes gegen die Benachrichtigungspflicht nach § 33 BDSG (§ 44 Abs. 1 Nr. 3 BDSG). Daher habe ich im Januar 1996 gegen eine niedersächsische Firma, die auch in großem Umfang Telefon- und Faxbuch-CD-ROM herausgibt, ein Bußgeld in Höhe von 20.000 DM verhängt. Der Betroffene legte Einspruch ein. Eine erste frühe Verhandlung platzte aus Termingründen. Eine erneute Terminierung des Verfahrens ist bisher nicht erfolgt. Inzwischen wird von dieser Firma eine CD-ROM herausgegeben, die ebenso wie ein Konkurrenzprodukt die sog. Invertsuche zuläßt.

Angesichts der allzu begrenzten Möglichkeiten der Datenschutzaufsicht lag es für viele von der CD-ROM betroffene Personen nahe, Strafverfahren anzustrengen. Auch insoweit wurden in Baden-Württemberg erste Entscheidungen getroffen. In einem frühen Stadium wurden die Verfahren eingestellt. In diesem Zusammenhang stellte die Generalstaatsanwaltschaft Karlsruhe jedoch klar, daß eine Strafbarkeit nur ausgeschlossen war, weil den Beschuldigten ein unvermeidbarer Verbotsirrtum nicht widerlegbar gewesen sei. Bzgl. der Frage, ob Daten im Sinne des § 43 BDSG "offenkundig" seien, was die Strafbarkeit ausschließen würde, wird auf die umfassenden Such- und Selektionsmöglichkeiten hingewiesen. Es sei für die Beschuldigte nicht naheliegend gewesen, daß die Aufbereitung der Daten durch Such- und Selektionsmöglichkeiten die Offenkundigkeit im Nachhinein beseitigen könnte. Dies bedeutet: Nachdem die Rechtswidrigkeit der genannten CD-ROM von mehreren Stellen festgestellt worden ist, können sich Herausgeber nicht mehr auf einen "unvermeidbaren Verbotsirrtum" berufen. Inzwischen ist auch allgemein bekannt, daß über das Papiertelefonbuch hinausgehende Auswertungsmöglichkeiten dazu führen, daß insofern keine Offenkundigkeit vorliegt. Dies gilt insbesondere für die Invertsuche. § 11 Abs. 5 TDSV sieht vor, daß die Auskunftserteilung über Namen und andere Daten von Kundinnen und Kunden, von denen nur die Rufnummer bekannt ist, unzulässig ist. Wenn dies schon für die Auskunft im Einzelfall gilt, so muß dies erst recht für ein Angebot mit über 30 Mio. Datensätzen gelten. Voraussetzung für die Strafverfolgung ist, daß innerhalb von drei

Monaten nach Kenntniserlangung vom CD-ROM-Eintrag ein Strafantrag bei der zuständigen Staatsanwaltschaft gestellt worden ist.

8.1.4.4 ... und kein Ende ?!

Die Erfahrungen mit personenbezogenen CD-ROM sind aus Datenschutzsicht frustrierend. Obwohl rechtlich nicht ernsthaft bestritten werden kann, daß solche CD-ROM illegal sind, überschwemmen diese seit mehr als einem Jahr den Markt, ohne daß bisher gegen diese Praktiken erkennbar ein Kraut gewachsen wäre. Ein Marktanbieter erklärte mir gegenüber, Großdistributoren, also Kaufhäuser, Spezialhandel usw., hätten ihm gegenüber erklärt: "Entweder Sie führen bei Ihrem Produkt die Invertsuche ein, oder sie fliegen aus dem Regal". Angesichts euphorischer Presseberichte über die "irren" Möglichkeiten der Adreß-CD-ROM scheint bei den Herausgebern auch kein Unrechtsbewußtsein aufzukommen. Eine schnelle Mark läßt sich damit allemal verdienen. Diese Situation wird dadurch verschärft, daß es immer leichter ist, Daten auf CD-ROM zu pressen. Inzwischen gibt es nicht nur Telefonbuch-CD-ROM. Jedes bisher auf Papier gedruckte Verzeichnis kann ohne großen Aufwand als elektronisches Verzeichnis erstellt und verkauft werden. Es gibt inzwischen schon ca. 30 Stadt- bzw. Regionaladreßbücher, nicht aber in Niedersachsen (vgl. 11.2). Außerdem finden wir auf dem Markt gut ein Dutzend Branchen-CD-ROM, auf denen nicht nur juristische Personen bzw. Firmen, sondern auch zigtausend gewerblich oder geschäftlich tätige Privatpersonen aufgeführt werden. Auch diese CD-ROM verstoßen zweifellos gegen die §§ 29 und 33 BDSG, was von den Herausgebern nicht in Abrede gestellt wird. Selbst wenn einzelne Betroffene keinen formellen Widerspruch eingelegt haben, ist dies kein Indiz dafür, daß sie mit der Veröffentlichung ihrer Angaben einverstanden wären. Die meisten wissen offensichtlich noch gar nicht, wo ihre Daten überall gespeichert sind. Angesichts dieses Sachverhaltes ist der Bundesgesetzgeber im Rahmen der BDSG-Novellierung aufgefordert, klare und effektiv durchsetzbare Regelungen zur Veröffentlichung elektronischer Verzeichnisse zu erlassen.

8.2 Datenschutz und Medien

8.2.1 Die Medienlandschaft verändert sich

Die rasante Entwicklung der Medientechnik, bunte Angebote interaktiver Online-Dienste, die Einführung des digitalen Fernsehens und auch die zunehmende kommerzielle Nutzung von Pressearchiven sind nicht nur als Segen der Technik in einer Informationsgesellschaft anzusehen, sondern stellen eine besondere Gefährdung des Rechts auf informationelle Selbstbestimmung dar. Bei der Vermittlung und Abrechnung dieser Dienste entstehen umfassende Kundendatensätze, aus denen sich individuelle Vorlieben, Interessen und Sehgewohnheiten ableiten lassen. Daraus können Mediennutzungsprofile einzelner Zuschauerinnen und Zuschauer erstellt werden.

Der Arbeitskreis Medien hat im Auftrage der Konferenz der

Datenschutzbeauftragten des Bundes und der Länder im März 1995 einen ausführlichen Bericht zum Thema "Medien und Persönlichkeitsschutz" vorgelegt. Darin werden die neuen Formen der Informationsverbreitung und die Öffnung der Medienarchive beschrieben. Die Reichweite des datenschutzrechtlichen Medienprivilegs wird in Frage gestellt und eine Verbesserung der Rechte der Betroffenen gegenüber den Medien gefordert. Während von der Berichterstattung in Rundfunk und Fernsehen Betroffene Auskunft über die den Berichten zugrundeliegenden, zu ihrer Person gespeicherten Daten verlangen können, besteht gegenüber der Presse bisher kein entsprechendes Auskunftsrecht. Im Gegensatz zu den Rundfunkveranstaltern sind Presseunternehmen auch nicht verpflichtet, etwaige Gegendarstellungen zu den gespeicherten Daten zu nehmen (Mitspeicherungspflicht). Da bei der Presse immer stärker digitale Medien Anwendung finden, die zunehmend interaktiv genutzt werden, ist eine Angleichung an das bestehende Rundfunkrecht geboten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 9./10. März 1995 eine Neubestimmung des datenschutzrechtlichen Medienprivilegs und eine Verbesserung der Betroffenenrechte gefordert (vgl. Anlage 7).

Der Berliner Datenschutzbeauftragte hat Berichte und Entscheidungen über den Persönlichkeitsschutz im Medienbereich sowie aktuelle medien- und presserechtliche Gerichtsentscheide im Rahmen seiner Reihe "Materialien zum Datenschutz" veröffentlicht. Die Broschüre kann beim Berliner Datenschutzbeauftragten gegen Portoerstattung durch Zusendung von Briefmarken bezogen werden.

8.2.2 Der "gläserne" Fernsehzuschauer

Mit dem digitalen Fernsehen erwächst die Gefahr, daß Sehgewohnheiten, Vorlieben und Interessen der Fernsehzuschauer registriert und ausgewertet werden. In ihrer Entschließung vom 22./23. Oktober 1996 weisen die Datenschutzbeauftragten des Bundes und der Länder auf diese Gefahr hin und unterbreiten einen Gestaltungsvorschlag für eine datenschutzgerechte Mediennutzung. Die einzusetzende Zusatztechnik (Set-Top-Box) muß dazu so gestaltet werden, daß die Abrechnung anonym erfolgt und keine personenbezogenen Nutzerdaten erhoben, gespeichert und verbreitet werden. Im voraus bezahlte Wertkarten (Prepaid-Karten) könnten zur Abrechnung kostenpflichtiger Sendungen oder Nutzungen verwendet werden. Damit sollten die Mediennutzenden zumindest alternativ die Möglichkeit erhalten, Programmangebote anonym und unbeobachtet in Anspruch nehmen zu können, so wie sie dies auch beim heutigen Fernsehen können (Anlagen 23, 24). Die Forderung der Datenschützer entspricht dem "Gebot der Datenvermeidung", das in ein TDDSG (vgl. 8.1.1) aufgenommen werden soll.

8.2.3 Landesrundfunkgesetz

Das Landesrundfunkgesetz (LRG) wurde "modernisiert"; es gilt nunmehr neben den traditionellen Rundfunk- und Fernsehdiensten auch für Programme, bei denen die einzelnen Sendungen jeweils zum Abruf bereitgestellt werden (Abrufdienste), unabhängig davon, ob sie elektronisch gespeichert oder fortlaufend verbreitet werden (Nds. GVBl. 1993 S. 523 u. 1995 S. 480). Die besonderen Datenschutzvorschriften des LRG unterscheiden Verbindungs- und Abrechnungsdaten. Die Speicherung der Abrechnungsdaten darf Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter in Anspruch genommener Programmangebote nicht erkennen lassen, es sei denn, daß die Teilnehmerin oder der Teilnehmer ausdrücklich eine aufgeschlüsselte Abrechnung beantragt. Neu in § 48a LRG ist eine Erprobungsklausel, nach der Modellversuche mit neuartigen Rundfunkübertragungstechniken, neuen Programmformen oder rundfunkähnlichen Diensten für genau umrissene Anwendungsbereiche und für einen befristeten Zeitraum von maximal fünf Jahren ohne das hohe Erfordernis eines Gesetzgebungsverfahrens zulässig sind. Die Modellversuche sind so durchzuführen, daß eine Bewertung der gesellschaftlichen Folgen der erprobten Techniken, Programmformen oder Dienste möglich ist. Nach Bewährung sind diese Verfahren gesetzlich zu regeln.

Aber auch dieser erweiterte Rundfunkbegriff deckt bei weitem nicht die gesamte Angebotspalette von Multimedia ab. Seine Abgrenzung zur Individualkommunikation ist umstritten. Die notwendige Klarstellung wird durch das TDG (8.1.2) und den Mediendienste-Staatsvertrag (Mediendienste-StV) geschaffen werden. Das LRG ist ohnehin nach dem 3. Rundfunkänderungsstaatsvertrag, der vom Mediendienste-StV abgekoppelt und vorgezogen beschlossen wurde, zu ändern.

8.2.4 Staatsvertrag über Mediendienste

Die Länder haben schon 1983 in einem Bildschirmtext-Staatsvertrag (Btx-StV) geregelt, unter welchen Bedingungen Informationsdienste auf Abruf in Form von Texten, Standbildern oder Grafiken betrieben werden dürfen. § 10 Btx-StV hat vorbildliche Datenschutzregeln zur Begrenzung und Zweckbindung von Teilnehmerdaten geschaffen; er verpflichtet Netzbetreiber und Anbieter, durch technische und organisatorische Maßnahmen die Einhaltung der Datenschutzvorschriften sicherzustellen. Die Länder haben diesen Bereich trotz eines Meinungsstreits mit dem Bund eigenständig geregelt, weil sie Abrufdienste dem Medienrecht und damit ihrer Gesetzgebungskompetenz zuordneten. Der Btx-StV ist technisch längst überholt und muß dringend an die Entwicklung moderner Online-Dienste angepaßt werden. Dabei muß auch das integrierte Angebot von Bewegtbildern und von Audiodateien auf Abruf einbezogen werden, die bisher überwiegend dem Rundfunk zugeordnet werden. Durch die neuen Online-Dienste ist das Fundament des Btx-StV, die Trennung zwischen dem Betreiber des Dienstes und den Anbietern der Inhalte (Content-Provider), faktisch aufgehoben. Da Online-Diensteanbieter in aller Regel ihre Angebote unter eigener Regie und auf eigene Rechnung zur Verfügung stellen, fallen ihnen auch die Abrechnungsdaten zu, die ihnen nach § 10 Abs. 3 Btx-StV aber nur in

Ausnahmefällen übermittelt werden dürften. Die Mediennutzung wird so auch dem Content-Provider bekannt. Durch eine Neuregelung muß gewährleistet werden, daß Online-Diensteanbieter nicht mehr Daten speichern, als Anbieter nach dem Btx-StV zulässigerweise erhalten dürften.

Den Ruf nach Neuregelung haben die Medienreferenten der Länder längst vernommen. In enger Zusammenarbeit mit den Datenschutzbeauftragten der Länder haben sie einen Entwurf für einen Mediendienste-StV erarbeitet. Dabei konnten die Datenschutzbeauftragten "Eckpunkte für die datenschutzrechtliche Regelung von Mediendiensten" einbringen, die in der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29. April 1996 fixiert worden sind (vgl. Anlage 20). Schwierig bei den Entwurfsarbeiten war die Frage der Regelungskompetenz zwischen Bund und Ländern. Im Rahmen des "Friedensgesprächs" (vgl. 8.1.2) fand man einen Kompromiß. § 2 des Entwurfs des Mediendienste-StV definiert jetzt: "Der Staatsvertrag gilt für das Angebot und die Nutzung von an die Allgemeinheit gerichteten Mediendiensten in Text, Ton oder Bild, die unter Benutzung elektromagnetischer Schwingungen ohne Verbindungsleitung oder längs oder mittels eines Leiters verbreitet werden". Und weil es trotz komplizierter Definition immer noch nicht klar genug war, wurde dem Protokoll eine Zuordnungsliste beigefügt. Danach wird

Pay-TV, Pay-per-view, Near-video-on-demand, Video-on-demand und Elektronische Presse

dem Rundfunk zugeordnet; auch das lange umstrittene Teleshopping durch einseitige Erklärung von den Ländern in Anspruch genommen wird. Die Individualkommunikation (Teledienste, s.o. 8.1.2) unterfällt der Bundeskompetenz.

Die Datenschutzregelungen für Mediendienste sollen, bis auf wenige Besonderheiten, denen des TDDSG entsprechen. Dissens besteht allerdings auch beim Mediendienste-StV hinsichtlich der Überwachungsforderungen des Bundes. Eine solche Regelung wäre dem Medienrecht fremd und zudem datenschutzrechtlich bedenklich.

Die Datenschutzkontrolle der Mediendienste soll nach der Entwurfsfassung des Mediendienste-StV der nach Landesrecht zuständigen Aufsichtsbehörde zugeordnet werden. Die Datenschutzbeauftragten unterstützen diesen Regelungsvorschlag.

9. Personenstandsrecht:Ungewollte amtliche Beihilfe zur Kindesentführung?

Eine Petentin hatte sich vor Jahren von ihrem ausländischen Ehemann scheiden lassen und war mit ihrem Kind nach Deutschland zurückgekehrt. Aus gutem Grund hatte sie ihre hiesige Wohnanschrift gegenüber dem Kindesvater geheimgehalten. Sie befürchtet die Entführung ihres Kindes.

Ausländische Ehescheidungen sind in der Bundesrepublik nicht unmittelbar wirksam. Um wieder heiraten zu können, mußte die Petentin bei ihrem Standesamt den Antrag auf Anerkennung der Ehescheidung durch die Justizverwaltung stellen. Sie befürchtete nun, ihr Ex-Ehemann könne ihre derzeitige Anschrift in diesem Verfahren erhalten. Der Standesbeamte versicherte ihr, er würde ihre Anschrift nicht weitergeben. Ihm war jedoch nicht bekannt, daß die Justiz den Ex-Ehemann im Anerkennungsverfahren beteiligt. Die Justiz wiederum ahnte nichts von den besonderen Umständen und übersandte eine Ausfertigung des Anerkennungsbescheides mit der Anschrift der Petentin an den Ex-Ehemann. Damit waren alle Vorsichtsmaßnahmen zunichte gemacht.

Dieser Sachverhalt darf sich nicht wiederholen. Ich habe vorgeschlagen, das Antragsformular umzugestalten, damit Antragsteller ihren Wunsch auf Geheimhaltung der Anschrift darlegen können. Diese Anregung hat das Niedersächsische Justizministerium nicht aufgenommen. Es befürchtet, daß dann zahlreiche Antragsteller irrationalen Ängsten folgen und die Geheimhaltung der Anschrift zum Regelfall wird. Das Ministerium hält es für ausreichend, wenn das Standesamt auf besonderen Wunsch einen entsprechenden Vermerk in den Antrag aufnimmt. Die Standesämter sind über diese Neuerung informiert worden. Es bleibt zu hoffen, daß diese Maßnahmen ausreichen, um vergleichbare Situationen zu verhindern.

10. Ausweis- und Melderecht

10.1 Chancen für ein bürgerfreundlicheres Melderecht

Derzeit liegt ein Entwurf zur Änderung des Niedersächsischen Meldegesetzes vor. Wesentlicher Grund der Novelle ist der Anpassungsbedarf an das geänderte Melderechtsrahmengesetz des Bundes. Es geht dabei u.a. um Bestimmungen zur Hauptwohnung und zur Meldepflicht beim Beziehen einer Gemeinschaftsunterkunft.

Leider keine Berücksichtigung im Entwurf fand mein Vorschlag, Datenverkäufe an Adreßbuchverlage und die Datenweitergabe an Parteien, Presse, Rundfunk und einzelne Mandatsträger von der vorherigen Zustimmung der Betroffenen abhängig zu machen. Bisher dürfen Meldeämter bestimmte Angaben an die genannten Empfänger weitergeben, wenn die betreffenden Personen den Übermittlungen nicht widersprochen haben. Nach dem geltenden Recht sind Datenweitergaben zunächst einmal erlaubt. Erst wenn die Betroffenen sich regen, bestimmen sie selbst über den Umgang mit ihren Daten. Die Grundrechtsträger müssen sich ihr Recht auf informationelle Selbstbestimmung also zurückholen. Häufig kommen sie dabei zu spät. Die Werbeflut im Briefkasten ist ein erster Hinweis, daß interessierte Firmen über Adreßbücher die Daten schon längst in ihren Computern haben (vgl. XII 11.5.).

Die von mir vorgeschlagene Einwilligung als Voraussetzung für spätere Übermittlungen vermeidet unangenehme Überraschungen. Sie setzt auf informierte Bürgerinnen und Bürger, die individuell entscheiden, ob sie mit den zukünftigen Datentransfers einverstanden sind oder nicht. Also: Erst fragen und dann übermitteln. In den mir vorliegenden Beschwerden und vielen Anrufen ist die Empörung über das gegenwärtige Verfahren überaus deutlich. Häufig wird die Frage gestellt: "Wo bleibt der Datenschutz?" Vor Wahlen, zuletzt vor der Kommunalwahl 1996, erhielt ich regelmäßig Eingaben, in denen sich Betroffene verwundert zeigen, daß ihre Anschriften den Parteien bekannt sind. "Kann die Verwaltung mit den Daten, die der Bürger angeben muß, machen, was sie will?" Alle Beschwerdeführer ärgern sich besonders über die ihnen unbekannten Übermittlungsmöglichkeiten. Für die Betroffenen ist es eine Selbstverständlichkeit, doch bitte selbst über diese Datenweitergaben entscheiden zu können, und zwar vorher. Für das Melderecht ist es das noch nicht.

Ein Wort zum Thema Hotel- und Krankenhausmeldepflicht: Diese im Interesse der Sicherheitsbehörden bestehenden Pflichten waren auf den Widerstand der Datenschutzbeauftragten des Bundes und der Länder gestoßen, weil damit alle Hotelgäste bzw. Patienten als Gefahrenquelle

oder potentielle Straftäter angesehen werden (vgl. XI 11.3). Dennoch halten sowohl der Bund im Melderechtsrahmengesetz als auch das Land im Niedersächsischen Meldegesetz daran fest. Etwas Bewegung gab es im Zusammenhang mit der Krankenhausmeldepflicht. Im Rahmenrecht des Bundes erfolgte eine Änderung, nach der die Offenbarung von Patientendaten aus Verzeichnissen der Krankenhäuser an Sicherheitsbehörden auf Auskünfte im Einzelfall beschränkt wird. Grund hierfür waren praktische Erfahrungen. Diese Vorgabe übernimmt nun auch der Entwurf zur Änderung des Niedersächsischen Meldegesetzes.

Bemerkenswert ist die Entwicklung bei der Hotelmeldepflicht. Art. 45 des Schengener Durchführungsabkommens verpflichtet die Mitgliedsstaaten, als Ausgleich für den Wegfall von Grenzkontrollen innerstaatliche Hotelmelde- und Identitätsnachweispflichten für Ausländer vorzusehen (vgl. XI 6.3). Der Bund hat diese Verpflichtung im Rahmenrecht umgesetzt. Niedersachsen folgt dem nun. Vorgesehen ist im Entwurf eine besondere Melde- und Identitätsnachweispflicht für ausländische Hotelgäste. Die Frage zu stellen, welchen Sinn die Hotelmeldepflicht hat, und hierüber zu diskutieren, ist angesichts der europäischen Vorgaben ohne praktischen Nutzen.

10.2 Schöne neue Welt: Meldedaten auf CD-ROM und im Internet

Das Problem der Herausgabe von Meldedaten an Adreßbuchverlage hat sich durch die technische Entwicklung zugespitzt. Nachdem verstärkt Telefonbücher auf CD-ROM angeboten werden (vgl. 8.1.4), wollen Privatfirmen Meldedaten auch zur Herstellung von elektronischen Adressenverzeichnissen nutzen. Damit eröffnen sich im Vergleich zum örtlichen Adreßbuch ganz neue Möglichkeiten. Die Adreßdaten können elektronisch mit anderen Datenbeständen zusammengeführt und nach nicht mehr überschaubaren Kriterien ausgewertet werden. Es wäre nur noch ein kleiner Schritt bis zum Aufbau des bundesweiten Melderegisters auf CD-ROM. Im privaten Bereich würde damit eine Datensammlung entstehen, die der Gesetzgeber der öffentlichen Verwaltung nicht erlauben wollte. Eine solche Verwendung von Meldedaten ist nicht zulässig.

Das Niedersächsische Innenministerium hat sich nach einigem Ringen meiner Meinung angeschlossen. Die Meldebehörden wurden durch Erlaß aufgerufen, sich zu vergewissern, daß die anfordernden Stellen die Daten nur für die Herausgabe eines Adressenverzeichnisses in gedruckter Form nutzen wollen. So sehr ich diese Klarstellung begrüße: Es wird nicht zu verhindern sein, daß sich andere der Adreßbücher bedienen und z.B. durch Einscannen letztlich doch ein elektronisches Adressenverzeichnis erstellen. Angesichts der Entwicklung in der automatisierten Datenverarbeitung können die Betroffenen nicht mehr überblicken, welche Konsequenzen die Veröffentlichung ihrer Adreßdaten hat. Die Entscheidung des niedersächsischen Gesetzgebers, die Weitergabe von Meldedaten an Adreßbuchverlage zu ermöglichen, sollte grundsätzlich überdacht werden. Die neuen technischen Möglichkeiten erfordern eine neue Bewertung dieses Eingriffs in das Recht auf informationelle Selbstbestimmung.

In einer niedersächsischen Stadt wurde ein Vorstoß unternommen, einen Teil der Meldedaten in das Internet einzustellen. Name, Vorname, Doktorgrad und Anschrift aller Einwohnerinnen und Einwohner sollten auf diesem Weg der Öffentlichkeit zur Verfügung gestellt werden. Eine solche Veröffentlichung von Meldedaten ist unzulässig. Auch das Niedersächsische Innenministerium sieht dies so. Der Gesetzgeber hat die Meldebehörde verpflichtet, bei der Erteilung einer einfachen Melderegisterauskunft über Namen, Doktorgrad und Anschrift zu prüfen, ob im Einzelfall Anhaltspunkte für eine mögliche Beeinträchtigung schutzwürdiger Belange vorliegen. Eine Auskunft über eine Vielzahl von Personen, die der Empfänger namentlich nicht kennt, setzt darüber hinaus noch ein öffentliches Interesse voraus. Diese gesetzlichen Vorgaben würden bei der Internet-Speicherung nicht mehr beachtet. Es gäbe einen kontrollfreien weltweiten Zugriff auf den Datenbestand. Das Verfahren würde im übrigen zum Bereithalten von Meldedaten für den Abruf durch Private führen, was in § 12 Abs. 4 Satz 1 NDSG ausdrücklich untersagt ist.

10.3 Technische Mängel in Meldeämtern: Die Rechte der Betroffenen kommen zu kurz

Das Melderecht enthält beispielhaft klare Vorgaben für die Verarbeitung von personenbezogenen Daten. Entsprechend problemlos müßte eigentlich die Umsetzung vor Ort sein. Überraschend war nun das Ergebnis meiner Prüfungen bei drei Meldeämtern: Die dort eingesetzten automatisierten Verfahren gewährleisten zwar die Verwaltungsabläufe, vernachlässigen aber die Rechte von Einwohnerinnen und Einwohnern.

- Melderegisterauskünfte über Namen und Anschrift kann grundsätzlich jedermann ohne besondere Voraussetzungen erhalten. Um so wichtiger ist es, diejenigen Einwohnerinnen und Einwohner, die der Meldebehörde glaubhaft gemacht haben, sie seien besonders gefährdet, durch Auskunftssperren zu schützen. Es geht hier z.B. um Polizeibeamte, die im Bereich der organisierten Kriminalität ermitteln. Die im Meldeamt eingesetzte Technik muß gewährleisten, daß das gesetzliche Übermittlungsverbot uneingeschränkt beachtet wird. Vorgefunden habe ich Meldeprogramme, die dem nicht gerecht werden. Z.B. sah die Technik vor, selbst bei Lebensgefahr für die Betroffenen Auskunftssperren nur befristet zu speichern. Dadurch war nur vorübergehend sichergestellt, daß die Meldebehörde keine gesetzlich verbotenen Auskünfte erteilt.

- Zum Schutz der Betroffenen muß bei jeder Abfrage ihrer Meldedaten ein deutlicher Hinweis auf die Auskunftssperre erscheinen. Nicht bei allen Meldeprogrammen werden die Auskunftssperren in der Darstellung auf dem Bildschirm so hervorgehoben, daß sie "ins Auge springen". Trotz bestehender Auskunftssperre kann hier versehentlich eine unzulässige Auskunft erteilt werden.

- Auch für die Meldeämter gilt der Grundsatz der Erforderlichkeit. Meldedaten dürfen nur gespeichert werden, solange sie für die Aufgabenerfüllung benötigt werden. Dieser Grundsatz gewinnt

insbesondere nach dem Wegzug eines Einwohners aus der Gemeinde an Bedeutung. Für diesen Fall enthält § 26 NMG eindeutige Vorgaben. Da auch nach dem Wegzug des Einwohners mit Anfragen zu seiner Person gerechnet werden muß, sieht das Gesetz eine zeitlich abgestufte Löschung und Archivierung seiner Meldedaten vor. Nach fünf Jahren dürfen die Daten nur noch für die im Gesetz genannten Zwecke verarbeitet werden. Ansonsten unterliegen sie einem Nutzungsverbot. Die Meldebehörden müssen durch eine gesonderte Aufbewahrung der Daten sicherstellen, daß ihre Verarbeitung nur noch für bestimmte Zwecke möglich ist. Bei keiner der geprüften Meldebehörden erfüllten die eingesetzten Programme die gesetzlichen Vorgaben. Ein Programm sah überhaupt keine Löschung und Archivierung vor.

- § 22 NMG legt die im Melderegister zu speichernden Daten abschließend fest. Bei allen drei Meldebehörden waren mehr Datenfelder als im Gesetz vorgesehen eingerichtet.

Meine Feststellungen müssen zu Veränderungen bei den automatisierten Verfahren führen. Konsequenzen sind also nicht nur bei den drei geprüften Meldebehörden nötig, sondern bei allen Stellen, die mit einem der geprüften Programme arbeiten.

Das Ergebnis der Prüfungen veranlaßt mich, auf etwas eigentlich Selbstverständliches hinzuweisen: Bei der Entwicklung und dem Einsatz von ADV- Programmen muß über interne Abläufe sichergestellt werden, daß die Beachtung der rechtlichen Regelungen durch die Technik möglich ist. Die Fachabteilungen, die für die Rechtmäßigkeit der Datenverarbeitung verantwortlich sind, müssen vor dem Einsatz automatisierter Verfahren neben der Funktionalität auch die technische Umsetzung der rechtlichen Vorgaben auf Herz und Nieren überprüfen. Das ist nichts Ungewöhnliches. Im Finanzbereich ist eine derartige Vorsorge ausdrücklich vorgeschrieben. Die automatisierte Abwicklung des Kassenwesens in der Gemeinde muß nach § 12 der Gemeindekassenverordnung förmlich freigegeben werden.

Bei meinen Prüfungen ist mir folgendes aufgefallen: Geben Behörden ihre Datenverarbeitung bei Datenzentralen in Auftrag, so können sie teilweise ihre Verantwortung für den rechtmäßigen Umgang mit den personenbezogenen Daten nicht mehr wahrnehmen. Wenn etwa die Meldebehörden die Datenzentralen beauftragen, die Daten aller volljährigen Einwohner, die keinen Widerspruch erhoben haben, aus dem eigenen Bestand zum Zweck der Übermittlung an einen Adreßbuchverlag zu selektieren, werden die Daten von der Datenzentrale in der Regel auf einem Magnetband gespeichert. Den von mir geprüften Meldebehörden fehlte die erforderliche technische Ausrüstung, um dieses Magnetband zu lesen. Sie konnten also nicht kontrollieren, welche personenbezogenen Daten sie dem Verlag zur Verfügung stellen. Sie konnten auch nicht überprüfen, ob alle Widersprüche gegen die Übermittlung von Meldedaten berücksichtigt worden sind. Dafür tragen die Meldebehörden aber die Verantwortung. Sie sind Ansprechpartner, wenn die Betroffenen ihre Rechte wie Auskunft, Berichtigung, Löschung, Widerspruch oder Schadensersatz geltend machen. Die Meldebehörden sollten gegenüber den

Datenzentralen auf Verfahren bestehen, bei denen sie ihre Verantwortung ausüben können.

Ein letzter Punkt: Wer glaubt, die drei von mir geprüften Meldebehörden könnten die aufgezeigten Mängel an der eingesetzten Technik ohne weiteres umgehend abstellen und so die Rechtmäßigkeit ihres Handelns sichern, der irrt sich. Meldebehörden, die das gleiche Programm einsetzen, haben oft mit anderen einen Verbund gebildet. Notwendige Änderungen im Programm müssen von den anderen Anwendern erst abgesegnet werden. Am Ende ist vielleicht noch eine Software-Firma zu beteiligen, die Änderungen gern vornimmt - natürlich gegen gute Bezahlung. So kann es zu einem schwierigen und teuren Unterfangen werden, ein eingesetztes Produkt auf Rechtmäßigkeit zu trimmen.

11. Polizei

11.1 Eindrücke

Datenschutz im Niedersächsischen Gewahrenabwehrgesetz (NGefAG) war Thema vieler Veranstaltungen mit Bediensteten der Polizei. Initiiert wurden die Treffen von an der Sache interessierten Polizisten. Auch meine Informationsgespräche und Prüfungen in den Dienststellen gaben immer wieder Gelegenheit, mit jenen ins Gespräch zu kommen, die vor Ort arbeiten. Die Vorträge und Diskussionen waren für mich sicherlich keine Heimspiele, aber - das haben etliche Beiträge bewiesen - auch keine Auswärtsspiele. Einige Erfahrungen waren bemerkenswert. Ein wesentlicher Umstand ist, Zeit zu haben - Zeit, um Alltagsprobleme in den jeweiligen Aufgabenbereichen zu besprechen - Zeit für das Kennenlernen anderer Sichtweisen, verbunden mit dem Rückschluß auf das eigene Tun. Die Bereitschaft war groß, sich prüfend neben sich zu stellen.

Der Zugang zum NGefAG wird durch den gewählten Aufbau nicht eben erleichtert. Dadurch entstehen und verstärken sich Vorbehalte auch gegen datenschutzrechtliche Bestimmungen. Ging es dann nach Überspringen dieser Hürde um konkrete Anwendungsfragen, so kam es fast immer zu einer einvernehmlichen Beantwortung. Gelassenheit machte sich breit. Als hilfreich wurde empfunden, daß die datenschutzrechtlichen Regelungen weitestgehend abschließend im Gefahrenabwehrgesetz zu finden sind und damit die Materie mit dem Blick in ein einziges Gesetz erfaßt werden kann.

Besonders ärgerlich - und dem NGefAG zur Last gelegt - ist eine häufige Reaktion anderer Behörden auf Anfragen der Polizei: "Ich darf Ihnen aus Datenschutzgründen keine Auskunft geben." Diese Aussage entpuppt sich zumeist als leerer Spruch. Es mag sein, daß Auskunftsgeber über ihre Rechte wenig informiert sind; andere Gründe für Auskunftsverweigerungen sind möglich. Auf jeden Fall können nach dem NGefAG alle erforderlichen Anfragen an Behörden oder sonstige Dritte gestellt werden (Datenerhebung). Eine Antwort setzt allerdings eine Weitergabebefugnis der angegangenen Stelle voraus (Datenübermittlung). Eine solche Übermittlungsnorm steht nun allerdings nicht im Gefahrenabwehrgesetz, sondern in dem Gesetz, das sachlich für die angefragte Behörde gilt. Wie sich während der Veranstaltungen zeigte, gibt es Weitergabebefugnisse. Das rechtliche Problem liegt also in der Verzahnung von verschiedenen Gesetzen. Trotzdem: Auskunftsverweigerungen hemmen erst einmal die Ermittlungen.

Die Veranstaltungen und Gespräche führten zu weiteren Kontakten, bei

denen ich immer versuchte, möglichst schnell zu Lösungen beizutragen. Einmal mehr wurde deutlich, wie wichtig fachaufsichtliche Beratung sowie Aus- und Fortbildung sind.

11.2 Weniger Datenschutz wagen: Über den Abbau von Bürgerrechten im Gefahrenabwehrgesetz

1. Akt - Juni 1994

Inkrafttreten des Niedersächsischen Gefahrenabwehrgesetzes. Erstmals erhält die Polizei gesetzliche Befugnisse, im Vorfeld konkreter Gefahren heimlich und mit besonderen technischen Mitteln bis in Wohnungen hinein ermitteln zu dürfen. Erlaubt wird z.B. der verdeckte Einsatz von Videotechnik und Mikrofonen. Das war die präventive Wende. Die Polizei ist nicht mehr nur für die Abwehr konkreter Gefahren zuständig, sondern auch für die Abwehr möglicher Risiken. Die gesetzlich erweiterten Handlungsmöglichkeiten haben zur Folge, daß - häufig technisch bedingt - sehr schnell Informationen über viele unverdächtige Dritte miterfaßt und verwendet werden (vgl. XII 12.1).

Zur Begrenzung der sehr weit angelegten Befugnisse für den Einsatz besonderer Mittel und in Respekt vor Bürgerrechten sieht das Gesetz zwei Ausgleichsmaßnahmen (Hürden) vor:

1. Die besonderen Mittel dürfen im Vorfeld von Gefahren nur eingesetzt werden, wenn Straftaten von erheblicher Bedeutung verhindert werden sollen. Diese Straftaten werden in einem zwar umfänglichen, aber immerhin abschließenden Katalog aufgezählt.

2. Als Ausgleich für die möglichen sehr intensiven Eingriffe wird ein "Grundrechtsschutz durch Verfahren" verankert. Hierzu gehören u.a. Richtervorbehalte vor dem Einsatz besonderer Mittel, spezielle Prüf- und Löschungspflichten für Daten unverdächtiger Dritter, Unterrichtungspflichten. Der Innenminister: "Polizeiliches Handeln soll gerade mit Hilfe der verfahrensmäßigen Vorkehrungen überprüfbar und akzeptanzfördernd ausgestaltet sein."

Schon während der Gesetzesberatungen setzte eine bis heute andauernde teilweise polemische Kritik ein. Das neue Gesetz sei für die Polizei untauglich, es verhindere Polizeiarbeit. Mit unrichtigen Beispielen wurde suggeriert, notwendige Befugnisse seien nicht oder nicht mehr vorhanden. Forderungen nach einer Überarbeitung des NGefAG standen im Zusammenhang mit der Aussage, Niedersachsen werde ein Eldorado der Kriminalität. Im Gesetz vorhandene und auf das Volkszählungsurteil zurückgehende datenschutzrechtliche Verfahrensbestimmungen wurden damit abqualifiziert, sie würden fehlerhaftes Polizeihandeln provozieren.

Nicht auszuschließen ist, daß die vorhandene Unruhe bei der Umsetzung der Polizeireform ablehnende Positionen zum NGefAG begünstigten.

2. Akt - Mai 1996

Die Kritik zeigt erste Wirkungen. Das Gefahrenabwehrgesetz wird geändert (Gesetz vom 20. Mai 1996, Nds. GVBl. S. 230). Die erste Hürde zur Begrenzung der weitreichenden Vorfeldbefugnisse, der begrenzende Straftatenkatalog in § 2 Nr. 9, fällt weg bzw. wird geöffnet. Nunmehr dürfen besondere Mittel heimlich zur Verhütung auch solcher Straftaten eingesetzt werden, die nach dem geschützten Rechtsgut und der Strafandrohung den bereits aufgezählten Vergehen vergleichbar sind. Dunkel bleibt, welche Vergehen damit gemeint sind. Die Strafandrohungen bei den schon bisher genannten Vergehen sind unterschiedlich. Diese Vergehen betreffen zehn verschiedene Rechtsgüter. Meine Hoffnung, die für die praktische Anwendung so wichtigen Verwaltungsvorschriften würden in diesem Punkt Klarheit schaffen, trog. In den Bestimmungen, vor deren Erlaß ich nicht beteiligt wurde, werden die "vergleichbaren Vergehen" eher wolkig erläutert. Sie müßten u.a. mindestens der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung zu beeinträchtigen. Welche Vergehen, frage ich mich, werden nicht vergleichbar sein? Steine statt Brot - von einer normenklaren Regelung, die das BVerfG fordert, kann jedenfalls nicht die Rede sein.

Die Folgen der Öffnung des Straftatenkataloges sind klar. Die Einschätzung, ob eine Straftat von erheblicher Bedeutung vorliegt oder nicht, geht auf Dienststellenleiter über - mit allen rechtlichen Unsicherheiten, wie Gerichte später die vorgenommene Einschätzung bewerten. Die noch während der ersten Gesetzesberatungen überwiegende Meinung, der Katalog sei aus Gründen der Rechtssicherheit für alle Beteiligten ganz wesentlich und nur das Parlament solle den möglichen Rahmen heimlicher Ermittlungen im Vorfeldbereich bestimmen, ist nur noch Geschichte. Klar ist auch, daß eine Schlüsselnorm des NGefAG in unüberschaubarer Weise zugunsten polizeilicher Handlungsmöglichkeiten erweitert wurde. Weshalb dies aufgrund welcher praktischen Situationen unerläßlich sein soll, wurde nicht dargelegt. Die neue unklare Bestimmung über Straftaten von erheblicher Bedeutung wirkt sich in insgesamt fünfzehn Vorschriften des Gesetzes aus, z.B. bei der Frage, ab wann jemand als Kontaktperson gespeichert werden kann, ab wann Wohnungen betreten werden dürfen oder ab wann verdeckte Ermittlungen mit besonderen Mitteln im Vorfeld konkreter Gefahren bei einem ersten vagen Hinweis stattfinden dürfen.

Die Änderungen des NGefAG erfolgten unter dem Eindruck der sogenannten Chaostage '95. Es galt, Flagge zu zeigen. Ziel der Änderung war es, die angekündigten Chaostage '96 zu bewältigen. Eingeführt wurde u.a. ein bundesweit einmaliges präventives Aufenthaltsverbot. Niemand hat aber bisher behauptet, der Straftatenkatalog habe irgendetwas mit der Nichtbewältigung oder Bewältigung von Chaostagen zu tun.

3. Akt?

Das Innenministerium trägt sich mit dem Gedanken, durch eine weitere Änderung des Gefahrenabwehrgesetzes den "Grundrechtsschutz durch

Verfahren" abzubauen. Welche konkreten Änderungen erfolgen sollen, war bei Redaktionsschluß noch nicht bekannt. Die Rede ist von einer Änderung der Anordnungskompetenzen und von der Streichung von Unterrichtungspflichten sowie besonderer Prüf- und Löschungspflichten.

Schon jetzt möchte ich folgendes bzgl. einer eventuellen weiteren Änderung des NGefAG zu bedenken geben: Mir liegen keine praktischen Belege dafür vor, daß das NGefAG einen unverhältnismäßigen Arbeitsaufwand verursachen würde. Auf der anderen Seite ist mir kein Vorhaben bekannt, wonach technische Möglichkeiten auch zugunsten der Rechte von Betroffenen genutzt würden, z.B. für die nachträgliche Unterrichtung nach heimlichen Ermittlungen. Ich hielte es für betrüblich, wenn nach zwei Jahren das damals politisch Gewollte zur Wahrung von Bürgerrechten zu den Akten gelegt würde.

Außerdem rege ich an, vor jedem Abbau von verfahrensrectlichen Sicherungen die Entscheidung des Sächsischen Verfassungsgerichtshofs (SächsVerfGH) vom 14. Mai 1996 zum dortigen Polizeigesetz zu berücksichtigen (JZ 1996, 957 ff.). Das Gericht behandelt in mehr als einem Drittel seiner Ausführungen den "Grundrechtsschutz durch Verfahren". Dabei räumt es dem Gesetzgeber einen Gestaltungsspielraum ein. Bemerkenswerterweise mahnt der Verfassungsgerichtshof aber Verfahrensregelungen in Sachsen an, von deren Streichung in Niedersachsen die Rede ist. Eine Ergänzung des NGefAG um Bestimmungen, die nach Auffassung des SächsVerfGH in ein Polizeigesetz hineingehören, wird, soweit für mich ersichtlich, derzeit noch nicht erwogen. Hier geht es unter anderem um das Verbot des Einsatzes besonderer Mittel im Vorfeld ausschließlich zugunsten von Individualrechtsgütern und um Bestimmungen zum Schutz besonderer Vertrauensverhältnisse, z.B. zwischen Patient und Arzt oder zwischen Mandant und Rechtsanwalt. Angemerkt sei, daß an der Entscheidung des Sächsischen Verfassungsgerichtshofs ein niedersächsischer Staatsrechtslehrer mitgewirkt hat.

Ich appelliere an die Landesregierung, dem NGefAG in der derzeitigen Fassung eine Chance zu geben. Ich habe Zweifel, ob schnelle Änderungen zu mehr Rechtssicherheit bei den Anwendern führen. Änderungen sind sicherlich zu erwägen, wenn sich ein Handlungsbedarf aufgrund längerer Umsetzungserfahrung und richterlicher Entscheidungen ergibt. Hilfreich könnte eine Entscheidung des Bundesverfassungsgerichts sein, die im ersten Halbjahr 1997 erwartet wird. Gegenstand der zu entscheidenden Verfassungsbeschwerde sind datenschutzrechtliche Bestimmungen des Hamburger Polizeigesetzes.

11.3 EUROPOL : Über uns nichts als blauer Himmel

11.3.1 EUROPOL-Konvention

Die Beratungen zur EUROPOL-Konvention auf europäischer Ebene sind beendet. Der Konventionstext wurde am 25. Juli 1995 beschlossen. Der Streit über die ursprünglich vorgesehene Kompetenz des Europäischen Gerichtshofes, über Meinungsverschiedenheiten der Vertragsstaaten zur

Auslegung der Konvention zu befinden, ist ausgeräumt. Nach einem am 24. Juli 1996 unterzeichneten Protokoll kann jeder Staat für sich entscheiden, ob nationale Gerichte Auslegungsfragen zur Konvention dem Gerichtshof vorlegen dürfen oder nicht. Verfahrensmäßig sind jetzt die nationalen Parlamente am Zuge, mit dem Ratifizierungsgesetz auch über die notwendigen Umsetzungsregelungen zu entscheiden.

Meine schon im XII. Tätigkeitsbericht unter Nr. 12.4.3 dargestellte Kritik an den datenschutzrechtlichen Bestimmungen fällt angesichts der beschlossenen Fassung eher noch stärker aus. Die Landeshoheit für Daten im Polizeibereich geht wegen der Anlieferungspflichten verloren. EUROPOL erhält eigenständige Informationsbefugnisse, die z.B. bei Speicherungen von Daten über unverdächtige Dritte über das in Niedersachsen erlaubte Maß hinausgehen. Die Ausgestaltung der Rechte von Betroffenen bleibt hinter dem niedersächsischen Standard zurück. Diese haben bei EUROPOL kein Akteneinsichtsrecht. Berichtigungs- und Löschungsansprüche orientieren sich nicht nur an der Rechtslage; ihre Durchsetzung hängt auch von der Zustimmung des anliefernden Staates ab. Das Auskunftsrecht wurde verschlechtert, indem die Ablehnungsmöglichkeiten noch erweitert wurden. Die Betroffenen können keine Gerichte in Anspruch nehmen, um die Datenverarbeitung bei EUROPOL überprüfen zu lassen. Eingeräumt wird ihnen nur eine Beschwerde an die Gemeinsame Kontrollinstanz.

Ohne Zweifel kann international operierende Kriminalität nicht allein durch nationale Aufklärungsarbeit bewältigt werden. Es ist aber schon mehr als erstaunlich, daß für die notwendige Zusammenarbeit ein Modell gewählt wurde, das weder parlamentarische noch fachaufsichtliche noch staatsanwaltschaftliche Kontrollen vorsieht. Eine ausreichende Verankerung von Bürgerrechten wird vermieden. Die gerichtliche Durchsetzung von Individualansprüchen gegen die Datenverarbeitung bei EUROPOL wird nicht ermöglicht.

Denkbar wäre auch gewesen, EUROPOL als reine Vermittlungsinstanz auszugestalten mit einem elektronischen Informationssystem, in das Daten online eingegeben und abgefragt werden können, um die Ermittlungsbehörden direkt zueinander zu bringen. Dann allerdings hätte das nationale - auch datenschutzrechtliche - Regelwerk ganz wesentlich den Ablauf gesteuert. Die Tür wäre nicht verschlossen gewesen, EUROPOL aufgrund von Erfahrungen weiter zu entwickeln.

11.3.2 Das BKA als nationale Verbindungsstelle

Nach der EUROPOL-Konvention sind die nationalen Stellen der Mitgliedsstaaten verpflichtet, für die innerstaatliche Datenanlieferung zu sorgen und sodann an EUROPOL weiterzugeben. Sie sind die ausschließlichen Ansprechpartner für EUROPOL. Bei uns wird das Bundeskriminalamt (BKA) nationale Stelle sein. Für die Datenverarbeitung beim BKA gibt es aber nach wie vor keine bereichsspezifischen Rechtsgrundlagen. Der zwischenzeitlich mit der Bundestags-Drucksache 13/1550 vorgelegte Gesetzentwurf der Bundesregierung wird zur Zeit im Bundestag beraten. Er enthält einige

datenschutzrechtliche Verbesserungen gegenüber dem Vorentwurf (vgl. XII 12.3.1). Dennoch bleiben aber gewichtige Einwände bestehen (vgl. die Entschließung der DSB-Konferenz vom 9./10. März 1995, Anlage 5). Der Bundesrat teilt einige dieser Bedenken. Die Länderstellungnahme betont besonders die föderale Struktur der Polizeien in Deutschland. Aus Effizienzgesichtspunkten sollte zudem bei bundesweit gespeicherten Daten eine Beschränkung auf länderübergreifende bzw. internationale Kriminalität erfolgen.

11.3.3 Ratifizierungsgesetz zur EUROPOL-Konvention

Kurz vor Redaktionsschluß habe ich den Entwurf eines Gesetzes zur EUROPOL-Konvention erhalten. Dieser behandelt vor allem die Ausgestaltung der Zusammenarbeit zwischen dem BKA und den datenanliefernden Länderpolizeien. Damit werden die Landes-Kompetenzen im Polizei- und Datenschutzrecht berührt. Die Datenschutzbeauftragten des Bundes und der Länder haben frühzeitig darauf aufmerksam gemacht, daß die Verantwortung für die von den Ländern erhobenen Daten weiterhin bei ihnen liegt (vgl. XII Anlage 20). Dies betonen auch die Stellungnahmen der Innenministerkonferenz und des Bundesrates. Es waren also Umsetzungsregelungen zu erwarten, die die Geltung der Länderpolizeigesetze sichern. Ich hoffte außerdem, daß die Rechte Betroffener im nationalen Recht umfassender ausgestaltet würden.

Der vom Bundesinnenministerium vorgelegte Entwurf erfüllt diese Erwartungen nicht. Ergänzende Regelungen zum Rechtsschutz Betroffener fehlen. Die Verantwortung der Länder für ihre Daten wird zwar erwähnt. Rechtliche Folgerungen werden daraus aber nicht gezogen. Der Entwurf enthält im wesentlichen nur Festlegungen zu Gunsten von Dienststellen des Bundes und zur Anwendung von Bundesrecht. Der Weg, Kompetenzen der Länder auf den Bund zu verlagern, wird unbeirrt fortgesetzt. Niedersachsen steht nun vor der Frage, ob es solche Kompetenzverlagerungen hinnehmen will. Die Landesregierung ist bisher davon ausgegangen, daß die Länderverantwortlichkeit bei der Umsetzung der Konvention in deutsches Recht beachtet wird (vgl. LT-Drs. 13/1314, zu 9 b bis d).

11.4 Statt einer Bilanz nur eine Sammlung spektakulärer Einzelfälle

Anliegen der Datenschutzbeauftragten des Bundes und der Länder ist es, die Diskussion über die Erforderlichkeit besonderer Erhebungsmethoden und deren Auswirkungen für Rechte der Betroffenen auf Erkenntnisse zu stützen, die stärker als bisher gesichert sind. Wir haben Vorschläge unterbreitet, die eine offene, systematische Überprüfung bzw. Auswertung ermöglichen (vgl. XII 12.2). Die Vorschläge deckten sich weitgehend mit Vorstellungen des Bundeskriminalamtes (BKA). Auch die Vertreter aller Fraktionen haben im Innenausschuß des Deutschen Bundestages diese Linie unterstützt.

Beim BKA wurde eine Rechtstatsachensammelstelle eingerichtet. Der

Auftrag dieser Stelle ist allerdings auf Betreiben einer Reihe von Ländern zusammengeschmolzen auf das Führen einer Bund/Länder-Fallsammlung. Es sollen ausschließlich plakative Einzelfälle aus der Praxis zur Begründung polizeilicher Forderungen gesammelt werden. Die Erfahrung zeige - so die Begründung -, daß ohne solche Beispiele neue gesetzliche Ermächtigungen politisch praktisch nicht durchsetzbar seien. Auf die systematische Erfassung von Erfahrungen mit neuen Befugnissen und der durch sie erzielten Erfolge wird verzichtet. Damit ist die Katze aus dem Sack. Eine Rechenschaftslegung ist nicht gewollt. Warum eigentlich nicht? Die Antwort gibt der zuständige Staatssekretär, indem er auf den Bericht der vorbereitenden Projektgruppe verweist. Danach könne ein umfassende Dokumentation zu rechtspolitisch unerwünschten Konsequenzen führen, etwa dazu, daß Telefonüberwachungen - um nur ein Beispiel zu nennen - nur noch in geringerem Umfang angeordnet werden (vgl. Deutscher Bundestag, Sten. Ber., 33. Sitzung am 26. April 1995, S. 2609 f.).

Die Begründung der Verantwortlichen läßt aufhorchen. Auf der einen Seite sollen spektakuläre Einzelfälle gesammelt und - entsprechend aufbereitet - öffentlich bekanntgemacht werden, um zu zeigen, daß noch mehr Polizeibefugnisse nötig sind - und Grundrechte weiter eingeschränkt werden können (vgl. hierzu schon XII 12.1). Auf der anderen Seite werden einmal erhaltene Eingriffsmöglichkeiten gehütet wie ein kostbarer Schatz, über den man tunlichst nichts verlauten läßt. Mit demokratischer Transparenz hat dies wohl kaum etwas zu tun.

Bei einigen obersten Innenbehörden scheint der Wunsch nach Grundlagenmaterial über die fachliche "Produktivität" eher schwach ausgeprägt zu sein, da daraus evtl. Konsequenzen gezogen werden müßten. Ein ganz anderer Eindruck besteht, wenn es um Fragen der Polizei-Organisation geht. In diesem - sicher wichtigen - Bereich arbeiten Projektgruppen, es wird geforscht, gestritten und verbessert. In Niedersachsen z.B. hat sich eine Projektgruppe mit der Ablauforganisation in der Kriminalitätsbekämpfung befaßt. Gegenstand einer anderen Untersuchung sind die Effektivität und Effizienz kriminalpolizeilicher Organisationsformen auf Zeit (Soko's). Auch in anderen Bereichen, wie z. B. bei der wirtschaftlichen Tätigkeit des Staates, sind Erfolgskontrollen üblich.

Eine weitergehende Behandlung der Vorschläge der Datenschutzbeauftragten soll im Zusammenhang mit einer Überprüfung der Arbeit der Bund/Länder-Fallsammlung 1997 erfolgen.

11.5 Lauschangriff zur Gefahrenabwehr

In der Landtags-Drucksache 13/1638 von Ende 1995 gibt die Landesregierung einen ersten Bericht über die Entwicklung und die Schwerpunkte polizeilicher Arbeit zur Vorsorge für die Verfolgung und zur Verhütung von Straftaten. Dargestellt wird vor allem der Einsatz besonderer Mittel, wie längerfristige Observationen, technische Mittel, Vertrauensleute und Kontrollmeldungen, im Berichtszeitraum Juni 1994 bis Mai 1995. Der Bericht erwähnt einen Anwendungsfall des § 35

Abs. 2 NGefAG, also den umgangssprachlich so bezeichneten "Lauschangriff" in einer Wohnung zur Gefahrenabwehr. Ich habe diese Aktion datenschutzrechtlich überprüft. Meine Kontrolle konnte nur Akten würdigen, die den Verfahrensablauf dokumentieren. Die ursprünglichen Unterlagen aus dem Jahr 1994 waren bereits vernichtet, weil die Informationen für die beabsichtigte Gefahrenabwehr nichts erbracht haben.

Die durchführende Polizeidienststelle war verfahrensmäßig korrekt vorgegangen. So wurde z.B. die notwendige richterliche Anordnung eingeholt. Der Betroffene wurde auch über die durchgeführte Datenverarbeitung unterrichtet, weil eine Gefährdung der Maßnahme auszuschließen war.

11.6 Aus der Praxis der polizeilichen Arbeit

Wenn die Polizei Erkenntnisse über eine Person speichert, hat das Konsequenzen. Jedem Polizisten, der auf den Eintrag stößt, wird signalisiert, daß er es mit einem "zweifelhaften Kunden" zu tun hat. Er wird dann sein Verhalten bzw. seine weiteren Maßnahmen darauf abstellen. Die Erkenntnisse werden darüber hinaus nicht nur polizeiintern genutzt, sondern bei gegebenem Anlaß an andere Behörden übermittelt (z.B. bei der Überprüfung der gewerberechtlichen Zuverlässigkeit). Angesichts der Auswirkungen für die Betroffenen muß es für die Verarbeitung von personenbezogenen Daten bei der Polizei handfeste Gründe geben. Die folgenden Beispiele zeigen, daß dies in der Praxis nicht immer beachtet wird.

11.6.1 Die Angst des Staates vor seinem Bürger

Ein Bürger hat mir folgende Frage gestellt: "Sind wir schon wieder so weit, daß eine Äußerung über einen Politiker ausreicht, um erfaßt zu werden?" Er hält es für einen Skandal, daß sich der polizeiliche Staatsschutz für ihn interessiert. Was ist passiert? Der Petent hat Politikern und einem Richter Briefe geschrieben. Darin hat er seine Meinung über die Politik bzw. über ein Urteil zum Teil in heftigen Worten geäußert. Die Briefe haben zu strafrechtlichen Ermittlungen wegen Beleidigung geführt; verurteilt worden ist der Petent bislang nicht. Einen Brief, der an einen ehemaligen niedersächsischen Minister gegangen ist, hat die Polizei zum Anlaß genommen, den Petenten in den kriminalipolizeilichen Meldedienst in Staatsschutzangelegenheiten aufzunehmen. Dieser Meldedienst soll Informationen über extremistische und terroristische Straftäter in der Staatsschutzdatei APIS zusammenführen. Betroffen sind politisch motivierte Straftäter, die eine Gefahr für den Staat und die Gesellschaft darstellen. Gehört der Petent zu diesem Personenkreis? Ich bezweifle, ob ein solcher Briefeschreiber an den Grundfesten unseres Staates rütteln kann. Ich halte es nicht für gerechtfertigt, den Petenten als Staatsfeind zu betrachten und habe deswegen das Innenministerium um Überprüfung des Falles gebeten.

11.6.2 Kinder werden wie Kriminelle behandelt

Ich habe landesweit bei vier Polizeiinspektionen die Kriminalaktenhaltung überprüft. Dabei habe ich festgestellt, daß solche Akten auch über Kinder geführt werden. Hierfür drei Beispiele:

- Eine zur Tatzeit Fünfjährige hat mit einem zweiten Kind aus dem verschlossenen Gartenhaus des Kindergartens zwei Dreiräder geholt. Der Vorfall wurde als besonders schwerer Fall des Diebstahls in einer Kriminalakte gespeichert.

- Ein Siebenjähriger wurde landesweit als "sexueller Nötiger" geführt. Das Kind soll unter Bedrohung mit einem Taschenmesser zwei andere Kinder gezwungen haben, die "Hosen runter zu lassen". Das Kind bestreitet dies.

- Der zur Tatzeit etwa Achtjährige wollte aus einer Kindertagesstätte ein Bobbycar mitnehmen. Drei Jahre lang wollte die Polizei ihn mit der Kriminalakte im Auge behalten. Im polizeilichen Auskunftssystem wurde er als "Bobbycar-Dieb" gespeichert.

Kriminalakten sollen Ermittlungsansätze für die Aufklärung von Straftaten liefern. Konsequenterweise dürfen Kriminalakten nur angelegt werden, wenn die Betroffenen strafmündig sind. Kinder sind dies nicht. Deshalb erlaubt das NGefAG auch keine Kriminalakten über Kinder. In Niedersachsen werden jedoch nach einer Auswertung zum Zeitpunkt meiner Prüfung (Stand: 1. Dezember 1995) 4.635 Kinderakten bei der niedersächsischen Polizei geführt. Im Anschluß an meine Prüfung, für die ich Diebstahls- und Kinderakten ausgesucht hatte, wurden etwa 40 % der geprüften Akten von den Dienststellen sofort vernichtet. Das Niedersächsische Innenministerium kam nach der Durchsicht meines Berichts zu dem Ergebnis, bei der Praxis der Kriminalaktenhaltung müsse es zu Änderungen kommen. Zu diesem Zweck soll durch eine Arbeitsgruppe unter Berücksichtigung meiner Feststellungen eine neue Kriminalaktenrichtlinie erarbeitet werden.

11.6.3 Wie aus friedfertigen Besuchern Gewalttäter wurden

Die Ereignisse bei den Chaostagen 1995 in Hannover werden wohl noch für einige Zeit in Erinnerung bleiben. Vergessen werden darf dabei aber nicht, daß nicht alle, die im August 1995 nach Hannover gekommen sind, Gewalttäter waren.

Die Polizeidirektion Hannover hatte in einer besonderen Datei die Personen registriert, die bei dem Einsatz in Gewahrsam waren. Die Datei sollte die Übersicht geben, welche Personen bei welcher Gefangenen-Sammelstelle untergebracht waren.

Gegen die Datei selbst habe ich keine datenschutzrechtlichen Bedenken. Die Polizei ist berechtigt, Angaben über in Gewahrsam genommene Personen zu erfassen und zur eigenen Aufgabenerfüllung, z.B. zur Beantwortung von Anfragen besorgter Eltern, zu nutzen. Am 24. August

1995 wurde der gesamte Dateiinhalt (Angaben über 1.084 Personen) jedoch an die Stuttgarter Polizei weitergegeben, weil es dort Hinweise auf bevorstehende Chaostage gab. Das hätte nur geschehen dürfen, wenn es in der Datei nur Angaben über Störer und Gewalttäter gab. Ob das so war, habe ich bei 295 Betroffenen überprüft.

Bei über der Hälfte der Personen gab es entsprechende Erkenntnisse nicht. Teilweise waren sie nur in Gewahrsam genommen worden, damit ihre Identität festgestellt werden konnte. Oft handelte es sich nicht um Einträge vom Chaos-Wochenende 4. bis 6. August 1995. Bereits ab Dienstag, dem 1. August, wurden Personen in der Datei erfaßt ("Voraufsicht Chaostage"). Bei anderen war der Grund für die Gewahrsamnahme überhaupt nicht erkennbar. Eine Person befand sich nur eine Minute in Gewahrsam. Bei anderen war auf den Einsatzberichten vermerkt:

- "Anlaß: Durchsetzung Platzverweis". Bei dem Betroffenen wurden ein Fotoapparat und ein Stadtplan sichergestellt.

- Tathergang: 05.08.1995, Hauptbahnhof Hannover, Gleis 7. "Der Zug kam um 19.15 Uhr an. Da es sich bei den Personen um sogenannte Punker handelte, wurden sie durch den Bundesgrenzschutz in den Postkeller unter Gleis 7 verbracht."

- Ein Betroffener: "Ich wollte Hannover ohne böse Absichten besuchen und einigen Bands zuhören und mich mit Leuten (Menschen/Punks) treffen. Ich wurde sofort im Bahnhof festgenommen und ohne große Erklärung hierher in Gewahrsam gebracht. Begründung: Mein Aussehen (lange Haare, kurze Hose). Na ja, schönen Tag noch."

Die Speicherungen sahen so aus:

>********

#LNR: 03333 (******* Kurzbericht zur Freiheitsentziehung **********)**

#GES: PG Polizei Gewahrsam(Ort der Gefangenensammelstelle)

#AUF: 030895 (Uhrzeit) 1205 H(Aufnahme am/Uhrzeit)

#ENT: 030895 (Uhrzeit) 1840 H JA(Entlassung am/Uhrzeit)

#ERG:(Ergebnisstand)

(******** Personalien **********)**

(NAME/VORNAME) #NAM:Muster, Carsten

(GEB. AM/IN)< #GEB:110380 (IN) Neudorf

(ANSCHRIFT)#ORT:55555 Bad Oberstein, Wiesenweg 5

(******** Zielrichtung der Maßnahmen **********

(GEFAHRENABWEHR) #GEF: X (STRAFVERFOLGUNG) #STV: (OWI) #OWI:

(******** Vorgang **********)**

#GEG: Fotoapparat(Sichergestellte Gegenstände)

***TATORT: BAHNHOF VORPLATZ*TATZEIT: 030895 1205 UHR**

***KURZBESCHREIBUNG: IDENTITÄT**

****

Im Ergebnis wurden mehr als die Hälfte der Personen ohne triftigen Grund mit Gewalttätern in einen Topf geworfen. Die Polizeidirektion Hannover hat für eine Korrektur der fehlerhaften Datenweitergaben nach Stuttgart gesorgt. Die Datei in Hannover wurde gelöscht. Zukünftig wird durch interne Vorgaben sichergestellt, daß vorschnelle Übermittlungen dieser Art unterbleiben.

11.7 Nachtrag zum XII. TB

11.7.1 Speicherungen über Suizidversuche neu geregelt

Drei Jahre nach meiner Beanstandung (vgl. XII 12.8) hat das Niedersächsische Innenministerium die Suizidspeicherungen bei der Polizei durch Erlaß neu geregelt. Zukünftig wird es keine Kriminalakten und keinen Vermerk "Freitodgefahr" im polizeilichen Auskunftssystem nur deshalb geben, weil jemand versucht hat, sich das Leben zu nehmen. Solche Personen dürfen aber registriert werden, wenn der Suizidversuch im Zusammenhang mit der Begehung einer Straftat erfolgt ist oder wenn Wiederholungsgefahr besteht und dabei mit einer Gefahr für Dritte zu rechnen ist, beispielsweise die Verwendung von Sprengstoff befürchtet werden muß. Außerdem darf bei den Personen, über die die Polizei bereits eine Kriminalakte führt, ein entsprechender Sachverhalt zugespeichert werden.

Niedersachsen folgt damit nicht den Bundesländern, die den Hinweis "Freitodgefahr" überhaupt nicht mehr verwenden. Die Neuregelung hat allerdings zu einer erheblichen Reduzierung von Speicherungen bei der niedersächsischen Polizei geführt. Während vor meiner Prüfung über 5.000 Datensätze mit dem Hinweis "Freitodgefahr" im polizeilichen Auskunftssystem gespeichert waren, fanden sich nach der Bereinigung zum 1. April 1996 nur noch 364 Datenbestände.

11.7.2 Hinweise auf Aids **im Polizeicomputer**

Unter XII 12.7 habe ich berichtet, daß im polizeilichen Informationssystem POLAS im Zusammenhang mit dem personengebundenen Hinweis "Ansteckungsgefahr" entgegen dem ausdrücklichen Verbot in einem Erlaß aus dem Jahr 1988 bei drei Personen Speicherungen vorlagen, die den Rückschluß auf eine HIV-Infizierung zuließen. Bei der anschließenden Prüfung aller von den niedersächsischen Polizeidienststellen vergebenen Hinweise "Ansteckungsgefahr" habe ich insgesamt 18 solcher Einträge festgestellt. Alle Speicherungen wurden nach meiner Prüfung gelöscht.

12. Ausländerangelegenheiten

In der Ausländer- und Asylverwaltung tauchen ständig völlig neue datenschutzrechtliche Fragen auf, da die Rechtsgrundlagen wie die eingesetzten Verarbeitungsmethoden einem dauernden Wandel unterworfen sind. Zwei Schwerpunkte der Auseinandersetzungen waren in den letzten zwei Jahren die Planungen für eine "Asylcard" und die Probleme beim Beschaffen von Reisepapieren für Flüchtlinge.

12.1 Der Chip-Flüchtling

Anfang 1995 mußte ich mich mit Plänen der Bundesverwaltung zur "Harmonisierung der Verwaltungsabläufe im Asylverfahren" auseinandersetzen. Hinter so populären Begriffen wie "Verfahrensoptimierung, Effektivitätssteigerung, Kostenminimierung, Verfügbarkeit/Aktualität, Mißbrauchsreduzierung" versteckte sich nichts anderes als der Plan, für Asylsuchende eine Zwangs-Chipkarte einzuführen mit folgenden, ausdrücklich nicht abschließend aufgezählten Funktionen: Identifizierung, Zutrittskontrollfunktion, Aufenthaltskontrolle, Verfahrensdaten (Antrag, Anhörungen usw.), Empfang von Sach- und Unterstützungsleistungen, Arbeitserlaubnis, Leistungen von Dritten, z.B. Unterkunftsbetreiber. Das Verfahren sollte sich an dem Grundsatz orientieren: "Ohne Asylcard keine Leistungen. Der Karteninhaber sorgt für den Transport der auf dem Chip gespeicherten Daten, indem er die Asylcard, die gleichzeitig als Ausweis dient, bei sich zu führen hat".

Ich teilte dem Niedersächsischen Innenministerium mit, daß ich die Einführung einer derartigen Zwangs-Chipkarte mit Daten aus allen Lebensbereichen und zur multifunktionalen Nutzung wegen des Verstoßes gegen die Menschenwürde und gegen das Recht auf informationelle Selbstbestimmung für verfassungswidrig halte. Über die Karte würden Persönlichkeitsbilder entstehen, die die Flüchtlinge zu gläsernen Menschen, zu reinen Objekten, zu chipgespeicherten Informationsmustern für die Verwaltung machen würden. Ich konnte den Eindruck nicht verhehlen, daß die Asylcard nur der Anfang für die Umsetzung weiterer Überwachungsvisionen bei bestimmten Bevölkerungsgruppen ist.

Das Ministerium distanzierte sich zunächst von den Planungen des Bundes. Wenig später stimmte es jedoch der Durchführung einer "Machbarkeitsstudie" zu, ohne daß bisher jemand die Notwendigkeit der fragwürdigen Chipkarte nachgewiesen hätte, etwa nach dem Motto: "Wir haben da eine neue Technik - mal sehen, was wir damit machen können". Offensichtlich beeindruckte - aller grundrechtlichen Überlegungen zum Trotz - ein vergleichbares holländisches

"Vreemdelingendocument". Die konkrete Vergabe und Durchführung der Machbarkeitsstudie ist für das Jahr 1997 vorgesehen.

12.2 Deutsche Behörden als Informationsbeschaffer der Heimatstaaten

Ist die Verarbeitung von Ausländerdaten im Inland oft schon eine delikate Angelegenheit, so gilt dies erst recht für die Weitergabe der Daten ausländischer Staatsangehöriger ins Ausland. Besonders interessiert sind an solchen deutschen Ausländerdaten die Heimatländer der hier lebenden Nichtdeutschen. Aus datenschutzrechtlicher Sicht liegt das Problem zunächst darin, daß es in den Heimatländern regelmäßig keinen akzeptablen Datenschutzstandard gibt. Dies gilt für Algerien ebenso wie für die Türkei oder Vietnam. Werden z.B. Angaben zur Beschaffung von Paßersatzpapieren an ausländische Behörden gegeben, so ist nicht ausgeschlossen, daß diese Angaben zur politischen Verfolgung der Betroffenen genutzt werden. Auf der anderen Seite dürfte es unstreitig sein, daß deutsche Behörden in Einzelfällen zur Erfüllung ihrer Aufgaben Ausländerdaten ins Ausland übermitteln müssen. Dies ist z.B. im Rahmen der internationalen Rechtshilfe für Strafsachen der Fall.

12.2.1 Beschaffung von Paßersatzpapieren

Die Notwendigkeit von Datenübermittlungen an die Heimatländer besteht auch dann, wenn eine Person abgeschoben werden soll, die Abschiebung aber nicht möglich ist, weil keine Reisedokumente vorliegen. Hier muß es den Ausländerbehörden möglich sein, Paß- bzw. Paßersatzpapiere im Herkunftsstaat zu beschaffen und zu diesem Zweck Angaben an die Heimatbehörden weiterzugeben. Die Herkunftsstaaten weigern sich nämlich, Flüchtlinge zurückzunehmen, wenn diese nicht über gültige Papiere verfügen. Der Förderverein Niedersächsischer Flüchtlingsrat berichtete mir von einigen Fällen, bei denen Paßersatzpapiere von Asylsuchenden beantragt worden sind, obwohl das Asylverfahren noch nicht abgeschlossen war. Es wurden sogar Fälle bekannt, wo die mit der Beantragung der Paßersatzpapiere verbundene Datenübermittlung direkt nach Beantragung des Asyls erfolgt sein soll. Dies kann zu einer massiven Gefährdung der Betroffenen führen: Sollte sich im Nachhinein herausstellen, daß der Flüchtling verfolgt ist, so wird dem Verfolgerstaat anläßlich der Dokumentenbeschaffung ein neuer Ansatzpunkt für diese Verfolgung verschafft. Auch die im Heimatland lebenden Angehörigen könnten gefährdet werden. Da ich der Meinung bin, daß sich die deutschen Behörden auch nicht indirekt zu Komplizen von Verfolgerstaaten machen dürfen, wies ich das Niedersächsische Innenministerium darauf hin, daß das Datenschutzrecht und das Asylrecht eine Paßersatzbeschaffung, die nach § 43b AsylVfG zum "frühestmöglichen" Zeitpunkt erfolgen soll, erst nach Abschluß des Asylverfahrens erlaubt. Unter keinen Umständen dürfen bei der Beantragung der Heimreisedokumente Informationen über das Asylverfahren weitergegeben werden, die auch für die Ausstellung der Papiere nicht erforderlich sind. Derartige Informationen unterliegen einer Art "Asylgeheimnis".

Erfreulicherweise hat sich das Niedersächsische Innenministerium dem Grunde nach meinen Überlegungen angeschlossen. In einem Erlaß an die Bezirksregierungen und die Ausländerbehörden weist es darauf hin, daß es einem politisch Verfolgten nicht zugemutet werden kann, zum Zweck der Paßbeschaffung an die Behörden seines Heimatlandes heranzutreten. Solange die Gefahr politischer Verfolgung besteht, dürfen deutsche Behörden den Dienststellen des Herkunftsstaates keine Angaben über den Asylsuchenden machen. Daher sollen Anträge auf Ausstellung von Paßersatzpapieren erst dann den Behörden des Heimatlandes zugeleitet werden, wenn die Aufenthaltsgestattung nach § 67 AsylVfG erloschen ist. Nach § 67 Abs. 1 Nr. 4 AsylVfG erlischt die Aufenthaltsgestattung, wenn die Abschiebungsandrohung vollziehbar ist. Hinweise zu eventuellen Asylverfahren dürfen nicht gegeben werden.

Der Bundesbeauftragte für den Datenschutz setzte sich gemeinsam mit dem Bundesinnenministerium gegenüber dem Auswärtigen Amt dafür ein, über Verhandlungen mit den jeweiligen Botschaften eine "Neutralisierung" der Antragsvordrucke zu erreichen.

12.2.2 Abschiebung von kurdischen Volkszugehörigen

In besonders krasser Form stellt sich das Problem der Datenübermittlung an den Heimatstaat bei der Abschiebung von türkischen Kurdinnen und Kurden dar. Mitte 1995 lief der Abschiebestopp für diese Personengruppe aus. Betroffen sind insbesondere Personen, denen Straftaten im Zusammenhang mit der kurdischen PKK-Organisation vorgeworfen werden. Wegen der Verfolgung von Kurdinnen und Kurden in der Türkei liegt nicht nur in den Abschiebungen selbst, sondern auch in den damit verbundenen Datenübermittlungen sozialer und politischer Konfliktstoff. Der Bundesinnenminister hat schon im März 1995 mit der türkischen Regierung ein Verfahren vereinbart, wonach vor der Abschiebung ein zu beantwortendes Auskunftsersuchen an die türkischen Behörden gerichtet wird, ob der betreffenden Person in der Türkei Strafverfolgung oder Bestrafung droht. Die Türkei verpflichtet sich sicherzustellen, "daß eine abgeschobene Person vor unzulässigen Übergriffen geschützt ist". Gegenüber dem Niedersächsischen Innenministerium äußerte ich Kritik an dem Verfahren. Durch die Anfrage bei den türkischen Behörden wird nämlich diesen zur Kenntnis gebracht, daß gegen die jeweilige Person ein Straftatvorwurf "im Zusammenhang mit der PKK und anderen Terrororganisationen in Deutschland" gemacht wird. Damit wird unter Umständen genau das Gegenteil dessen erreicht, was mit dem Konsultationsverfahren angestrebt wird: die Gefährdung der Abzuschiebenden. Es ist aktenkundig, daß türkische Behörden Personen verhaften und foltern, bei denen der Verdacht der Sympathie zur PKK besteht. Das Niedersächsische Innenministerium entgegnete mir, die letztendliche Verantwortung für die Unterrichtung läge beim Auswärtigen Amt und damit beim Bund. Das Ministerium stimmte ausdrücklich mit mir überein, daß in der Türkei kein angemessener Datenschutzsstandard bestehe. Da die Datenübermittlung aber Voraussetzung für die gesamte Abschiebungsprozedur nach § 53 AuslG

sei, könne die datenschutzrechtliche Bewertung nicht anders ausfallen als die ausländer- bzw. asylrechtliche Beurteilung. Zwar sei keine förmliche Einwilligung der Betroffenen für die Einleitung des Verfahrens erforderlich, das Bundesinnenministerium habe aber die Aussage getroffen, daß diese um ihr Einverständnis gebeten würden. Obwohl mich dieses Ergebnis nicht befriedigt, sehe ich keine Möglichkeit für eine weitergehende Intervention.

12.3 Asylbewerberleistungsgesetz

Erhielten Asylsuchende bisher ebenso wie Deutsche Sozialleistungen, so hat sich dies mit dem Asylbewerberleistungsgesetz von 1993 grundlegend geändert. Dieses Gesetz hatte nicht nur zur Folge, daß die Leistungen gegenüber Asylsuchenden eingeschränkt wurden, sondern auch, daß die datenschutzrechtlichen Regelungen des Sozialgesetzbuches und das Sozialgeheimnis (§ 35 SGB I, §§ 67 ff. SGB X) nicht mehr anzuwenden sind. Dieses Vorenthalten bereichsspezifischen Datenschutzes halte ich im Hinblick auf den Gleichheitsgrundsatz für problematisch. Zur Umsetzung des Gesetzes wurde im Sommer 1995 ein Grundsatzerlaß herausgegeben. Hierbei konnte ich mich mit meinem Vorschlag durchsetzen, darauf zu verzichten, den Namen der berechtigten Personen auf die Wertgutscheine aufzudrucken. Meint man schon, statt Geld den Asylsuchenden Wertgutscheine ausgeben zu müssen, so sollte ihnen zumindest die Möglichkeit des anonymen Einkaufens erhalten bleiben. Es war für mich nicht einsichtig, daß die Namensnennung auf den Wertgutscheinen deren Mißbrauch zu verhindern in der Lage gewesen wäre. Die privaten Ladenbesitzer sind nicht in der Lage und dazu bereit, vor jeder Einlösung von Wertgutscheinen eine Identitätskontrolle durchzuführen. Außerdem konnte ich auf den Behandlungs- bzw. Krankenscheinen die Streichung des Aufdrucks "Asylbewerberin/Asylbewerber" erreichen. Notwendig und ausreichend ist dagegen ein Hinweis für die behandelnden Ärztinnen und Ärzte auf den durch das Gesetz begrenzten Leistungsumfang.

12.4 Ausnahmslose ED-Behandlung von Bürgerkriegsflüchtlingen

Im letzten Tätigkeitsbericht habe ich von Planungen berichtet, Bürgerkriegsflüchtlinge ebenso wie Asylsuchende ausnahmslos erkennungsdienstlich behandeln zu lassen, um so Identitäts-Täuschungen auf die Schliche zu kommen (XII 13.2). Eine entsprechende Regelung war im Entwurf eines Ausländerleistungsgesetzes des Bundessozialministeriums vorgesehen, der aber nicht weiterverfolgt wurde. In ihrer Stellungnahme zu meinem Tätigkeitsbericht (LT-Drs. 13/1230, S. 15 f.) hat die Landesregierung ausführlich begründet, weshalb sie diese erkennungsdienstliche Totalerfassung von Flüchtlingen befürwortet. Es gäbe dringende Hinweise, daß sich kroatische Staatsangehörige unter Zurückhaltung oder Vernichtung ihrer Pässe als "bosnische" Flüchtlinge ausgegeben haben, um in die Bundesrepublik visumsfrei einreisen zu können. Außerdem hätten die niedersächsischen Ausländerbehörden dem Landeskriminalamt 30 verdächtige Ausweispapiere vorgelegt, von denen

nur ein Paß unzweifelhaft als echt erkannt werden konnte. Bei zehn Ausweisen habe es sich um Totalfälschungen gehandelt. Außerdem gäbe es viele Hinweise, daß mit echten und gefälschten bosnischen Ausweisen massenhafter Mißbrauch geschehe; im Steintorbereich in Hannover werde damit ein schwunghafter Handel getrieben. Diese Angaben werden von mir nicht bezweifelt. Sie sollten Grund sein für die aufmerksame Identitätsprüfung und für das konsequente Aufklären aller Verdachtsfälle. Sie können aber nicht als Argument dafür herhalten, daß auch bei Flüchtlingen, deren Identität unzweifelhaft ist, erkennungsdienstliche Maßnahmen durchgeführt werden. Eine derartige Vorratsdatenverarbeitung halte ich nach wie vor verfassungsrechtlich für unzulässig.

Damit nicht genug der Mißbrauchskontrolle: Inzwischen forderten Bonner Politiker, daß Ausländern generell nur noch Sozialhilfe gezahlt werden soll, wenn diese eine erkennungsdienstliche Behandlung über sich ergehen lassen.

13. Verfassungsschutz

13.1 Änderung des Niedersächsischen Verfassungsschutzgesetzes

Mit Gesetz vom 4. April 1995 wurde das Niedersächsische Verfassungsschutzgesetz geändert (vgl. Nds. GVBl. S. 103). Unter anderem wurde die "Aggressionsklausel" gestrichen, nach der Bestrebungen im Sinne des Gesetzes nur dann beobachtet werden dürfen, wenn deren Verhaltensweisen auf Anwendung von Gewalt gerichtet sind oder sich in aktiv kämpferischer, aggressiver Weise gegen die freiheitliche demokratische Grundordnung richten. Meine Position zur Änderung ergibt sich aus dem XII. Tätigkeitsbericht unter 14.1.

Überlegungen, nach denen sich das Land Niedersachsen bei den Beobachtungsvoraussetzungen an Vorgaben des Bundes halten müsse, ist das Bundesverwaltungsgericht inzwischen entgegengetreten. Es hat die Gestaltungsfreiheit des Landesgesetzgebers betont. Er kann festlegen, unter welchen näheren Voraussetzungen politische Parteien mit nachrichtendienstlichen Mitteln beobachtet werden dürfen (DÖV 1995, 692 f.).

13.2 Bundesverfassungsgericht bremst bei strategischer Rasterfahndung des BND

Der Bundesnachrichtendienst (BND) erhielt über eine Änderung des G 10-Gesetzes neue Befugnisse zum Abhören des internationalen, nicht leitungsgebundenen Fernmeldeverkehrs (vgl. XII 14.2). Dem BVerfG liegen mehrere Verfassungsbeschwerden zu diesem Komplex vor. Das Gericht hat im Wege einer einstweiligen Anordnung ein erstes Signal gesetzt. Das Gesetz läßt Datenweitergaben des BND an andere Sicherheitsbehörden bereits zu, wenn dies zur Erfüllung der Aufgaben des Empfängers erforderlich ist. Das BVerfG hat die Datenübermittlungen vorläufig nur erlaubt, wenn bestimmte Tatsachen den Anfangsverdacht von im Gesetz genannten Straftaten begründen (NJW 1996, 115). Die Anordnung läßt erkennen, wie hoch das Gericht den tatsächlichen Eingriffscharakter des Gesetzes einschätzt. Angesichts der Anordnungsgründe dürften in der Hauptsacheentscheidung nicht nur Fragen zur unbeobachteten Kommunikation einzelner angesprochen werden, sondern auch Auswirkungen heimlicher Fernmeldeüberwachungen auf die Kommunikationsfreiheit und das Kommunikationsverhalten aller Teilnehmerinnen und Teilnehmer am Fernsprechverkehr.

13.3 Unterstützungsunterschriften für Wahlvorschlag landen beim Verfassungsschutz

Eine Partei, die nicht im Parlament vertreten ist, muß besondere Voraussetzungen erfüllen, um für die Wahl zugelassen zu werden. Sie muß dazu von einer gesetzlich festgelegten Anzahl von Wahlberechtigten unterstützt werden. Hierfür werden Listen verwendet, in die man sich mit Name, Anschrift und Unterschrift eintragen kann. In den Wahlgesetzen ist eine sehr enge Zweckbindung dieser personenbezogenen Daten festgelegt. Sie dürfen nur für Wahlzwecke verarbeitet werden.

Das Niedersächsische Landesamt für Verfassungsschutz hat von einer anderen Verfassungsschutzbehörde eine Aufstellung von niedersächsischen Personen erhalten, die die Zulassung einer Partei bei der Europa-Wahl 1994 mit ihrer Unterschrift unterstützt haben. Die rechtlichen Bedenken, die gegen die Nutzung der Unterstützungsunterschriften durch die Verfassungsschutzbehörde bestehen, teilte das Landesamt zunächst nicht. Erst als das Bundesamt für Verfassungsschutz vom Bundesinnenministerium angewiesen worden ist, dort vorgehaltene Unterlagen zu vernichten, löschte auch die niedersächsische Verfassungsschutzbehörde die in diesem Zusammenhang gespeicherten Daten.

13.4 Sicherheitsüberprüfung

Der Entwurf für ein Niedersächsisches Sicherheitsüberprüfungsgesetz liegt vor. Das Verfahren kommt jedoch seit längerem nicht voran.

13.5 Zuverlässigkeitsüberprüfungen nach dem Atomgesetz

Zuverlässigkeitsüberprüfungen ähneln den Verfahren der Sicherheitsüberprüfungen. Maßgeblich handelt hier jedoch nicht das Landesamt für Verfassungsschutz, sondern die jeweilige Fachbehörde. Das ist für den Bereich der kerntechnischen Anlagen in Niedersachsen das Umweltministerium. Das Ministerium befragt verschiedene Behörden, auch die Verfassungsschutzbehörde, ob über die Betroffenen etwas bekannt ist, was gegen ihre Beschäftigung in kerntechnischen Anlagen spricht. Betroffen sind davon in Niedersachsen pro Jahr 5.500 Personen.

Die Zuverlässigkeitsüberprüfung von Personal in kerntechnischen Anlagen, wozu auch Arbeiter von Fremdfirmen gehören, führt zu erheblichen Eingriffen in schützenswerte Lebensbereiche der Betroffenen. Es werden sensible Daten verarbeitet, wobei Behörden mitwirken, deren Erkenntnisse auf dem Einsatz besonderer Mittel und Methoden der Datenerhebung, auch nachrichtendienstlicher Mittel, beruhen. Gesammelt werden z.B. Angaben über politische Ansichten und über Schulden. Derartige Einschränkungen des Rechts auf informationelle Selbstbestimmung bedürfen einer verfassungsgemäßen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen und Vorkehrungen treffen muß, um den Gefahren einer Verletzung des Persönlichkeitsrechts entgegenzuwirken. 1989 hat der Bundestag § 12b in das Atomgesetz eingefügt. Danach darf die

Zuverlässigkeit von Personen, die bei der Errichtung und dem Betrieb von kerntechnischen Anlagen sowie sonst im Umgang mit radioaktiven Stoffen tätig sind, mit deren Einverständnis überprüft werden. Der Gesetzgeber hat vorgeschrieben, die Einzelheiten der Überprüfung in einer Rechtsverordnung festzulegen. Diesen Auftrag des Gesetzgebers haben die Fachleute bis heute ignoriert.

Statt eine Rechtsverordnung zu erlassen, haben sie eine Richtlinie für die Überprüfung der Zuverlässigkeit erarbeitet. 1996, also sieben Jahre nach der Änderung des Atomgesetzes, ist die Richtlinie im Gemeinsamen Ministerialblatt veröffentlicht worden (GMBl. Nr. 29, S. 613 ff.). Die vom Gesetzgeber geforderte Verordnung ist bis heute nicht in Sicht. Es gibt also für die Zuverlässigkeitsüberprüfung nach dem Atomgesetz bisher keine den verfassungsrechtlichen Anforderungen entsprechende Rechtsgrundlage.

Das Überprüfungsverfahren ist in den Richtlinien ähnlich angelegt wie beim Flughafenpersonal (vgl. XII 14.8). In meiner Stellungnahme zu dem Richtlinienentwurf habe ich zahlreiche Verbesserungsvorschläge unterbreitet. Sie bezogen sich zum einen darauf, den Umfang der Datenerhebung über die Betroffenen zu begrenzen, beispielsweise durch einen Verzicht auf die Regelanfrage beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes. Zum anderen ging es darum, die verfahrensrechtliche Position der Betroffenen zu stärken (vgl. auch die Entschließung der DSB-Konferenz vom 9./10. März 1995, Anlage 8). Bedauerlicherweise sind meine Empfehlungen nur teilweise berücksichtigt worden.

14. Personalangelegenheiten

Im XII. Tätigkeitsbericht (15.4) hatte ich verstärkte Prüfungen im Personalbereich angekündigt, um mir einen Überblick über die Umsetzung der neuen datenschutzrechtlichen Regelungen zu verschaffen. Ich habe deshalb im Berichtszeitraum die Verarbeitung von Beschäftigtendaten in der Schulabteilung einer Bezirksregierung, bei zwei Schulaufsichtsämtern und in einer Polizeidienststelle überprüft. Trotz mancher Unterschiede im einzelnen waren die Prüfungsergebnisse insgesamt nicht erfreulich. Sie lassen darauf schließen, daß in diesem Bereich erhebliche datenschutzrechtliche Defizite bestehen.

Dies ist sicher auch auf die schwer überschaubare Rechtslage zurückzuführen. Das Neunte Gesetz zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992, mit dem das Beamtenrechtsrahmengesetz datenschutzgerecht ausgestaltet worden ist (vgl. XI 15.1), ist von Niedersachsen bisher nicht in Landesrecht umgesetzt worden. Das Niedersächsische Innenministerium hat statt dessen die wesentlichen datenschutzrechtlichen Bestimmungen in seine Verwaltungsvorschriften zum Niedersächsischen Beamtengesetz (NBG) übernommen (Nds. MBl. 1993, 93). Sie sind allerdings für die Kommunen und die sonstige mittelbare Landesverwaltung nicht verbindlich. Die Grundnorm der Datenverarbeitung bei Dienst- und Arbeitsverhältnissen enthält § 24 NDSG, daneben gelten weitere Vorschriften des allgemeinen Datenschutzrechts. Dieses Ineinandergreifen verschiedener Regelungsbereiche ist für die Personalsachbearbeiterinnen und Personalsachbearbeiter verwirrend. In besonderem Maße gilt dies für Bedienstete, deren Behörde nicht selbst personalaktenführende Stelle ist, sondern - wie z.B. Schulaufsichtsämter oder Polizeiinspektionen - nur Personalnebenakten führt.

Viele Personalsachbearbeiterinnen und Personalsachbearbeiter haben mir freimütig erklärt, sie hätten von den einschlägigen Vorschriften bisher nichts gehört. Zum Beispiel waren den geprüften Schulaufsichtsämtern die Regelungen auch dienstlich nicht zugänglich. Die Aufsichtsbehörden hatten ihnen weder die Rechts- und Verwaltungsvorschriften zur Verfügung gestellt noch Hinweise zum Umgang mit Personaldaten gegeben.

Die Erwartung, die Bediensteten würden sich auch ohne nachhaltige Unterstützung mit dieser komplexen Materie selbst vertraut machen, ist unrealistisch. Ich halte es deshalb für dringend erforderlich, durch Fortbildungsmaßnahmen und geeignete Hinweise dafür zu sorgen, daß die Personalsachbearbeiterinnen und Personalsachbearbeiter in diesem Bereich die notwendige Rechtskenntnis erhalten.

Die Reaktion der geprüften Stellen, der Aufsichtsbehörden und der zuständigen Fachressorts auf meine Prüfungsfeststellungen ist leider oft unbefriedigend. Den Ressorts ist zwar zum Teil bewußt, daß im Bereich der Personaldatenverarbeitung manches im argen liegt, eigenen Handlungsbedarf sieht man jedoch in der Regel offenbar nicht. So hat das Niedersächsische Kultusministerium bezüglich der festgestellten Defizite im nachgeordneten Bereich meinem Prüfungsergebnis zwar zugestimmt, die zuständige Bezirksregierung hat dagegen bei meiner Prüfung zunächst "kein Prüfkonzept" erkennen können, eine Bewertung, die das nachgeordnete Schulaufsichtsamt zur eigenen Entlastung dankbar übernommen hat. Soweit ich gegenüber dem Kultusministerium die Notwendigkeit von Fortbildungsmaßnahmen nachdrücklich betont habe, hat das Fachressort darauf verwiesen, das eingesetzte Personal unterstehe dem Innenministerium. Somit sei dieses für die Qualifikation und Fortbildung der Bediensteten zuständig. Das Innenressort wiederum prüft zur Zeit, wie es auf diese Aussage reagiert. In der Sache ist bisher wenig geschehen.

Meine Prüfungen können nur die Funktion haben, anhand von Einzelfeststellungen problematische Verfahrensweisen aufzuzeigen und Hinweise zu einem datenschutzgerechten Vorgehen zu geben. Ergeben sich dabei Anhaltspunkte, daß über den Einzelfall oder die geprüfte Behörde hinaus Handlungsbedarf besteht, ist es Aufgabe der jeweiligen obersten Landesbehörde, dafür Sorge zu tragen, daß die notwendigen Änderungen in der Verwaltungspraxis vorgenommen werden.

Das NDSG hat bis zur Neufassung von 1993 die Verantwortlichkeit der obersten Landesbehörden besonders herausgestellt. Nach § 16 Satz 1 der damaligen Gesetzesfassung hatten diese - soweit der Bereich der unmittelbaren Landesverwaltung betroffen war - die Beachtung der Rechtsvorschriften über den Datenschutz sicherzustellen. Aus Rechtsvereinfachungsgründen ist diese Bestimmung gestrichen worden. Eine materielle Rechtsänderung ist damit nicht verbunden. Die obersten Landesbehörden sind selbstverständlich auch weiterhin dafür verantwortlich, daß in ihrem Geschäftsbereich datenschutzgerecht verfahren wird. Aus diesem Grunde ist eine Beanstandung wegen Datenschutzverstößen in der Landesverwaltung nach § 23 NDSG nur ihnen gegenüber auszusprechen. Nach meiner Einschätzung haben die Ressorts in einem solchen Fall über die Bereinigung des konkreten Rechtsverstoßes hinaus jeweils zu prüfen, ob weitergehende Maßnahmen zur Sicherstellung des Datenschutzes auch bei anderen Behörden zu treffen sind.

14.1 Inhalt der Personalakte/Abgrenzung zur Sachakte

Ob ein Vorgang, der einen Beschäftigten betrifft, zur Personalakte oder zur Sachakte zu nehmen ist, läßt sich im Einzelfall nicht immer leicht entscheiden. Zur Personalakte gehören die die Bediensteten betreffenden Unterlagen - einschließlich der in Dateien gespeicherten -, die in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis stehen. Dazu zählen vor allem Vorgänge, die den Inhalt des Dienstverhältnisses insgesamt oder einzelne Rechte und Pflichten

bestimmen, die Aufschluß über die Art und Weise der Vorbereitung einer dienstrechtlichen Entscheidung bzw. über die Gründe für eine dienstrechtliche Maßnahme oder deren Unterlassen geben. Im Zweifel ist die Zweckbestimmung entscheidend. Personenbezogene Unterlagen, die zwar die dienstlichen Verhältnisse der Beschäftigten berühren, allerdings vorrangig einem anderen prägenden Zweck dienen, sind zur Sachakte zu nehmen (vgl. dazu Nr. 2 VV zu § 101 NBG).

Bei meinen Prüfungen habe ich erhebliche Unsicherheiten in der Zuordnung festgestellt. So waren z.B. Schreiben über personelle Veränderungen bei Lehrkräften einer Schule, Schriftwechsel zu Problemen der Schulstatistik und der Geschäftsverteilung innerhalb der Schulleitung, Vorgänge über Störungen in der Zusammenarbeit von Lehrkräften, Meldungen über den Verlust von Dienstschlüsseln oder den Aufbruch eines Aktenschrankes sowie Durchschrift einer Bescheinigung für eine Versicherung über die Zugehörigkeit zum öffentlichen Dienst in Personalakten abgeheftet. Alle diese Unterlagen sind zu Sachakten zu nehmen.

Zuordnungsschwierigkeiten bestehen nach meiner Einschätzung besonders in solchen Dienststellen, die nur Personalnebenakten führen, weil sie nicht Beschäftigungsbehörde der Bediensteten sind oder nur einen Teil der personalrechtlichen Befugnisse ausüben. Zwar enthalten die VV zum NBG allgemeine Beispiele für die Aktenzuordnung, die aber naturgemäß auf spezielle Fragen keine Antwort geben können. Die dargestellten Probleme lassen sich befriedigend lösen, wenn die Aufsichtsbehörden ergänzende Hinweise zur ordnungsgemäßen Aktenbearbeitung geben, die auf die jeweiligen Besonderheiten des betreffenden Verwaltungsbereichs abgestellt sind.

14.2 Inhalt der Personal(neben)akte

In Personalakten sowie Personalnebenakten dürfen nur solche Unterlagen aufgenommen werden, die zur rechtmäßigen Aufgabenerfüllung erforderlich sind (Nr. 4.5 der VV zu § 101 NBG). Hiergegen wird nach meinem Eindruck häufig verstoßen.

In vielen geprüften Vorgängen befanden sich im Original oder in Kopie Unterlagen, die die jeweilige Dienststelle zur Aufgabenwahrnehmung nicht benötigte. Besonders ausgeprägt zeigte sich dies bei den Personalnebenakten der Schulaufsichtsämter. Hier fanden sich z.B. Arbeitsunfähigkeitsbescheinigungen, Sachschadensmeldungen, Beschäftigungs- und Dienstzeitenberechnungen, Geburtsurkunden, Dienstreiseanträge sowie Reisekostenrechnungen in den Personalvorgängen. Eine Erklärung, warum diese Vorgänge, die im übrigen ohnehin zu den Personal- bzw. Sachakten der Bezirksregierung genommen werden, auch in den Schulaufsichtsämtern aufbewahrt werden, konnte zumeist nicht gegeben werden. Vielfach hat sich herausgestellt, daß die Aktenführung insoweit auf reinem Zufall beruht. Sofern die Lehrkraft oder die Schule eine Durchschrift oder Kopie der vorgelegten Unterlagen beigefügt hatte, wurde diese jeweils von den Schulaufsichtsämtern zur Personalnebenakte genommen. Fehlte eine

solche Kopie, wurde sie regelmäßig auch von den Dienststellen nicht angefertigt. Irgendwelche Verwaltungsmaßnahmen wurden aufgrund der aufbewahrten Unterlagen nicht getroffen.

14.3 Hinweise in der Personalakte auf andere Bedienstete

Wenn der notwendige innere Zusammenhang mit dem Dienstverhältnis besteht, können auch Ablichtungen, Abschriften etc. aus anderen Akten zur Personalakte eines Beschäftigten genommen werden.

Betreffen die Unterlagen auch andere Bedienstete, dürfen deren personenbezogene Daten jedoch nicht in der Personalakte erscheinen, außer wenn dies zum Verständnis des Sachzusammenhangs unerläßlich ist. Die Aufnahme fremder personenbezogener Daten in die Personalakte ist im Hinblick auf den jeweiligen Bediensteten zur Aufgabenerfüllung nicht erforderlich. Sie verstößt, wenn es sich um Personalaktendaten Dritter handelt, zudem gegen den Vertraulichkeitsgrundsatz, wenn dem Beschäftigten z.B. im Falle einer Akteneinsicht fremde geschützte personenbezogene Daten zugänglich gemacht werden.

Von den geprüften Stellen wurde dies durchweg nicht beachtet. In den Personalakten des Schulbereichs befand sich z.B. eine Vielzahl von "Sammelschreiben" zur Gewährung von Anrechnungsstunden für Lehrkräfte, zu Abordnungen und Versetzungen sowie zur Teilnahme an Fortbildungsmaßnahmen. Schreiben dieser Art werden aus Vereinfachungsgründen von der Schule bis zum Kultusministerium auf allen Verwaltungsebenen gefertigt. Solange durch diese Verwaltungspraxis nicht gegen Datenschutzvorschriften verstoßen wird, ist hiergegen selbstverständlich nichts einzuwenden. Werden derartige Unterlagen aber zur Personalakte genommen, müssen die geschützten personenbezogenen Daten Dritter unleserlich gemacht werden. Denn das Dienstverhältnis eines einzelnen Beschäftigten berührt es selbstverständlich nicht, wenn eine bestimmte Personalmaßnahme auch für andere Bedienstete getroffen wird.

Bei der geprüften Polizeidienststelle ist die geschilderte Verfahrensweise auch im Zusammenhang mit Stellenbesetzungs- und Beförderungsvorschlägen gängige Praxis. Die Vorschläge enthalten neben den detaillierten Personaldaten der Bewerberinnen und Bewerber eine Abwägung der Gesichtspunkte, die jeweils für oder gegen die Eignung sprechen. Ablichtungen der Vorschläge werden zur Personalnebenakte eines jeden Bewerbers genommen, so daß dieser im Falle der Akteneinsicht sich jeweils auch Kenntnis von der Leistungsfähigkeit seiner Mitbewerberinnen und Mitbewerber verschaffen kann.

14.4 Kriminalpolizeiliche Erkenntnisse in einer Personalnebenakte

Die unzulässige Aufbewahrung von Hinweisen auf andere Bedienstete lieferte in einem Fall zugleich Hinweise auf einen in der Vergangenheit

liegenden Datenschutzverstoß. In einer Personalnebenakte der Polizeidienststelle fand sich ein Bericht der früher zuständigen Stelle, in der die personalaktenführende Bezirksregierung gebeten wurde, aus der Personalakte des Bediensteten ein Schreiben zu vernichten. Dieses enthielt eine Stellungnahme über eine beabsichtigte Stellenbesetzung. In dem Schreiben wurden kriminalpolizeiliche Erkenntnisse über einen Dritten mitgeteilt, der sich u.a. mit dem Bediensteten um eine andere Stelle beworben hatte. Nachdem die kriminalpolizeilichen Erkenntnisse in der Kriminalakte gelöscht worden waren, bat man die Bezirksregierung, nun auch aus der Personalakte des Bediensteten die Angaben über den Dritten zu entfernen. Dem kam die Bezirksregierung laut Akteninhalt nach.

Eine abschließende Klärung des Sachverhalts war nicht möglich, da die geprüfte Polizeidienststelle die Personalnebenakten von der früher zuständigen Stelle übernommen hatte und deshalb keine Angaben zum Sachverhalt machen konnte.

Die Angaben im Bericht an die Bezirksregierung lassen - über die Aufbewahrung in der Personalakte sowie Nebenakte des Bediensteten hinaus - auf einen Rechtsverstoß schließen. Kriminalpolizeiliche Erkenntnisse aus laufenden oder abgeschlossenen Ermittlungsverfahren gegen einen Stellenbewerber dürfen nur mit dessen Zustimmung in Bewerbungsverfahren verwendet werden, es sei denn, gegen den Beamten ist wegen der strafrechtlichen Vorwürfe bereits ein Disziplinarverfahren eingeleitet worden. Eine Polizeidienststelle darf eine Personalauswahlentscheidung dagegen nicht zum Anlaß nehmen, um sich etwaige kriminalpolizeiliche Erkenntnisse über einen der Bewerber zu beschaffen. Da Kriminalakten nicht zum Zweck einer Stellenauswahl geführt werden, wäre eine Weitergabe von Daten aus diesen Akten ein Verstoß gegen den das gesamte Datenschutzrecht beherrschenden Zweckbindungsgrundsatz. Das NGefAG läßt eine solche Verfahrensweise nicht zu.

Daß die Aufnahme von polizeilichen Ermittlungsunterlagen über Dritte in die Personalakten von Bediensteten offenbar kein Einzelfall darstellt, zeigt das Verhalten einer anderen Polizeidienststelle. Bei dieser wurden im Zuge einer Geschäftsprüfung durch die Aufsichtsbehörde festgestellt, daß derartige Unterlagen (z.B. über beschuldigte Familienangehörige, Geschädigte, Zeugen) in eine Vielzahl von Personalakten aufgenommen wurden. Das Niedersächsische Innenministerium prüft zur Zeit die Ahndung dieser Fälle unter disziplinar- und ordnungswidrigkeitsrechtlichen Gesichtspunkten.

14.5 Beschwerden und ungünstige Bewertungen in der Personalakte

Auch gegen die Pflicht zur Anhörung des Beamten, bevor Beschwerden oder Behauptungen tatsächlicher Art, die für ihn ungünstig sind oder ihm nachteilig werden können, in die Personalakte aufgenommen werden (§ 101 Abs. 2 NBG), ist häufig verstoßen worden.

So hätte ein Bediensteter, über den ein Vorgesetzter schriftlich festhielt: "Ich halte den Beamten für einen typischen Drückeberger, der die günstigen Versorgungsregelungen schamlos ausnutzt", vor Aufnahme des Schriftstücks in die Personalakte angehört werden müssen. Denn die Anhörungspflicht gilt auch für ungünstige Bewertungen (vgl. § 56 b BRRG, Nr. 2.1 Buchst. k der VV zu § 101 NBG). Ebenso durfte bei einem Lehrer, der von seiner Beschäftigungsbehörde als Querulant angesehen wird, nicht etwa angesichts der Vielzahl der gegen ihn erhobenen Beschwerden von einer Anhörung abgesehen werden.

In beiden Fällen betonten die Behörden, die Bediensteten hätten durch spätere Akteneinsicht ohnehin Kenntnis von den zur Personalakte genommenen Unterlagen erlangt. Sie hätten damit - wenn auch nur nachträglich - zu den Vorgängen Stellung nehmen können.

Zwar ist es nach der Rechtsprechung in derartigen Fällen entbehrlich, die Anhörung nachzuholen. Die personalaktenführende Stelle darf sich jedoch nicht darauf verlassen, daß ein Bediensteter von ungünstigen Informationen ggf. schon durch eine spätere Akteneinsicht Kenntnis erlangen werde. Sie ist vielmehr in jedem Falle gehalten, die Anhörung vor Aufnahme der entsprechenden Unterlagen in die Personalakte durchzuführen. Außerdem muß nachweisbar sein, daß dem Bediensteten die Beschwerden, Behauptungen oder Bewertungen bekanntgegeben worden sind, damit er die Möglichkeit der Stellungnahme hat.

Ein Hinweis auf eine Akteneinsicht ergibt sich im übrigen aus der Personalakte nicht. Nr. 7.7 der VV zu § 101 NBG bestimmt, daß nach erfolgter Einsichtnahme schriftliche Anträge auf Akteneinsicht zu vernichten sind und Aktenvermerke über die Einsicht zu unterbleiben haben. Damit ist im nachhinein nicht feststellbar, ob eine Einsichtnahme erfolgt ist. Wegen des insoweit fehlenden Nachweises kann somit regelmäßig eine "Heilung" des Verstoßes gegen die Anhörungspflicht durch eine spätere Akteneinsicht nicht in Betracht kommen. Wenn diese Rechtsfolge als problematisch angesehen wird, müßte die genannte Verwaltungsvorschrift geändert werden.

14.6 Unbegründete Dienstaufsichtsbeschwerden

Nur Vorgänge über zutreffende Beschwerden, nachteilige Behauptungen und Bewertungen dürfen in die Personalakte aufgenommen werden. Stellt sich erst nach der Aufnahme in die Akte heraus, daß eine Beschwerde unbegründet oder eine Behauptung falsch war, sind die Vorgänge nach § 101 Abs. 3 NBG auf Antrag des betroffenen Bediensteten zu vernichten. Unbegründete Vorwürfe sollen sich nicht zu seinem Nachteil auswirken können.

Erweist sich eine Beschwerde jedoch schon nach erster Prüfung als unbegründet, wird sie in der Praxis zwar nicht zur Personalakte der Mitarbeiterin oder des Mitarbeiters, statt dessen aber zur Sachakte genommen. So führt z.B. die von mir geprüfte Bezirksregierung eine Akte "Dienstaufsichtsbeschwerden". Damit ist es ohne weiteres möglich,

z.B. bei anstehenden Personalauswahlentscheidungen auf die unbegründeten Beschwerden zurückzugreifen und sie in die Entscheidungsfindung nach dem Motto "Wir konnten dem Bediensteten zwar nichts beweisen, aber irgend etwas wird an den Vorwürfen schon dran gewesen sein" einfließen zu lassen.

Ich habe deshalb gegen die Aufbewahrung solcher unbegründeter Beschwerden in Sachakten Bedenken erhoben. Das für das Beamtenrecht federführende Innenministerium teilt diese nicht. Es ist der Auffassung, die Aufbewahrung sei aus Gründen einer sachgerechten Dokumentation notwendig. Es müsse möglich sein, bei wiederholten Dienstaufsichtsbeschwerden organisatorische oder personalwirtschaftliche Konsequenzen zu ziehen, um fehlerhaftes Verhalten oder Verfahrensmängel abzustellen. Die Aufbewahrung könne auch für eine spätere Bearbeitung (z.B. bei Landtagsanfragen, Petitionen, weiteren Dienstaufsichtsbeschwerden) von Bedeutung sein. Im übrigen ergebe sich ja aus dem Entwurf des Schreibens an den Beschwerdeführer, daß die Beschwerde unbegründet sei.

Aus Sicht des Datenschutzes sind diese Aussagen unbefriedigend. Ich sehe keinen sachlichen Grund dafür, Dienstaufsichtsbeschwerden, deren Unbegründetheit sich schon bei einer ersten Prüfung ergibt, anders zu behandeln als solche, bei denen sich diese erst nach Aufnahme in die Personalakte herausstellt. Ich bezweifele auch die Erforderlichkeit der Speicherung. Dem Gesichtspunkt, daß sich ein Beschwerdeführer mit der Zurückweisung seines Vorbringens möglicherweise nicht zufrieden gibt und hiergegen wiederum Beschwerde einlegt oder sich in einer Petition an den Landtag wendet, ist selbstverständlich Rechnung zu tragen. Solange dies bei realistischer Einschätzung noch in Betracht gezogen werden muß, ist die Bearbeitung aus datenschutzrechtlicher Sicht noch nicht vollständig abgeschlossen. Erst wenn dies der Fall ist, ist eine weitere Aufbewahrung nicht mehr notwendig. Die bloße Möglichkeit, daß in der Folgezeit noch andere Dienstaufsichtsbeschwerden gegen den betroffenen Mitarbeiter erhoben werden könnten, kann dagegen aus Sicht des Datenschutzes keine darüber hinausgehende Aufbewahrung rechtfertigen. Dies würde zu einer Datenspeicherung auf Vorrat führen.

Die Ansicht des Innenministeriums führt schließlich dazu, daß eine unbegründete Beschwerde nach § 18 der Niedersächsischen Aktenordnung in der Regel erst nach fünf Jahren auszusondern ist. Bei einer begründeten Beschwerde, die zur Personalakte genommen wird, hätte dagegen nach § 56e Abs. 1 Nr. 1 BRRG eine Tilgung nach drei Jahren zu erfolgen. Bedienstete, gegen die unbegründete Vorwürfe erhoben werden, sind demnach schlechter gestellt, als dies bei einer begründeten Beschwerde der Fall wäre. Das Innenministerium will deshalb bei einer Neufassung der Aktenordnung die in Rede stehenden Aufbewahrungsfristen erheblich reduzieren. Ein Zeitpunkt für diese Änderung ist allerdings nicht absehbar.

14.7 Übermittlung von Personaldaten an dritte Stellen

14.7.1 Mitteilungen an die Presse

Mehrfach habe ich mich mit der unerlaubten Weitergabe von Personaldaten an die Presse beschäftigen müssen. Hierzu folgender Fall: Ein Informationsdienst aus Hannover nimmt sich besonders liebevoll aller Spekulationen um Personalveränderungen - vor allem in den obersten Landesbehörden - an. Unentwegt ist dort zu lesen, wer für eine Stelle in Betracht kommt, wer das Vertrauen seiner Ministerin oder seines Ministers genießt oder gerade wieder verloren hat, wer sich für eine Stelle beworben hat und wen man möglichst bald in den Ruhestand schicken möchte.

Neben dem Unterhaltungs- und Informationswert haben diese Veröffentlichungen allerdings auch eine datenschutzrechtliche Seite. Sie sind nur möglich durch Rechtsverstöße von Beschäftigten, die ihre dienstlichen Kenntnisse mißbrauchen. Die Weitergabe solcher Daten - etwa der Angabe, ein namentlich genannter Bediensteter habe sich für eine bestimmte Stelle beworben - an Presseorgane ist datenschutzrechtlich eine Übermittlung von Beschäftigtendaten an Personen oder Stellen außerhalb des öffentlichen Bereichs. Sie ist nach § 24 Abs. 1 Satz 3 NDSG nur zulässig, wenn die Empfänger ein rechtliches Interesse an diesen Daten haben, d.h. sie zur Verfolgung oder Abwehr von Rechtsansprüchen benötigen oder wenn der Dienstverkehr es erfordert. Beides ist nicht der Fall.

Die Aufklärung solcher Verstöße gelingt leider nur selten. Das Innenministerium, aus dem die Namen von Bewerberinnen und Bewerbern um einen herausgehobenen Dienstposten auf die beschriebene Weise an die Öffentlichkeit gelangt waren, hat auf meine Veranlassung entsprechende Verwaltungsermittlungen angestellt. Obwohl der in Betracht kommende Personenkreis sehr klein war, konnte nicht herausgefunden werden, von wem die Informationen stammten. Trotz der vom Minister ausgesprochenen eindeutigen Mißbilligung solcher "Öffentlichkeitsarbeit" hat sich diese im übrigen in der Folgezeit fortgesetzt.

Alle Bediensteten, die sich in dieser Weise verhalten, müssen wissen, daß sie damit nicht nur gegen ihre dienstrechtliche Verschwiegenheitspflicht, sondern auch gegen Datenschutzbestimmungen verstoßen. Sie verletzen das Datengeheimnis (§ 5 NDSG) und begehen damit eine Ordnungswidrigkeit (§ 29 NDSG) oder gar eine Straftat (§ 28 NDSG). Dies gilt z.B. auch für Mitglieder kommunaler Vertretungskörperschaften, die Personaldaten an die Öffentlichkeit bringen.

14.7.2 Argloser Austausch zwischen öffentlichen Stellen

Während man bei der geschilderten Datenweitergabe an die Presse ein Unrechtsbewußtsein der Informanten unterstellen darf, fehlt dieses häufig, wenn Beschäftigtendaten an eine Behörde oder eine andere öffentliche Stelle übermittelt werden. So gab ein Gemeindedirektor dem

Wahlprüfungsausschuß des Deutschen Bundestages auf den Wahleinspruch eines Bürgers hin nicht nur die erbetenen Sachinformationen, sondern teilte arglos - damit sich der Ausschuß ein zutreffendes Bild über den Beschwerdeführer machen konnte - auch gleich noch mit, daß dieser früher eine Ausbildung bei der Gemeinde begonnen, die Laufbahnprüfung aber trotz Wiederholung nicht bestanden hatte. Die Kommune berief sich vor allem darauf, daß diese Tatsachen unter den Gemeindebediensteten bekanntgewesen seien, man habe sie deshalb auch nicht der Personalakte entnommen. Hierauf kommt es jedoch nicht an. Das NDSG schützt nicht nur Personalaktendaten, sondern auch solche, die sich in Sachakten befinden. Ebenso wie Personaktendaten dürfen auch sie nach § 24 Abs. 1 Satz 1 NDSG nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen erforderlich ist.

14.7.3 Personalnachrichten

An der Erforderlichkeit scheitert auch die Veröffentlichung von Personalnachrichten (z.B. über Einstellungen, Ernennungen, Beförderungen, Versetzungen und Ausscheiden von Bediensteten) im Ministerialblatt, Amtsblättern u.ä. Publikationsorganen der öffentlichen Verwaltung. Da diese regelmäßig jedermann zugänglich sind, handelt es sich datenschutzrechtlich um eine Datenübermittlung an Personen und Stellen außerhalb des öffentlichen Bereichs (§ 24 Abs. 1 Satz 3 NDSG). Auch unter Berücksichtigung des Gesichtspunktes, daß solche Veröffentlichungen zur Transparenz der Verwaltung beitragen mögen, läßt sich nicht davon ausgehen, daß der Dienstverkehr sie unabdingbar erfordert. Mit dem Dienstverkehr ist grundsätzlich die Situation angesprochen, daß die Verwaltung mit dem Bürger oder Geschäftspartner in Kontakt tritt und die Ansprechbarkeit im konkreten Fall herstellt. Das datenschutzrechtliche Erforderlichkeitsprinzip verlangt dabei eine differenzierte Betrachtung nach den jeweiligen Adressaten- und Betroffenenkreisen. Derartige Veröffentlichungen können deshalb nur mit einer Einwilligung der Betroffenen, die § 4 NDSG entspricht, in Betracht kommen.

Aus den dargestellten Gründen hat das Niedersächsische Justizministerium die bisherige Veröffentlichung von Personalnachrichten in der "Niedersächsischen Rechtspflege" eingestellt.

14.7.4 Nur mit vollständiger Personalakte in den Ruhestand?

Um die Beachtung des Erforderlichkeitsprinzips geht es auch in folgendem Fall: Die Landesregierung hat beschlossen, die Versetzung von Beamtinnen und Beamten in den Ruhestand wegen Dienstunfähigkeit vor Vollendung des 58. Lebensjahres von der vorherigen Zustimmung des Niedersächsischen Finanzministeriums abhängig zu machen. Das Fachressort hat deshalb in seinem Runderlaß vom 24. Juni 1996 (Nds. MBl. S. 1090) bestimmt, daß ihm zur entsprechenden Prüfung die "vollständigen Personalakten" der

Bediensteten vorzulegen sind. Zur Personalakte gehören neben der nicht selten mehrbändigen Grundakte auch Teilakten, z.B. über Besoldung, Urlaub, Nebentätigkeit usw. Bei guter Aktenführung kann neben der Grundakte eine Vielzahl von Teilakten angelegt werden.

Selbstverständlich benötigt das Finanzressort zur Prüfung der ihm übertragenen Aufgabe die notwendigen Personaldaten. Eine Vorlage der "vollständigen" Personalvorgänge ist hierfür jedoch keineswegs erforderlich. In Übereinstimmung mit § 24 Abs. 1 Satz 1 NDSG betonen die VV zu § 101 NBG an mehreren Stellen (z.B. Nrn. 8.2.1, 8.2.2), daß die Personalakte anderen Stellen für deren Aufgabenwahrnehmung nur "im erforderlichen Umfang" zur Verfügung zu stellen ist.

Ich habe das Finanzministerium gebeten, dies nachträglich klarzustellen, um Datenschutzverstößen vorzubeugen. Dieses weigert sich jedoch und beruft sich darauf, daß in den VV zu § 101 NBG gerade dieser Fall - den es zum Zeitpunkt des Inkrafttretens der Bestimmungen noch nicht gab - nicht angesprochen werde. Man brauche zur Prüfung, ob die beabsichtigte Versetzung in den Ruhestand sachgerecht sei, eine ganze Reihe von Informationen, die von Fall zu Fall unterschiedlich sein könnten. Es liege keinesfalls auf der Hand, daß bestimmte Vorgänge von Anfang an für die Meinungsbildung ohne Belang wären und deshalb auszuscheiden seien.

Daß diese Einschätzung nicht zutrifft, braucht hier - da offenkundig - nicht weiter begründet zu werden. In einer weiteren Stellungnahme hat das Ressort betont, bei der Prüfung der Zuruhesetzungsanträge werde man nur in die Teile der Personalakte Einsicht nehmen, die für die Entscheidungsfindung notwendig seien.

Auch diese Argumentation kann nur Kopfschütteln hervorrufen. Dem Finanzministerium habe ich schon mehrfach im Zusammenhang mit der Verarbeitung von Beschäftigtendaten das Erforderlichkeitsprinzip erläutert. Unkenntnis kann den zitierten Stellungnahmen somit nicht zugrunde liegen. In ihnen zeigt sich vielmehr zum wiederholten Male das beharrliche Bemühen dieses Ressorts, im Personalbereich datenschutzrechtliche Grundsätze und Rechtsvorschriften möglichst nicht für sich gelten zu lassen. Erst nach zeitraubendem Schriftwechsel, zum Teil unter Einschaltung des Niedersächsischen Innenministeriums, hat sich das Finanzministerium jeweils im Einzelfall dazu bequemt, das geltende Recht zu akzeptieren. Es wäre nicht nur ein Gewinn für den Datenschutz, sondern auch ein Beitrag zum Abbau überflüssiger Verwaltungsarbeit und damit zur Kostenersparnis, wenn diese Haltung sich künftig ändern würde.

14.8 Akteneinsicht in Sachakten

In mehreren an mich herangetragenen Fällen wurde Bediensteten eine begehrte Akteneinsicht nur in die Personalakte gewährt, in Sachakten dagegen verweigert. Eine von mir geprüfte Behörde machte mich hierzu auf einen Gerichtsbescheid des Verwaltungsgerichts Hannover vom 3. August 1990 (Az. 2 HiA 30/89) aufmerksam. In dieser Entscheidung

hat das Verwaltungsgericht einen Rechtsanspruch eines Lehrers auf Einsicht in eine bei der Bezirksregierung geführte Schulakte seiner Schule verneint. Zur Begründung hat das Gericht ausgeführt, daß eine Akteneinsicht außerhalb eines laufenden Verwaltungsverfahrens nur nach pflichtgemäßem Ermessen gewährt werde. Eine fehlerfreie Ermessensentscheidung setze zunächst ein berechtigtes Interesse an der Einsichtnahme voraus. Dies hat das Gericht im konkreten Falle verneint.

Diese Entscheidung ist überholt. Die Rechtslage hat sich inzwischen geändert. Nach § 56c Abs. 4 BRRG hat der Beamte ein Recht auf Akteneinsicht auch in Sachakten, die personenbezogene Daten über ihn enthalten. Niedersachsen hat diese Regelung zwar noch nicht in das NBG aufgenommen. Bis zur Umsetzung in das niedersächsische Dienstrecht ergibt sich der Anspruch jedoch aus § 16 NDSG. Hiernach hat jeder Betroffene nach seiner Wahl ein Recht auf Einsicht in die zu seiner Person gespeicherten Daten oder entsprechende Auskunft. Die Vorschrift gilt für jede Person, deren Daten sich in Sachakten befinden, im Schulbereich u.a. für Lehrkräfte, Schüler, Eltern.

14.9 Aufbewahrung von Bewerbungsunterlagen

Nach § 24 Abs. 3 NDSG sind personenbezogene Daten, die zur Aufzeichnung eines Bewerbungsvorganges nicht erforderlich sind, unverzüglich zu löschen, sobald feststeht, daß ein Dienst- oder Arbeitsverhältnis nicht zustande kommt, es sei denn, daß die Betroffenen in die weitere Speicherung eingewilligt haben. Vorgänge über die Auswahl bei der Besetzung von Dienstposten sind - im erforderlichen Umfang - gemäß Nr. 2.2 Buchst. f der VV zu § 101 NBG zu den Sachakten zu nehmen; enthält ein solcher Vorgang eine selbständige Beurteilung des Bediensteten, ist diese im Wortlaut in der Personalakte zu vermerken. Die Löschung von Bewerbungsunterlagen ist - soweit es sich nicht um die Aufzeichnung des Bewerbungsvorganges selbst handelt - nur vorzunehmen, wenn ein Dienst- oder Arbeitsverhältnis nicht zustande kommt. Der Gesetzeswortlaut könnte darauf hindeuten, daß Bewerbungsunterlagen von Bewerbern, die bereits im niedersächsischen Landesdienst stehen, in einer Sachakte aufbewahrt werden dürfen. So wird in der Praxis auch verfahren.

Diese Verfahrensweise ist zu ändern. Bei abschlägig beschiedenen Bewerberinnen und Bewerbern dürfen z.B. nicht neben dem Bewerbungsschreiben weitere Bewerbungsunterlagen, wie Lebenslauf, Zeugnisse, zusätzliche Belege über Aus- und Fortbildungsmaßnahmen, in einer Sachakte aufbewahrt werden, die nicht den strikten Zugriffsbeschränkungen einer Personalakte unterliegt (vgl. § 56 BRRG, Nrn. 6.1, 6.2 und 8.1 der VV zu § 101 NBG). Dies ist zur Aufgabenerfüllung nicht erforderlich. Ausreichend ist vielmehr eine Dokumentation des ordnungsgemäßen Auswahlverfahrens. Lebensläufe und Materialien, die einer Bewerbung als weitere Unterlagen beigefügt wurden, sind deshalb nach § 17 Abs. 2 NDSG zu löschen, d.h. den Bewerberinnen und Bewerbern zurückzugeben oder zu vernichten. Das Niedersächsische Innenministerium teilt diese Auffassung.

14.10 Heftung, Paginierung von Personalakten

Die zur Personalakte gehörenden Schriftstücke sind gemäß Nr. 4.8 der VV zu § 101 NBG in zeitlicher Reihenfolge zu ordnen und fortlaufend und dauerhaft zu numerieren. Dies bezieht sich auch auf Nebenakten. Die Regelung soll u.a. sicherstellen, daß im Falle einer Akteneinsicht die vollständige Akte vorgelegt wird und Veränderungen des Akteninhalts durch nicht gekennzeichnete Herausnahme einzelner Aktenbestandteile unterbleiben.

Auch dies wird nach meinem Eindruck weitgehend nicht beachtet. In keiner der kontrollierten Stellen wurde in der vorgeschriebenen Weise verfahren. In der geprüften Polizeidienststelle bestehen die Personalnebenakten z.T. lediglich aus einer Hängetasche, in die die Schriftstücke lose eingelegt werden. Eine Heftung oder Paginierung erfolgt nicht. Auch die anderen geprüften Stellen paginieren ihre Personalvorgänge nicht. Die Bezirksregierung numeriert Personalakten nur dann, wenn sie von dritter Stelle - etwa Verwaltungsgerichten - im Einzelfall angefordert werden.

14.11 Abschottung von Personalakten

Im Hinblick auf den Akteninhalt ist die Geheimhaltungsbedürftigkeit von Personal- und Personalnebenakten von besonderer Bedeutung. In Übereinstimmung mit dem Beamtenrechtsrahmengesetz (§ 56 Abs. 3) bestimmen deshalb die Nrn. 6.1, 6.2 und 8.1 der VV zu § 101 NBG, daß Personalakten der Bediensteten vertraulich zu behandeln und so aufzubewahren sind, daß keine Unbefugten Einblick erlangen können. Zugang zu diesen Akten dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur, soweit dies zu Zwecken der Personalverwaltung und -wirtschaft erforderlich ist.

Meine Prüfungen und die Bearbeitung von Einzelfällen haben gezeigt, daß mit diesem Abschottungsgebot oft recht lax umgegangen wird. Die größten Defizite ergaben sich bei den (kleineren) Dienststellen, die nicht die Personalakten selbst, sondern nur Nebenakten führen. So fanden sich in den Räumen der Personalsachbearbeiter etwa Personalvorgänge in offenen Schrankregalen, in altersschwachen, mit einfachsten Bartschlössern versehenen Schränken, die sich nicht mehr abschließen ließen, oder in nicht abgeschlossenen Flurschränken. In einer Dienststelle, die in einem von mehreren Parteien genutzten Gebäude untergebracht war, wurden die Diensträume bis zum Eintreffen der Reinigungskraft offengelassen. Jeder Besucher hätte sich hier mit den Personalakten vergnügen können. Eine andere Dienststelle hatte in einem Aktenraum Fax-und Kopiergerät untergebracht, so daß Personalratsmitglieder und die Schwerbehindertenvertretung, die diese Geräte ebenfalls benutzten, zugleich auf die Personalvorgänge hätten zugreifen können. Ein Schulaufsichtsamt lagerte seine Altakten - die zum Teil längst ausgeschiedene und verstorbene Lehrkräfte betrafen - zusammen mit den Akten eines benachbarten Schulaufsichtsamts. Bei

meiner Kontrolle waren Bauarbeiter gerade dabei, eine Kellerwand neu zu errichten. Die Personalvorgänge lagen offen zu ihrer Verfügung.

Das Abschottungsgebot erfordert die Unterbringung von Personalakten in mit Sicherheitsschlössern ausgestatteten stabilen Schränken, zu denen nur die jeweils mit der Bearbeitung beauftragten Bediensteten Zugang haben. Bei deren Abwesenheit müssen die Schränke verschlossen werden. Die Schlüssel sind von den verantwortlichen Sachbearbeiterinnen und Sachbearbeitern ebenfalls sicher und verschlossen aufzubewahren. Um den behördeninternen Aktentransport datenschutzgerecht abzuwickeln, schreibt Nr. 6.5 der VV zu § 101 NBG vor, daß Personalvorgänge auch innerhalb der Behörde nur verschlossen versandt werden.

Meine Hinweise auf eine datenschutzgerechte Verfahrensweise stießen nicht immer auf Verständnis. So verwies eine Frauenbeauftragte einer Mittelbehörde nachdrücklich darauf, daß es in ihrer Abteilung allgemein nicht üblich sei, Schränke bzw. Schreibtische oder gar Zimmertüren beim Verlassen des Dienstzimmers zu verschließen.

14.12 Probleme bei Organisationsuntersuchungen und Mitarbeiterbefragungen

Im Zuge der Überlegungen zur Verschlankung der Verwaltung werden in verstärktem Maße Mitarbeiterbefragungen durchgeführt. Aus meiner Sicht ist es notwendig, zwischen Befragungen im Rahmen von Organisationsuntersuchungen und sonstigen Mitarbeiterbefragungen zu unterscheiden. Eine Organisationsuntersuchung zielt auf die Prüfung ab, ob Aufgaben der öffentlichen Verwaltung mit geringerem Personal- oder Sachaufwand oder auf andere Weise wirksamer erfüllt werden können. Diese Prüfung ist eine Daueraufgabe, die sich aus dem Gebot sparsamer Mittelverwendung und effektiver Aufgabenwahrnehmung ergibt. Durch Mitarbeiterbefragungen sollen dagegen allgemein Auffassungen und Wertungen, also Meinungen von Bediensteten ermittelt werden (z.B. über die Außendarstellung der Behörde, das Betriebsklima, die Arbeitsmotivation). Auskünfte über Einstellungen, Erwartungen, das Maß der Arbeitszufriedenheit, die Bewertung eingefahrener Verhaltensweisen etc. sollen Schwachstellen u.a. in Organisation und Führungsverhalten einer Behörde deutlich machen.

Nach § 24 Abs. 1 Satz 1 NDSG dürfen Beschäftigtendaten auch zur Durchführung organisatorischer Maßnahmen verarbeitet werden. Zudem bestimmt § 10 Abs. 3 NDSG, daß die Verwendung solcher Daten keine Änderung des mit der Datenerhebung ursprünglich verfolgten Verwaltungszwecks darstellt. Die Datenverarbeitung im Rahmen von Organisationsuntersuchungen ist somit nicht als eigene Aufgabe, sondern als Bestandteil der jeweilige Fachaufgabe anzusehen. Die Bediensteten können sich Fragen im Rahmen einer Organisationsprüfung grundsätzlich nicht entziehen, sie sind zur Mitwirkung bei der Überprüfung der Wirtschaftlichkeit und Organisation der Verwaltung verpflichtet. Dies gilt auch für Fragen nach ihrer persönlichen Einschätzung, sofern sich diese auf ihre dienstlichen

Verrichtungen, die Arbeitsabläufe oder ihr konkretes Arbeitsumfeld beziehen.

Die Personalvertretung hat nach § 66 Nr. 13 Nds. PersVG bezüglich des Inhalts von Fragebogen zur Organisationsuntersuchung kein Mitbestimmungsrecht. Enthält ein solcher Fragebogen jedoch nicht nur Fragen, die auf Inhalt, Umfang und Bedeutung des konkreten Arbeitsbereichs ohne Rücksicht auf den jeweiligen Bediensteten ausgerichtet sind, sondern werden zusätzlich Fragen gestellt, die zumindest objektiv geeignet sind, Rückschlüsse auf Leistung und Eignung des Beschäftigten zuzulassen, so unterliegen diese der Mitbestimmung, wie sie für Personalfragebogen vorgesehen ist (§ 66 Nr. 13 Nds. PersVG).

Personalfragebogen sind Erhebungsbogen, die zwar in erster Linie Fragen nach der Person, den persönlichen Verhältnissen, dem beruflichen Werdegang, fachlichen Kenntnissen sowie sonstigen Fähigkeiten von Bewerbern oder Bediensteten enthalten. Sie können als Grundlage für die Beurteilung der Eignung oder Befähigung herangezogen werden. Von der Rechtsprechung des Bundesverwaltungsgerichts (z.B. BVerwG, Die Personalvertretung 1990, 170) werden aber überdies Fragen, die sich zwar auch auf die sachlichen Anforderungen des Arbeitsplatzes beziehen, aus denen aber zugleich Rückschlüsse auf die persönliche Ausbildung, die Arbeitsbereitschaft und die Belastbarkeit sowie die Fähigkeit zu rationeller Arbeitseinteilung gewonnen werden können, als Inhalt eines Personalfragebogens betrachtet. Dies ist z.B. bei Fragen nach einer Verbesserung von Arbeitsabläufen und Arbeitsbedingungen oder nach der Möglichkeit einer Übertragung von Tätigkeiten auf andere Dienstkräfte anzunehmen. Hinter dieser Bewertung steht der Gesichtspunkt, daß dem Personalrat die Möglichkeit gegeben werden soll, darüber zu wachen, ob Bedienstete - wenn auch nur mittelbar - zu einer sie belastenden Selbstbeurteilung veranlaßt werden sollen.

Das Landesarbeitsgericht Frankfurt hat in einer Entscheidung vom 26. Januar 1989 (CR 1990, 274) für einen Fall, in dem der verwendete Fragebogen außer den rein organisationsbezogenen Fragen auch solche enthielt, die Rückschlüsse auf die Leistungsfähigkeit der Bediensteten zuließen, entschieden, daß keine Trennung des Fragebogens in einen mitbestimmungspflichtigen und einen nicht der Mitbestimmung unterliegenden Teil erfolgen dürfe, dieser vielmehr als Einheit zu sehen sei und damit insgesamt der Mitbestimmungspflicht unterliege. Hat der Personalrat der Verwendung eines derartigen Fragebogens nicht zugestimmt, entfällt nach dieser Rechtsprechung für die Bediensteten die Pflicht zur Beantwortung.

Mitarbeiterbefragungen, die darauf abzielen, Meinungen der Bediensteten in Erfahrung zu bringen, werden im Nds. PersVG nicht angesprochen. Für sie ist eine Mitbestimmung des Personalrats bewußt nicht vorgesehen. Die Teilnahme an einer solchen Befragung ist freiwillig. Sie kann nicht etwa mit der Unterstützungspflicht der Bediensteten (vgl. § 63 Satz 2 NBG) begründet werden. Auf die Freiwilligkeit muß ausdrücklich hingewiesen werden. Die Bediensteten

sind über den Verwendungszweck der erhobenen Daten sowie die Art und Dauer der Speicherung aufzuklären. Diese dürfen - ebenso wie bei einer Organisationsuntersuchung - nicht für andere Verwaltungszwecke verwendet werden und damit auch nicht in Personalentscheidungen einfließen. Werden Dritte, z.B. Beratungsunternehmen, eingeschaltet, müssen umfassende Vereinbarungen über die Datenverarbeitung, die zu treffenden Datensicherungsmaßnahmen und die Vernichtung der Datenträger durch den Auftragnehmer getroffen werden.

Vertrauensbildung bei den Bediensteten ist für die erfolgreiche Durchführung sowohl einer Organisations- wie einer sonstigen Mitarbeiterbefragung wesentlich. Daß ihr neben dem Akzeptanzgesichtspunkt auch rechtliche Bedeutung zukommen kann, zeigt folgender Fall:

Der Landesrechnungshof (LRH) nahm eine Organisations- und Wirtschaftlichkeitsprüfung in der Straßenbauverwaltung vor. In den verteilten Fragebogen wurde den Bediensteten mehrfach eine vertrauliche Behandlung ihrer Angaben zugesichert und auf die Freiwilligkeit bei der Beantwortung bestimmter Fragen hingewiesen. Die ausgefüllten Erhebungsbogen konnten in verschlossenem Briefumschlag bei der Dienststelle abgegeben werden. Nach der Auswertung leitete der LRH jedoch solche Erhebungsbogen, die unvollständig ausgefüllt waren, den betroffenen Bediensteten offen über deren jeweiligen Amtsleiter mit der Bitte um Ergänzung zu. Dazu bemerkte er, die zugesagte vertrauliche Behandlung müsse aus Kostengründen leider eingeschränkt werden.

Ein Mitarbeiter der betroffenen Verwaltung hat diese Vorgehensweise zu Recht kritisiert. Es muß davon ausgegangen werden, daß teilweise gerade im Hinblick auf die gegebenen Zusicherungen Stellungnahmen abgegeben worden sind, die bei fehlender Vertraulichkeit unterblieben wären. Zwar unterliegt der LRH nicht meiner datenschutzrechtlichen Kontrolle, im Hinblick auf meine Beratungsfunktion habe ich ihm aber diese Bewertung seines Verfahrens mitgeteilt.

14.13 Trennung von Beihilfe- und Personalsachbearbeitung

Vor allem von kommunalen Bediensteten erreichen mich immer wieder Anfragen, in denen die Befürchtung geäußert wird, Informationen aus Beihilfevorgängen könnten auch bei Personalentscheidungen eine Rolle spielen.

Der Schutz des Persönlichkeitsrechts der Beschäftigten erfordert eine organisatorische und personelle Trennung von Beihilfe- und Personalbearbeitung. Beihilfevorgänge sollen deshalb nach § 56a BRRG in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden. Zugang dürfen nur die mit der Bearbeitung der Vorgänge betrauten Bediensteten haben (Nr. 8.1 der VV zu § 101 NBG). Zweck dieses Abschottungsgebots ist, daß die besonders sensiblen Beihilfedaten nicht für Personalzwecke - insbesondere Personalentscheidungen - herangezogen werden.

Die öffentlichen Stellen haben alles zu unternehmen, um die gesetzlich geforderte organisatorische Trennung zwischen Beihilfe- und Personalbearbeitung durchzuführen. Dabei kommt für die Kommunen auch die Möglichkeit in Betracht, die Bearbeitung ihrer Beihilfeangelegenheiten den niedersächsischen Versorgungskassen zu übertragen. Insbesondere Gemeinden, bei deren Größenordnung eine Mitarbeiterin oder ein Mitarbeiter mit der ausschließlichen Bearbeitung von Beihilfesachen nicht ausgelastet wäre, sollten unter Datenschutzgesichtspunkten eine Übertragung dieser Aufgabe ernsthaft prüfen.

Läßt sich die Trennung der Beihilfe- von der Personalbearbeitung aus zwingenden Gründen ausnahmsweise nicht verwirklichen, so muß jedoch mindestens sichergestellt werden, daß

- Beihilfesachbearbeiter und Personalsachbearbeiter räumlich getrennt sind,

- Beihilfeakten von der übrigen Personalakte getrennt aufbewahrt werden,

- nur Beihilfesachbearbeiter Zugriff auf Beihilfevorgänge haben,

- der Personalamtsleiter in die regelmäßige Beihilfebearbeitung nicht eingeschaltet wird.

Bedenken bestehen, wenn im Vertretungsfall eine Dienstkraft der Personalstelle die Beihilfebearbeitung übernimmt. Die Befürchtung von Betroffenen, daß in einem solchen Fall ein Personalsachbearbeiter entgegen seiner rechtlichen Verpflichtung aus der Beihilfebearbeitung gewonnene Informationen in die Personalsachbearbeitung einfließen läßt, ist nicht von der Hand zu weisen. Aus demselben Grunde kann eine Mitwirkung von Vorgesetzten der Personalstelle bei der Beihilfebearbeitung nicht in Betracht kommen. Es geht nicht an, daß z.B. ein Personalamtsleiter schwierige Fälle selbst bearbeitet.

Dem Abschottungsgebot wird es auch nicht gerecht, wenn der für Beihilfe- wie für Personalangelegenheiten zuständige gemeinsame Vorgesetzte Beihilfebescheide unterzeichnet und dabei Einsicht in die vorgelegten Unterlagen nehmen kann. Die in der kommunalen Praxis häufiger anzutreffende Verfahrensweise, daß der Hauptamtsleiter, der zugleich das Personalamt führt, die Zeichnungsbefugnis in Beihilfeangelegenheiten und für Kassenanordnungen ausübt, ist aus meiner Sicht änderungsbedürftig. In einem mir vorgetragenen Fall hat die Gemeinde die Zeichnungsbefugnis auf den Kämmerer übertragen. Dies zeigt, daß sich bei entsprechender Bereitschaft durchaus datenschutzgerechte und praktikable Lösungen finden lassen.

Angemerkt sei in diesem Zusammenhang, daß nach den gemeindekassenrechtlichen Vorschriften einer schriftlichen

Kassenanordnung - anders als bei der sachlichen und rechnerischen Feststellung - nicht die begründenden Unterlagen beigefügt werden müssen. Ein Anordnungsbefugter kann deshalb keine Einsicht in die Beihilfeunterlagen verlangen.

Abschließend sei darauf hingewiesen, daß die Aufsichts- und Kontrollbefugnisse von Vorgesetzten - insbesondere des Behördenleiters - durch das dargestellte Trennungsgebot nicht eingeschränkt werden. Die in diesem Bereich eingesetzten Mitarbeiterinnen und Mitarbeiter sind nicht etwa aus Datenschutzgründen einer Aufsicht entzogen. Diese darf allerdings nur im Rahmen der Verhältnismäßigkeit erfolgen.

14.14 Wenn Ärzte mit Patientinnen telefonieren ...

Ein Chefarzt eines kommunalen Krankenhauses und eine Patientin haben sich bei mir zu Recht darüber beschwert, daß nach der Praxis des Krankenhauses bei dienstlich geführten Telefonaten eine Aufzeichnung der Verbindungsdaten (Organisationseinheit, Nebenstellennummer, Datum und Uhrzeit, Telefonnummer des angerufenen Anschlusses) erfolgt. Dies ist unzulässig.

Zwar darf ein Dienstherr/Arbeitgeber zur Kontrolle der Wirtschaftlichkeit und Sparsamkeit in diesem Bereich grundsätzlich die genannten Daten unverkürzt erfassen und - zeitlich begrenzt - speichern (vgl. insbesondere VGH Baden-Württemberg, NJW 1991, 2721). Bei einem Arzt ergibt sich jedoch wegen dessen Schweigepflicht eine besondere Situation. Das BAG (NJW 1987, 1509) hat entschieden, daß im Hinblick auf § 203 StGB bei dienstlichen Telefonaten eines in der Beratungsstelle eines Landkreises eingesetzten Psychologen die vollständige Rufnummer des Gesprächspartners nicht erfaßt werden darf, soweit der Arbeitnehmer in seiner Eigenschaft als Berater Klienten anruft. Dabei hat das Gericht darauf abgestellt, daß eine fachgerechte psychologische Beratung und Behandlung ein Vertrauensverhältnis zwischen der zu betreuenden Person und dem Psychologen voraussetzt. Vom Bestehen dieses Vertrauensverhältnisses gehe auch § 203 StGB aus. Diese Rechtsprechung ist auf dienstliche Telefonate eines im Krankenhaus beschäftigten Arztes übertragbar. Denn auch zwischen Arzt und Patient besteht ein Vertrauensverhältnis, das durch § 203 Abs. 1 Nr. 1 StGB strafrechtlich geschützt wird.

Die Dienstanschlußvorschriften einiger Länder sehen deshalb bereits ausdrücklich vor, daß bei Ärzten, die in staatlichen Krankenhäusern beschäftigt sind, keine vollständige Erfassung der in Rede stehenden Telefonverbindungsdaten erfolgt. Dies gilt selbstverständlich auch für (Zahn-)Ärzte, Psychologen, Geistliche, Sozialarbeiter und -pädagogen, Bewährungs- und Gerichtshelfer, Suchtkrankenhelfer sowie Berater der AIDS-Hilfe und der Tuberkulose-Überwachung in Gesundheitsämtern, Vollzugsanstalten, Gerichten, Schulämtern, Gewerbeaufsichtsämtern, Versorgungsämtern und Versorgungskurkliniken - also für die Berufsgruppen, die nach § 203 StGB einer besonderen beruflichen Verschwiegenheitspflicht unterliegen.

Mit dem Niedersächsischen Sozialministerium und dem Niedersächsischen Finanzministerium habe ich Einvernehmen darüber erzielt, daß die Nichterfassung von Telefonverbindungsdaten für alle Bediensteten gilt, die einem besonderem Berufsgeheimnis unterliegen. Das Finanzministerium wird dies im einzelnen noch in einer Verwaltungsvorschrift regeln.

14.15 Datenübermittlungen zwischen Personalrat, Stufenvertretung, Gesamtpersonalrat

Eine Schule hatte dem Schulpersonalrat die Unfallmeldung eines Bediensteten sowie das von ihm vorgelegte ärztliche Attest zugeleitet. Der Unfall ging nach Darstellung des verletzten Beamten auf Tätlichkeiten eines Kollegen zurück. Der Schulpersonalrat gab eine Ablichtung der Unfallmeldung sowie des ärztlichen Attests an den Schulbezirkspersonalrat weiter. Begründet wurde dies mit der Erwägung, der Bezirkspersonalrat sei als zuständige Stufenvertretung zuständig, weil im Unfallbericht eine Regreßpflicht des verursachenden Lehrers angesprochen worden sei.

Abgesehen davon, daß die Schule das ärztliche Attest nicht dem Schulpersonalrat zur Verfügung stellen und dieser es auch nicht der Stufenvertretung weiterleiten durfte (vgl. § 77 Abs. 5 Nds. PersVG), war auch die Weitergabe des Unfallberichts unzulässig. Dies folgt schon daraus, daß die Stufenvertretung im Falle der Verfolgung eines Regreßanspruchs gegen den Schädiger von der Bezirksregierung ohnehin zu beteiligen gewesen wäre. Die vorherige Unterrichtung "ins Blaue hinein" war überflüssig. Tatsächlich wurde ein Regreßanspruch von der Bezirksregierung auch gar nicht in Erwägung gezogen.

Der Fall gibt mir Veranlassung, darauf hinzuweisen, daß das Nds. PersVG, das die Datenverarbeitung der Personalräte in mehreren Einzelvorschriften näher regelt, einen generellen Datenaustausch zwischen dem Personalrat und den Stufenvertretungen nicht zuläßt. Nach § 79 Abs. 4 Satz 1 Nds. PersVG hat die Stufenvertretung, soweit sie zu beteiligen ist, den zuständigen Personalräten Gelegenheit zur Stellungnahme zu geben. Dies gilt auch für den Gesamtpersonalrat (§ 80 Abs. 1 Satz 2 Nds. PersVG). In diesem Rahmen dürfen - unter strikter Beachtung des Erforderlichkeitsprinzips - personenbezogene Daten zwischen Personalvertretung und Stufenvertretung/Gesamtpersonalrat übermittelt werden. Eine Rechtsgrundlage für einen weitergehenden Datenaustausch ist dagegen nicht vorhanden. In diesem Zusammenhang kann auch nicht etwa auf die Übermittlungsvorschrift des allgemeinen Datenschutzrechts (§ 11 NDSG) zurückgegriffen werden. Der Gesetzgeber ist vielmehr davon ausgegangen, daß die Personalvertretung, die mit der Dienststelle vertrauensvoll und partnerschaftlich zusammenzuarbeiten hat, von dieser die zur Aufgabenerfüllung erforderlichen personenbezogenen Daten erhält und Datenübermittlungen außerhalb des im Personalvertretungsrecht vorgesehenen Rahmens auch zwischen Personalrat und Stufenvertretung/Gesamtpersonalrat unterbleiben.

14.16 Einsicht der Schwerbehindertenvertretung in Bewerbungsunterlagen und Teilnahme an Vorstellungsgesprächen

Wenn sich Schwerbehinderte um die Einstellung oder die Besetzung eines Dienstpostens/Arbeitsplatzes beworben haben, ist die Schwerbehindertenvertretung an der Auswahl von Bewerberinnen und Bewerbern zu beteiligen. Nach Nrn. 3.6 und 3.7 der Schwerbehindertenrichtlinien (Nds. MBl. 1993, S. 361) ist die Schwerbehindertenvertretung in einem solchen Fall auch über die persönlichen und leistungsbezogenen Daten der nichtschwerbehinderten Mitbewerberinnen und Mitbewerber zu unterrichten. In der Praxis erhält sie zumeist Einsicht in die Bewerbungsunterlagen bzw. eine von der Dienststelle erstellte Synopse sämtlicher Bewerber. Zudem hat die Schwerbehindertenvertretung das Recht, an allen Vorstellungsgesprächen - auch der Nichtschwerbehinderten - teilzunehmen, sofern sich Schwerbehinderte beworben haben.

In den Bundesländern wird zum Teil unterschiedlich verfahren. Ich halte die niedersächsische Praxis für sachgerecht, weil es der Schwerbehindertenvertretung nur bei Einräumung dieser Rechte möglich sein dürfte, sich ein abgewogenes Meinungsbild zu verschaffen. Im übrigen kann sich die Schwerbehindertenvertretung aufgrund ihres Teilnahmerechts an den Personalratssitzungen ohnehin Kenntnis von allen dem Personalrat in diesem Zusammenhang zur Verfügung gestellten personenbezogenen Daten verschaffen. Die Verfahrensweise entspricht überdies der für Frauenbeauftragte geltenden Rechtslage.

Das Schwerbehindertenrecht enthält allerdings derzeit keine Grundlage für die geschilderte Praxis. Da die Einsicht der Schwerbehindertenvertretung in Unterlagen nichtbehinderter Bewerber sowie die Teilnahme an Vorstellungsgesprächen solcher Bewerber deren Recht auf informationelle Selbstbestimmung beeinträchtigt, müßte dieser Rechtseingriff durch Gesetz zugelassen werden. Ich habe deshalb darauf gedrungen, daß Niedersachsen sich gegenüber dem Bund anläßlich der anstehenden Einordnung des Rehabilitations- und Schwerbehindertenrechts ins Sozialgesetzbuch für eine entsprechende Rechtsänderung einsetzt. Sollte diese allerdings ausbleiben, muß die bisherige niedersächsische Praxis aufgegeben werden.

14.17 Öffentliche Bedienstete als Wahlhelfer

Viele Anfragen erreichten mich im Zusammenhang mit den Kommunalwahlen 1996. Im XII. Tätigkeitsbericht (15.15) habe ich dargestellt, unter welchen Voraussetzungen Behörden und andere öffentliche Stellen Daten der bei ihnen Beschäftigten ohne deren Einwilligung für einen Einsatz als Wahlhelfer übermitteln dürfen. Nach der damaligen Rechtslage war dies ausschließlich für Landtagswahlen (§ 25 Abs. 2 des Niedersächsischen Landeswahlgesetzes) zulässig. Um entsprechendes auch für die Kommunalwahlen zu ermöglichen, hat der Landesgesetzgeber § 12 des Niedersächsischen Kommunalwahlgesetzes (NKWG) ergänzt. Danach dürfen die erforderlichen Daten der im Gebiet

der anfragenden Gemeinde wohnhaften Bediensteten (d.h. Name, Vorname, akademischer Grad, Anschrift) mitgeteilt werden. Die Angaben dürfen in einer Wahlhelferdatei gespeichert und für künftige andere Wahlen verarbeitet werden, wenn die Betroffenen der Speicherung nicht widersprochen haben. In die Datei dürfen auch alle von Parteien und Wählergruppen gemachten Vorschläge zur Berufung von Wahlhelfern und alle sonst von der Gemeinde erhobenen Wahlhelferdaten im Rahmen der Erforderlichkeit aufgenommen werden. Sie können für alle künftigen Wahlen, d.h. auch für Landtags-, Bundestags- und Europawahlen, genutzt werden.

Wenn der Betroffene der Speicherung widerspricht, muß diese unterbleiben. Auf das Widerspruchsrecht ist er schriftlich hinzuweisen. Dies hat in deutlicher Form zu geschehen. Aus meiner Sicht zeigt es eine Geringschätzung der Rechte von Bürgerinnen und Bürgern, wenn man - wie mir dies in einigen Fällen vorgetragen wurde - den Hinweis im Text so zu verstecken sucht, daß er übersehen wird.

Die Übermittlung durch die Beschäftigungsbehörde beschränkt sich nach dem Gesetz auf die Daten "geeigneter" Bediensteter. Was damit gemeint ist, bleibt unklar. Ich halte es für unzulässig, wenn bereits die Beschäftigungsbehörde eventuelle Hinderungsgründe bei der Bestellung potentieller Wahlhelfer berücksichtigt und z.B. davon absieht, besondere Funktionsträger, Schichtdienstleistende, Schwerbehinderte etc. zu benennen. Gegen eine solche Verfahrensweise spricht neben Praktikabilitäts- und Gleichbehandlungsgründen vor allem der Gesichtspunkt, daß die Ausübung eines Wahlehrenamtes und das Beschäftigungsverhältnis nichts miteinander zu tun haben. Deshalb muß es den Bediensteten selbst überlassen bleiben, aus dem dienstlichen Bereich herrührende Hinderungsgründe gegenüber der Wahlbehörde geltend zu machen. In der Praxis dürfte es neben Fällen schwerer körperlicher Behinderung (z.B. bei Blindheit) kaum Fälle geben, in denen eine Datenübermittlung wegen Ungeeignetheit von Bediensteten unterbleiben dürfte.

Bei der Vorbereitung der Gesetzesänderung habe ich mich in diesem Punkt gegen die genannte Regelung ausgesprochen, jedoch kein Gehör gefunden. Daß die Vorschrift zu Mißverständnissen führen kann, zeigt z.B. die Beschwerde eines Petenten, nach dessen Darstellung die Gemeinde bei seiner Beschäftigungsbehörde nähere Informationen über ihn - u.a. über seine Funktion und charakterliche Eigenschaften - einzuholen versuchte. Eine derartige Anfrage ist ebenso wie ihre Beantwortung unzulässig. Unzulässig wäre es auch, wenn eine Gemeinde, die im Einzelfall bei der Bestellung eines öffentlichen Bediensteten auf Widerstand stößt, hierüber seiner Beschäftigungsbehörde Mitteilung machen würde.

15. Kommunalverwaltung

15.1 Kommunalverfassungsrecht

Im Berichtszeitraum ist das Gesetz zur Reform des Niedersächsischen Kommunalverfassungsrechts in Kraft getreten. Neben grundlegenden Änderungen wie der Einführung der Eingleisigkeit der Verwaltungsführung, der Stärkung der Bürgerbeteiligung und der Verbesserung der Wirkungsmöglichkeiten für die kommunalen Mandatsträger enthält es auch einige Bestimmungen mit datenschutzrechtlicher Relevanz.

Das Auskunftsrecht der Rats- bzw. Kreistagsmitglieder (§§ 40 Abs. 3 NGO, 36 Abs. 3 NLO) wurde erweitert. Die Beschränkung, daß kommunale Mandatsträger nur im Zusammenhang mit einer auf der Tagesordnung stehenden Angelegenheit einen Auskunftsanspruch haben, wurde aufgegeben. Rats- bzw. Kreistagsmitglieder können nun "zum Zwecke der Überwachung und zum Zwecke der eigenen Unterrichtung" in allen Angelegenheiten der Kommune die erforderlichen Auskünfte verlangen. Das Problem, daß in der bisherigen Praxis oft über das beschränkte Auskunftsrecht hinaus auch personenbezogene Daten ohne Rechtsgrundlage weitergegeben wurden, ist damit entfallen. Auf meine Anregung hin ist auch die Datenübermittlung an Mitarbeiterinnen und Mitarbeiter von Fraktionen und Gruppen geregelt worden. Diese Hilfskräfte, die nicht der kommunalen Vertretungskörperschaft angehören, müssen für die Erledigung ihrer Aufgaben ebenso wie die Fraktionsmitglieder Kenntnis von personenbezogenen Daten erhalten. §§ 39b NGO und 39b NLO lassen diese Datenübermittlung ausdrücklich zu. Im übrigen sind für die Datenverarbeitung der Fraktionen die Fraktionsvorsitzenden verantwortlich. Sie haben u.a. Auskünfte und Akteneinsicht nach § 16 NDSG zu gewähren und dafür Sorge zu tragen, daß nicht mehr benötigte personenbezogene Daten zu löschen sind (§ 17 NDSG).

Die - aus datenschutzrechtlicher Sicht zwar begrüßenswerten, aber auch nicht zu überschätzenden - Änderungen sollten allerdings nicht dazu verleiten, das Kommunalverfassungsrecht insgesamt als datenschutzgerecht anzusehen. Es weist vielmehr weiterhin erhebliche Defizite auf. Dies zeigt sich beispielhaft daran, daß die Landesregierung und der Landtag meinem Vorschlag, über die Datenübermittlung an Fraktions- und Gruppenmitarbeiterinnen und -mitarbeiter hinaus auch die Zulässigkeit der Datenübermittlungen an die Fraktionen und Gruppen selbst gesetzlich zu regeln, nicht gefolgt sind. §§ 39b NGO und 39b NLO setzen vielmehr die Zulässigkeit einer solchen Datenübermittlung ausdrücklich voraus. Diese heute nicht mehr haltbare Handhabung liegt dem gesamten Kommunalverfassungsrecht

zugrunde. Die Forderung des Bundesverfassungsgerichts, daß der in einer Verarbeitung personenbezogener Daten liegende Grundrechtseingriff (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) einer normenklaren Rechtsgrundlage bedarf, aus der sich Voraussetzungen und Umfang der Beschränkungen dieses Rechts für die Bürgerinnen und Bürger eindeutig ergeben, wird hier beharrlich verdrängt. Auch § 4 Abs. 1 Nr. 1 NDSG verlangt - abgesehen vom Falle der Einwilligung - für die Zulässigkeit einer Datenverarbeitung eine Rechtsvorschrift.

Für eine Übergangszeit - auch wenn seit dem sogenannten Volkszählungsurteil des Bundesverfassungsgerichts inzwischen mehr als 10 Jahre verstrichen sind - mag es in einigen Verwaltungsbereichen noch hinnehmbar sein, die Datenverarbeitung vorübergehend auf Regelungen zu stützen, die den verfassungsrechtlichen Anforderungen (noch) nicht genügen. Auf längere Sicht müssen jedoch auch im Kommunalverfassungsrecht eindeutige Befugnisnormen für die Datenverarbeitung geschaffen werden.

15.2 Amtsverschwiegenheit

Mehrfach haben Bürgerinnen und Bürger den Verdacht geäußert, daß Rats-/ Kreistagsmitglieder personenbezogene Daten, die sie aus ihrer Mandatstätigkeit erfahren hatten, an die Öffentlichkeit gebracht hätten. So hatte ein Ratsmitglied u.a. eine von der Verwaltung für die Beratung im Verwaltungsausschuß gefertigte Aufstellung mit den Namen der Personen, die Änderungsvorschläge zum Flächennutzungsplan gemacht hatten, an ein lokales Anzeigenblatt weitergegeben. In einem anderen Fall waren im Zusammenhang mit einer Stellenbewertung Angaben über kommunale Bedienstete an die Öffentlichkeit gelangt.

Ich gehe davon aus, daß die kommunalen Mandatsträger jedenfalls bei der Übernahme ihrer Aufgabe von der Verwaltung eingehend über die Pflicht zur Amtsverschwiegenheit belehrt werden. Dennoch scheint über deren Reichweite nicht immer die nötige Klarheit zu bestehen. Zu Unrecht berief sich z.B. ein Ratsmitglied darauf, daß die von ihm in die Öffentlichkeit getragenen personenbezogenen Daten einer Beratungsunterlage entstammten, die von der Verwaltung nicht als vertraulich gekennzeichnet worden war. Betrifft die in Rede stehende Angelegenheit ein Verwaltungsverfahren, das auf die Prüfung der Voraussetzungen eines Verwaltungsakts oder den Abschluß eines öffentlich-rechtlichen Vertrages gerichtet ist, so ergibt sich die gesetzliche Verpflichtung zur Geheimhaltung schon aus dem Verwaltungsverfahrensrecht (§ 30 VwVfG i.V.m. § 1 Nds. VwVfG). Die am Verwaltungsverfahren Beteiligten, insbesondere die Antragsteller, haben Anspruch darauf, daß schützenswerte Tatsachen oder Umstände nicht gegenüber Dritten offenbart werden. Die Amtsverschwiegenheit ist zudem in Angelegenheiten zu wahren, die "ihrer Natur nach" geheimzuhalten sind (z.B. solche, die in nicht-öffentlicher Sitzung beraten werden).

Neben den kommunalverfassungsrechtlichen Bestimmungen zur Amtsverschwiegenheit gilt für kommunale Mandatsträger auch § 5

NDSG. Hiernach ist es jeder Person, die bei einer öffentlichen Stelle dienstlichen Zugang zu personenbezogenen Daten hat, untersagt, diese zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren. Über die Regelungen des Kommunalverfassungsrechts hinaus sind damit nicht nur aus Sicht der Betroffenen (besonders) geheimhaltungsbedürftige Angelegenheiten geschützt, sondern jedes personenbezogene Datum ohne Rücksicht auf dessen Gewicht für den Betroffenen. Außerdem betont § 5 NDSG den Rechtsgedanken, daß Daten nicht zu einem anderen Zweck als dem, für den sie beschafft worden sind, verwendet werden dürfen. Ein Verstoß gegen diese Vorschrift stellt zumindest eine Ordnungswidrigkeit dar (§ 29 NDSG), bei Handeln gegen Entgelt oder in Bereicherungs- und Schädigungsabsicht eine Straftat (§ 28 NDSG).

15.3 Weitergabe von Tonbandabschriften einer öffentlichen Ratssitzung

Eine Gemeinde, die von öffentlichen Ratssitzungen Tonbandaufnahmen zur Erstellung der Sitzungsniederschrift fertigte, händigte den Vertretern mehrerer Fraktionen auf deren Bitte hin die Tonbandabschriften einer Sitzung aus, in der besonders heftig über ein kommunalpolitisches Thema gestritten wurde. Um die Abschriften für politische Angriffe gegen ein Ratsmitglied zu nutzen, gab eine Fraktion sie an Dritte weiter.

Dies war unzulässig. Zwar enthielt im konkreten Fall die Geschäftsordnung des Rates keine Regelung über den Umgang mit Tonbandaufzeichnungen, auch hatte das betroffene Ratsmitglied der Aufnahme nicht zugestimmt; im Kommunalrecht ist jedoch anerkannt, daß für die Erstellung von Sitzungsniederschriften Tonbandaufzeichnungen auch ohne ausdrückliche Zustimmung der Mandatsträger und sonstiger Sitzungsteilnehmer erfolgen dürfen. Der Verwendungszweck der Aufzeichnungen ist aber strikt auf eine bloße Hilfsfunktion für die Protokollierung beschränkt. Ratsmitglieder dürfen die Aufzeichnungen zwar im Zusammenhang mit der Anfertigung des Protokolls abhören, um z.B. Zweifel an der Richtigkeit der Niederschrift zu klären und etwaige Einwendungen zu begründen. Ein Abhören zu anderen Zwecken ist jedoch unzulässig. Erst recht darf eine Tonbandabschrift nicht an Ratsmitglieder ausgehändigt werden, damit die Aufzeichnungen nicht - wie in diesem Fall - zu Zwecken genutzt werden können, die mit der Anfertigung des Protokolls nichts mehr zu tun haben. Auch die Ratsmitglieder dürfen die Abschriften nicht an Dritte weitergeben.

Aus der Zweckbestimmung der Tonbandaufzeichnungen folgt, daß diese vernichtet werden müssen, sobald die Niederschrift genehmigt ist und ein Rechtsstreit über deren Inhalt sich nicht abzeichnet. Nach § 17 Abs. 2 Satz 1 Nr. 2 NDSG sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die datenverarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist. Das ist der Fall, weil die Tonbandaufzeichnung mit der Erstellung des Protokolls ihren Zweck erfüllt hat. Ebenso wie die Tonbandaufzeichnung selbst sind auch entsprechende Tonbandabschriften zu löschen, d.h. zu vernichten.

Die Weitergabe der Tonbandabschriften durch die Gemeinde wie auch durch Ratsmitglieder stellt jeweils eine zweckwidrige Nutzung personenbezogener Daten im Sinne des § 5 NDSG dar und erfüllt bei vorsätzlichem Verhalten den Tatbestand einer Ordnungswidrigkeit (§ 29 NDSG).

16. Ungeahnte Lesarten des Umweltinformationsgesetzes

Ein Anwaltsbüro wandte sich bundesweit an die zuständigen Stellen und beantragte, ihm aktuelle Listen der dort kontrollierten, ökologisch wirtschaftenden, landwirtschaftlichen Betriebe zur Verfügung zu stellen. Dieses Ansinnen wurde auf das Umweltinformationsgesetz gestützt - zu Unrecht. Nach dem Umweltinformationsgesetz besteht Anspruch auf Herausgabe von Informationen über die Umwelt. Es ging dem Anwaltsbüro nicht um die Erlangung von Informationen über die Umwelt oder über den Umweltschutz, sondern offensichtlich um eine Marktübersicht, hinter der ein kommerzielles Interesse stand. Ich habe mich daher gegen die Herausgabe der fraglichen Listen gewandt. Dem haben sich andere Landesbeauftragte für den Datenschutz und die zuständigen Fachbehörden angeschlossen.

17. Bau-, Wohnungs- und Vermessungswesen

17.1 Novellierung des Vermessungs- und Katastergesetzes

Im Niedersächsischen Innenministerium liegt hausintern ein erster Entwurf für die Novellierung des Vermessungs- und Katastergesetzes vor. Damit soll die längst überfällige Anpassung an die Grundsätze des Volkszählungsurteils erfolgen. Dateninhalt, Nutzung, regelmäßige Datenübermittlung und automatisierter Abruf werden spezialgesetzlich geregelt. Übergangsweise wurde eine Abrufregelung für das Liegenschaftskataster in einer übergreifenden Verordnung der Landesregierung (Nds. GVBl. 1995 S. 172) festgelegt.

17.2 Mittagsruhestörung durch Veröffentlichung des Baulückenverzeichnisses

Viel Überzeugungsarbeit sowohl bei der betroffenen Kommune als auch beim Niedersächsischen Sozialministerium hat es mich gekostet, ein datenschutzgerechteres Verfahren bei der Veröffentlichung von Baulückenverzeichnissen durchzusetzen. Eine Petentin hatte sich darüber beschwert, daß Makler und Bauwillige sie zu den "unmöglichsten Zeiten" aufgesucht hätten, um sie nach ihren Verkaufsabsichten zu einem ihr gehörenden Baulückengrundstück zu befragen. Mein Vorschlag, vor einer Veröffentlichung in Baulückenverzeichnissen mit personenbezogenen Daten die Grundstückseigentümer über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise rechtzeitig zu unterrichten und auf ihr Widerspruchsrecht hinzuweisen, wurde dann aber letztlich akzeptiert.

17.3 Erforderlich? - Weitergabe von Daten einer bauaufsichtlichen Anordnung

Nachbarstreitigkeiten in Baurechtsangelegenheiten sind leider gang und gäbe. Wenn dann noch jemand aufgrund einer nachbarrechtlichen Anhörung keine Genehmigung erhält, ein Nachbar jedoch eine vollständige Kopie des Untersagungsbescheides in die Hand bekommt, wird der Ruf nach dem Datenschutz laut. Im betreffenden Fall war die vor jeder Datenübermittlung durchzuführende Erforderlichkeitsprüfung unterblieben. Bei einer Überprüfung wäre festgestellt worden, daß kein berechtigtes Interesse auf Mitteilung aller im Bescheid enthaltenen Daten vorlag und diese zur Unterrichtung des Beschwerdeführers über das auf seine Beschwerde Veranlaßte nicht erforderlich waren. Da das Niedersächsische Sozialministerium meinte, hier habe es sich um einen Einzelfall gehandelt, hat es von einer generellen Unterrichtung aller Baugenehmigungsbehörden abgesehen.

17.4 Verteilerlisten für die Versendung von Planfeststellungsbeschlüssen an die

Grundstückseigentümer

Immer wieder passiert es, daß es durch vermeidbare Unachtsamkeiten zu fehlerhaften Datenübermittlungen kommt. So auch im Fall der Zustellung von Planfeststellungsbeschlüssen an von einem Bauvorhaben Betroffene. Durch ein "Büroversehen" wurden keine Einzelbriefe versandt, sondern der gesamte Verteilerentwurf mit Anschreiben und Planfeststellungsangaben. Die betroffene Bezirksregierung sah den Fehler ein und gelobte Besserung. Die Mitarbeiterinnen und Mitarbeiter wurden darauf hingewiesen, daß die Angaben über andere Verfahrensbeteiligte in Planfeststellungsverfahren nicht mitgeteilt werden dürfen.

18. Finanzverwaltung

18.1 Wie gehabt: Abgabenordnung weiter ohne Datenschutzregelungen

Die für die Abgabenordnung (AO) zuständigen Referenten des Bundes und der Länder tun sich in Sachen Datenschutz schwer. Die seit Jahren von den Datenschutzbeauftragten des Bundes und der Länder geforderten datenschutzrechtlichen Regelungen in der AO gibt es immer noch nicht. Die zwischen dem Bundesbeauftragten und den Landesbeauftragten abgestimmten Vorschläge sollen nunmehr Ende des Jahres mit den Vertretern der obersten Finanzbehörden der Länder erörtert werden. Das Niedersächsische Finanzministerium hat mir seine Unterstützung zugesagt.

18.2 Steuerdatenabrufverordnung - jetzt nur noch als Verwaltungsregelung?

Nachdem eine einvernehmliche Regelung für die Gemeinden in der Steuerdatenabrufverordnung nicht möglich war, soll statt der ursprünglich vorgesehenen Rechtsverordnung eine bundeseinheitliche "Steuerdaten-Abruf-Verwaltungsregelung" geschaffen und durch Erlasse des Bundes gegenüber dem Bundesamt für Finanzen und den Ländern umgesetzt werden. Zu diesem Entwurf wurden dem Bundesminister der Finanzen datenschutzrechtliche Verbesserungsvorschläge zugeleitet. Es bleibt abzuwarten, inwieweit diese Vorschläge berücksichtigt werden. Da in Niedersachsen die Einrichtung automatisierter Abrufverfahren der Zulassung durch eine Verordnung bedürfen, habe ich das Niedersächsische Finanzministerium gebeten, mir mitzuteilen, wie die Vorschriften des § 12 Abs. 2 NDSG umgesetzt werden sollen.

18.3 Steuerberaterdaten für die Bundesversicherungsanstalt für Angestellte (BfA)

Die Steuerberaterkammer fragte an, ob ein Namens- und Anschriftenverzeichnis der Steuerberaterinnen und Steuerberater in Niedersachsen für Prüfungszwecke an die BfA gegeben werden könne. Hierfür gibt es keine spezialgesetzliche Übermittlungsregelung. Bei Anwendung des allgemeinen Datenschutzrechts bedarf es wegen der damit verbundenen Zweckänderung der Einwilligung der Betroffenen. Das Niedersächsische Finanzministerium unterrichtete die Steuerberaterkammer über diese Rechtslage.

18.4 Anträge auf Wohnungsbauprämie - von wegen freiwillig!

Die Diskussion über das Verfahren bei der Beantragung einer Wohnungsbauprämie (vgl. XII 19.3) ist noch nicht abgeschlossen. Der Bundesminister der Finanzen vertritt (nunmehr) die Auffassung, daß es sich bei den steuerlichen Angaben auf dem Wohnungsbauprämien-Antrag um freiwillige Angaben handelt, um die der Antragsteller lediglich im Interesse einer schnellen Bearbeitung seines Antrages gebeten wird. Dieser Auffassung habe ich widersprochen. Zum einen wird im Antrag entgegen den Vorschriften der Datenschutzgesetze nicht auf die Freiwilligkeit hingewiesen, zum anderen wird durch den Hinweis auf § 88 AO i.V.m. § 8 des Wohnungsbauprämiengesetzes eine Verpflichtung für den Antragsteller suggeriert.

19. Soziales

19.1 Berufliche Eingliederung von arbeitslosen Sozialhilfeempfängern

Gemäß § 19 BSHG sollen für arbeitslose Empfängerinnen und Empfänger von Sozialhilfe Arbeitsgelegenheiten geschaffen werden. Diese sollen von vorübergehender Dauer und für eine bessere Eingliederung der Hilfesuchenden in das Arbeitsleben geeignet sein. Bei der Schaffung und Erhaltung von Arbeitsgelegenheiten sollen die Träger der Sozialhilfe und die Dienststellen der Bundesanstalt für Arbeit zusammenwirken. Mehrere Kommunen haben sich deshalb dafür ausgesprochen, daß der Arbeitsverwaltung mitgeteilt wird, welche Personen mit welchem erlernten Beruf und welcher Berufserfahrung von ihnen in sozialversicherungspflichtige Maßnahmen vermittelt werden konnten. Diese Mitteilung erfolgt bereits zu Beginn der Beschäftigung gemäß § 19 BSHG, weil die Vorplanungen der Arbeitsverwaltung langfristig angelegt sein müssen. Die Datenübermittlung ist gemäß § 69 Abs. 1 Nr. 1 SGB X jedoch nur zulässig, wenn sie im Einzelfall erforderlich ist. Die Einzelfallhilfe sieht zwar das Zusammenwirken beider Behörden und ggf. die Erstellung eines Gesamtplans nach § 19 BSHG vor. Eine ungefilterte Übermittlung von Daten aller Betroffenen ist aber nicht notwendig. Auch die Prüfung, wer für Fortbildungs- und Umschulungsmaßnahmen in Frage kommt, ist grundsätzlich aus dem Datenbestand des Arbeitsamtes zu beantworten, wo alle erwerbsfähigen Hilfeempfänger erfaßt sind. Diese Bewertung wird auch vom Niedersächsischen Sozialministerium geteilt.

Da nach Angaben von Kommunen Hilfeempfänger immer häufiger Arbeitsangebote der Arbeitsverwaltung ablehnen, haben diese sich vielfach dafür ausgesprochen, daß die Arbeitsverwaltung die Sozialämter unterrichtet, wenn sich ein Arbeitssuchender weigert, eine ihm zumutbare Erwerbstätigkeit anzunehmen. Auch eine solche pauschale Datenübermittlung scheitert an der Erforderlichkeit, die in jedem Einzelfall festzustellen ist (§ 69 Abs. 1 Nr. 1 SGB X). Zwar dürfte das Arbeitsamt dem Sozialamt eine solche Mitteilung machen, wenn es im Einzelfall weiß, daß der Betreffende Sozialhilfe bezieht. Ist diese sichere Kenntnis aber nicht vorhanden, so darf auf die bloße Vermutung hin, der Arbeitssuchende werde wohl Sozialhilfe beziehen, eine Datenübermittlung nicht erfolgen. Andernfalls bestünde die Gefahr, daß dem Sozialhilfeträger auch Informationen über Personen zugänglich gemacht werden, die eine Leistung nicht in Anspruch nehmen. Datenschutzgerecht ist folgende Verfahrensweise: Das Arbeitsamt bestätigt die Bemühungen von erwerbsfähigen Sozialhilfeempfängern um Arbeit in einer Bescheinigung für das Sozialamt. Auf dieser Bescheinigung kann auch vermerkt werden, daß die bzw. der Arbeitssuchende eine vom Arbeitsamt vorgeschlagene konkrete

Arbeitsstelle abgelehnt hat. Das Sozialamt kann dann prüfen, ob aus diesem Verhalten der Empfängerin bzw. des Empfängers von Sozialhilfe Konsequenzen nach § 25 BSHG (vgl. § 18 Abs. 3 BSHG) zu ziehen sind.

19.2 Datenübermittlung an Straßenverkehrsbehörden - rechtfertigender Notstand ?

Unter XII 20.12 berichtete ich über die Problematik der Weitergabe von personenbezogenen Daten von Sozialleistungsträgern an die Straßenverkehrsbehörden zum Zwecke der Überprüfung der Eignung zum Führen von Kraftfahrzeugen.

Ich meine, daß durch die Regelung der Übermittlungsbefugnis von Sozialdaten an Behörden der Gefahrenabwehr in § 68 SGB X sowie an Strafverfolgungsbehörden nach § 73 SGB X ein Rückgriff auf die Bestimmung über den rechtfertigenden Notstand nach § 34 StGB zur Rechtfertigung der Übermittlung von Sozialdaten an Straßenverkehrsbehörden grundsätzlich ausgeschlossen ist. In den Bestimmungen des SGB X hat der Gesetzgeber bewußt eine abschließende Abwägung zwischen den Sicherheitsinteressen und dem Recht auf informationelle Selbstbestimmung vorgenommen. Zudem entspricht § 34 StGB nicht den Erfordernissen der Normenklarheit hinsichtlich Inhalt, Zweck und Ausmaß der erforderlichen Datenübermittlung nach den Entscheidungen des Bundesverfassungsgerichts. Probleme macht auch die praktische Anwendung des § 34 StGB auf die Übermittlung von Sozialdaten an Straßenverkehrsbehörden: Diese Notstandsregelung erfordert das Vorliegen einer gegenwärtigen Gefahr. Bedienstete des Sozialamts sind - von Ausnahmefällen abgesehen - kaum in der Lage, einzuschätzen, ob ein solcher Gefährdungsgrad besteht. Im Rahmen der Diskussion der Thematik ist erwogen worden, die Übermittlung an das Straßenverkehrsamt auf den in § 68 Abs. 1 SGB X genannten Datensatz (Name, Geburtsdatum, Geburtsort, Anschrift) zu beschränken, um sich nicht in Widerspruch zu dieser Regelung zu setzen, und daneben lediglich den "Betreff" anzugeben. Auch dies ist keine befriedigende Lösung, da die Straßenverkehrsämter wegen mangelnder Konkretisierung der Mitteilung im Ergebnis gravierende Zweifel an der Fahreignung nicht prüfen können.

Nach Erörterung des Problembereichs mit dem Niedersächsischen Innenministerium, dem Sozialministerium und dem Ministerium für Wirtschaft, Technologie und Verkehr hat das letztgenannte Ressort eine Ergänzung des § 68 SGB X vorgeschlagen. Danach dürfen Tatsachen, die auf nicht nur vorübergehende Mängel bezüglich der Eignung oder der Befähigung der Person zum Führen von Kraftfahrzeugen schließen lassen, den Fahrerlaubnisbehörden von Sozialleistungsträgern mitgeteilt werden. Dieser Vorschlag ist bei den Datenschutzbeauftragten des Bundes und der Länder auf Ablehnung gestoßen, weil es keine Notwendigkeit für eine generelle Übermittlungsregelung im SGB X gibt. Ich teile diese Kritik. Der leider mit mir nicht abgestimmte Vorschlag setzt die Übermittlungsschwelle entschieden zu niedrig an. Selbst gegenüber den Anforderungen, die bei einem Rückgriff auf § 34 StGB bestünden, ist der konkrete Vorschlag uferlos weit. Eine künftige

Regelung, die ich nach wie vor für notwendig halte, wird eine Übermittlung nur zur Abwehr von Gefahren für Leib oder Leben zulassen können. Auf der anderen Seite halte ich eine Beschränkung der Regelung auf Sozialleistungsträger nicht für sachgerecht. Auch Gesundheitsämter stehen vor der Frage, ob sie in einschlägigen Fällen eine Übermittlung vornehmen dürfen. Ich halte es deshalb für erforderlich, daß die Angelegenheit unabhängig von dem o.g. Gesetzgebungsverfahren - diesmal in Abstimmung mit den betroffenen Landesressorts und mir und nach gründlicher Vorbereitung durch die zuständigen Arbeitskreise - weiterverfolgt wird.

19.3 Sozialdaten auf Überweisungsträgern

Mit Urteil vom 23. Juni 1994 hat das Bundesverwaltungsgericht (DVBl. 1994, 1313) entschieden, daß es nicht zulässig ist, die Zahlung von Sozialhilfe auf Überweisungsträgern generell ohne Zustimmung des Hilfeempfängers mit dem Vermerk "Sozialleistung" zu kennzeichnen. Soweit es um die Sicherung des Hilfeempfängers unter dem Blickwinkel des Pfändungsschutzes nach §§ 54, 55 SGB I gehen könnte, ist es Sache des Hilfeempfängers, sich für den Pfändungsschutz zu entscheiden und zu diesem Zweck der Offenbarung des Bezugs von "Sozialleistung" zuzustimmen. Da diese Entscheidung für alle Sozialleistungen beachtet werden muß, haben die Fachressorts auf meine Bitte hin die Sozialleistungsträger ihres Geschäftsbereichs entsprechend unterrichtet.

19.4 Pauschale Einwilligungserklärung - ein Dauerbrenner

Auch im Berichtszeitraum 1995/96 hat sich das schon häufig angesprochene Problem (zuletzt XII 20.10) nicht erledigt. In den mir immer wieder vorgetragenen Fällen geht es vor allem um Einwilligungserklärungen zur Einholung von Bankauskünften und zur Entbindung von der ärztlichen Schweigepflicht.

Die Rechtslage ist eindeutig. Der Antragsteller oder Empfänger von Sozialleistungen hat auf Verlangen des Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen (§ 60 SGB I). Für dieses Verlangen muß der Leistungsträger konkrete Gründe darlegen können, die sich aus dem jeweiligen Einzelfall ergeben. Das Bestreben, durch die Einschaltung Dritter eine Absicherung von Angaben des Antragstellers zu erhalten, reicht hierfür nicht aus. Ein diffuses Mißtrauen gegenüber den Bürgerinnen und Bürgern rechtfertigt es nicht, von diesen die Zustimmung zur Einholung von Auskünften Dritter zu verlangen.

Auch das Niedersächsische Sozialministerium vertritt diese Auffassung seit langem. Ihre Richtigkeit wurde jüngst durch den Beschluß des VGH Hessen vom 7. Juni 1995 (DVBl. 1995, 702) bestätigt. Um ein allgemein rechtskonformes Verhalten der Sozialleistungsträger zu erreichen, hat das Sozialministerium auf meine Bitte hin die Problematik in einem Schreiben an die Arbeitsgemeinschaft der kommunalen Spitzenverbände vom 29. November 1995 aufgegriffen. Darin heißt es u.a.: "Ich weise

darauf hin, daß eine Einwilligungserklärung zur Einholung von Bankauskünften nur dann verlangt werden kann, wenn der Antragsteller die entscheidungserheblichen Tatsachen selbst nicht nachweisen kann oder will oder in Fällen des berechtigten Zweifels an den Angaben des Antragstellers (§ 60 Abs. 1 Nr. 1 SGB I)."

Ich hoffe, daß die fortwährenden Probleme mit Einwilligungserklärungen auch durch die demnächst zu erwartenden ausführlichen "Hinweise über Datenschutzklauseln in Vordrucken und Merkblättern der in § 35 SGB I genannten Stellen" des Bundesministeriums für Arbeit und Sozialordnung gelöst werden können. Eine Beachtung dieser Hinweise, an deren Erarbeitung u.a. auch die Datenschutzbeauftragten des Bundes und der Länder beteiligt waren, wäre eine wesentliche Verbesserung.

19.5 Aktenübermittlung an die Fachaufsichtsbehörde im Widerspruchsverfahren

Wie personenbezogene Daten im allgemeinen dürfen auch Sozialdaten im besonderen an Fachaufsichtsbehörden nur im Rahmen der Erforderlichkeit übermittelt werden. Dies gilt auch im Widerspruchsverfahren. Daran ändert sich nichts durch den Wortlauf des § 69 Abs. 5 SGB X, der die Datenweitergabe an Rechnungshöfe, Aufsichts- und Kontrollstellen regelt und keine entsprechende ausdrückliche Beschränkung enthält. Der Gesetzgeber ist im SGB X davon ausgegangen, daß eine Verarbeitung und Nutzung von Sozialdaten für die in § 67c Abs. 3 genannten Aufsichts- und sonstigen Aufgaben nicht als Zweckänderung anzusehen ist. Nach § 69 Abs. 5 SGB X soll dies auch gelten, wenn eine Übermittlung erfolgt. Diese Bestimmung ist wiederum in Verbindung zur grundlegenden Übermittlungsvorschrift des § 69 Abs. 1 SGB X zu sehen, die das Erforderlichkeitsprinzip betont. Auch § 67c Abs. 3 SGB X stellt auf die Erforderlichkeit für die Aufgabenerfüllung ab.

Dies bedeutet, daß in einem Widerspruchsverfahren der Fachaufsichtsbehörde nur die zur Überprüfung der Recht- und Zweckmäßigkeit des angegriffenen Verwaltungshandelns notwendigen Unterlagen vorzulegen sind. Für Aktenbestandsteile, die mit dem Widerspruchsverfahren nichts zu tun haben, besteht keine Übermittlungsbefugnis. Zu der Übersendung von Akten an Gerichte verweise ich auf die Kapitel 15.5 und 20.12 des XI. Tätigkeitsberichts.

19.6 Mitteilung der Anwesenheit von zur Fahndung ausgeschriebenen Sozialhilfeempfängern im Sozialamt an die Polizei

Die Zulässigkeit einer Mitteilung über den Aufenthalt eines Sozialleistungsempfängers im Sozialamt richtet sich nach § 68 Abs. 1 Satz 1 SGB X. Diese Angabe ist ein personenbezogenes Datum, das in den Schutzbereich des § 35 Abs. 1 SGB I fällt. Wie sich aus § 35 Abs. 2 SGB I ergibt, ist deshalb eine Verarbeitung dieses Datums nur unter den in §§ 67 ff. SGB X genannten Voraussetzungen zulässig. Auf § 161 StPO

kann in diesem Zusammenhang nicht zurückgegriffen werden. Die Voraussetzungen für die Übermittlung von Sozialdaten u.a. an Polizeibehörden und Staatsanwaltschaften zu Zwecken der Strafverfolgung sind in den §§ 68 und 73 SGB X spezialgesetzlich abschließend geregelt. Die genannte Vorschrift läßt u.a. eine Übermittlung der derzeitigen Anschrift des Betroffenen zu, soweit kein Grund zu der Annahme besteht, daß dadurch dessen schutzwürdige Interessen beeinträchtigt werden. Ob unter den Begriff der Anschrift auch ein Aufenthalt im Sozialamt subsumiert werden kann, ist umstritten. Das Kammergericht Berlin hat dies in seiner Entscheidung vom 26. Mai 1983 für den Fall des momentanen Aufenthalts bejaht (JR 1985, 24). Das Gericht meint, daß die Mitteilung über die aktuelle Anwesenheit in einer Sozialbehörde ein Weniger im Vergleich zur Angabe der Anschrift sei. Diese Auffassung wird vom Niedersächsischen Sozialministerium und von mir geteilt. Auch der Gesetzgeber ist bei der Beratung des Zweiten SGB-Änderungsgesetzes hiervon ausgegangen, wie die Gesetzesmaterialien zeigen.

Dies bedeutet jedoch nur, daß der Sozialleistungsträger Polizei und Staatsanwaltschaft den aktuellen Aufenthalt eines Leistungsempfängers zum Zeitpunkt der Anfrage mitteilen darf. Ein Sozialamt ist dagegen nicht befugt, Aufenthaltsanfragen der Polizei bzw. der Staatsanwaltschaft zu speichern und Auskünfte über künftige Aufenthalte des Betroffenen in der Sozialbehörde - z.B. auch einen vereinbarten Gesprächstermin mit dem Sozialamt - zu geben. Polizei und Staatsanwaltschaft dürfen also nicht unterrichtet werden, wenn ein gesuchter Sozialhilfeempfänger nach Anfrage das Sozialamt betritt. Selbstverständlich ist auch ein Abgleich von Fahndungs- und etwaigen Besucherlisten unzulässig. Auch über diese Grundsätze besteht Einvernehmen zwischen mir und dem Niedersächsischen Sozialministerium. Angesichts dieser Rechtslage hat die Mitteilung an Polizei oder Staatsanwaltschaft keine nennenswerte praktische Relevanz.

19.7 Haltet den Dieb!

Als die Mitarbeiterin eines Sozialamtes während ihrer Arbeit aus dem Fenster schaute, sah sie, wie zwei Männer, von einem Wochenmarkt kommend, vergeblich hinter einem dritten Mann herrannten. Der Dritte war ihr persönlich bekannt: Es handelte sich um einen ihrer Klienten - einen Sozialhilfeempfänger. Die Sozialamtsmitarbeiterin machte sich zunächst keine weiteren Gedanken. Dies änderte sich schlagartig, als sie am Tag darauf in der Zeitung las, auf dem Wochenmarkt sei ein Dieb ertappt und von den Bestohlenen verfolgt worden. Der Lump habe aber entkommen können. Die Sozialamtsmitarbeiterin griff zum Telefon und teilte der Polizei den Namen des Verdächtigen mit. Der daraufhin veranlaßte polizeiliche Zugriff war erfolgreich.

Erst als dies alles passiert war, erinnerte man sich im Sozialamt des Sozialgeheimnisses: Durfte die Mitarbeiterin die Polizei überhaupt unterrichten? Meine Antwort fiel differenziert aus: Die Übermittlung von Sozialdaten zum Zweck der Strafverfolgung ist nach § 73 SGB X nur auf Anordnung eines Richters zulässig. Ein Richter wurde hier nicht gefragt.

Daher kommt es darauf an, ob die telefonische Mitteilung ein Sozialgeheimnis betraf: Wurde der Polizei nur der Name der verfolgten Person mitgeteilt, so handelte es sich nicht um eine unzulässige Übermittlung. Das Aussehen einer Person fällt ebenso nicht unter das Sozialgeheimnis wie allein deren Name. Daß eine Sozialamtsmitarbeiterin einem Gesicht einen Namen zuordnet, berührt keinen sensiblen Sachverhalt, auch wenn sie sich das Gesicht gelegentlich des Sozialamtsbesuchs eingeprägt hat. Ganz anders würde sich der Fall darstellen, wenn der Polizei mitgeteilt worden wäre, daß der Verdächtige Sozialhilfeempfänger ist. Dies hätte die Polizei nur mit richterlichem Segen interessieren dürfen.

19.8 Verschlüsselung von Diagnosen, ICD-10-Schlüssel

Eine Vielzahl von Personen hat sich bei mir über die Verschlüsselung der Diagnosen nach dem ICD-10-Schlüssel bei der Abrechnung ärztlicher Leistungen durch die gesetzlichen Krankenkassen beschwert. Gemäß § 295 Abs. 1 SGB V sollten ab 1. Januar 1996 die an der vertragsärztlichen Versorgung teilnehmenden Ärztinnen und Ärzte verpflichtet werden, die auf den Arbeitsunfähigkeitsbescheinigungen und in den Abrechnungsunterlagen einzutragenden Diagnosen nicht mehr im Klartext anzugeben, sondern sie nach dem vierstelligen Code der internationalen Klassifikation der Krankheiten in der jeweiligen vom Deutschen Institut für Medizinische Dokumentation und Information im Auftrag des Bundesministers für Gesundheit herausgegebenen deutschen Fassung zu verschlüsseln.

Die Verwendung dieses Codes wurde insbesondere von der Ärzteschaft heftig kritisiert: Als ganzheitliche Gesundheitsstörungen empfundene Behandlungskomplexe müßten künstlich in Einzeldiagnosen zerlegt werden, so daß sich eine unzureichende Gesamtdarstellung ergibt. Zahlreiche in der Praxis relevante Diagnosen fehlten, so daß die Ärztin bzw. der Arzt eine andere nicht genau zutreffende Diagnose auswählen muß. Aus dem Code sei nicht erkennbar, ob es sich um Verdachts- oder Ausschlußfälle handelt, was zu einer erheblichen Verzerrung des Sachverhalts führen kann. Die Verwendung eines vierstelligen Codes sei sehr fehleranfällig. Darüber hinaus wird von den Ärztinnen und Ärzten kritisiert, daß die Angaben aufgrund des ICD-10-Codes sehr viel detaillierter sind als die bisher vorgenommenen Datenübermittlungen und damit im Ergebnis die Gefahr des "gläsernen Patienten bzw. Versicherten" bestehe. Vielen dieser aus medizinischer Sicht vorgetragenen Kritikpunkte konnte ich mich aus datenschutzrechtlicher Sicht anschließen. Die Verfassungsbeschwerde zweier Ärzte gegen die Verwendung des ICD-10-Codes hat das BVerfG wegen unzureichender Begründung nicht zur Entscheidung angenommen (BVerfG, NJW 1996, 771).

Zwischenzeitlich wurde von den Bundesverbänden der Krankenkassen, der Kassenärztlichen Bundesvereinigung und der Deutschen Krankenhausgesellschaft eine Rahmenvereinbarung abgeschlossen. Nach dieser Vereinbarung soll der seit dem 1. Januar 1996 im ambulanten Bereich vorgeschriebene Diagnoseschlüssel im Hinblick auf

Umfang und Feinheit der darin enthaltenen Diagnosen überprüft werden. Die Überprüfung soll Ende 1996 abgeschlossen sein. Im Jahr 1997 soll der Schlüssel in ausgewählten Krankenhäusern und Kassenärztlichen Vereinigungen im Hinblick auf die Praktikabilität unter wissenschaftlicher Begleitung erprobt werden. Nach fachlicher und rechtlicher Prüfung durch den Bundesminister für Gesundheit soll die überarbeitete Fassung des Diagnoseschlüssels zum 1. Januar 1998 verbindlich eingeführt werden. Die Datenschutzbeauftragten sollen an diesem Verfahren beteiligt werden.

19.9 Übermittlung von Sozialdaten an Behörden der Gefahrenabwehr

Immer wieder erreichen mich Zuschriften von Bußgeldstellen, die von den Krankenkassen die in § 68 SGB X genannten Daten erheben wollen. Von den Krankenkassen wird dies häufig unter Datenschutzgesichtspunkten abgelehnt.

Wenn es sich bei der anfordernden Kommune um eine Behörde der Gefahrenabwehr handelt, ist eine Datenübermittlung nach § 68 Abs. 1 Satz 1 1. Alternative SGB X zulässig. Zwar beeinträchtigt die Übermittlung die Interessen der Betroffenen; schutzwürdig sind diese jedoch offenkundig nicht. Vor den Folgen eines ordnungswidrigen Verhaltens wird der Betroffene durch § 68 SGB X grundsätzlich nicht geschützt. Eine Beeinträchtigung schutzwürdiger Interessen kann sich nur bei besonderen Umständen im Einzelfall ergeben, wenn die mit der Übermittlung verbundene Verletzung der Vertraulichkeit als unangemessen zu bewerten ist. Da die Übermittlung aber nur zur Erfüllung von Aufgaben der Behörden der Gefahrenabwehr erfolgen darf, ist die Nutzung der übermittelten Daten für die Durchführung von OWi-Ermittlungen gegen die Betroffenen nicht zulässig. Die Ahndung von Ordnungswidrigkeiten ist eine Sanktion für begangenes Verwaltungsunrecht. Sie dient nicht mehr der Gefahrenabwehr, kann damit nicht als Aufgabe der Gefahrenabwehrbehörde angesehen werden und fällt somit nicht unter § 68 Abs. 1 Satz 1 1. Alternative SGB X. Eine Übermittlung kommt deshalb nur nach der 2. Alternative der genannten Vorschrift in Betracht, wenn es um die Beitreibung eines Bußgeldes von mindestens 1.000 DM geht.

Zur Auslegung des § 68 SGB X weise ich im übrigen noch auf folgendes hin: Zu den Aufgaben der Gefahrenabwehrbehörde gehört nach meiner Einschätzung auch der Einsatz der in § 65 NGefAG genannten Zwangsmittel Ersatzvornahme, Zwangsgeld und unmittelbarer Zwang. Denn diese Mittel sind als Beugemittel (vgl. § 65 Abs. 3 NGefAG) dazu bestimmt, einen angestrebten ordnungsgemäßen Zustand wiederherzustellen. Sie dienen damit jedenfalls mittelbar der Gefahrenabwehr. Nach meinem Verständnis sind deshalb nicht nur die Androhung und die Festsetzung, sondern auch die Beitreibung eines Zwangsgeldes von § 68 Abs. 1 Satz 1 1. Alternative SGB X erfaßt.

Die 2. Alternative der Vorschrift sieht eine Datenübermittlung zur Durchsetzung öffentlich-rechtlicher Ansprüche, d.h. nur für

Vollstreckungszwecke, vor. Der Wortlaut der Vorschrift ist damit enger als z.B. in der vergleichbaren Bestimmung des § 39 Abs. 3 Nr. 1 StVG, wonach Fahrzeughalterdaten u.a. übermittelt werden dürfen, wenn der Empfänger sie zur Geltendmachung, Sicherung oder Vollstreckung von bestimmten öffentlich-rechtlichen Ansprüchen, die sich auf mindestens 1.000 DM belaufen, benötigt. Da im SGB nur die Vollstreckung angesprochen wird, bedeutet dies, daß die in § 68 SGB X genannten Daten nicht bereits für die Anhörung im Bußgeldverfahren oder die Festsetzung des Bußgeldes übermittelt werden dürfen. Es muß vielmehr bereits eine Vollstreckungsgrundlage vorhanden sein, ehe zur Durchsetzung der Forderungen eine Datenübermittlung in Betracht kommen kann. Das Niedersächsische Sozialministerium teilt diese Rechtsauffassung.

Die Übermittlung der derzeitigen Arbeitgeberanschrift ist auch dann zulässig, wenn die Fahrerlaubnis mit rechtskräftigem Urteil entzogen wurde und die Verkehrsbehörde die zwangsweise Einziehung dieser Führerscheine vornimmt. Voraussetzung ist aber, daß die Behörde nachweist, daß bereits andere Versuche zur Ermittlung des Aufenthaltsortes des Betroffenen fehlgeschlagen sind bzw. diese Angaben auf andere Weise nicht beschafft werden können.

19.10 Fremdbefunde für gutachtliche Stellungnahmen des Medizinischen Dienstes

Soweit es für gutachtliche Stellungnahmen und Prüfungen erforderlich ist, die von den Krankenkassen nach § 275 Abs. 1 bis 3 SGB V beim Medizinischen Dienst (MDK) veranlaßt werden, sind die Leistungserbringer - also auch die niedergelassenen Ärztinnen und Ärzte - verpflichtet, Sozialdaten auf dessen Anforderung hin unmittelbar an den MDK zu übermitteln. Man geht inzwischen überwiegend auch davon aus, daß der in Satz 2 des § 276 Abs. 2 SGB V verwendete Begriff "Sozialdaten" ein Redaktionsversehen des Gesetzgebers darstellt und im Sinne von "Patientendaten" bzw. "Versichertendaten" zu interpretieren ist. Auch bin ich der Auffassung, daß durch diese Vorschrift nicht nur die Übermittlung selbst erhobener Daten legitimiert wird, sondern auch die Übermittlung von Fremdbefunden, Krankenhausberichten, Stellungnahmen von Kurkliniken und sonstigen ärztlichen Angaben. Soweit Fremdbefunde in die Entscheidung der Leistungserbringer (Ärztinnen und Ärzte) eingeflossen sind, sind diese untrennbarer Bestandteil der Behandlung und der dazugehörigen Aufzeichnungen und Dokumentationen des jeweiligen Leistungserbringers.

19.11 Ärgerlich: Die sprechende Mitgliedsnummer der Ärzteversorgung

Ein Arzt wies mich im August 1994 darauf hin, daß die von der Ärztekammer geführte Ärzteversorgung Niedersachsen Mitgliedsnummern benutzt, in denen das Geburtsdatum enthalten ist. Seit Jahren vertrete ich die Ansicht, daß derartige sprechende Ordnungsmerkmale vermieden werden sollten (vgl. X 15.15), da diese

Ähnlichkeit mit dem ursprünglich vorgesehenen, aber aus verfassungsrechtlichen Gründen abgelehnten bundeseinheitlichen "Personenkennzeichen" haben. Die Ärztekammer rechtfertigte sich mit dem Verweis auf die ähnliche Gestaltung der Rentenversicherungsnummer (§ 147 SGB VI). Abgesehen von dem einmaligen Umstellungserfordernis konnten auch dort keine Gründe für die Notwendigkeit einer "sprechenden Nummer" vorgebracht werden. Um den Mißbrauch der Rentenversicherungsnummer zu verhindern, bedurfte es flankierender Regelungen und Maßnahmen (vgl. z.B. § 290 SGB V, § 18 f. SGB IV). Das von mir eingeschaltete Niedersächsische Sozialministerium teilte meine Bewertung, daß es für die Verwendung der Geburtsdaten in der Mitgliedsnummer einer ausdrücklichen gesetzlichen Grundlage bedarf (§ 4 Abs. 1 NDSG) und daß hierfür keine Erforderlichkeit gemäß § 10 Abs. 1 NDSG besteht.

Obwohl ich bei derartigen Gesetzesverstößen nach § 23 NDSG verpflichtet bin, eine Beanstandung auszusprechen, verzichtete ich hierauf in der Hoffnung auf eine einvernehmliche Lösung. Diese glaubte ich im Juni 1995 gefunden zu haben, als die Ärztekammer ihre Bereitschaft signalisierte, die Geburtsangaben der bestehenden Mitgliedsnummern zu verfremden. Dies sollte gemäß meinem Vorschlag in der Form erfolgen, daß der Geburtstag verdreifacht, der Geburtsmonat vervierfacht und das Geburtsjahr verdoppelt würde. Eine solche einfache Verschlüsselung hätte zumindest verhindert, daß Personen, die ohne Zusatzwissen Kenntnis von der Mitgliedsnummer erhalten, Rückschlüsse daraus ziehen können. Eine Umstrukturierung der Daten und Akten wäre nicht nötig gewesen. Äußerst verwundert war ich, als mir die Ärzteversorgung im September 1995 mitteilte, es solle nicht entsprechend der Absprache verfahren werden, da Umstellungskosten in Höhe von 400.000 DM entstehen würden (Umprogrammierung, Neubeschriftung von 60.000 Akten, Information der Mitglieder).

Anfang 1996 erfuhr ich dann, daß der Sozialausschuß des Landtags, abweichend von der Vorlage der Landesregierung, bei den Beratungen zum Kammergesetz für die Heilberufe beschlossen hat: "Die Satzung kann eine Mitgliedsnummer vorsehen, die das Geburtsdatum enthält". Ich wandte mich sofort an den Ausschuß und erläuterte die Problematik. Aufgrund meiner Prüferfahrung weiß ich, daß es immer wieder zur Weitergabe von Mitgliedsnummern an Dritte kommt, z.B. bei der Adressierung von Schreiben, oder wenn Mitgliedsnummern enthaltende Unterlagen anderen Stellen vorgelegt werden müssen (z.B. Kopien von Banküberweisungen und Bescheinigungen). Die ungewollte und unnötige Kenntnisgabe des Geburtsdatums kann nur vermieden werden, wenn eine nichtsprechende Mitgliedsnummer gewählt wird. Das Kostenargument war für mich nicht nachvollziehbar. Es ist kaum vorstellbar, daß die von mir vorgeschlagene Umstellung Kosten in der genannten Höhe verursacht hätte.

Weder durch die Ärzteversorgung noch im Landtagsausschuß wurde auf meine Argumente, auch nicht auf meine Zweifel bezüglich der Kosten, eingegangen. Ohne weitere Diskussion wurde dem Wunsch der Ärztekammer entsprochen. Sicher: Es gibt Wichtigeres als die

Mitgliedsnummern eines Versorgungswerks für Ärztinnen und Ärzte. Das Erforderlichkeitsprinzip als Bestandteil des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit findet aber auch in Nebenpunkten Anwendung. Ich bedauere, daß der Gesetzgeber einen jahrelangen datenschutzwidrigen Zustand einfach dadurch beendet, daß er ihn für zulässig erklärt. Die gesetzliche Zulassung sprechender Ordnungsnummern kann meines Erachtens eine unheilvolle Eigendynamik entwickeln. Unter Berufung auf entsprechende Regelungen könnten sich immer mehr Verwaltungen veranlaßt sehen, ohne Not derartige sprechende Nummern zu fordern.

20. Gesundheit

20.1 Gesetzgebung

Ich müßte es eigentlich leid sein, gesetzliche Grundlagen für die Datenverarbeitung im Gesundheitswesen einzufordern. Allzu lang blieben meine seit 1984 vorgetragenen Aufforderungen ohne sichtbare Reaktion (vgl. zuletzt XII 21.1 und 21.2). Vor zwei Jahren schien dann Bewegung ins politische Geschehen gekommen zu sein: Sowohl die Arbeiten für ein Gesetz über Hilfen für psychisch Kranke und Schutzmaßnahmen (PsychKG) wie eines Niedersächsischen Gesundheitsdienstgesetzes (NGDG) wurden auf den Weg gebracht. Das PsychKG wird nunmehr - schon seit September 1994 - vom zuständigen Gesundheitsausschuß des Landtags beraten. Das Niedersächsischen Sozialministerium rechnet damit, daß die Beratungen bis zum Ende der Legislaturperiode abgeschlossen sein werden.

Hoffnungen hatte ich auch bzgl. des geplanten NGDG. Erste Vorarbeiten dafür gab es im Sozialministerium schon 1984. In der Koalitionsvereinbarung 1990 zwischen der SPD und den Grünen war das Gesetzesprojekt aufgeführt. 1993 lag dann ein erster Referentenentwurf vor. Nicht wenig erstaunt war ich, als ich Mitte 1996 in der Zeitung las, man wolle im Interesse der finanziellen Entlastung der Kommunen auf das NGDG in der laufenden Legislaturperiode verzichten. Ich wies gegenüber dem Niedersächsischen Sozialministerium darauf hin, daß Regelungen zur ärztlichen Schweigepflicht zwecks Gewährleistung des Vertrauensverhältnisses zwischen Hilfesuchenden und Helfenden dringlich sind, daß die europäische Datenschutzrichtlinie ein Handeln erforderlich macht und daß die Datenschutzregelungen im Gesundheitssektor weitgehend kostenneutral sind. Ein längeres Hinausschieben sei nicht zu verantworten. Ich schlug vor, die Datenschutzregelungen von evtl. kostenintensiven Gesetzesteilen zu entkoppeln, so wie dies in Nordrhein-Westfalen mit einem Gesundheitsdatenschutzgesetz der Fall war. Die Antwort des Ministeriums war kurz: Die Arbeiten am NGDG seien eingestellt worden - und dabei bleibe es auch. Es sei einiges geleistet worden: Ein Heilkammergesetz (vgl. 19.11), der Entwurf des PsychKG, Vorbereitungen zum Landeskrebsregister (vgl. XII 21.5) und ein Vorentwurf eines Gesetzes zum Leichen- und Friedhofswesen. Das Vorhaben NGDG sei lediglich verschoben worden.

20.2 Einblick des Rechnungshofes in Patientenakten

Mit der Frage, ob der Rechnungshof zu Prüfungszwecken in Patientenakten Einblick nehmen darf, beschäftige ich mich immer wieder. Zwei Professoren einer niedersächsischen Universitätsklinik

führten seit 1982 einen Rechtsstreit mit dem Landesrechnungshof, der nach einer für sie negativen Entscheidung des Bundesverwaltungsgerichts im Jahre 1989 (CR 1989, 1112 ff.) als Beschwerde beim BVerfG anhängig wurde. Im Rahmen dieses Verfahrens habe ich gegenüber dem BVerfG eine Stellungnahme abgegeben. Am 29. April 1996 beschloß nun das höchste deutsche Gericht, daß dem Rechnungshof ein Prüfrecht in Patientenakten zusteht. Von einer freien Entscheidungsmöglichkeit für den Rechnungshof, wo und wie er Einblick in die Unterlagen nehmen will, kann aber keine Rede sein. Das BVerfG stellte vielmehr klar, daß sich der verfassungsrechtlich verankerte Untersuchungsauftrag des Rechnungshofes (Art. 70 Niedersächsische Verfassung) und der grundrechtlich verbürgte Datenschutz gleichrangig gegenüberstehen. Je nach den Umständen des Einzelfalles muß eine Abwägung erfolgen. Nur wenn die Wirksamkeit der Kontrolle gefährdet würde, darf der Zugriff auf geheimhaltungsbedürftige Unterlagen erfolgen. Dem Geheimnisschutz muß dann aber durch Schutzvorkehrungen gegen eine zweckwidrige Weitergabe der Informationen Rechnung getragen werden. Der Entscheidung ist die Empfehlung zu entnehmen, die Aktenführung und Abrechnung so zu gestalten, daß eine Finanzprüfung ohne Einblick in die sensiblen medizinischen Angaben möglich ist (RDV 1996, 184).

20.3 Auswertung von Patientenunterlagen für "Verwaltungszwecke"

Aus der Ärzteschaft eines kommunalen Krankenhauses wurde ich gefragt, ob für betriebswirtschaftliche Prüfungen die Vorlage kompletter Patientenakten, OP-Journale u.ä. bei der Verwaltung des Hauses zulässig ist. In der jüngeren Vergangenheit war eine Nachkalkulation erfolgt, die sich auf Diagnosen bezog, welche zukünftig über Fallpauschalen bzw. Sonderentgelte abzurechnen sind. Einige Ärzte waren in Sorge, mit dieser Vorgehensweise gegen die ärztliche Schweigepflicht zu verstoßen. Auch ich hatte Zweifel, ob für die Nachkalkulation patientenbezogene Unterlagen herangezogen werden können.

Das Krankenhaus hielt es dagegen für nötig, im Hinblick auf das neue Abrechnungsverfahren im Krankenhausbereich Kalkulationen "am praktischen Fall", d.h. auf der Grundlage tatsächlich durchgeführter Patientenbehandlungen durchzuführen. Die dafür erforderlichen Patientenunterlagen waren nicht "der Verwaltung" des Krankenhauses vorgelegt worden, sondern ausschließlich einer besonders für die Aufgabe eingesetzten Gruppe mit einer Diplombetriebswirtin, einer Diplom-Kauffrau und einem Assistenzarzt. Diese Bediensteten waren zuvor auf die Bestimmungen des Datenschutzes hingewiesen und schriftlich zur Verschwiegenheit verpflichtet worden. Es war sichergestellt, daß weder die Leitung des Hauses noch anderes Krankenhauspersonal Einsicht in die Akten erhielt. Diese wurden ausschließlich im räumlichen Bereich des Krankenhauses genutzt.

Nach Ansicht der Rechtsprechung ist die ärztliche Schweigepflicht von liquidationsberechtigten Krankenhausärztinnen und -ärzten gewahrt, wenn diese ihr Honorar durch das Krankenhaus einziehen lassen. Die

Abrechnung erfolgt innerhalb des überschaubaren Bereiches des Krankenhauses, das insoweit an die Stelle der ärztlichen Praxis tritt. Die für die Abrechnung zuständigen Bediensteten unterliegen gemäß § 203 StGB ebenfalls der Schweigepflicht. Diese Rechtsprechung ist hier übertragbar. Für die Assistenzärztinnen und -ärzte ist die Errechnung der Fallpauschalen selbst regelmäßig nicht leistbar. Die vom Krankenhaus bestimmten Mitarbeiterinnen und Mitarbeiter der betriebswirtschaftlichen Abteilung sind als Hilfspersonen anzusehen, die im Rahmen des Erforderlichen zur Kenntnisnahme von Patientendaten befugt sind. Es gehört zum sozialen Geschehen eines Krankenhauses, daß das Arzt-Patienten-Verhältnis als eine in sich geschlossene Einheit nicht existiert. Bei Inanspruchnahme des Krankenhauses hat man es zwangsläufig mit einer hochgradig arbeitsteiligen Organisation zu tun.

20.4 Übersendung ärztlicher Berichte an Aufnahmeeinrichtungen

Der Geschäftsführer einer Behinderteneinrichtung erhielt von einem niedersächsischen Landeskrankenhaus (Fachkrankenhaus für Psychiatrie und Psychotherapie) Arztberichte einiger Patientinnen und Patienten dieses Hauses zugesandt. Im Rahmen der Eingliederungshilfe nach den §§ 39, 40 BSHG wurden für die betroffenen Personen Aufnahmeeinrichtungen in und außerhalb Niedersachsens gesucht. Die Berichte enthielten Angaben zu Anamnese, psychischen Befunden und diagnostischen Bewertungen. Von den Betroffenen bzw. deren Betreuungspersonen waren offensichtlich Entbindungen von der ärztlichen Schweigepflicht zur Legitimation der Versendung der Unterlagen an Betreuungseinrichtungen eingeholt worden. Auch wenn hier Einwilligungen vorlagen, bin ich der Ansicht, daß die ärztlichen Berichte den in Frage kommenden Einrichtungen ohne die personenidentifizierenden Angaben zur Verfügung gestellt werden sollten. Für die Entscheidung, ob ein geeigneter Heimplatz zur Verfügung steht, werden diese Daten nicht benötigt. Das Landeskrankenhaus ist meiner Empfehlung gefolgt. Bei künftigen Anfragen werden nur noch anonymisierte ärztliche Berichte mitgeschickt.

20.5 Ungeklärt: Wie gelangte die Psychiatrieakte zur Zeitungsredaktion?

Der Patient eines niedersächsischen Landeskrankenhauses hatte mich darüber unterrichtet, daß Kranken- und Gerichtsunterlagen aus dem Verfügungsbereich der Einrichtung bei der Redaktion einer Zeitung in Hamburg eingegangen waren. Die Unterlagen wurden dort vertraulich behandelt und schließlich von einem Mitarbeiter des Niedersächsischen Sozialministeriums in Empfang genommen.

Die Recherchen des Ministeriums ergaben, daß die Unterlagen anonym per Post an die Zeitung gesandt worden waren. Die vor Ort im Krankenhaus geführten Gespräche konnten keine Klärung herbeiführen, wer für die Versendung verantwortlich war. Als Motiv für das Versenden der Unterlagen an die Presse hielt das Ministerium für denkbar, daß dem betroffenen Landeskrankenhaus bzw. dessen Fachabteilung

geschadet werden sollte. Da die Unterlagen stets im verschlossenen Dienstzimmer aufbewahrt würden, könnte lediglich jemand, der im Besitz eines entsprechenden Schlüssels ist, an diese gelangt sein. Konkrete Anhaltspunkte ließen sich bei dem in Frage kommenden Personenkreis nicht ermitteln.

Der Betroffene hatte bei der zuständigen Staatsanwaltschaft eine Strafanzeige gegen Unbekannt erstattet. Als Sofortreaktion wurden in einem Runderlaß alle niedersächsischen Landeskrankenhäuser zum Aufbewahren von Krankenunterlagen wie folgt angewiesen: "Aus gegebenem Anlaß weise ich darauf hin, daß die Krankenblattunterlagen stationär untergebrachter Patienten auch in den abschließbaren Zimmern der Ärzte/Ärztinnen bzw. Therapeuten/Therapeutinnen unter gesondertem Verschluß aufzubewahren sind. Ich bitte um Vollzug dieser Weisung und schriftliche Bestätigung ..., daß entsprechend verfahren wird."

Besonders hervorzuheben ist, daß die Zeitungsredaktion sich ausgesprochen datenschutzfreundlich verhalten hat und mich einschaltete, statt skandalisierend zu berichten.

20.6 Tonträgerkontrolle bei Krankentransporten

Aufgrund eines Beschlusses des Verwaltungsgerichts Hannover war eine Stadtverwaltung gehalten, die Durchführung qualifizierter Krankentransporte durch ein privates Unternehmen im Umfang der in der Vergangenheit erteilten und auf § 49 Beförderungsgesetz gestützten Genehmigung zu dulden. Dem Unternehmen wurde eine Reihe von Auflagen erteilt. Zu diesen gehörte, daß alle dort eingehenden Gespräche mittels Tonträger aufzuzeichnen waren. Die Tonträger sollten mindestens drei Monate aufbewahrt und jeweils monatlich der Verwaltungsbehörde vorgelegt werden. Damit hätte die Kommune nicht nur Daten über das Transportunternehmen, sondern auch in einem Übermaß Krankendaten erhalten. Die Auflage war auch nicht durch § 24 des Niedersächsischen Rettungsdienstgesetzes abgedeckt. Die Stadt änderte aufgrund der von mir geäußerten Bedenken die Duldungsverfügung und verlangt die Vorlage von Tonträgeraufzeichnungen nur noch im Einzelfall im Rahmen der konkreten Ausübung der Aufsichts- und Kontrollbefugnisse.

21. Kinder- und Jugendhilfe

21.1 Kinder- und Jugendhilfedaten als Basis zur Berechnung von Sozialleistungen?

Eine Kommune teilte mir folgendes mit: Eine Mutter habe im Antrag auf Übernahme des Elternbeitrages für eine Kindertagesstätte gegenüber dem Jugendamt angegeben, sie erhalte für ihr Kind Unterhaltsvorschuß. Zugleich teilte sie mit, daß sie mit dem Kindesvater in eheähnlicher Gemeinschaft lebe. Aus diesen Angaben läßt sich schließen, daß der Unterhaltsvorschuß zu Unrecht gezahlt wird. Der betroffene Landkreis warf nun die Frage auf, ob die Mitteilung der Angaben der Kindesmutter über die eheähnliche Gemeinschaft mit dem Kindesvater vom Sachgebiet "Kindertagesstätten" an das Sachgebiet "Unterhaltsvorschuß" zulässig ist. Und: Dürfen die Daten wegen der Annahme, daß die eheähnliche Gemeinschaft bei der Berechnung des Wohngeldes nicht berücksichtigt wurde, auch an die Wohngeldstelle übermittelt werden?

Die bereichsspezifischen Vorschriften für die Träger der Jugendhilfe (§§ 64 f. SGB VIII) verschärfen den auch im Sozialdatenschutz geltenden Grundsatz der Zweckbindung. Während dieser Grundsatz in § 69 Abs. 1 Nr. 1 SGB X für eine Übermittlung an andere Sozialleistungsträger gelockert ist, sind die Träger der Jugendhilfe nach § 64 Abs. 1 SGB VIII strikt darauf verwiesen, Sozialdaten nur zu dem Zweck zu übermitteln, zu dem sie erhoben worden sind. Damit scheidet - auch nach Meinung des Niedersächsischen Kultusministeriums sowie des Niedersächsischen Innenministeriums - eine Datenübermittlung aus. Es bleibt nur der Weg, daß eine Stelle eines Jugendhilfeträgers, die konkrete Hinweise auf eine andere zu Unrecht bezogene Sozialleistung erhält, den Empfänger hierauf anspricht und ihn auffordert, sich deswegen an den anderen Leistungsträger zu wenden.

21.2 Und wie steht es mit vertraulichen Informationen?

Es kommt vor, daß der kommunale Sozialdienst von Klientinnen bzw. Klienten vertrauliche Informationen erhält (z.B. über das Verlassen der elterlichen Wohnung), die auch für die Sozialhilfe benötigt werden. Dürfen die Angaben für die Bearbeitung eines Sozialhilfeantrags genutzt werden?

Zunächst ist festzustellen, daß hier die Datenempfänger im datenschutzrechtlichen Sinne Dritte sind, die Weitergabe also eine Übermittlung wäre. Dies kann auch innerhalb eines Amtes oder einer Abteilung der Kommunalverwaltung der Fall sein. Dritter ist jede Person oder Stelle außerhalb der speichernden Stelle (§ 67 Abs. 10 SGB X);

speichernde Stelle aber sind bei Gebietskörperschaften die Organisationseinheiten, die eine Aufgabe nach einem der besonderen Teile des SGB funktional durchführen (§ 67 Abs. 9 Satz 3 SGB X). Die Stelle, deren Aufgabe die Beratung entwichener Kinder und Jugendlicher ist, und die Stelle, die über Hilfe zum Lebensunterhalt entscheidet, sind verschiedene Stellen, auch wenn sie demselben Amt für Jugend und Soziales angehören. Es gelten also die Bestimmungen über die Übermittlung von Sozialdaten. Auch hier gilt: Während der Zweckbindungsgrundsatz in § 69 Abs. 1 Nr. 1 SGB X für eine Übermittlung an andere Sozialleistungsträger gelockert ist, sind die Träger der Jugendhilfe nach § 64 Abs. 1 SGB VIII strikt darauf verwiesen, Sozialdaten nur zu dem Zweck zu übermitteln, für den sie erhoben worden sind. Eine weitere Einschränkung enthält § 64 Abs. 2 SGB VIII. Wenn schließlich die Voraussetzungen des § 65 SGB VIII vorliegen, die Informationen also einem Mitarbeiter oder einer Mitarbeiterin des Jugendhilfeträgers im Rahmen einer persönlichen Helferbeziehung anvertraut worden sind, ist eine Übermittlung ohne Einwilligung des Anvertrauenden nahezu ausgeschlossen.

21.3 Auskünfte an die Polizei

Immer wieder werde ich mit der Frage konfrontiert, ob vom Jugendamt oder von einem Sozialdienst einer Kommune gewonnene Erkenntnisse über Mißhandlungen von Schutzbefohlenen auf Anforderung der Polizei übermittelt werden dürfen. Dazu stelle ich in Übereinstimmung mit dem Niedersächsischen Kultusministerium fest, daß der Sozialdienst des Jugendamtes die Informationen, über die er verfügt, nur für eine Lösung des Problems mit sozialpädagogischen Mitteln nutzen darf und muß. Er darf sie nicht für Zwecke der Strafverfolgung zur Verfügung stellen. Allerdings kommt in einem "besonders schweren Fall" der Mißhandlung von Schutzbefohlenen (§ 223 b Abs. 2 StGB) eine gerichtliche Anordnung zur Datenübermittlung in Betracht. Sie ist seit dem Inkrafttreten der Neufassung des § 73 SGB X ab 1. Juli 1994 nicht nur zur Durchführung eines Strafverfahrens wegen eines Verbrechens, sondern auch wegen einer "Straftat von erheblicher Bedeutung" zulässig.

Sofern die Beantwortung der von der Polizei gestellten Fragen im Einzelfall im Interesse der Familienangehörigen liegt, kann der Sozialdienst versuchen, die Einwilligung aller Betroffenen in die Auskunftserteilung einzuholen.

22. Forschung

Auf Bundesebene unternahmen einige Forschungsinteressenverbände Anstrengungen, das Gleichgewicht zwischen Forschungsfreiheit und Datenschutz zu Lasten des letzteren zu verschieben. Besonders tat sich eine "Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften" (AWMF) mit ihrer Forderung nach Einführung eines medizinischen Forschungsgeheimnisses hervor. Derartige Bestrebungen fänden meine volle Unterstützung, ginge es darum, die oft hochsensiblen und streng zweckgebundenen Forschungsdaten vor dem Zugriff Dritter zu bewahren. Darum geht es aber der AWMF nur in zweiter Linie. In erster Linie besteht deren Ziel darin, "unverantwortliche Blockaden medizinischer Forschung" durch den Datenschutz zu beseitigen. Handfeste Belege, daß der Datenschutz in unverantwortlicher Weise wichtige wissenschaftliche Vorhaben verhindert hätte, konnten bis heute nicht vorgelegt werden. Daher trat ich den teilweise äußerst unsachlich vorgetragenen Argumenten der AWMF entgegen. Nicht erbaut war ich, als wenig später die renommierte Deutsche Forschungsgemeinschaft (DFG) in dasselbe Horn wie die AWMF stieß.

Mein Ziel ist es ebenso wie das meiner Kolleginnen und Kollegen im Bund und in den Ländern, mit den Forschenden in einen Dialog zu treten und beiden Seiten gerecht werdende Lösungen zu finden. Meine Erfahrung ist, daß die gegen den Datenschutz vorgetragenen Argumente weitgehend auf Unkenntnis des Datenschutzrechts und auf Unverständnis beruhen. Ich gehe davon aus, daß bei Wissenschaftlerinnen und Wissenschaftlern die vorgenannten Defizite durch Information und Argumente behoben werden können. Die Datenschutzbeauftragten des Bundes und der Länder sind zu Erläuterungen und Hilfen bereit.

In Niedersachsen gibt es keinen Konflikt zwischen Forschenden und meiner Dienststelle. Die Forschungsklausel des § 25 NDSG hat sich als sachgerecht und praktikabel erwiesen (vgl. XII 24.1). Die Pflicht, mir bei konkreten Projekten das Ergebnis der Abwägung zwischen Forschungs- und Betroffeneninteresse mitzuteilen, führte in vielen Fällen dazu, daß datenschutzrechtliche Defizite, insbesondere bei der Datensicherheit, bei der frühestmöglichen Anonymisierung und beim Einholen von Einwilligungen behoben werden konnten. Ich habe ein kleines Merkblatt herausgegeben, in dem die Anwendung des § 25 NDSG erläutert wird. Trotz meiner Informationstätigkeit habe ich den Eindruck, daß entgegen der zwingenden Vorschrift von § 25 Abs. 2 und 7 NDSG viele anzeigepflichtigen Forschungsvorhaben nicht mitgeteilt werden. Dies kann für ein Forschungsvorhaben fatale Konsequenzen haben. Stellt sich erst im Rahmen der Durchführung eines Projektes heraus, daß dessen "Design" gegen Datenschutzbestimmungen

verstößt, so kann dies zum Scheitern des gesamten Projektes führen; bis dahin können viel Arbeit und viel Geld umsonst investiert worden sein.

23. Hochschulen

Seit Ende 1993 finden in Niedersachsen regelmäßig Tagungen der Datenschutzbeauftragten der Hochschulen statt, an denen auch meine Dienststelle beteiligt ist. Diese Tagungen dienen dem Informations- und Erfahrungsaustausch, der Diskussion gemeinsamer Probleme und der Absprache von Maßnahmen zur Durchsetzung des Datenschutzes. Gegenstand der gemeinsamen Erörterung waren u.a.

- die Evaluation des Hochschulangebots (vgl. XII 25.1),

- die datenschutzgerechte elektronische Abwicklung von Globalhaushalten,

- die Zulassung von Forschungsvorhaben mit personenbezogenen Daten (vgl. 22),

- Datenschutz im Internet (23.1),

- Computerdiebstahl und Hacking an den Hochschulen und

- die Mitteilung über abgelehnte Promotionsvorhaben (23.2).

23.1 Telefon- und Vorlesungsverzeichnisse im Internet?

Alles drängt ins Internet. Da wollen die Hochschulen nicht zurückstehen, zumal das Internet ehedem vorrangig ein Wissenschaftsnetz war. Dabei geht es den Hochschulen nicht nur um den Austausch wissenschaftlicher Ergebnisse oder um allgemein gehaltene Selbstdarstellungen. Mit Hilfe des Internets soll weltweit in Erfahrung gebracht werden, was vor Ort in Wissenschaft und Lehre geboten wird, wer an welchem Thema gerade arbeitet. Hiergegen ist grundsätzlich nichts einzuwenden. Doch muß wegen der Offenheit des eingesetzten Mediums der Datenschutz beachtet werden. Nachdem aus allen Ecken des Landes Anfragen bei mir eingingen, habe ich zur Frage der Veröffentlichung von Telefon- und Vorlesungsverzeichnissen im Internet ausführlich Stellung genommen. Ich habe klargestellt, daß gegen eine interne Verbreitung des Fernsprechverzeichnisses einer Hochschule, evtl. auch in elektronischer Form, keine Bedenken bestehen, ebensowenig gegen die Veröffentlichung eines Vorlesungsverzeichnisses in Buchform, soweit nur Daten von Beschäftigten aufgenommen werden, die im Rahmen ihrer Dienstausübung Kontakt nach außen haben. Für die Aufnahme privater Adressen und Telefonnummern besteht jedoch grundsätzlich keine Notwendigkeit. Ohne Einwilligung der Betroffenen darf insofern eine Veröffentlichung nur erfolgen, wenn die Bediensteten außerhalb

der Dienstzeiten erreichbar sein müssen. Für die Veröffentlichung personenbezogener Beschäftigten- und Studierendenangaben im Internet sehe ich überhaupt keine Notwendigkeit. Daher bedarf es hierfür jeweils der Einwilligung der Betroffenen. Diese zu erhalten, dürfte bei einem entsprechenden Interesse der Betroffenen regelmäßig auch kein Problem sein.

Das Niedersächsische Ministerium für Wissenschaft und Kultur und die Hochschulen habe ich über die Rechtslage unterrichtet. Mir wurde signalisiert, daß meine Vorgaben - trotz zunächst bestehender weitergehender Planungen - beachtet werden sollen. In jüngster Zeit sind mir auch keine Beschwerden mehr vorgetragen worden.

23.2 Warnung vor dem erfolglosen Doktoranden

Einige Hochschullehrer haben die Angewohnheit, mit Hilfe von Faxen ihren Kolleginnen und Kollegen über das endgültige Scheitern von Promotionsvorhaben bundesweit Mitteilung zu machen. Damit sollen die Betroffenen daran gehindert werden, sich mit demselben Thema und derselben Arbeit an einem anderen Fachbereich zu bewerben. Das Niedersächsische Ministerium für Wissenschaft und Kultur sah hierin zunächst nichts Verwerfliches. Dieses Mitteilungswesen entspräche den Besonderheiten des weltweit öffentlichen Wissenschaftsbetriebes. Dem kann ich nicht beipflichten.

Für derartige Vorratsdatenübermittlungen gibt es keine Rechtsgrundlage. Außerdem erscheinen mir diese zur Erreichung des verfolgten Zieles ungeeignet: Nur wenige abgelehnte Promotionen werden an einer anderen Hochschule erneut vorgelegt. Diesen kann der Doktorvater bei der Befragung über den wissenschaftlichen Werdegang zumeist problemlos auf die Spur kommen. Außerdem dürfte der Warneffekt der Mitteilungen gering sein, da diese nicht dateimäßig vorgehalten, sondern weggelegt werden und bald in Vergessenheit geraten. Ich habe nun erfahren, daß die Hochschulrektorenkonferenz die Absicht verfolgt, ein Zentralregister für Dissertationen anzulegen. Hiergegen habe ich keine Einwände, wenn damit die Doppelbelegung von Themen verhindert werden soll - eine Namensnennung ist dafür nicht erforderlich. Sollen in einer solchen Datei personenbezogene Daten gespeichert werden, so ist ein Gesetz notwendig. Die Meinungsbildung ist hier auf Ministeriumsebene noch nicht abgeschlossen.

23.3 "Akten mit Sexopfern in Unibibliothek"

Mit dieser Überschrift wurde in einer niedersächsischen Zeitung über folgenden Vorgang berichtet: Ein Lehrbeauftragter des Fachbereichs Psychologie machte in einer Universitätsbibliothek Interessierten Auszüge aus psychologischen Gutachten öffentlich zugänglich. Bei den Gutachten ging es um den sexuellen Mißbrauch von Kindern mit personenbezogenen Angaben über Tatverdächtige, mutmaßliche Opfer und andere Verfahrensbeteiligte als Teil einer Materialsammlung für Teilnehmerinnen und Teilnehmer eines Seminars über

"Zeugenglaubwürdigkeit". Im Vorwort der in dem jedermann zugänglichen Semesterapparat aufgestellten Materialsammlung machte der Lehrbeauftragte die Leserinnen und Leser darauf aufmerksam, daß in den zum Teil authentischen Materialien "ohne Absicht" Personen identifiziert werden könnten: "Ich verweise daher ausdrücklich auf die Gebote der Schweigepflicht, die entsteht, wenn man sich in wissenschaftlicher Zielsetzung mit individuellen Schicksalen auseinandersetzt". Zunächst kursierte in der Universität die Auffassung, die Sache sei unbedenklich, da die Akten in öffentlicher Gerichtsverhandlung benutzt worden seien. Dem mußte ich widersprechen.

Das Zugänglichmachen war eine Datenübermittlung der Universität an einen unbestimmten Kreis von privaten Personen nach § 13 NDSG. Für Lehrzwecke hätte es ausgereicht, die Unterlagen zu anonymisieren und den Zugriff hierauf auf die Studierenden zu beschränken. Es bestand zudem ein besonderes Geheimhaltungsinteresse, da psychologische Gutachter dem besonderen Berufs- und Amtsgeheimnis nach § 203 StGB unterliegen. Abwegig war die Überlegung, daß die in einer öffentlichen Gerichtsverhandlung benutzten Akten veröffentlicht werden dürften. Die Öffentlichkeit von Gerichtsverhandlungen nach § 169 GVG dient dem Informationsinteresse der Allgemeinheit, der öffentlichen Kontrolle der Justiz und dem Schutz vor Willkür. Dadurch wird aber der Persönlichkeitsschutz der Verfahrensbeteiligten nicht aufgehoben. Studierende unterfallen auch keiner besonderen wissenschaftlichen Schweigepflicht; für sie gilt wie für alle Angehörige der Universität nur das Datengeheimnis (§ 5 NDSG). Studierende genießen generell auch keine durch die Forschungsfreiheit (Art. 5 Abs. 3 GG) legitimierten Privilegien.

Sofort nach Bekanntwerden der Sache sind - so die Angaben der Universität - die Unterlagen aus dem Verkehr gezogen und nach vollständiger Anonymisierung wieder in den Semesterapparat gestellt worden. In der Hoffnung, daß sich ein solcher Datenschutzverstoß nicht wiederholt, sah ich von einer förmlichen Beanstandung ab. Das staatsanwaltliche Ermittlungsverfahren gegen den Lehrbeauftragten wurde gegen eine Geldauflage an den Kinderschutzbund eingestellt.

24. Schulen

24.1 Novellierung des Niedersächsischen Schulgesetzes

Der Entwurf eines Fünften Gesetzes zur Änderung des Niedersächsischen Schulgesetzes enthielt u.a. eine Änderung der Vorschriften über den Findungsausschuß (§ 46 NSchG). Der Findungsausschuß, in dem die Schulbehörde, die Schulgesamtkonferenz und der Schulträger vertreten sind, wirkt bei der Besetzung der Stellen von Schulleiterinnen und Schulleitern mit. Nach der Gesetzesbegründung soll künftig die Pflicht der Findungsausschußmitglieder zur Verschwiegenheit gegenüber den sie entsendenden Stellen hinsichtlich des Ergebnisses und Verlaufes der Beratungen nicht mehr gelten, weil Schule, Schulträger und Schulbehörde ein nachvollziehbares Interesse haben, zu erfahren, wie ein bestimmter Vorschlag zur Besetzung einer Schulleiterstelle zustande gekommen ist und wie die von ihnen entsandten nicht weisungsgebundenen Mitglieder abgestimmt haben.

Ich habe im Gesetzgebungsverfahren vorgeschlagen, ausdrücklich zu regeln, daß Unterlagen mit personenbezogenen Daten, die den Mitgliedern zur Verfügung gestellt werden, nach Abschluß des Findungsverfahrens an die Schulbehörde zurückzugeben sind. Da personenbezogene Daten zu löschen sind, wenn ihre Kenntnis für die datenverarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist, sind die den Ausschußmitgliedern zur Verfügung gestellten Unterlagen zu vernichten oder der Schulbehörde zurückzugeben, wenn die Arbeit des Findungsausschusses beendet wurde. Ich gehe davon aus, daß die Ausschußmitglieder sich dieser Löschungspflicht oft nicht bewußt sind. Es ist deshalb zu befürchten, daß mit den Unterlagen in nicht datenschutzgerechter Weise verfahren wird. Dies muß im Hinblick auf die Sensibilität der hier in Rede stehenden personenbezogenen Daten und angesichts der auch gegenüber den entsendenden Stellen bestehenden grundsätzlichen Schweigepflicht verhindert werden. Der von mir gemachte Vorschlag orientiert sich an der Regelung von § 61 Abs. 1 Niedersächsisches Personalvertretungsgesetz.

Der Vorschlag wurde von den Mitgliedern des Kultusausschusses des Landtags mehrheitlich abgelehnt. Der Ausschuß gelangte zu der Einschätzung, eine Rückgabeverpflichtung ergebe sich bereits aus allgemeinen Rechtsgrundsätzen. Das Niedersächsische Kultusministerium hat zugesagt, dieses Problem in Verwaltungsvorschriften anzusprechen. Dies ist bis heute nicht geschehen.

24.2 Erfassungsbogen für Schulabgänger

Vielfach werden von den Schulen sog. Erfassungsbogen für Schulabgängerinnen und Schulabgänger ausgefüllt. Diese Erfassung ist zur Überwachung der Schulpflichterfüllung erforderlich. Die Bogen enthalten oft eine Vielzahl von Daten, die nicht erforderlich sind und somit nicht weitergegeben werden dürfen. Der Umfang der personenbezogenen Daten von Schülerinnen und Schülern, die beim Übergang an eine andere Schule übermittelt werden dürfen, ist in § 2 der Verordnung über die Verarbeitung personenbezogener Daten von Schülerinnen und Schüler sowie ihrer Erziehungsberechtigten geregelt. Angaben zu dem zu erwartenden Abschluß, zu beabsichtigtem Schulbesuch in Vollzeitschulen, zu beabsichtigter betrieblicher Ausbildung oder betrieblichem Praktikum, zu beruflichen Interessen/Berufswunsch und zur Beratung durch das Arbeitsamt dürfen hiernach nicht übermittelt werden und werden auch zur Überwachung der Schulpflichterfüllung nicht benötigt. Auch die gesonderte Übermittlung des Namens der Klassenlehrerin oder des Klassenlehrers ist nicht erforderlich. Sollen die Daten für Planungszwecke verwendet werden, ist eine anonymisierte Übermittlung - ohne Angabe von Namen - ausreichend. Das Niedersächsische Kultusministerium hat sich dieser Rechtsauffassung angeschlossen und die Bezirksregierungen hierüber unterrichtet.

24.3 Zusammenarbeit zwischen Jugendamt und Schule

Schulen dürfen personenbezogene Daten einer Schülerin oder eines Schülers oder ihrer Erziehungsberechtigten an das Jugendamt übermitteln, soweit dies zur Erfüllung des Bildungsauftrags der Schule und der Fürsorgeaufgaben (§ 31 Abs. 2 NSchG) erforderlich ist.

Die Fürsorgeaufgaben der Schule sind nicht umfassend, sondern nur punktuell (z.B. Aufsichtspflicht nach § 62 NSchG) geregelt. Die Schülerinnen und Schüler sind zeitweise der Schule anvertraut. In dieser Zeit muß die Schule für sie sorgen, wenn sie der Hilfe bedürfen und diese von den Erziehungsberechtigten nicht geleistet werden kann. Das gilt z.B. bei Unfällen oder Erkrankungen in der Schule. Dies gilt auch, wenn einer Lehrkraft Problembelastungen einer Schülerin oder eines Schülers auffallen, die aus dem außerschulischen Bereich rühren. Die Fürsorgeaufgaben gebieten dann in erster Linie das Gespräch mit den Erziehungsberechtigten. Wenn jedoch der Eindruck besteht, daß so die notwendige Hilfe für das Kind nicht erreicht werden kann, kann auch eine Unterrichtung des Jugendamtes geboten sein, damit eine Gewährung von Hilfe zur Erziehung (§§ 27 ff. SGB VIII) geprüft wird. Die damit verbundene Übermittlung von personenbezogenen Daten ist durch § 31 Abs. 2 NSchG legitimiert.

Im Einzelfall hängt die Antwort auf die Frage, ob die Übermittlung von personenbezogenen Daten von der Schule an das Jugendamt zur Erfüllung einer Fürsorgeaufgabe der Schule erforderlich - und damit zulässig - ist, wesentlich davon ab, wie alle Beteiligten ihre Mitverantwortung für das Wohl des Kindes wahrnehmen. Eine pauschale abschließende Antwort hierauf kann nicht gegeben werden. Der Erlaß über "Zusammenarbeit zwischen Schule, Jugendamt und freien Trägern

der Jugendhilfe" vom 25. Januar 1994 (Nds. MBl. S. 335) betont deshalb und auch im Hinblick darauf, daß in diesem Zusammenhang in der Regel besonders sensible Daten berührt werden, das einvernehmliche Zusammenwirken zwischen Erziehungsberechtigten, Schule und Jugendamt. Letztlich kommt es wegen der oftmals sehr diffizilen Sachverhalte in ganz besonderem Maße auf die Einzelfallbeurteilung durch die Lehrkraft an.

Zu der Frage der Teilnahme von Mitarbeiterinnen und Mitarbeitern der Jugendhilfe an Konferenzen und Dienstbesprechungen der Schule vertrete ich in Abstimmung mit dem Niedersächsischen Kultusministerium die Auffassung, daß diese nur zulässig ist, wenn entweder persönliche Angelegenheiten einzelner Schülerinnen oder Schüler nicht erörtert werden, deren Erziehungsberechtigte zustimmen oder die Fürsorgepflicht der Schule die Unterrichtung des Jugendamtes gebietet.

25. Landwirtschaft und Forsten

25.1 Tierschutzgesetz

Das Niedersächsische Ministerium für Ernährung, Landwirtschaft und Forsten hat vielfältige Änderungen des Tierschutzgesetzes vorgeschlagen. Meine Anregung, die bislang nur unzureichenden datenschutzrechtlichen Regelungen, z.B. in § 16 TierSchG (behördliche Aufsicht, Auskunftspflichten), zu ergänzen, hat das Ministerium aufgegriffen. Es ist vorgesehen, in § 16 einen neuen Absatz 6 zu schaffen, nach dem personenbezogene Daten erhoben werden dürfen, soweit dies durch das Tierschutzgesetz vorgesehen oder ihre Kenntnis für die Erfüllung der Aufgaben nach dem Tierschutzgesetz oder aufgrund des Tierschutzgesetzes erlassener Rechtsverordnungen für die erhebende Stelle notwendig ist. Die näheren Einzelheiten über den Umfang der zu verarbeitenden Daten sollen in einer Rechtsverordnung geregelt werden. Inwieweit die Bemühungen des Ministeriums erfolgreich sein werden, wird von den Beratungen in Bundesrat und Bundestag abhängen.

25.2 Zentrale Registratur Zirkus

Zirkusse unterliegen nach § 11 Tierschutzgesetz (TierSchG) der Erlaubnispflicht und nach § 16 TierSchG der regelmäßigen Überwachung. Bei Kontrollen der Zirkusse wurden und werden immer wieder Mißstände festgestellt, deren Beseitigung und Ahndung tierschutzrechtlich geboten ist. Die Kontrollen werden jedoch durch ständige Ortswechsel der Zirkusse - über Ländergrenzen hinweg - erheblich erschwert. Aus fachlicher Sicht ist mir die Notwendigkeit für eine bundesweite Erfassung der Zirkusse nachvollziehbar dargelegt worden. Nur so kann sich eine örtlich zuständige Behörde kurzfristig über die tierschutzrechtliche "Vorgeschichte" des geprüften Betriebs informieren und ggf. früher ergangene Verwaltungsakte übernehmen und vollziehen. Ein derartiges zentrales Register bedarf einer gesetzlichen Grundlage. Der Änderungsentwurf zum TierSchG (vgl. 25.1) sieht nun in § 16 Abs. 5 die zentrale Erfassung aller Zirkusbetriebe mit ständig wechselnden Standorten und aller überregional tätigwerdenden Einrichtungen nach § 11 TierSchG vor.

26. Wirtschaft

26.1 Datenschutzrechtliche Regelungen in der Gewerbeordnung

Mit dem Gesetz zur Änderung der Gewerbeordnung (GewO) und sonstiger gewerberechtlicher Vorschriften gibt es seit dem 1. Januar 1996 bereichsspezifische Regelungen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Diese längst überfälligen Rechtsgrundlagen entsprechen insgesamt den Vorgaben des Volkszählungsurteils.

Nicht befriedigen kann jedoch die in § 14 Abs. 8 GewO geschaffene Regelung, nach der Auskunftsbegehrende ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft zu machen haben, wenn sie den Namen, die betriebliche Anschrift und die angezeigte Tätigkeit des Gewerbetreibenden erfahren möchten. "Berechtigt" ist jedes Interesse, das bei vernünftiger Betrachtung in einer bestimmten Situation nicht abwegig ist. Das Interesse kann auf wirtschaftlichen Erwägungen basieren; erfaßt werden aber auch Interessen ideeller Art, sofern sie im Rahmen der geschäftsmäßigen oder beruflichen oder gewerblichen Zwecken dienenden Datenverarbeitung zum Tragen kommen können. Bei Anlegung dieser sehr niedrigen Hürde können Dritte sehr leicht an die Gewerbedaten herankommen. Die Empfänger von Gewerbeanzeigen wie Industrie- und Handelskammern, Handwerkskammern, Allgemeine Ortskrankenkassen, Finanzämter usw. sind gemäß § 14 Abs. 8 GewO nach Prüfung des berechtigten Interesses befugt, diese Daten an Versicherungen, Marktforschungsinstitute usw. weiterzugeben. Damit ist eine allzu einfache Verbreitung dieser Daten vom Gesetz angelegt.

26.2 Gewerbeanzeigenverwaltungsvorschrift - Beispiel für gute Zusammenarbeit

Infolge der oben beschriebenen Änderung der Gewerbeordnung mußte auch die entsprechende Verwaltungsvorschrift neu gefaßt werden. Ich habe mich gegen die Zulassung von Gruppenauskünften aus dem Gewerberegister, automatische Mitteilungen an das Vormundschaftsgericht bei Gewerbeanmeldungen durch Jugendliche sowie die regelmäßige Einholung von Auskünften aus dem Bundeszentralregister bei der Anmeldung überwachungsbedürftiger Gewerbe ausgesprochen. In der "Allgemeinen Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c der Gewerbeordnung (GewAnzVwV)" vom 6. März 1996 (Nds. MBl. S. 594) ist meinem Anliegen in vollem Umfang entsprochen worden.

27. Verkehr

27.1 Zentrales Fahrerlaubnisregister

Die Planungen für ein Zentrales Fahrerlaubnisregister (vgl. XII 30.1) werden weitergeführt. Zum Stand der Diskussion: Auch das Bundesverkehrsministerium räumt jetzt ein, daß europäisches Recht die Schaffung eines zentralen Führerscheinregisters nicht vorschreibt. Immer noch nicht hinreichend dargelegt ist aus meiner Sicht, weshalb für den Informationsaustausch innerhalb der EU-Staaten eine Datensammlung angelegt werden muß, von der ca. 50 Mio. Personen betroffen sein werden.

Die Automatisierung der örtlichen Fahrerlaubnisregister bei den Fahrerlaubnisbehörden ist in den letzten Jahren forciert worden. Die damit verbundenen Aufwendungen erweisen sich möglicherweise bald als hinfällig. Nach dem Entwurf eines Gesetzes zur Schaffung eines zentralen Fahrerlaubnisregisters sollen die örtlichen Fahrerlaubnisregister aufgelöst werden, sobald das Zentralregister seine volle Funktionsfähigkeit erreicht hat. Damit will man den Bedenken Rechnung tragen, die gegen die Doppelspeicherung von personenbezogenen Daten im örtlichen und im zentralen Register bestehen. Ich habe allerdings Zweifel, ob die Fahrerlaubnisbehörden ihre Aufgaben ohne eine eigene automatisierte Datenverarbeitung ordnungsgemäß erledigen können. Es liegt nahe, weiterhin örtliche Dateien bestehen zu lassen, gegebenenfalls nur nicht mehr unter der Bezeichnung "Örtliches Fahrerlaubnisregister".

Die Verwirklichung der Planungen würde zu einer bemerkenswerten Änderung führen: Die Straßenverkehrsbehörden sind bei ihrer Aufgabenerfüllung auf die im Register gespeicherten personenbezogenen Daten angewiesen. Den Ländern werden aber über die Schaffung der Zentraldatei jegliche Einwirkungsmöglichkeiten und Kontrollkompetenzen entzogen. Die Arbeit muß "unten" erledigt werden, die dafür notwendigen Informationen muß man sich aber "oben" holen. Die Landesstellen begeben sich damit in die Abhängigkeit des Bundes. Planungen dieser Art tragen zur Veränderung der föderalen Struktur in der Bundesrepublik bei.

27.2 Ärztliche Zeugnisse für Bus- und Taxifahrer

Wer Fahrgäste befördert, braucht eine besondere Fahrerlaubnis. In der Regel wird dafür ein Zeugnis eines Facharztes verlangt, in dem die körperliche und geistige Eignung der Bewerberin bzw. des Bewerbers bescheinigt wird. Nur im Ausnahmefall kann die Erlaubnisbehörde ein fachärztliches Gutachten oder das Gutachten einer anerkannten

medizinisch-psychologischen Untersuchungsstelle verlangen.

Es gibt keine Regelungen darüber, welchen Inhalt und Umfang das ärztliche Zeugnis haben muß. Müssen die Betroffenen ihre gesamte Krankheitsgeschichte offenbaren? Oder reicht - insbesondere wenn keine gesundheitlichen Bedenken bestehen - die Bestätigung der Eignung durch den Arzt aus? Bei den niedersächsischen Fahrerlaubnisbehörden wird ein Vordruck "Ärztliches Zeugnis" verwendet, mit dem z.B. Hals-, Nasen- und Ohrenkrankheiten, Verletzungen, Unfälle, Knochenbrüche, Gemütskrankheiten, Magenleiden, Operationen und Krankenhausaufenthalte abgefragt werden. In einem anderen Bundesland hat die Verwendung eines solchen Vordrucks dazu geführt, daß ein Arzt in dem Zeugnis detaillierte Angaben zu den Geburten einer Bewerberin aufgelistet hat. Derartig detaillierte Krankengeschichten muß die Erlaubnisbehörde nicht kennen. Das Bundesverwaltungsgericht sieht dies ebenso. In einer Entscheidung vom 17. Mai 1995 (DÖV 1995, 915) hat es ausgeführt, grundsätzlich genüge als Nachweis für die Eignung, Fahrgäste zu befördern, ein Zeugnis. Das Zeugnis dürfe sich auf die Angabe des Gesamtergebnisses beschränken. Nur bei besonderem Anlaß könne ein qualifizierterer Nachweis, also ein Gutachten, verlangt werden. Dort müßten die Untersuchungen und Einzelergebnisse nachvollziehbar dargestellt werden.

Das Niedersächsische Ministerium für Wirtschaft, Technologie und Verkehr hatte nach Bekanntwerden dieses Urteils zunächst beabsichtigt, den Fahrerlaubnisbehörden ein neues Muster für das ärztliche Zeugnis vorzugeben. Es sollte sich in zwei Teile gliedern. Der erste Teil mit einzelnen Untersuchungsergebnissen sollte beim Arzt verbleiben und nur Teil 2 mit den Schlußfolgerungen des Arztes als ärztliches Zeugnis der Fahrerlaubnisbehörde vorgelegt werden. Die Einführung des neuen Musters wird sich allerdings noch verzögern. Das Bundesverkehrsministerium arbeitet an einer Fahrerlaubnisverordnung, in der auch die hier angesprochene Problematik geregelt werden soll. Es ist geplant, das Muster des ärztlichen Zeugnisses als Anlage in die Fahrerlaubnisverordnung aufzunehmen. Es bleibt zu hoffen, daß die Neuregelung bald in Kraft tritt.

27.3 Parksünderdateien ohne Rechtsgrundlage

Bei kleineren Gesetzesverstößen, wie Falschparken, sollen die Behörden nach dem Willen des Gesetzgebers Milde walten lassen. Dafür hat er das Verwarnungsgeld geschaffen. Die Behörden sollen kein förmliches Verfahren durchführen. Die Betroffenen können den gegen sie erhobenen Vorwurf durch Zahlung eines kleineren Geldbetrages aus der Welt schaffen. Nach dem Motto: Bezahlt und vergessen.

Nicht so in Niedersachsen. Hier werden die Fahrzeughalter zum Zwecke der Erkennung von wiederholten Parkverstößen in einer Datei gespeichert. Niedersachsen ist nach meinem Kenntnisstand das einzige Bundesland, das eine Nutzung von abgeschlossenen Verwarnungsverfahren zuläßt. Ich führe bereits seit längerer Zeit

hierüber eine Diskussion mit dem Niedersächsischen Innenministerium (vgl. XII 30.3). Auch das Ministerium räumt inzwischen die Notwendigkeit einer speziellen Rechtsgrundlage für dieses Verfahren ein. Aus dieser Meinungsänderung werden jedoch keine Konsequenzen gezogen. Es stützt die Weiterführung des Verfahrens bis zur entsprechenden Entscheidung des Gesetzgebers auf den sogenannten Übergangsbonus. Diese Auffassung kann ich nicht teilen. Die Wirkung des Übergangsbonus beschränkt sich darauf, während der gesetzlich ungeregelten Übergangszeit staatliche Eingriffe zuzulassen, die für die Aufrechterhaltung des Behördenbetriebes fortgeführt werden müssen. Die Einführung neuer Verfahren - und darum handelt es sich hier - kann daher niemals auf den Übergangsbonus gestützt werden.

Es gibt bereits erstinstanzliche Gerichtsentscheidungen, in denen die Verwertung früherer Verwarnungsgelder auf der Grundlage der Parksünderdateien für unzulässig erklärt wurde. Ich habe dem Ministerium dringend empfohlen, die Weiterführung der Dateien zu überdenken.

28. Rechtspflege

28.1 Informationsverarbeitung im Strafverfahren

Leider hat sich auch im Berichtszeitraum hinsichtlich des Fehlens gesetzlicher Datenverarbeitungsregeln im Strafverfahren nichts geändert (vgl XII 31.1). Nach wie vor fehlen konkrete Normen für die Erhebung und Weiterverarbeitung personenbezogener Daten.

28.2 Justizmitteilungsgesetz - Never ending story ohne happy end

Immer wieder habe ich über die Bemühungen berichtet, ein Gesetz über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen zu formulieren (zuletzt XI 31.8). Darin sollen z.B. Mitteilungen über Strafverfahren gegen Mitarbeiterinnen und Mitarbeiter des öffentlichen Dienstes an deren Dienststelle oder Mitteilungen über Strafverfahren gegen Inhaber von Fischereischeinen an die für die Bewilligung dieser Scheine zuständigen Behörden geregelt werden. Im Bereich des Zivilrechts soll z.B. die Einleitung der mietrechtlichen Räumungsklage dem zuständigen Sozialamt mitgeteilt werden, um durch eine möglichst frühzeitige Intervention die evtl. drohende Obdachlosigkeit zu vermeiden. Der Gesetzentwurf, der 1992 vorgelegt worden ist, verfiel der Diskontinuität. 1995 wurde er erneut in den Gesetzgebungsprozeß eingebracht - nicht ohne weitere Verschlechterungen hinsichtlich der datenschutzrechtlichen Regelungen. Die Datenschutzbeauftragten des Bundes und der Länder nahmen detailliert Stellung, was wiederum der Bundesrat souverän ignorierte, der eine weitere Zurücknahme datenschutzrechtlicher Sicherungen forderte. Zur Begründung wird auf die hohe Belastung der Justiz verwiesen, der nicht noch weitere Verwaltungsarbeiten aufgebürdet werden könnten. Die einfachste Möglichkeit, diesem Bedürfnis entgegenzukommen, nämlich die Abschaffung vieler Mitteilungspflichten, wird dabei vorsichtshalber gar nicht erst ins Auge gefaßt. Die Datenschutzbeauftragten des Bundes und der Länder haben sich an die Justizministerkonferenz gewandt und ihre Einwände erneut vorgetragen.

Insbesondere ist hier auf zwei Punkte aufmerksam zu machen:

- Derjenige, über den eine Mitteilung erfolgt, soll nur noch in wenigen Fällen davon benachrichtigt werden; in der Regel soll ihm nur auf Antrag Auskunft erteilt werden. Der Nachteil liegt auf der Hand: Wenn der Betroffene nichts von dem Informationsfluß weiß, kann er gegenüber dem Informationsempfänger auch keine Richtigstellung veranlassen.

- In Fällen, die besonders sensibel sind, war bisher vorgesehen, die Entscheidung darüber, ob eine Mitteilung erfolgen soll, besonders qualifizierten Justizbediensteten (Richter, Staatsanwälte und Beamte des gehobenen Dienstes) vorzubehalten; dies soll entfallen. Solche Informationsweitergaben können erhebliche Auswirkungen für die Betroffenen haben. Das Bundesverfassungsgericht hat in seiner Volkszählungsentscheidung gefordert, derartigem durch organisatorische Vorgaben entgegenzuwirken. Dies wurde jüngst vom Sächsischen Verfassungsgerichtshof in seiner Entscheidung zum Sächsischen Polizeigesetz erneut betont (vgl. 11.2). Eine organisatorische Absicherung kann in einer Höherverlagerung der Entscheidungskompetenz liegen. Mithin bedeuten die neuen Vorschläge eine Schwächung des Grundrechtsschutzes.

Viel Hoffnung auf Berücksichtigung der vorgetragenen Einwände im weiteren Gesetzgebungsverfahren besteht nicht. Allerdings ist völlig unklar, ob es in dieser Legislaturperiode noch zur Verabschiedung des Gesetzes kommen wird. Es fällt mir schwer, dies angesichts des zu erwartenden Inhalts zu bedauern.

28.3 Errichtungsanordnung für ein länderübergreifendes staatsanwaltschaftliches Verfahrensregister

Bereits im letzten Tätigkeitsbericht habe ich unter 31.2 von der Einführung des zentralen staatsanwaltschaftlichen Verfahrensregisters durch das Verbrechensbekämpfungsgesetz berichtet. Im Berichtszeitraum wurde die hierfür erforderliche Errichtungsanordnung erlassen. An deren Entstehung war ich über das Niedersächsische Justizministerium beteiligt. Die Datenschutzbeauftragten des Bundes und der Länder haben die vom Bundesministerium der Justiz vorgelegten Entwürfe einer detaillierten Kritik unterzogen. Die Vielzahl vorgesehener personenbezogener Daten geht weit über das in § 474 Abs. 2 Nr. 1 StPO erlaubte Maß hinaus. Die Installation eines sogenannten "Ähnlichen-Service" ist umstritten. Hiermit soll es ermöglicht werden, auch die Angaben zu Personen aus dem Bundesregister zu erhalten, deren Daten denen des Beschuldigten nur ähneln, aber nicht gleich sind. Diese Möglichkeit sieht das Gesetz nicht vor. Sie bedürfte aber einer gesetzlichen Regelung. Ein weiterer Schwachpunkt liegt in der mangelhaften Festlegung der technischen oder organisatorischen Maßnahmen zur Datensicherheit, obwohl gerade dies von § 476 Abs. 5 Nr. 5 StPO gefordert wird. Die datenschutzrechtlichen Einwände blieben trotz mühevoller und geduldiger Kleinarbeit im wesentlichen ohne Wirkung.

28.4 Justiz und Medien - zwei Welten treffen aufeinander

Immer wieder kommt es zu Datenschutzproblemen, wenn die Justiz Kontakt zu den Medien hat. Dies kann in zwei Konstellationen der Fall sein. Einmal wenden sich Medien an die Justiz, um Einzelheiten über interessante Verfahren zu recherchieren. Aber auch die Justiz wendet sich hin und wieder an Presse und Rundfunk und bittet um Unterstützung bei Fahndungsmaßnahmen. In beiden Fallgestaltungen

sind Zielkonflikte mit den Rechten der Betroffenen angelegt. Mehrfach wurden solche Einzelfälle an mich herangetragen.

Die Betroffenen haben grundsätzlich ein Interesse, nicht in den Medien stigmatisiert zu werden; die Medien sind an schlagzeilenträchtiger Berichterstattung interessiert. Der Justiz schließlich ist an wirksamer Außendarstellung und effektiver Nutzung der Öffentlichkeitsfahndung gelegen. Dabei trifft die hochdifferenzierte, stets zur Selbstabsicherung neigende Justizsprache auf das mediale Bedürfnis zur einfachen und plakativen Sprache. Derjenige, der noch nicht schuldig gesprochen wurde, möchte nicht in seinem gesamten Lebensumfeld durch Medienberichte diskreditiert und "erledigt" werden.

In diesem Konfliktfeld sucht der Datenschutz den Ausgleich der Interessen des Einzelnen und der Allgemeinheit und gerät dabei immer wieder selbst in die Schußlinie. So wurde in der Presse behauptet, aus Datenschutzgründen sei eine effektive Fahndung nach Gefängnisausbrechern in Niedersachsen nicht möglich gewesen. Auf Nachfrage ergab sich allerdings die völlige Haltlosigkeit des Vorwurfs. Die Polizei hatte allein nach eigenen fachlichen Kriterien über die Art und Weise der Fahndung entschieden und hierbei keinerlei datenschutzrechtliche Überlegungen, sondern ermittlungstaktische Erwägungen zugrunde gelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in Entschließungen eine gesetzliche Regelung der Öffentlichkeitsarbeit der Justizbehörden und der öffentlichen Fahndung gefordert (Anlagen 14 und 18). Gesetzliche Regelungen haben neben ihrer verfassungsrechtlichen Notwendigkeit den Vorteil, klar abgrenzbare und nachvollziehbare Entscheidungsmaßstäbe zu liefern. Damit werden die Verantwortlichen von erheblichem Legitimationsdruck entlastet. Das Niedersächsische Justizministerium wurde von mir um Unterstützung gebeten, hat sich mir gegenüber aber inhaltlich nicht geäußert.

28.5 Die Einführung des großen Lauschangriffs ist nach wie vor abzulehnen

Derzeit wird wieder über die Einführung des sogenannten großen Lauschangriffs diskutiert. Darunter wird das Abhören von Wohnungen zu Zwecken der Strafverfolgung verstanden.

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits 1992 erklärt, sie seien grundsätzlich gegen die Einführung des großen Lauschangriffs (vgl. XI 31.1). Zur Begründung haben sie auf die verfassungsgerichtliche Rechtsprechung zur Intimsphäre hingewiesen. Danach muß um der freien und selbstverantwortlichen Entfaltung der Persönlichkeit willen ein "Innenraum" verbleiben, in dem der Einzelne sich selbst besitzt und in den er sich zurückziehen kann, zu dem die Umwelt also keinen Zutritt hat, in dem er in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt. Dieser Bereich müsse heimlicher, obrigkeitlicher Ausforschung entzogen bleiben (BVerfGE 27, 1 ff). Hierin

sind ein wesentliches Merkmal und eine Entstehungsbedingung für den demokratischen Prozeß zu sehen. Die vorwegnehmende Selbsteinschränkung bei der Willens- und Meinungsbildung wäre sonst zu befürchten. Seit dieser Zeit sind keine neuen Argumente für diesen tief in die Privatsphäre einschneidenden Eingriff vorgebracht worden. Zu verzeichnen ist lediglich ein publizistisches und populistisches Dauertrommelfeuer mit dem immer gleichen Totschlagsargument "Organisierte Kriminalität". Was sich hinter dieser Formel verbirgt, vermag allerdings bis zum heutigen Tage trotz vieler einschlägiger Versuche niemand exakt zu definieren. Einer solchen greifbaren und handhabbaren Definition bedürfte es aber, um die Notwendigkeit neuer, tiefer Einschnitte in Bürgerrechte nachweisen zu können.

Nach wie vor gilt, daß durch große Lauschangriffe voraussichtlich keine Geländegewinne im Kampf gegen schwere Kriminalität zu erzielen sind, weil diese über Mittel und Wege verfügt, sich abzuschotten. Etwas anderes ergibt sich auch nicht aus den Erfahrungen der Länder, die bereits über diese Möglichkeiten verfügen. Eindringlich hat insbesondere der Bürgermeister von Palermo - ein in Italien bekannter Kämpfer gegen die Mafia - darauf hingewiesen, der Wendepunkt im Kampf gegen die Mafia sei nicht mit der Einführung neuer technischer Mittel gekommen, sondern durch eine Veränderung im Verhalten der Bürgerinnen und Bürger. Erst nachdem immer mehr Menschen bereit waren, gegen die Mafia auszusagen, hätten sich erste Erfolge eingestellt. Amerikanische Erfahrungen zeigen ebenfalls keine erheblichen Fortschritte im Kampf gegen das organisierte Verbrechen durch den Lauschangriff; es gab zwar einige spektakuläre Einzelerfolge, insgesamt ist aber ein Anwachsen der Kriminalität zu verzeichnen.

Sollte nun aber politisch entschieden werden, den großen Lauschangriff einzuführen, so müssen unbedingt folgende, begrenzende Voraussetzungen beachtet werden:

- Lauschangriffe dürfen nur auf Anordnung eines Richterkollegiums durchgeführt werden. Damit werden die Strafverfolgungsbehörden gezwungen, die Anhaltspunkte, die es in ihren Augen rechtfertigen, einen Lauschangriff einzuleiten, nachvollziehbar darzulegen. Dies hat einerseits zur Folge, daß sie sich einer Selbstreflexion unterziehen müssen. Zum anderen wird die Notwendigkeit der Maßnahme von einer unabhängigen, außen stehenden Instanz geprüft. Durch die Verlagerung der Entscheidungskompetenz auf ein Richterkollegium soll erreicht werden, daß die richterliche Prüfung auf einem hohen Niveau und mit größter Sorgfalt geschieht. Hiergegen wird oft eingewandt, die Erfahrungen der Vergangenheit hätten gezeigt, wie wenig der Richtervorbehalt geeignet sei, die Strafverfolgungsbehörden sinnvoll zu kontrollieren. Gerade bei einem Richterkollegium spricht aber eine Vermutung dafür, auf erfahrene und eingearbeitete Richter zu treffen. Die schwerere Kriminalität wird ja auch bei den Landgerichten verhandelt. Das Richterkollegium ist im übrigen auch im Bereich der Telefonüberwachungen nach dem Außenwirtschaftsgesetz vorgesehen.

In den USA müssen Gerichte, die derartige Überwachungen anordnen, in der Öffentlichkeit - nach Abschluß des Verfahrens - über die von

ihnen angeordneten Maßnahmen berichten (Wiretap Report). In Bereichen, in denen dies Pflicht ist, ist eine hohe richterliche Kontrolldichte erreicht worden.

- Voraussetzung für die Durchführung des Lauschangriffs muß das Vorliegen eines dringenden Tatverdachtes sein. Nur wenn nach dem bisherigen Ermittlungsergebnis in seiner Gesamtheit eine große Wahrscheinlichkeit für die Täterschaft des Beschuldigten besteht, darf zur Erforschung eventueller Hintermänner oder Mittäter der große Lauschangriff eingesetzt werden. Von polizeilicher Seite wird dem entgegengehalten, bei einem derart hohen Verdachtsgrad könne der Täter gleich verhaftet und müsse nicht erst belauscht werden. So griffig und einleuchtend dieses Argument auch klingt, so falsch ist es. Grund für die Einführung des großen Lauschangriffes sind bestimmte Erscheinungsformen des organisierten Verbrechens, in denen die Schwierigkeit besteht, an Hintermänner und Komplizen heranzukommen. Also soll der große Lauschangriff gerade für solche Konstellationen geschaffen werden, in denen ein Täter bereits mit großer Wahrscheinlichkeit feststeht und es "nur" noch darum geht, weitere damit zusammenhängende Straftäter zu ermitteln. Damit wird für den großen Lauschangriff als schwerwiegenden Eingriff in Grundrechte ein höherer Verdachtsgrad vorausgesetzt, als er für die Einleitung eines Ermittlungsverfahrens erforderlich ist. Es soll gerade nicht darum gehen, ein weiteres "normales" polizeiliches Ermittlungsinstrument hinzuzugewinnen. Ziel soll nicht die Verschiebung der historisch entwickelten Grenzen zwischen Bürgerrechten und Rechten der Strafverfolgungsbehörden zu Gunsten der letzteren sein. Dies meint z.B. der Bundesinnenminister, der immer wieder davon spricht, es solle nur in "Gangsterwohnungen" abgehört werden. Davon kann nur gesprochen werden, wenn die Eigenschaft "Gangster" feststeht.

- Der große Lauschangriff darf nur zur Erforschung im einzelnen bestimmter, schwerer Straftaten eingesetzt werden. In Betracht kommen hier etwa Verbrechen, die sich gegen Leib und Leben richten und durch ihre Begehungsform besondere Gefährlichkeit entfalten. Dagegen wird eingewandt, mit einer solchen Definition ließen sich die mannigfaltigen Erscheinungsformen des organisierten Verbrechens nicht erfassen. Den Sicherheitsbehörden würden damit überflüssige und zu strenge Fesseln angelegt. Darin komme ein nicht gerechtfertigtes Mißtrauen gegen die Polizei zum Ausdruck. Hier wird die Problematik der Unklarheit der Definition des "Organisierten Verbrechens" deutlich. Solange auch Gruppen von jugendlichen Fahrraddieben durch Ermittlungsbehörden als "kriminelle Vereinigung" oder "Bande" verfolgt werden und damit das gesamte Instrumentarium verdeckter Ermittlung anwendbar wird, muß durch einen streng gefaßten Straftatenkatalog dafür gesorgt werden, daß die Rechte der Strafverfolger nicht in Bereiche ausgedehnt werden, die keinesfalls mit dem zu tun haben, was im allgemeinen mit organisierter Kriminalität bezeichnet wird.

Das hat mit Mißtrauen nichts zu tun. Historisches, organisationssoziologisches und systemtheoretisches Wissen über das Funktionieren großer Organisationen und Bürokratien - also auch der

Polizei - deutet auf eine solchen Systemen innewohnende Tendenz zur extensiven Zuständigkeitsinterpretation hin. In einer demokratisch verfaßten Gesellschaft ist es jedoch nicht Aufgabe der exekutiven Bürokratien, über ihre Befugnisse zu entscheiden, sondern allein die des Gesetzgebers. Steuerung soll im Bereich der Legislative erfolgen, nicht durch die Exekutive selbst. Eine detaillierte Regelung von Eingriffsvoraussetzungen ist nichts anderes als die Umsetzung des Funktionsprinzips der demokratischen Gesellschaft. Dies gilt insbesondere dort, wo der Polizei historisch neue Eingriffsbefugnisse zugestanden werden.

- Es ist sicherzustellen, daß anläßlich großer Lauschangriffe "per Zufall" entdeckte Delikte nicht auf Grund der Erkenntnisse aus dem großen Lauschangriff verfolgt und hieraus auch keine Ermittlungsansätze gezogen werden dürfen. Damit soll die Umgehung der hohen Eingangshürden vermieden werden, indem ein Ermittlungsverfahren nach einer Katalogstraftat eingeleitet wird, obwohl absehbar ist, daß sich dieser Tatverdacht nicht erhärten lassen wird. Immer wieder heißt es hierzu, es könne dem Staat nicht zugemutet werden, ihm bekanntes kriminelles Unrecht nicht zu verfolgen. Dem ist zunächst entgegenzuhalten, daß solche Verwertungsverbote auch in anderen Rechtsgebieten durchaus bekannt sind. Auch im Bereich der Strafprozeßordnung gibt es solche Instrumente. Diese werden von den Gerichten auch angewandt. Ein bekanntes Beispiel sind etwa Verwertungsverbote bei auf unzulässige Weise gewonnenen Beweismitteln (unzulässige Vernehmungsmethoden). Auch in anderen Bereichen nimmt der Staat rechtswidriges Verhalten hin, ohne dies immer zum Anlaß einer Strafverfolgung zu machen, z.B. bei Steuerstraftaten.

- Es ist sicherzustellen, daß Lauschangriffe nur in den Wohnungen der Beschuldigten eines förmlichen Strafverfahrens, nicht aber in den Wohnungen unbeteiligter Dritter durchgeführt werden dürfen. Hiergegen wird eingewandt, damit würden Kriminelle geradezu aufgefordert, die einschlägigen Vorschriften zu umgehen, indem sie sich in fremde Wohnungen begeben, um relevante Gespräche abzuhalten. In den meisten Fällen einer solchen Gewährung von "Obdach" sind die Wohnungsbesitzer Teilnehmer der relevanten Straftaten und wären damit von dem zu schaffenden Katalog mit erfaßt. In anderen Fällen, in denen die fragliche Wohnung nur gelegentlich zu derartigen Zwecken genutzt wird, ist das "Verwanzen" schon deswegen meist undurchführbar, weil das Benutzen gerade dieser Wohnung nicht voraussehbar ist. Gerade hier zeigt sich die Untauglichkeit des großen Lauschangriffs als Allzweckwaffe im Kampf gegen organisierte Kriminalität. Kriminelle großen Kalibers sind den Strafverfolgungsbehörden immer wieder durch die Umgehung rechtlicher Regelungen oder die Nutzung moderner Technik voraus.

28.6 Eine Landtagsabgeordnete in der Telefonüberwachung

Es mehren sich die Fälle, in denen auch Politiker in Telefonüberwachungsmaßnahmen hineingeraten. Bekannt geworden ist derartiges in Baden-Württemberg und Hamburg. Nunmehr ist auch der

erste niedersächsische Fall zu verzeichnen. Im Zuge der Ermittlungen gegen die "Autonome Antifa - M" sind insgesamt neun Telefonanschlüsse überwacht worden. Dabei wurden 9.836 Gespräche aufgezeichnet (LT-Drs. 13/1255, S. 15). In zwei Fällen ist auch der Anschluß einer Landtagsabgeordneten angerufen worden. Die hierbei aufgezeichneten Informationen standen ganz offensichtlich in keinerlei Zusammenhang mit dem Strafverfahren. Sie sind trotzdem auf Band gespeichert bzw. als Kurzprotokoll zu den Akten genommen worden. Nach der Strafprozeßordnung sind aber durch Telefonüberwachung erlangte personenbezogene Informationen unverzüglich unter Aufsicht der Staatsanwaltschaft zu vernichten, wenn sie für die Strafverfolgung von vornherein nicht von Bedeutung sind oder ihre Bedeutungslosigkeit sich nach Prüfung herausstellt. Die Vernichtung muß erfolgen, sobald dies festgestellt ist; dies gilt insbesondere für das gesamte Zufallsmaterial.

Daher habe ich mich an die Generalstaatsanwaltschaft in Celle gewandt, auf diese Rechtsverpflichtung hingewiesen und gebeten, die Unterlagen bezüglich der fraglichen Telefongespräche zu vernichten. Dies erfolgte im Juli 1995, allerdings - soweit für mich nachvollziehbar - nur soweit es die beiden Telefongespräche betraf. Der Vorgang macht Strukturen deutlich, die auch bei der von mir kontrollierten Telefonüberwachungsmaßnahme aufgefallen sind (vgl. 28.12.1). Im Unterschied zu anderen Ländern werden in Deutschland bei Abhörmaßnahmen ungleich mehr personenbezogene Daten erhoben und aufbewahrt als notwendig. Sind diese Daten erst einmal in den Akten, so haben sie dort ein langes Leben.

28.7 Informationen im OWi-Verfahren

Nach Erörterungen mit dem Niedersächsischen Justizministerium (vgl. XII 31.9) konnte Einvernehmen erzielt werden, daß der bzw. dem wegen einer Ordnungswidrigkeit Angezeigten nicht mehr routinemäßig eine Kopie des Schreibens des Anzeigeerstatters übersandt wird. Lediglich die sachlichen Gründe für die Anzeige sind mitzuteilen. Kenntnis von Namen und Anschrift der Informationsquelle sind für die Anhörung nicht notwendig. Nur in besonderen Einzelfällen kann es notwendig sein, dem Betroffenen eine Kopie der Anzeige zu übersenden oder ihm Akteneinsicht zu gewähren, wenn er sonst nicht sachgemäß zu dem Vorwurf gehört werden kann.

Darf die Polizei, die nach Abschluß ihrer Ermittlungen z.B. wegen eines Verstoßes gegen das Tierkörperbeseitigungsgesetz den Vorgang zwecks Durchführung eines Ordnungswidrigkeitenverfahrens an die Verwaltungsbehörde abgegeben hatte, über den Ausgang des Verfahrens unterrichtet werden? Meine Abstimmung mit dem Niedersächsischen Innenministerium führte zu folgendem Ergebnis: Das Ordnungswidrigkeitengesetz und die entsprechend anwendbaren Vorschriften der Strafprozeßordnung sehen eine Unterrichtungspflicht gegenüber der Polizei über den Ausgang des Bußgeldverfahrens durch die Ahndungsbehörden nicht vor. Damit sind die Daten über den Ausgang von Ordnungswidrigkeitenverfahren für die Aufgabenerfüllung

der Polizei grundsätzlich nicht erforderlich; die Anforderung und Übermittlung dieser Daten sind daher nicht zulässig.

28.8 Bewährungs- und Gerichtshilfe, Führungsaufsicht

Im Bereich der Bewährungs- und Gerichtshilfe sowie Führungsaufsicht wurde ich mit einer Vielzahl von Fragen konfrontiert: Gewährung der Einsicht in die von den Bewährungshelfern geführten Akten, Weitergabe von Durchschriften des die Probanden betreffenden Schriftverkehrs, Grundsatzfragen der Speicherung personenbezogener Daten, der Aktenaufbewahrung, Aktenvernichtung usw. Mit der Tätigkeit des Bewährungshelfers ist zwangsläufig die Verarbeitung personenbezogener Daten verbunden. Leider enthalten weder das Strafgesetzbuch und die Strafprozeßordnung noch das Gesetz über Bewährungshelfer vom 25. Oktober 1961 oder andere Rechtsvorschriften spezielle Befugnisnormen für die Verarbeitung personenbezogener Daten durch Bewährungshelfer. Nach Auffassung des Niedersächsischen Justizministeriums werden die Akten und Dateien der Bewährungshilfe von den geplanten Neuregelungen des Strafverfahrensänderungsgesetzes 1994 (StVÄG '94) erfaßt. Wann diese kommen werden, ist allerdings ungewiß. Das Ministerium meint, bis dahin seien die Nrn. 185 Abs. 3 und 4 und 187 der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) ausreichende Regelungen für die Datenverarbeitung durch die Bewährungshelfer. Akteneinsicht und Auskunft an Dritte dürfen danach gewährt werden, wenn ein berechtigtes Interesse dargelegt wird und sonstige Bedenken nicht entgegenstehen.

Das Ministerium hat sich bereit erklärt, meine Anregung zur Novellierung des Gesetzes über Bewährungshelfer vom 25. Oktober 1961 aufzugreifen. Seine Absicht, ein Gesetz für die sozialen Dienste in der Strafrechtspflege (Gerichtshilfe, Führungsaufsicht und Bewährungshilfe) zu initiieren, wird von mir begrüßt.

28.9 Schuldnerverzeichnis

28.9.1 Auskünfte aus dem Schuldnerverzeichnis an Vermieter - auch über Ehegatten

Wie schon früher (vgl. XII 31.13) mußte ich mich 1995 und 1996 wieder mit Problemen des Schuldnerverzeichnisses befassen. So beschwerte sich ein Bürger darüber, ein Amtsgericht habe auch über ihn Auskunft erteilt, obwohl nur seine Ehefrau einen Mietvertrag über ein Ladengeschäft mit der Auskunftssuchenden abgeschlossen habe. Die Rechtslage sieht wie folgt aus: Über die Erteilung einer Auskunft aus dem Schuldnerverzeichnis entscheidet die Geschäftsstelle des Gerichts, bei dem das Schuldnerverzeichnis geführt wird. Diese kann nicht darauf bestehen, daß das Interesse des Anfragenden an diesen Daten glaubhaft gemacht wird. Das Interesse muß nur dargelegt werden.

Solange diese Darlegung schlüssig ist, muß das Gericht die Auskunft erteilen. Die Auslegung der zivilprozeßrechtlichen Vorschriften war vom Gesetzgeber so gewollt. Dem Petenten mußte ich daher mitteilen, die Datenübermittlung könne von mir nicht beanstandet werden. Es wird allerdings überdeutlich, zu welch uferlosen Auskunftserteilungen diese Rechtslage führen kann.

28.9.2 Unterschiedliche Praxis bei Auskünften aus dem Schuldnerverzeichnis

Der Hinweis eines besorgten Bürgers gab mir Anlaß, der Frage nachzugehen, auf welche Weise ein Amtsgericht Auskünfte aus dem Schuldnerverzeichnis erteilt und welche Anforderungen es an die Auskunftserteilung stellt. Der Petent behauptete, die Auskunft sei ihm telefonisch erteilt worden - "ohne jede Rückfrage zur Person" und ohne näheres darlegen zu müssen. Das Niedersächsische Justizministerium nahm den Fall zum Anlaß, landesweit zu ermitteln, wie die Voraussetzungen der Auskunftserteilung aus dem Schuldnerverzeichnis geprüft und festgestellt werden. Es ergab sich eine uneinheitliche Gerichtspraxis. Einige Gerichte erteilen grundsätzlich keine telefonischen Auskünfte. Andere geben telefonische Auskünfte nur bei Anfragen der Staatsanwaltschaften, anderer Gerichte oder Behörden. Der überwiegende Teil der befragten Amtsgerichte erteilt regelmäßig fernmündlich Auskünfte aus dem Schuldnerverzeichnis, wobei zum Teil unterschiedliche Anforderungen gestellt werden. Teilweise werden umfängliche tatsächliche Erklärungen sowie hinreichende Identifizierungsangaben verlangt. Ein Gericht erteilt nur Auskünfte, wenn das Aktenzeichen des Schuldtitels genannt wird. Andere wiederum legen bei telefonischen Auskunftsersuchen den Schwerpunkt ihrer Rückfragen auf Angaben zur Person des Anrufenden. Grundsätzlich wird für telefonische Auskünfte aus dem Schuldnerverzeichnis jedoch die hinreichende Darlegung der Zwecke verlangt.

Der konkrete Fall führte zu einem Hinweis des Gerichts an die Geschäftsstellen, telefonische Auskünfte nur mit Zurückhaltung und unter Berücksichtigung des Datenschutzes zu erteilen; in Zweifelsfällen soll auf einen schriftlichen Antrag oder persönliches Erscheinen verwiesen werden. Aufgrund der Uneinheitlichkeit der Auslegung von § 915 Abs. 2 ZPO wird das Niedersächsische Justizministerium Maßnahmen zur Vereinheitlichung ergreifen, was ich ausdrücklich begrüße.

28.9.3 Der laufende Bezug von Abdrucken aus dem Schuldnerverzeichnis

Gemäß § 915e Abs. 1 Buchst. c ZPO erhalten Antragsteller Abdrucke aus dem Schuldnerverzeichnis zum laufenden Bezug, deren berechtigtem Interesse durch Einzelauskünfte nicht hinreichend Rechnung getragen werden kann. Wie ich aus den mir gemäß § 6 Abs. 4 Schuldnerverzeichnisverordnung (SchuVVO) zugeleiteten Mitteilungen

entnehme, handelt es sich bei denjenigen, die die Erteilung von Abdrucken beantragen, um ein breit gefächertes Spektrum von öffentlichen und privaten Stellen. Schon bei der Bewilligung des Bezugs von Abdrucken und Listen aus dem Schuldnerverzeichnis zugunsten von Stadt-, Kreis-, Gemeinde- bzw. Samtgemeindekassen oder auch Sparkassen und Banken usw. habe ich Zweifel an der Erforderlichkeit. Die Bewilligungen für eine AOK, das Krankenhaus einer Stadt, ein ev.-luth. Kirchenkreisamt, die Verkehrsabteilung eines städtischen Ordnungsamtes oder gar eine Landwirtschaftliche Bezugs- und Absatzgenossenschaft eG vermag ich indes nicht nachzuvollziehen.

28.10 Ehescheidungsverbundurteile

Für das seit Jahren von mir verfolgte Problem der Ehescheidungsverbundurteile (vgl. XII 31.10) konnte eine zufriedenstellende Lösung gefunden werden. Das Niedersächsische Justizministerium erklärte, es sei im Rahmen der programmierten Textverarbeitung für einen nicht anwaltlich vertretenen Beteiligten eines Ehescheidungsverbundurteils nunmehr ein schriftlicher Hinweis auf die Möglichkeit der Erteilung von Auszügen und Teilausfertigungen der Entscheidung vorgesehen. Der in Niedersachsen Mitte 1994 begonnene Einsatz automatisierter Datenverarbeitung bei den Familiengerichten berücksichtigt damit künftig in ausreichender Weise die Belange der Betroffenen.

28.11 Datenschutz im Notariat

Anknüpfend an meinen Beitrag in XII 31.15.1 muß ich bedauerlicherweise feststellen, daß die Rechtsgrundlagen, die nach dem Volkszählungsurteil erforderlich sind, im Notarbereich noch immer fehlen. Ich habe das Niedersächsische Justizministerium erneut darauf hingewiesen, daß in vielen Sachbereichen des Notariats Befugnisnormen für die Verarbeitung personenbezogener Daten fehlen. Die Datenverarbeitung durch Notare ist für eine Vielzahl von Aufgaben allenfalls übergangsweise und nur in dem Umfang zulässig, der für die Aufrechterhaltung des Notariatsbetriebes unabweisbar ist.

Auch der Entwurf eines Dritten Gesetzes zur Änderung der Bundesnotarordnung und anderer Gesetze enthält keine bereichsspezifischen Befugnisnormen. Geregelt sind "sonstige Pflichten des Notars" (§§ 25 bis 32 BNotO) und Übermittlungsbefugnisse von Gerichten und Behörden (§ 64a Abs. 3 BNotO); bei diesen Bestimmungen handelt es sich jedoch um Spezialregelungen für die dort bezeichneten besonderen Fälle - gleiches gilt für § 34a Beurkundungsgesetz - und nicht um Befugnisnormen zur Verarbeitung personenbezogener Daten im Rahmen des breiten Spektrums notarieller Tätigkeiten. Nötig sind Regelungen, aus denen sich die Voraussetzungen und der Umfang der Datenverarbeitung für die Bürgerin bzw. den Bürger klar erkennbar ergeben.

Schon im letzten Tätigkeitsbericht wies ich darauf hin, daß weite Teile der notariellen Datenverarbeitung mangels gesetzlicher Ermächtigungen nur auf der Grundlage von Einwilligungserklärungen - ähnlich der anwaltlichen Prozeßvollmacht - erfolgen können. Allerdings stellt sich die Frage, ob diese Einwilligungserklärungen noch als freiwillig angesehen werden können, wenn die Betroffenen auf die Inanspruchnahme eines Notars angewiesen sind. Das Justizministerium teilt meine Bedenken bzgl. der Freiwilligkeit von Einwilligungen nicht; die Betroffenen hätten in der Regel zwar keine Alternative zur Einschaltung eines Notars; dieser sei jedoch grundsätzlich nicht berechtigt, seine Amtstätigkeit etwa von der Zustimmung der Beteiligten zur Speicherung und Verarbeitung ihrer Daten abhängig zu machen. Ich halte eine Einverständniserklärung von Mandantinnen und Mandanten jedenfalls dann für notwendig, wenn der Notar die Daten auch noch nach Abschluß der jeweiligen Amtsgeschäfte speichert, obwohl das Vorhalten dieser Daten für seine Tätigkeit nicht erforderlich ist. Durch die Schaffung von gesetzlichen Regelungen könnte dieses Problem gelöst werden.

28.12 Kontrollen

28.12.1 Kontrolle von Telefonüberwachungsmaßnahmen

Bereits im letzten Tätigkeitsbericht habe ich ausführlich von der Kontrolle einer Telefonüberwachungsmaßnahme berichtet (XII 31.5.1). In bestimmten Punkten ist es bei dem Dissens zwischen mir und den zuständigen Ressorts, dem Niedersächischen Innenministerium und dem Niedersächsischen Justizministerium, geblieben.

Nach wie vor meine ich, daß ein Verfahren zur Durchführung der Telefonüberwachung gefunden werden muß, das sicherstellt, daß zur Strafverfolgung nicht oder nicht mehr erforderliche Daten "unverzüglich" vernichtet werden (§ 100b Abs. 6 StPO). Bei Telefonüberwachungsmaßnahmen fallen in hohem Maße Daten unbeteiligter Dritter an. Bei der von mir geprüften Maßnahme beispielsweise war über einen längeren Zeitraum auch eine Telefonzelle abgehört worden. Hierbei sind in weit überwiegendem Umfang Gespräche aufgezeichnet worden, die nach Ansicht aller Beteiligten mit dem Strafverfahren nicht das Geringste zu tun hatten. Daher könnten diese Gespräche und die über sie angelegten Protokolle eigentlich gelöscht werden. Dem wird vom Niedersächsischen Innenministerium entgegengehalten, ein solches Vorgehen berge im Strafverfahren die Gefahr des Manipulationsvorwurfs. "Unverzüglich" im Sinne von § 100b Abs. 6 StPO heißt aber nicht "nach Abschluß des Strafverfahrens", welches sich unter Umständen noch sehr lange hinziehen kann. Diese strafprozeßrechtliche Vorgabe muß umgesetzt werden.

Über ein noch zu findendes Verfahren müssen die Rechte der Verteidigung besser abgesichert werden. Ebenso wie die Gespräche unbeteiligter Dritter werden nämlich grundsätzlich auch die Gespräche mit Anwälten zunächst einmal aufgezeichnet. Zur Begründung wird auf das automatische Aufzeichnungsverfahren und auf die Notwendigkeit

zur Kontrolle, ob der Beschuldigte denn auch wirklich mit seinem Anwalt gesprochen habe, verwiesen. Das Verbot der Kenntnisnahme von Verteidigergesprächen ist strafprozeßrechtlich eindeutig geklärt. Insoweit wird die StPO bisher nicht beachtet.

Interessant sind erste Erkenntnisse, die ich bei der Prüfung des Verfahrens der Telefonüberwachung im Mobilfunkbereich gewonnen habe. Teilweise erfolgt hier die Speicherung der durch die Telefonüberwachung erlangten Daten nicht mehr in analoger Form auf Bändern, sondern digitalisiert auf optischen Speicherplatten. Dies wird künftig auch bei der Überwachung des Festnetzes möglich sein, da auch dort immer mehr auf digitale Vermittlung umgestellt wird. Sprache wird nicht mehr als akustisches Signal übertragen, sondern in digitale Zeichen umgewandelt. Diese werden auf sogenannten WORMs gespeichert (vgl. 4.8.3). Auf diesem Speichermedium können einzelne Gespräche nicht gelöscht werden. Derart überspielt die moderne Technik die Vorschriften der Strafprozeßordnung. Bereits im Fall der in die Telefonüberwachung geratenen Landtagsabgeordneten (28.6) hatte ich auf § 100b Abs. 6 StPO hingewiesen, der die "unverzügliche" Löschung der Daten anordnet, die ersichtlich mit dem Strafverfahren nichts zu tun haben. Die Erfüllung dieser gesetzlichen Pflicht ist aber technisch nicht möglich. Es fragt sich, ob dieser Sachverhalt zu einer Streichung der Vorschrift oder zu einem Verbot dieser Technik führt.

Darüber hinaus wirft der Mobilfunkbereich mancherlei Ansatzpunkte für Bedenken auf. Verbindungssdaten in einem bisher nicht gekannten Umfang stehen zur Verfügung. Bei jedem digital vermittelten Telefongespräch kann dokumentiert werden, welche Telefonnummer angerufen wurde bzw. angerufen hat. Im Mobilfunknetz läßt sich auch dokumentieren, wo sich das Handy zur Zeit aufhält, da im Rechner des Betreibers die Funkzelle, über die das aktiv gemeldete Handy erreicht werden kann, erfaßt werden muß. Dies setzt noch nicht einmal voraus, daß überhaupt ein Telefongespräch geführt wird.

28.12.2 Kontrolle des staatsanwaltschaftlichen ADV-Systems SIJUS-STRAF

Die aufwendige Prüfung von SIJUS-STRAF habe ich nunmehr abschließen können (XII 31.5.2). Inzwischen sind fast alle niedersächsischen Staatsanwaltschaften mit diesem System ausgestattet. Das Verfahren wird auch in einigen anderen Bundesländern eingesetzt. Neben der Automation der Geschäftsstellenverwaltungen wird hierüber auch die elektronische Weitergabe von Daten über Datenfernübertragung an bundesweite Register bewerkstelligt - etwa an das zentrale staatsanwaltschaftliche Verfahrensregister bei dem Bundeszentralregister in Berlin oder in die sogenannte Verkehrssünderdatei in Flensburg. Um so wichtiger ist es, Wert auf die Richtigkeit der in der EDV enthaltenen Daten zu legen. Diese können bundesweit von anderen Behörden abgefragt werden. Befremdlich war es deshalb für mich, bei einem Abgleich mit den staatsanwaltschaftlichen Verfahrensakten eine sehr hohe Fehlerquote feststellen zu müssen. So waren Namen oder Geburtsdaten nicht richtig eingetragen, was zu Verwechslungen führen kann. Eine

Rechtsgrundlage für das Verfahren SIJUS-STRAF existiert derzeit nicht, wäre aber erforderlich (vgl. 28.1). Schleswig-Holstein hat dieses Problem durch die Schaffung eines Landesgesetzes gelöst.

Angesichts der Sensibilität der in SIJUS-STRAF enthaltenen Daten habe ich diverse technisch-organisatorische Forderungen erhoben - u.a. die Daten zu verschlüsseln. Über den Dialog mit dem Niedersächischen Justizministerium und im Zuge der Fortentwicklung des Systems ist es zur Erfüllung mancher Forderung gekommen. Eine Schwierigkeit besteht darin, daß Weiterentwicklungen von allen Anwenderländern getragen werden müssen.

Strukturell wird hierbei wieder eines deutlich: Die Technik für dieses Verfahren ist beschafft worden, ohne zuvor die rechtlichen Rahmenbedingungen und Anforderungen zu beachten. Nunmehr wird Datenschutzforderungen entgegengehalten, ihre Umsetzung sei zu teuer bzw. im Länderverbund nicht leistbar. Auf diese Weise bleibt Datenschutz außen vor.

29. Strafvollzug

29.1 Novellierung des Strafvollzugsgesetzes - kalter Kaffee neu aufgewärmt

Im Juni 1996 übersandte mir das Niedersächsische Justizministerium einen "Vorläufigen Referentenentwurf zur Änderung des Strafvollzugsgesetzes". Seit dem Volkszählungsurteil von 1983 ist die Notwendigkeit bereichsspezifischer, normenklarer Regelungen über Datenverarbeitung im Strafvollzug unbestritten. Seitdem zeigt sich immer wieder der schwankende, rechtsunsichere Boden, auf dem die Strafvollzugsbehörden handeln müssen. Die vorangegangenen Tätigkeitsberichte enthalten dazu genügend Anschauungsmaterial (vgl. etwa XII 32.1). 1991 war ein "Vorläufiger Referentenentwurf zur Änderung des Strafvollzugsgesetzes" vom Bundesjustizministerium vorgelegt worden, zu dem ich kritisch Stellung nehmen mußte (XI 32.1). Der aktuelle Entwurf stimmt in wesentlichen Teilen mit dem Entwurf von 1991 überein und enthält immer noch von mir und anderen Landesdatenschutzbeauftragten kritisierte Mängel. Erneut habe ich dem Justizministerium eine ausführliche Stellungnahme zukommen lassen, verbunden mit der Hoffnung, daß die darin geäußerten Bedenken im Gesetzgebungsprozeß endlich Beachtung finden. Vielleicht wird uns aber in fünf Jahren erneut derselbe Referentenentwurf in dritter Auflage vorgelegt.

29.2 Anfertigung von Gefangenenlichtbildern

Nach Nr. 23 Abs. 2 Vollzugsgeschäftsordnung (VGO) sind von Strafgefangenen mit einer Vollzugsdauer von einem Jahr und mehr sowie von Sicherungsverwahrten Lichtbilder aufzunehmen und zur Personalakte zu nehmen. Die erkennungsdienstliche Maßnahme dient der Sicherung des Vollzugs (§ 86 Abs. 1 StVollzG). In Niedersachsen werden Lichtbilder zu diesem Zweck auch von Strafgefangenen angefertigt, die weniger als ein Jahr Freiheitsstrafe zu verbüßen haben. Begründet wird dies u.a. mit der Notwendigkeit, die Gefangenen jederzeit identifizieren zu können, um Verwechslungen zu vermeiden, z.B. bei der Entlassung, beim Ausgang und beim Transport. Das Argument ist einleuchtend. Die rechtliche Situation ist jedoch unbefriedigend. Nach § 86 StVollzG sind diese Aufnahmen nur "zur Sicherung des Vollzuges" zulässig. Der Gesetzgeber ging davon aus, daß diese Tatbestandvoraussetzung für die erkennungsdienstliche Maßnahme nicht regelmäßig vorliegt. Dem trägt Nr. 23 Abs. 2 VGO Rechnung. Regelmäßig wird bei Haftstrafen von einem Jahr und länger die Erforderlichkeit derartiger Maßnahmen angenommen. Eine Klarstellung des Gesetzgebers wäre meines Erachtens notwendig.

Für die Strafgefangenen relevanter ist jedoch die Vernichtung dieser Unterlagen nach Beendigung der Haft. Nach § 86 Abs. 3 Satz 2 StVollzG ist der Strafgefangene spätestens bei Entlassung darauf hinzuweisen, daß auf seinen Antrag hin dieses Material vernichtet wird. In der Vollzugspraxis erfolgt der Hinweis oft schon weit vor dem Entlassungszeitpunkt. Bei der Entlassung ist das Antragsrecht dann den zu Entlassenden oft nicht mehr gegenwärtig. Das Niedersächsische Justizministerium hat nun - auf meine Anregung hin - entschieden, die Belehrung bei Entlassung zu wiederholen.

30. Religionsgesellschaften: Wie kirchlich ist der Unfallhilfe-Verein?

Im Rettungstransportwesen herrscht ein harter Wettbewerb. Dies zeigen immer wieder Eingaben von Unternehmen, die sich gegen "Datenschutzverstöße" der Konkurrenz richten. Eine dieser Eingaben richtete sich gegen die Johanniter-Unfall-Hilfe e.V. (JUH), einen Fachverband des Diakonischen Werks. Mein Versuch der Sachverhaltsaufklärung war beendet, noch bevor er richtig begonnen hatte: Die JUH meinte, sich als Gliedbestandteil der Evangelischen Kirche nicht vom staatlichen Datenschutz kontrollieren lassen zu müssen. Dies veranlaßte mich, zu dieser Frage ein ausführliches Rechtsgutachten zu erstellen. Tatsächlich genießen die Religionsgesellschaften nach Art. 140 GG in Verbindung mit Art. 137 Abs. 3 Weimarer Reichsverfassung das Recht, ihre Angelegenheiten selbständig innerhalb der Schranken der für alle geltenden Gesetze zu ordnen und zu verwalten. Nach der verfassungsgerichtlichen Rechtsprechung sind nicht nur die Kirchen selbst und deren selbständige Teile, sondern alle der Kirche zugeordneten Einrichtungen privilegiert (BVerfG, NJW 1978, 581). Bei einer juristischen Person des Zivilrechts wie der JUH kommt es darauf an, wie intensiv die organisatorische Anbindung an die verfaßte Kirche und die Orientierung am kirchlichen Auftrag ist. Präsidium wie Bundesvorstand der JUH müssen anteilig einige Mitglieder des Johanniterordens angehören oder Pfarrer sein. Auf Landesebene ist die kirchliche Ausrichtung nur durch ein Mitglied des Ordens gewährleistet. Auf Kreis- bzw. Ortsebene gibt es bzgl. der Vorstände überhaupt keine direkte konfessionelle Bindung. Anders als bei Krankenschwestern in einem kirchlichen Krankenhaus geht es meines Erachtens bei der Tätigkeit der JUH im Bereich Krankentransport nicht auch um die Sorge für das geistliche Wohl der Kranken, sondern ausschließlich um Beförderung und medizinische Betreuung als Dienstleistung. Die Satzung der JUH sieht keine sakramentale, sondern praktische Hilfe vor. Daher halte ich das Kirchenprivileg nicht, wohl aber das staatliche Datenschutzrecht für anwendbar.

Der inzwischen eingeschaltete Bundesverband der JUH konnte sich diesem Ergebnis nicht anschließen. Rettungsdienst sei praktizierte Nächstenliebe im christlichen Sinne. Es gehe um die Vermittlung christlichen Handelns als gelebte Verantwortung vor Gott. Obwohl mich dies nicht überzeugte, nahm ich mich, als in geistlichen Fragen nicht autorisierter Datenschützer, zurück. Ich teilte dem Petenten mit, ich meine hier zwar zuständig zu sein; die datenverarbeitende Stelle fühle sich aber dem kirchlichen Datenschutz

unterworfen. Statt einen langwierigen Rechtsstreit auszutragen, empfahl ich, der Petent solle sich an den kirchlichen Datenschutzbeauftragten wenden. Dessenungeachtet hielte ich es für wünschenswert, wenn insofern mit den Kirchen eine Klärung herbeigeführt würde.

31. Grundsätzliches zum Datenschutz in der Wirtschaft

Seitdem ich als Aufsichtsbehörde nach § 38 BDSG für den Datenschutz bei nicht-öffentlichen Stellen, also in der Privatwirtschaft zuständig bin, expandiert dieser Aufgabenbereich. Die Gründe hierfür sind vielfältig. Zum einen hat sich sowohl bei den Unternehmen als auch bei den Bürgerinnen und Bürgern seit Anfang 1992 immer mehr herumgesprochen, daß in Niedersachsen nunmehr eine zentrale Stelle ansprechbar ist. Wichtiger dürfte jedoch sein, daß die informationstechnischen Innovationen zuerst in der Wirtschaft Eingang halten, sei dies die Nutzung von Chipkarten oder CD-ROM, von Online-Diensten oder Internet. Elektronische Medien kennen nicht den Unterschied zwischen "öffentlich" und "nicht-öffentlich". Bei Chipkarten im Gesundheitsbereich oder an der Universität, bei der Nutzung von Adreßdatensätzen, bei der Kommunikation über öffentliche Netze usw.; die Trennung zwischen öffentlichen und privaten Stellen wirkt oft künstlich. Es ist daher nachvollziehbar, daß die EU-Datenschutzrichtlinie diese Trennung aufgibt. Sicherlich gibt die Kompetenzordnung des Grundgesetzes zwischen Bund und Ländern die Trennung vor. Die Datenverarbeitung in einem Frisörladen wird sich auch künftig grundsätzlich von der der Polizei unterscheiden. Eine Annäherung der Rechtsbereiche bleibt dennoch geboten. Dies gilt insbesondere bezüglich der materiell-rechtlichen Regelungstiefe im privaten Bereich.

31.1 BDSG-Novellierungsbedarf

Bei der Novellierung des Bundesdatenschutzgesetzes zwecks Anpassung an die EU-Datenschutzrichtlinie besteht die Chance, bestehende Regelungsdefizite zu beheben. Regelungsbedarf sehe ich im Bereich des Direktmarketing. Bisher waren alle Appelle an die Unternehmen, mehr Transparenz dadurch herzustellen, daß die Herkunft der Daten sowie die Selektionskriterien benannt werden, erfolglos. Wünschenswert ist zudem ein Hinweis an die Beworbenen auf ihr Widerspruchsrecht (Art. 25 Abs. 2 EU-Datenschutzrichtlinie). Entsprechende Verpflichtungen würden mich als Aufsichtsbehörde massiv entlasten, wären ein Gewinn an Selbstbestimmung für die Verbraucherinnen und Verbraucher und würden Unternehmen, die korrekt mit Kundendaten umgehen, in keiner Weise belasten. Angesichts der Zunahme des Adressenhandels hielte ich außerdem eine Verbindlicherklärung von Sperrlisten (z.B. Robinsonliste des DDV) für sinnvoll, will man die Zulässigkeit von Direktmarketing nicht sogar von der Einwilligung der Betroffenen abhängig machen (vgl. 33).

Dringend geregelt werden muß meines Erachtens die Veröffentlichung von personenbezogenen elektronischen Verzeichnissen, z.B. auf CD-

ROM. Der bisherige § 29 BDSG paßt auf diese neue Erscheinung nicht. Auch hier geht es um Transparenz und das Bestimmungsrecht der Betroffenen einerseits, andererseits aber auch um die Befriedigung begründeter Informationsbedürfnisse der Öffentlichkeit (vgl. 8.1.4). Chipkarten sind ein vom BDSG bisher nur schwer greifbarer Datenträger. Der Gesetzgeber ist aufgerufen, die Verantwortlichkeit für die Datenspeicherung und die Möglichkeit zur Wahrnehmung der Betroffenenrechte (Auskunft, Löschung, Zugriffsbeschränkung) sicherzustellen (vgl. 4.7). Das derzeit gültige BDSG geht noch davon aus, daß Großrechner die Datenverarbeitung bestimmen. Inzwischen wird aber die Welt der Informationstechnik von vernetzten Kleinrechnern bestimmt. Diesen veränderten Bedingungen muß das BDSG, z.B. bei den Regelungen zur Datensicherheit, Rechnung tragen. Zumindest von der Tendenz her dürfte schließlich unstreitig sein, daß die Kontroll- und Interventionskompetenzen der Aufsichtsbehörden (Erfassung der Datenverarbeitung in Akten, anlaßunabhängige Kontrolle, Verbotsverfügungen bei materiell-rechtlichen Datenschutzverstößen) ausgeweitet werden müssen (vgl. XII 34.2).

32. Kontrolltätigkeit: Zahlen, Fakten und Erfahrungen

32.1 Datenverarbeitung als Dienstleistung: Meldepflicht nach § 32 BDSG

Unternehmen der Wirtschaft, die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung bzw. der anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen, sind gesetzlich verpflichtet, mir die Aufnahme oder Beendigung ihrer Tätigkeit mitzuteilen. Ich vermute, daß es noch immer eine größere Zahl an Unternehmen gibt, die dieser Meldepflicht nicht nachgekommen ist. In den letzten zwei Jahren stieg die Anzahl der Registermeldungen allerdings wiederum deutlich an, was darauf hindeutet, daß sich die Dunkelziffer weiter verringert hat. Dies ist aber auch darauf zurückzuführen, daß die Zahl der Unternehmen mit meldepflichtiger Tätigkeit insgesamt gestiegen ist.

1996 waren insgesamt 338 Firmen nach § 32 BDSG zum Register gemeldet. Dies entspricht einer Zunahme gegenüber Ende 1994 von ca. 25 %; damals waren 270 Firmen registriert. In den zwei Jahren gab es 83 Neuanmeldungen und 25 Löschungen. Von den insgesamt gemeldeten 318 Firmen

- speichern 36 Firmen personenbezogene Daten zum Zweck der Übermittlung (5 Adreßverlage und 31 Auskunfteien),

- beschäftigen sich 4 Firmen mit der Markt- und Meinungsforschung bzw. speichern personenbezogene Daten zum Zweck der anonymisierten Übermittlung,

- verarbeiten 298 Firmen personenbezogene Daten im Auftrag als Dienstleistungsunternehmen.

Die genaue Aufteilung nach Berufssparten und deren Veränderung gegenüber 1992 und 1994 zeigt die Abbildung. In nahezu allen Sparten sind die Registermeldungen gestiegen. Ein besonders starker Anstieg an registrierten Unternehmen ist bei den Service-Rechenzentren und den Vernichtungsbetrieben erkennbar. Unternehmen, die Mikroverfilmung im Auftrag betreiben, setzen zunehmend andere Techniken der optischen Archivierung ein (Speicherung auf einmalbeschreibbaren Platten "WORM"). Die bisher unter der Sparte "Mikroverfilmung" aufgeführten Betriebe finden sich daher jetzt in der Sparte "Datenarchivierung" wieder.

Neu hinzugekommen ist die Sparte "Mailboxen", in der die gemeldeten

Betreiber von Mailbox-Servern zusammengefaßt sind (vgl. XII 4.8.2). Zur Zeit sind bei mir fünf Mailboxen zum Register gemeldet. Diese Zahl ist weitaus geringer als die Zahl der in Niedersachsen betriebenen Mailboxen. Bei vielen Mailbox-Betreibern herrscht offenbar Unkenntnis oder zumindest Unsicherheit, wann eine Meldepflicht vorliegt. Die Gesetzeslage erlaubt oft keine leicht zu treffende Entscheidung und erfordert eine Beurteilung im Einzelfall. Die Meldepflicht einer Mailbox liegt nur vor, wenn eine Verarbeitung in oder aus Dateien, eine Datenverarbeitung im Auftrag und eine geschäftsmäßige Verarbeitung bzw. eine Verarbeitung für berufliche oder gewerbliche Zwecke erfolgt.

Die elektronischen Nachrichten einer Mailbox bilden eine Datei, wenn sie nach bestimmten Merkmalen, etwa nach Absender, Empfänger oder Datum/Uhrzeit der Speicherung ausgewertet werden können. Dies dürfte regelmäßig der Fall sein. Die Datenverarbeitung erfolgt bei den meisten Mailboxen auch im Auftrag, zumindest, wenn die technische Durchführung der Datenverarbeitung, also die technische Bereitstellung der Mailbox, im Mittelpunkt der Tätigkeit steht. Wird mehr gemacht, ist zu prüfen, ob eine Datenverarbeitung für eigene Zwecke vorliegt. Dies ist z.B. der Fall, wenn ein Pizza-Bringdienst sich für die Entgegennahme von Bestellungen eine Mailbox eingerichtet hat und diese zur Abwicklung des Services, also für eigene Zwecke, betreibt.

Aufteilung der gemeldeten Firmen nach Betriebsarten für Ende 1992, 1994 und 1996 (Service-Rechenzentren: überwiegend Auftragsdatenverarbeitung; Rechenzentren: überwiegend Datenverarbeitung für eigene Zwecke).

Bei "Hobby-Mailboxen" ist oft die "Geschäftsmäßigkeit" fraglich. Fehlt eine Gewinnerzielungsabsicht, also eine berufliche oder gewerbliche Nutzung, so muß die Geschäftsmäßigkeit im Einzelfall überprüft werden. Folgende Punkte sprechen für die Meldepflicht:

- Betreiben der Mailbox auf Dauer,

- regelmäßige Online-Zeiten,

- hohe Anzahl von Mailbox-Nutzern oder -Nutzerinnen,

- Forderung eines Nutzungsentgeltes,

- Einnahmen durch Werbungsanzeigen in der Mailbox,

- Deckung sämtlicher Kosten einschließlich Investitionskosten durch Nutzungsentgelte und/oder Werbung,

- mehrere Systembetreuer (sog. Sysop's),

- entgeltliche Beschäftigung von Mitarbeitern oder Mitarbeiterinnen,

- Werbung für die Mailbox.

Es sei nochmals darauf hingewiesen, 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.

32.2 Kontrolle vor Ort

In den Jahren 1995 und 1996 habe ich im Rahmen meiner Aufsichtstätigkeit nach § 38 Abs. 2 BDSG 17 Prüfungen vor Ort bei niedersächsischen Unternehmen durchgeführt. Prüfungsschwerpunkte legte ich wegen der überdurchschnittlichen Anzahl von Neuanmeldungen (vgl. 32.1) bei Mailboxen und Vernichtungsunternehmen. Bei den Mailbox-Prüfungen habe ich das dafür von mir erstellte Prüfkonzept verwendet (vgl. 4.9.3). Ein neuer Prüfungsschwerpunkt waren Großrechner mit MVS- oder VM-Betriebssystemen (vgl. 4.9.2).

Bei der Liste der am häufigsten kritisierten Punkte (vgl. XII 35.2) haben sich viele Punkte als Dauerbrenner herausgestellt, etwa mangelhafte Paßwortverfahren, mangelhafte Verträge bei Auftragsverhältnissen, fehlende Zugangssicherungen oder unsichere Datenübertragungen. Von zunehmender Bedeutung sind Mängel, die mit der fortschreitenden Vernetzung zusammenhängen, z.B. fehlende Absicherungen bei Fernwartung, und Mängel, die sich aus dem neuen Prüfungsschwerpunkt MVS/VM-Systeme ergeben, z.B. fehlende Abgrenzungen zwischen Administrator- und Auditor-Aufgaben.

32.3 Abberufung eines Datenschutzbeauftragten

Der Versuch der Kontrolle eines Unternehmens, das Mitglied einer bundesweiten Organisation ist, erwies sich als Hindernislauf: Seit Oktober 1988 versuchten zunächst die damals noch zuständige Bezirksregierung und danach ich, einen Prüftermin zu vereinbaren. Nachdem sechs Termine abgesagt werden mußten, vor allem, weil der für alle über 70 rechtlich selbständigen Mitglieder dieser Organisation zuständige Datenschutzbeauftragte verhindert war, kam im Mai 1994 eine Prüfung zustande. Der betriebliche Datenschutzbeauftragte nahm damals zugleich eine Prokuristenstellung der zentralen Organisation, die bestimmenden Einfluß auf die Mitglieder nehmen konnte, ein und war hier u.a. auch für den EDV-Bereich zuständig. Bei der Prüfung mußte ich gravierende rechtliche Mängel innerhalb der bundesweiten Organisation feststellen, die dazu führten, daß die datenschutzrechtlichen Verantwortlichkeiten unklar blieben; ein schriftlicher Auftrag nach § 11 BDSG konnte nicht vorgelegt werden. Außerdem mußte ich technische Mängel feststellen. Ich hatte den Eindruck, daß beim Datenschutzbeauftragten sowohl in technischer wie auch in rechtlicher Hinsicht in Bezug auf seine eigene Organisation Kenntnislücken bestanden. Dieser negative Eindruck konnte auch nicht durch sonstige positive Prüferfahrungen relativiert werden. Daher sah ich mich veranlaßt, von meinem Recht nach § 38 Abs. 5 BDSG Gebrauch zu

machen und die Abberufung des betrieblichen Datenschutzbeauftragten zu verlangen. Dieses Verlangen begründete ich mit der Interessenkollision der wahrgenommenen Funktionen, der ungenügenden Ansprechbarkeit, evtl. verursacht durch der Vielzahl der betreuten Stellen, sowie mit den festgestellten technisch-organisatorischen und rechtlichen Mängeln. Die kritisierte Stelle erhob gegen mein Abberufungsverlangen Widerspruch und dann Klage.

Im Laufe des Klageverfahrens erfolgten bei der Organisation viele gravierende Veränderungen: Die Rechtsform der Organisation wurde umgestellt, klare Verantwortlichkeiten und datenschutzrechtliche Vorgaben wurden festgelegt. Der Datenschutzbeauftragte wurde von seiner Aufgabe als Prokurist entbunden, so daß er sich zumindest überwiegend um den Datenschutz in den über 70 verarbeitenden Stellen kümmern kann. Das verwaltungsgerichtliche Verfahren fand ein unerwartetes Ende, als ich Ende 1995 die Mitteilung erhielt, die Firma des Klägers habe sich aufgelöst; deren Aufgaben würden nun von einer anderen Firma wahrgenommen: Das Verwaltungsgericht stellte das Verfahren ein und erlegte die Kosten des Verfahrens dem Kläger auf. Meine Hoffnung, die Abberufung des Datenschutzbeauftragten gerichtlich bestätigt zu bekommen, wobei zugleich generelle Kriterien für eine Abberufung festgelegt worden wären, erwies sich also als trügerisch. Dennoch hatte das aufwendige und langwierige Verfahren sein Gutes: Der Datenschutzstandard innerhalb der bundesweiten Organisation dürfte während des Verfahrens erheblich angehoben worden sein und der von mir festgestellte Interessenkonflikt zwischen den Funktionen Prokurist und Datenschutzbeauftragter besteht nicht mehr. Natürlich hatten all diese Änderungen und auch die Auflösung der klagenden Mitgliedsfirma - so wurde mir mitgeteilt - überhaupt nichts mit dem gerichtlichen Verfahren zu tun. Wie dem auch sei. Ein erstes Informationsgespräch in der Firma, die an die Stelle der aufgelösten Klägerfirma getreten war, zeigte mir, daß sich nicht nur in atmosphärischer, sondern auch in fachlicher Sicht im Interesse des Rechts auf informationelle Selbstbestimmung einiges zum Besseren gewendet hatte.

32.4 Streit um die Auskunftspflicht einer Bank: Viel Lärm um nichts?

Eine Stadt wandte sich an mich mit folgender Darstellung: Zur Veräußerung von Baugrundstücken in einem neuen Wohngebiet nahm die Stadt eine Ausschreibung vor. In einer nichtöffentlichen Informationsdrucksache wurden die Mitglieder des Stadtrates über die Bauinteressenten, die sich gemeldet hatten, unterrichtet. Mehrere dieser Bauinteressenten beschwerten sich nun bei der Stadt, daß sie mit Baufinanzierungsangeboten durch eine Bank angeschrieben worden sind. Der Datenschutzverstoß war offensichtlich: Die Angaben zu den Bauinteressenten sind schützenswerte personenbezogene Daten, die nicht an eine privatwirtschaftlich agierende Bank weitergegeben und von dieser auch nicht für Werbezwecke genutzt werden dürfen. Wer aber war für diesen Verstoß verantwortlich? Die Suche nach dem Schuldigen erwies sich als ein über zwei Jahre dauerndes mühsames Unterfangen, das letztlich ohne Ergebnis blieb.

Alle Versuche, bei der Stadt Langenhagen eine Aufklärung herbeizuführen, waren erfolglos. Die Bediensteten der Kommune versicherten, die Daten nicht herausgegeben zu haben. Der Versuch, bei der Bank Klarheit zu bekommen, begann mit Kontrollbesuchen: Beim ersten Mal gab es angeblich keinen kompetenten Ansprechpartner. Der zweite Besuch war ebensowenig befriedigend: Man habe die Daten von einem "seriösen Partner" erhalten; wer dies ist, konnte bzw. wollte man mir nicht sagen. Nach einer Recherche innerhalb der Bank wollte man mich per Fax unterrichten. Statt dieses Faxes kam mit Verspätung das Schreiben des Banken-Anwaltes, das die rechtlich unhaltbare Behauptung aufstellte, die Liste mit den Bauinteressenten habe lediglich Namen und keine personenbezogenen Daten enthalten. Nachdem sich die Bank weiterhin mehrfach weigerte, Angaben zu machen, leitete ich ein Bußgeldverfahren gegen die Bank wegen Verstoßes gegen ihre Auskunftspflicht ein. Mein Bußgeldbescheid gegen das zuständige Vorstandsmitglied der Bank in Höhe von DM 5000 führte nicht zur Nennung des Informanten, sondern zur Einlegung eines Einspruchs. Die Bank behauptete nun, die Werbemaßnahme nicht aus einer Datei heraus durchgeführt zu haben, so daß das BDSG nicht anwendbar sei (§ 27 BDSG). Die Adreßdaten seien sofort nach Erstellung der Werbebriefe wieder gelöscht worden. Über Unterlagen zu dem Vorgang verfüge man nicht mehr. Wer für diese Maßnahme verantwortlich gewesen ist, ließe sich nicht mehr eindeutig feststellen. Zwischenzeitlich meldete sich bei mir das Niedersächsische Innenministerium und äußerte - für mich nicht nachvollziehbar - Zweifel, daß Daten von Bauinteressenten geheimhaltungsbedürftig seien.

Circa ein Jahr nach der ersten Auskunftsverweigerung erfolgte dann durch das Amtsgericht Hannover der Freispruch des Vorstandsmitglieds der Bank: Ich hätte nicht nachweisen können, daß die Bank die Werbeadressen "in oder aus einer Datei" verarbeitet hat. Der Verdacht einer dateimäßigen Verarbeitung begründe noch keine Auskunftspflicht der Bank nach § 38 Abs. 3 BDSG (AG Hannover, CR 1995, 420 ff.). Dankenswerterweise legte die Staatsanwaltschaft gegen dieses Urteil Rechtsbeschwerde ein. Das Oberlandesgericht stellte dann mit unmißverständlicher Klarheit fest, daß die Bank auskunftspflichtig war und ist. Da Serienbriefe regelmäßig automatisiert hergestellt werden, konnte und mußte ich davon ausgehen, daß bei der Bank eine dateimäßige Verarbeitung erfolgt. In § 38 Abs. 1 BDSG ist nicht der Nachweis einer Dateiverarbeitung erforderlich; es genügen "hinreichende Anhaltspunkte". Das Gericht wies zu Recht darauf hin, daß Datenschutz nicht wirksam durchzusetzen wäre, "wenn die Aufsichtsbehörde nur auf freiwillige Angaben der nichtöffentlichen Stelle oder durch aufwendige eigene Recherchen vorab den Nachweis der (dateimäßigen) Datenverarbeitung erbringen müßte. Gerade Stellen, die sich Daten auf unzulässige Weise beschafft haben, werden zur Kooperation nicht bereit sein." Die Auskunftspflicht umfaßt auch die Datenerhebung und den Informanten, also, wie im konkreten Fall die Bank an die Namensliste gelangt ist (OLG Celle, NJW 1995, 3265 f.). Da hinsichtlich der subjektiven Seite vom Amtsgericht noch keine Beweiserhebung erfolgt war, wurde das Bußgeldverfahren an die erste Instanz zurückverwiesen.

Wer nun dachte, daß die Bank ihrer Auskunftspflicht nachkommen würde, wurde bald eines Besseren belehrt: Die Bank blieb mir gegenüber stumm. Sie holte vielmehr ein professorales Gutachten ein, mit dem sie erfolglos den Beweis zu führen versuchte, daß sie entgegen der Rechtsprechung des OLG Celle nicht auskunftspflichtig sei. Außerdem wandte sich die Bank - ebenfalls erfolglos - an den Generalstaatsanwalt mit der Bitte um Rücknahme des Ordnungswidrigkeiten-Vorwurfes. Erst nach meiner Drohung mit einem erneuten Verfahren und unter Verstreichenlassen der von mir gesetzten Frist teilte die Bank mehr als zwei Jahre nach meiner ersten Auskunftsaufforderung - nicht mir, sondern dem Amtsgericht - mit, wer ihr die Liste mit den Bauinteressenten gegeben hatte. Der Versuch, nun von diesem Informanten nähere Aufklärung über den Datenschutzverstoß zu erhalten, blieb erfolglos. Dieser behauptete, er habe die Adressen in der Annahme, diese gehörten der Bank, dieser zur Verfügung gestellt. Zu guter Letzt erhielt ich vom Amtsgericht die Mitteilung, das Bußgeldverfahren gegen das Vorstandsmitglied der Bank sei eingestellt worden. Die erwünschte Auskunft sei ja inzwischen erteilt.

Die Beschreibung dieses Vorgangs liest sich wie eine Satire. Der Berg kreißte und gebar ein Mäuschen. So unbefriedigend das konkrete Ergebnis auch war, so brachte der Fall doch einen letztinstanzlichen Gerichtsbeschluß, der die Prüfmöglichkeit der Aufsichtsbehörden sicherstellt. Wegen dieser Entscheidung und der Klarstellung, die damit erreicht wurde, haben sich der Aufwand und der Ärger gelohnt.

33. Adressenhandel und Markt- und Meinungsforschung

Mit Hilfe der Direktwerbung beschreiten Unternehmen immer neue Wege, um Kundinnen und Kunden an sich zu binden. Wichtigstes Kapital dabei sind "gute" Adressen. Diese stammen aus der eigenen Kundendatei, aus der Kundenliste eines anderen Unternehmens, das diese Daten über einen Listbroker vermietet, oder aus den gewaltigen Datenbeständen eines Adressenhändlers. Bei den Kauf- bzw. Bestell-Animationsversuchen kommt die Transparenz für die Angeschriebenen regelmäßig zu kurz. Die dadurch verursachte Irritation führt dann oft zu Eingaben bei der zuständigen Aufsichtsbehörde. Um den Betroffenen einen kleinen Einblick in den Dschungel des Adressenhandels zu geben, gebe ich gemeinsam mit Kollegen aus anderen Ländern eine Broschüre (Tips zum Adressenhandel - und gegen die Werbepapierflut im Briefkasten) heraus, die bei mir angefordert werden kann und die sich einer großen Nachfrage erfreut.

33.1 Listbroking

Ein Anbieter besitzt umfangreiche Adressenbestände über Kunden, Spender oder Vereinsmitglieder. Aus diesen möchte er Geld machen. Kein Problem: Er wendet sich an einen Listbroker, der die Adressen Werbeinteressenten vermittelt. Dabei gibt der Listbroker jedoch die Adressen nicht aus der Hand. Er läßt sich vom Werbeinteressenten das Werbematerial geben, adressiert dieses und bringt es in den Versand (das sog. Lettershop-Verfahren). Dieses Verfahren ist für alle genannten Beteiligten vorteilhaft: Die werbende Firma bringt gezielt ihre Angebote an die Frau bzw. den Mann. Der Adresseneigner verdient sich durch die Vermietung seiner Adressen ein Zubrot, ohne daß diese Daten ungewollt in fremde Hände, evtl. der Konkurrenz, geraten. Natürlich bleibt auch etwas für den Listbroker übrig. Wer unter Umständen wenig entzückt ist, das ist die umworbene Person. Diese fühlt sich u.U. belästigt und fragt sich: Wie kommt die Werbefirma an meine Adresse? Aus dem verschickten Werbematerial geht regelmäßig weder hervor, wer Adreßeigner noch wer der versendende Listbroker ist. Eine Anfrage bei der werbenden Firma ist oft wenig erhellend, weil diese zumeist nicht nur einen, sondern mehrere Adressenbestände angemietet hat. Die Herkunft der Adresse ergibt sich zumeist aus einem Zahlencode, der auf dem Adreßaufkleber aufgebracht ist. Daher sollte bei der Frage nach der Herkunft der Adresse immer eine Kopie des Anschreibens oder dieser Zahlencode mitgeschickt werden. Die Werbefirma teilt dann regelmäßig nur die Adresse des Listbrokers mit. Diese Auskunftspraxis ist wenig befriedigend. Den Beworbenen sollte zumindest zusätzlich mitgeteilt werden, aus welcher Liste und von welchem Adreßeigener die Angaben stammen. Folge der unbefriedigenden Antworten sind Eingaben an

meine Dienststelle. Mir ist es dann, regelmäßig unter Hinzuziehung weiterer zuständiger Aufsichtsbehörden, möglich, die Herkunft oder den Hintergrund der Werbeadressen aufzuhellen.

Nach dem BDSG von 1977 war es streitig, ob die Werbung durch Listbroker eine Datenübermittlung an die werbende Firma darstellt. Da der Listbroker selbst als Auftragnehmer des Adreßeigeners angesehen wird, führte dies bei Verneinung der Frage dazu, daß wenig gegen derartige Werbung unternommen werden konnte. Mit dem BDSG von 1990 hat sich die Rechtslage verbessert: Nicht nur die Übermittlung, auch die Datennutzung durch den Adreßeigener bzw. Listbroker wird nunmehr erfaßt. Das Versenden von Werbung für eine andere Firma ist eine solche Datennutzung.

33.2 Weshalb sollten "christliche Spender" gegen Abtreibung sein?

Ein Bürger aus Karlsruhe erhielt von einer Deutschen Vereinigung für eine christliche Kultur unverlangt direkt an ihn adressiertes Werbematerial gegen Abtreibung zugesandt. Da ihm dies überhaupt nicht gefiel, schaltete er die zuständigen Datenschutz-Aufsichtsbehörden ein. Nach umfangreichen Recherchen stellte sich der Fall wie folgt dar: Der Bürger war auf einer 260.000 Adressen enthaltenden Liste "christliche Spender" enthalten, die ein Unternehmen in Campione/Schweiz über einen niedersächsischen Listbroker anbot. Die Vereinigung mietete sich über 150.000 dieser Adressen und ließ die Agitation gegen die Abtreibung verschicken.

Das war zu viel der Werbung: § 28 Abs. 2 Nr. 1 Buchst. b BDSG läßt die listenmäßige Datennutzung nur zu, wenn kein Grund zu der Annahme besteht, daß die Betroffenen entgegenstehende schutzwürdige Interessen haben. Als Beispiel für solche entgegenstehenden Interessen werden im Gesetz Daten genannt, die sich auf religiöse Anschauungen beziehen. Darum handelte es sich im konkreten Fall zweifellos. Daten dieser Liste haben auch andere Werber genutzt, von der UNICEF über religiöse Missionszentralen, Dritte-Welt-Organisationen bis hin zu einer Denkmalschutz-Stiftung und einer politischen Gesellschaft. Dem niedersächsischen Listbroker mußte ich mitteilen, daß nicht der auftraggebende Listeigner in Campione für die Datennutzung verantwortlich war, sondern er selbst als Adreßmittler, da die Datenverarbeitung im Auftrag einer ausländischen Stelle als eigene Datennutzung zu bewerten ist. Wegen der Datenherkunft schaltete ich den Eidgenössischen Datenschutzbeauftragten der Schweiz ein. Dieser teilte mir mit, er sei nicht zuständig, da der Ort Campione eine italienische Enklave innerhalb des schweizerischen Staatsgebietes sei. Italien hat bis heute kein Datenschutzrecht. Meine direkten Aufklärungsversuche bei der ausländischen Firma stießen bei dieser auf wenig Mitteilungsbereitschaft. Die niedersächsische Listbroking-Firma dagegen stimmte mit mir letztendlich darin überein, daß die Werbeaktion nicht hätte stattfinden dürfen. Sie will in Zukunft nicht nur bei ausländischen, sondern auch bei deutschen Auftraggebern diesen einen Hinweis geben, wenn aus der Bezeichnung der zu vermittelten Listen erkennbar ist, daß schutzwürdige Betroffeneninteressen verletzt

sein können.

33.3 Die Crux mit den Widersprüchen und der Robinsonliste

Sind Listbroker als Auftragnehmer und sonstige Adreßhändler verpflichtet, ihre Werbedaten daraufhin zu überprüfen, ob bei ihnen oder in der Robinsonliste gegen Werbeaussendungen ein Sperrvermerk gespeichert ist? Ich meine: ja. Wäre dies nicht der Fall, so bliebe der Versuch von Verbraucherinnen und Verbrauchern, von Direktwerbung verschont zu bleiben, ein Glücksspiel mit geringer Gewinnchance. Die Wirtschaft ist sich in dieser Frage noch nicht schlüssig und prüft die Rechtslage.

Ausgelöst wurde die Debatte durch folgenden Sachverhalt: Ein Petent aus Hannover erhielt im Oktober 1995 das Kreditangebot einer Verbraucherbank zugesandt. Auf den Widerspruch gegen weitere Werbezusendungen nach § 28 Abs. 3 BDSG hin erhielt er von der Verbraucherbank die Mitteilung, ein Adressenhändler sei als Listbroker mit der Abwicklung dieser Direktwerbeaktion beauftragt gewesen. Das Auskunftsersuchen des Betroffenen ergab, daß seine Adresse von einer Firma in Wuppertal stammt, wo er Kunde ist. Lieferant des Datenbestandes sei jedoch eine Werbeagentur in Hamburg. Das Sperrgesuch des Betroffenen wurde vom Adressenhändler an die Firmen in Hamburg und Wuppertal weitergegeben. Außerdem wurde er auf die Möglichkeit der Eintragung in die Robinsonliste des Deutschen Direktmarketing Verbandes (DDV) hingewiesen. Für meine Dienststelle ein gewöhnlicher Vorgang - hätte es da nicht eine Vorgeschichte gegeben:

Der Betroffene hatte schon 1992 von der Wuppertaler Firma nach einem Widerspruch die Zusicherung erhalten, seine Daten würden nicht für Werbezwecke genutzt. Zu der Nutzung der Daten aus Wuppertal kam es offensichtlich dadurch, daß die Hamburger Firma Kundenadressen unzulässigerweise eigenmächtig nutzte, obwohl diese ihr nur zur Prüfung der postalischen Qualität übergeben worden waren. Widersprochen hatte der Betroffene damals auch gegenüber einer Firma in Lübeck, von der er mit Werbung angeschrieben worden war. Dessenungeachtet hatte der Bürger ein Jahr später wieder Post von der Lübecker Firma erhalten - vermittelt von dem Adressenhändler, der erneut als Listbroker auftrat. Auch damals wurde ich vom Betroffenen eingeschaltet und erhielt vom Adreßhändler die Zusicherung, daß der Betroffene sowohl bei der eigenen Adreßselektion als auch bei der Adreßvermietung nicht mehr berücksichtigt werde. Der Adressenhändler begründete die Werbung damit, man habe Telefonbuchdaten genutzt und eingetragene Sperrvermerke nicht berücksichtigt. Der Betroffene wurde schon damals an die Robinsonliste verwiesen. In dieser Liste ist der Betroffene seit 1989 aufgrund mehrfacher Meldungen eingetragen. Trotz alledem hatte der Petent schon wieder vom Adressenhändler vermittelte Werbung aus einem Adreßbestand erhalten, der eigentlich gesperrt hätte sein müssen. Ich mußte den Adreßhändler fragen: Was soll der von Werbung traktierte Mann noch unternehmen, um von an ihn adressierten Zusendungen verschont zu bleiben?

Zunächst halte ich es für fraglich, ob der Adreßhändler für die Verbraucherbank als Auftragnehmer tätig geworden ist. Die Adreßliste für die Mailingaktion war nämlich nicht nur aus einem, sondern aus mehreren Adreßbeständen zusammengestellt worden. In diesen Fällen erfolgt zur Vermeidung von Doppelbewerbung ein Dubletten-Abgleich. Meines Erachtens setzt eine solche Zusammenführung unterschiedlicher Adreßdateien Datenübermittlungen durch die "Auftraggeber" voraus. Als Übermittlungsempfänger mit tatsächlicher Datenherrschaft kommt allein der Adreßhändler, der vermeintliche Auftragnehmer, in Betracht. Dieser ist dann verarbeitende Stelle. Die "Listbroker" erhalten von den Listeignern praktisch nie besondere Weisungen und besitzen de facto die Herrschaft über die "angemieteten" Daten. Ein Auftragsverhältnis nach § 11 BDSG ist nach alledem zumindest dann nicht mehr möglich, wenn verschiedene Datenbestände für eine Werbeaktion zusammengeführt werden.

Bisher wurde die Ansicht vertreten, daß die Nutzung der Robinsonliste des DDV durch Direktwerber freiwillig wäre. Auch ich und die anderen Aufsichtsbehörden gingen hiervon aus. Neuerdings gibt es Stimmen, die aus der Eintragung in der Robinsonliste folgern, daß schutzwürdige Interessen des Betroffenen einer Nutzung für Werbeaussendungen entgegenstehen. Dies führt im Ergebnis dazu, daß die Eintragung in die Robinsonliste faktisch dem Widerspruch im Einzelfall nach § 28 Abs. 3 BDSG gleichkommt. Diese Interpretation, für die meines Erachtens viel spricht, liegt offensichtlich auch im Interesse des DDV, der zum Ausdruck brachte, daß der obligatorische Datenabgleich mit seiner Robinsonliste wünschenswert sei.

Auch Auftragnehmer sind meines Erachtens regelmäßig verpflichtet, gegenüber diesen nach § 28 Abs. 3 BDSG ausgesprochene Widersprüche zu berücksichtigen. Bei offensichtlichen Datenschutzverstößen müssen Auftragnehmer den Auftraggebern gemäß § 11 Abs. 3 Satz 2 BDSG einen Hinweis geben. Es ist für den Listbroker offensichtlich, daß schutzwürdige Interessen eines Betroffenen einer Datennutzung entgegenstehen, wenn von diesem beim Listbroker ein Widerspruch nach § 28 Abs. 3 BDSG vorliegt. Gibt der Auftraggeber dennoch die Weisung, bestimmte Daten (rechtswidrig) zu nutzen, so stellt sich die Frage, ob die Weisung für den Auftragnehmer bindend ist. Nach § 134 BGB ist ein Rechtsgeschäft, das gegen ein gesetzliches Verbot verstößt, nichtig. Beim Datenschutzrecht handelt es sich nicht um für Auftragnehmer und Auftraggeber unverbindliche Ordnungsvorschriften, sondern um gesetzliche Pflichten. Ich denke nicht, daß der Auftraggeber die Verwendung von Adressen wünscht, bzgl. derer bei ihm, beim Auftragnehmer oder in der Robinsonliste ein Widerspruch vorliegt.

Inzwischen hat mir der beteiligte Adreßhändler versichert, die Adreßdaten des Betroffenen in eine absolute Sperrdatei aufzunehmen, die sicherstellt, daß die Daten weder bei direkten Mailing-Aktionen noch im Rahmen der Adreßvermietung Verwendung finden. Er pflichtete mir bei, daß die aktuelle Praxis beim Umgang mit Widersprüchen nicht optimal sei. Um aber Wettbewerbsverzerrungen zu vermeiden, müsse

bundesweit ein einheitliches Vorgehen erreicht werden. Ob dies möglich ist, wird derzeit noch geprüft.

33.4 Mit dem Berliner Bären auf Kundenjagd

Mein Kollege in Berlin informierte mich über eine äußerst fragwürdige Werbemethode eines niedersächsischen Münzenvertriebs: Am 22. Oktober 1995 war in Berlin die Wahl zum Abgeordnetenhaus. Viele Bürgerinnen und Bürger der Stadt erhielten kurz zuvor eine mit einem Berliner Wappen versehene und einer Wahlbenachrichtigung nachempfundene "Benachrichtigung für Wahlberechtigte - persönlich, nicht übertragbar". Die Empfänger hätten bis zum 30. Oktober 1995 das "Sonderanrecht für eine von nur 5.000 Berliner-Kollektionen" einer Silbermünzen-Reihe mit örtlichen Motiven. Angeschrieben wurden u.a. auch Insassen einer Justizvollzugsanstalt. Mein Kollege hatte die nicht ganz unbegründete Sorge, daß das Wählerverzeichnis Berlins für Marketingzwecke mißbraucht worden ist. Diese Sorge war unbegründet. Was sich aus den Stellungnahmen des Münzvertriebs ergab, war aber nicht gerade beruhigend: Die Verwendung der offiziellen Abbildung des "Berliner Bären" beruhe auf einem "individuellen Fehler". Die Adressen stammten nicht aus dem Wählerverzeichnis, sondern von einer großen süddeutschen Direktmarketing-Agentur. Angeschrieben wurden nicht 5.000 ausgewählte Wählerinnen und Wähler, sondern 200.000 Personen, die aus 11 Zielgruppen, z.B. Zeitschriften- oder Weinkäufer, selektiert worden sind. Auswahlkriterien waren: Männer, Alter über 45 Jahre, PLZ-Gebiet Berlin. Die Datenbeschaffung erfolgte über einen großen süddeutschen Adressenhändler. Ich mußte den Münzvertrieb darauf hinweisen, daß seine Direktwerbemaßnahme einen Verstoß gegen das datenschutzrechtlich begründete Transparenzgebot (§§ 33, 34 BDSG) darstellt. Erfolgt eine Benachrichtigung der Betroffenen über eine Datenspeicherung, und sei dies auch nur indirekt durch die Zusendung von Werbung, so sind die beteiligten Stellen verpflichtet, korrekte Angaben z.B. über die Herkunft der Daten zu machen.

33.5 Der Brief an den Weihnachtsmann

In Niedersachsen gibt es Orte mit weihnachtlich anmutenden Namen: Himmelsthür, Nikolausdorf, Himmelpforten. In diesen Orten wird ein besonderer Weihnachtsservice angeboten: Kinder haben die Möglichkeit, ihre Weihnachtswünsche über das dortige Postamt an den Weihnachtsmann oder das Christkind zu schicken. Die Kinder bekommen dann vom Christkind bzw. dem Weihnachtsmann auch eine Antwort. Eine schöne Idee, bei der der Datenschutz zunächst nichts verloren hat. Eine Journalistin unterrichtete mich aber über einen fragwürdigen Umgang mit den Wunschzetteln der Kinder: Diese, im konkreten Fall waren es mehr als 10.000 Briefe, wurden an einen Verlag weitergeben, der daraus, teilweise durch Abdruck in Faksimile, ein Buch zusammenstellte. Dieses offenbart und dokumentiert, so die Verlags-Eigenwerbung, "die Wunsch- und Gedankenwelt der Kinder in eindringlicher Weise". Aber nicht nur das. So war zu lesen: "Meine Eltern haben nicht viel Geld, denn meine Mutter und ich mußten ausziehen, weil mein Papa und meine Mama sich nicht vertragen können. Deshalb schicke mir 1.000 DM zu Weihnachten". Oder: "Wir

sind drei kleine Kinder. Unsere Mutter ist vor 2 Jahren mit einem anderen Mann abgehauen und hat uns und Vati allein gelassen. Vati ist jetzt geschieden und muß die Schulden von Mama bezahlen. Vati ist mit den Nerven so fertig, weil er keine Arbeit und kein Geld kriegt. Wir wohnen bei Oma und die bekommt Kindergeld. Vati bekommt nirgends Geld her, um uns Spielsachen zu kaufen". Zwar wurden zu den Wunschbriefen regelmäßig nur Vorname und Ort genannt. In kleinen Orten sind aber unter Umständen die Briefe doch zuzuordnen, so daß Nachbarn, Verwandte oder Bekannte intime Familiendetails erfahren können. Die Eltern der Kinder wurden dann auch noch von dem Verlag angeschrieben mit dem Angebot, für knapp 25 DM das Buch zu erwerben. Für 15 DM Aufpreis wurde das Buch mit abgedrucktem persönlichen Wunschzettel des eigenen Kindes angeboten.

Der für die Post zuständige Bundesbeauftragte für den Datenschutz kritisierte den Umgang mit den vertraulichen Briefen durch die Post (vgl. 15. TB BfD, S. 311). Problematisch war nicht nur die Herausgabe der Briefe selbst, sondern auch die Weitergabe der Adressen der Eltern zum Zweck der Buchwerbung. Die Weihnachtspostämter wurden darauf hingewiesen, daß es nicht zulässig ist, die vertraulichen Briefe weiterzugeben. So wird es künftig möglich sein, daß Kinder wieder vertrauensvoll dem Weihnachtsmann ihr Herz ausschütten. Gegen die Veröffentlichung durch den Verlag konnte nichts weiter unternommen werden, da dieser die Pressefreiheit nach Art. 5 Grundgesetz sowie das Medienprivileg nach § 41 BDSG in Anspruch nehmen kann. Aus datenschutzrechtlicher Sicht nicht in Ordnung war dagegen die Nutzung der Adreßangaben der Eltern durch den Verlag, da diese Angaben nicht zu eigenen journalistisch-redaktionellen Zwecken genutzt wurden. Der Verlag beteuerte gegenüber meinem Kollegen in Hamburg als zuständiger Aufsichtsbehörde, daß es zu einer Wiederholung dieser Aktion nicht kommen wird.

33.6 Das Geschäft mit der Not

Ein Bürger, der soeben wegen Zahlungsunfähigkeit erleben mußte, daß sein Haus zur Zwangsversteigerung ausgeschrieben wurde, erhielt eine Postkarte eines Wirtschaftsberaters mit folgendem Text: "Ihre Vergangenheit: Ich weiß... Sie haben alles versucht und nichts hat geklappt! Nur leere Versprechungen! Ihre Zukunft: Keine Lohn-/Gehaltspfändungen, keine Pfändung Ihrer Einrichtung ... Schulden in den nächsten drei Jahren komplett abbauen. Keine leeren Versprechungen! Wir haben Kaufinteressenten!". Diesem Schreiben folgten 13 weitere "Hilfsangebote" von Immobilienmaklern, Unternehmensberatern, "Selbsthilfevereinen" u.ä., teilweise verbunden mit einem Fragebogen, aus ganz Deutschland. Soweit die Angebote aus Niedersachsen kamen, forderte ich Stellungnahmen zu Herkunft und Nutzung der Betroffenendaten an. Die Antworten gingen alle in die gleiche Richtung: Die Daten stammten vom Aushang der Zwangsversteigerung beim Amtsgericht, aus dem Niedersächsischen Staatsanzeiger oder aus der amtlichen Verlautbarung in der örtlichen Presse. Durchgängig wurde mir mitgeteilt, daß die Daten nur für eigene Zwecke genutzt würden, teilweise, daß sie schon wieder gelöscht worden seien. Ich mußte dem Petenten mitteilen, daß ich keinen

Rechtsverstoß erkennen kann: Aus öffentlichen Quellen zu entnehmende Daten dürfen für eigene Zwecke verarbeitet werden, wenn dem nicht schutzwürdige Interessen der Betroffenen offensichtlich entgegenstehen (§ 28 Abs. 1 Satz 1 Nr. 3 BDSG).

Das datenschutzrechtliche Problem des Vorgangs liegt nicht nur in der Nutzung der Zwangsversteigerungsdaten, sondern schon in deren Veröffentlichung. Nach den §§ 39 f. Zwangsversteigerungsgesetz ist die Terminsbestimmung einer Zwangsversteigerung öffentlich in einer Zeitung bekannt zu machen und an der "Gerichtstafel" anzuheften. Derartige Veröffentlichungsvorschriften, die allesamt aus einer Zeit stammen, in der es weder elektronische Datenverarbeitung noch überregionales Direktmarketing gab, müssen heute generell auf ihre Erforderlichkeit und Zeitgemäßheit hin überprüft werden. Im konkreten Fall habe ich zudem Zweifel, ob der Name der Schuldnerin bzw. des Schuldners bekanntgegeben werden muß.

34. Kundendaten und Werbung

34.1 Neue Zoo Card für Besucher des hannoverschen Zoos

Der Zoo in Hannover hat die bisherigen Dauerkarten aus Pappe durch eine Plastik-ZooCard mit Lichtbild des Inhabers ersetzt. Für die Ausstellung dieser Karte werden von den Antragstellern Familienname und Vorname, Adresse (Straße, Hausnummer, Postleitzahl, Ort), Beruf, Geburtsdatum und Telefonnummer erhoben. Das Foto auf der ZooCard dient der Identifizierung des Card-Inhabers beim Betreten des Zoos. Die Zoo GmbH hat versichert, daß die erhobenen Daten ausschließlich für eigene Geschäftszwecke gespeichert werden. Auf dem Antragsformular ist die Erklärung abgedruckt, daß der Unterzeichner mit der Speicherung seiner Daten einverstanden ist. Der entsprechende Hinweis bezieht sich auch auf die Zusendung von Wissenswertem über den Zoo. Die Daten bleiben bei der Zoo GmbH grundsätzlich so lange gespeichert, wie sie zur Erfüllung des Vertragszwecks benötigt werden. Nach Beendigung des Vertragsverhältnisses werden die Daten daher regelmäßig gelöscht, soweit sie nicht weiter für Zwecke der Zusendung von Informationen über den Zoo in zulässiger Weise entsprechend § 28 Abs. 1 Satz 1 Nr. 2 BDSG verwendet werden. In diesen Fällen erfolgt eine Löschung ein Jahr nach Ablauf des Vertragsverhältnisses. Einem schriftlichen Löschungsbegehren eines Besuchers hinsichtlich seines ebenfalls im EDV-System gespeicherten Fotos wird unmittelbar entsprochen.

Die Zoo GmbH will mit den auf dem Antragsformular eingeforderte Berufsangaben feststellen, welche Berufsgruppen den Zoo besonders häufig besuchen. Das Geburtsdatum dient zur Feststellung der Volljährigkeit. Außerdem wird damit die Absicht verbunden, insbesondere Kindern, aber ggf. auch Erwachsenen zu ihrem Geburtstag eine kleine Aufmerksamkeit seitens des Zoos zukommen zu lassen. Die Telefonnummer schließlich wird erhoben, um ggf. bei Verlust der Zoo Card oder bei Rückfragen, die die Zoo Card betreffen, den Inhaber schneller als auf schriftlichem Wege erreichen zu können. Die Telefonnummer werde nicht zu Werbezwecken erhoben oder verwendet. Der Zoo ist darüber informiert, daß eine Einwilligung zur Übersendung von Informationen nicht gleichbedeutend ist mit einem Einverständnis für Telefonmarketing-Maßnahmen.

Ich empfahl, auf dem Formular zusätzliche Hinweise auf die Freiwilligkeit der Angabe des Berufes und ihres Verwendungszweckes sowie auch der Telefonnummer aufzunehmen. Dies soll künftig berücksichtigt werden. Ich habe den Eindruck gewonnen, daß der Zoo nachdrücklich bereit ist, den Umgang mit Besucherdaten datenschutzkonform zu handhaben.

34.2 Parteienwerbung

Daß Werbung für den Betroffenen unter Umständen eine äußerst sensible Angelegenheit sein kann, zeigt folgender Vorfall: Eine Bürgerin erhielt von dem Ortsverband einer Partei über die Adresse ihres Arbeitgebers eine Einladung zu einer Parteiveranstaltung. Diese war darüber sehr irritiert und fragte nach der Herkunft der Adresse. Der Ortsverband entschuldigte sich zwar, legte aber die Herkunft der Daten, auch nach weiteren Nachfragen, nicht offen. Nachdem ich mich in diesem Vorgang einschaltete, kam ein wenig Licht ins Dunkel: Angeschrieben wurden nicht nur Personen, die dies ausdrücklich gewünscht haben. Es kommt häufig vor, daß Parteimitglieder telefonisch Anschriften von vermeintlich Interessierten weitergeben, denen dann Einladungen zugesandt werden. Im konkreten Fall ließ sich angeblich nicht ermitteln, wer die Anschrift zur Verfügung gestellt hatte. Der Name der Bürgerin würde, so die Partei, in jedem Fall nicht mehr gespeichert.

Die Zugehörigkeit oder das Nahestehen zu einer politischen Partei ist ein äußerst sensibles Datum, dessen Kenntnis beim Arbeitgeber zu Problemen führen kann. Parteien sollten äußerst vorsichtig mit den Daten ihrer Mitglieder und (vermeintlichen) Anhänger umgehen. Eine Weitergabe zu anderen als Parteizwecken ist prinzipiell durch § 28 Abs. 2 Nr. 1 Buchst. b BDSG ausgeschlossen.

34.3 Die private Telefonnummer im Bankeinzugsverfahren

Von dem Herausgeber eines Anzeigenblattes werden die Kosten für die Veröffentlichung von Kleinanzeigen auf dem Wege des Bankeinzugsverfahrens abgerechnet. Dabei wurde auf den bei der Bank eingereichten Abbuchungsbelegen unter dem Verwendungszweck neben der Rechnungsnummer auch die private Telefonnummer der Inserentin oder des Inserenten angegeben. Ein Kunde des Anzeigenverlages nahm Anstoß an diesem Verfahren. Er hatte eine geheime Telefonnummer und wolle nicht, daß die Bankmitarbeiter von dieser Kenntnis erhalten. Ebenso wie der Petent sah ich kein Erfordernis für die Übermittlung der dem Anzeigenblatt nur für Zwecke des Inserates zur Verfügung gestellten privaten Telefonnummer an die Bank. Der Verlag hat sich meinen datenschutzrechtlichen Bedenken angeschlossen und sich bereit erklärt, für die Zukunft auf die Angabe der Telefonnummer im Bankeinzugsverfahren zu verzichten.

35. SCHUFA: Viermal Klaus Müller, geb. am 4.4.1944

Ein Klaus Müller, geb. am 4.4.1944 (Angaben geändert), teilte mit, er sei " General director of board europe" eines großen amerikanischen Konzerns. Bei einer Bank habe er eine private Baufinanzierung vornehmen lassen wollen; zur Kreditabsicherung sei die Beleihung eines bisher unbelasteten Grundstücks vorgesehen gewesen. Wegen eines Suchvermerks bei der Schufa in Höhe von 16.000 DM sei es dann nicht zum Vertragsabschluß gekommen. Dieser Suchvermerk habe sich aber offensichtlich auf einen anderen Klaus Müller, geb. am 4.4.1944, bezogen. Die Konsequenzen der negativen Schufa-Eintragungen seien gravierend gewesen: Das Girokonto wurde sofort gekündigt, ein ausgestellter Scheck sei dadurch geplatzt - und wurde in der Schufa-Datei gespeichert. Beauftragte Handwerker seien von der Bank über die vermeintlichen Außenstände unterrichtet worden. Ein Gerichtsvollzieher habe schon vor der Tür gestanden und eine Forderung über DM 8.000 eines Klaus Müller aus Stuttgart aus dem Jahr 1987 eintreiben wollen. Durch die "Falschauskunft" der Schufa sei ihm ein Schaden von DM 200.000 entstanden. Er befürchte, wegen dieser Unregelmäßigkeiten Probleme mit seinem Konzern zu bekommen.

Tatsächlich kam es aufgrund der Schufa-Eintragung zum Abbruch mehreren Geschäftsbeziehungen. Eine erste Prüfung der Schufa ergab, daß die per Suchvermerk ausgeschriebene Person mit dem Petenten Klaus Müller nicht identisch sein dürfte, was zu einem Vermerk im Schufa-System führte, der auf die Verwechslungsgefahr hinwies. Von seiten der Schufa wurde in diesem Zusammenhang auf die Pflicht aller Schufa-Vertragspartner hingewiesen, sich eindeutig über die Identität der Kreditsuchenden zu vergewissern.

Der Fall bekam eine völlig neue Wendung, als mir die Schufa mitteilte, inzwischen hätte sie Erkenntnisse, daß es sich bei der Wohnadresse des Herrn Müller um eine Entlaßadresse aus einer Vollzugsanstalt handele. Weitere Recherchen ergaben, daß alle vier getrennt geführten Schufa-Datensätze einem einzigen, d.h. dem Petenten Herrn Müller zuzuordnen seien, der wegen Betrügereien schon mehrfach inhaftiert gewesen sei.

Der Fall war für mich Anlaß, gegenüber der Bundes-Schufa anzuregen, bei gleichen Identifizierungsdaten automatisch im Schufa-System Warnvermerke aufzunehmen, bei erstmaliger Eintragung von Negativmerkmalen eine Benachrichtigung der Betroffenen vorzunehmen oder die Schufa-Vertragspartner zumindest zu verpflichten, Kundinnen und Kunden über Eintragungen von Negativmerkmalen zu unterrichten. Angesichts des konkreten Falls wollte die Bundes-Schufa meinen Änderungsvorschlägen nicht folgen. Gegenüber den Kreditinstituten gäbe es aber die Empfehlung, mit den Betroffenen den Inhalt der

Schufa-Auskünfte abzustimmen, wenn die Schufa-Auskunft zu einer negativen Entscheidung führt oder wenn die Eigenangaben des Betroffenen gegenüber der Bank von dem Inhalt der Schufa-Auskunft abweichen. Diese Empfehlung sei erst vor ca. zwei Jahren von seiten des Zentralen Kreditausschusses (ZKA) gegenüber dessen Mitgliederinstituten erneuert worden.

Der außergewöhnliche Fall zeigt zweierlei: Zum einen ist nicht zu bestreiten, daß die Einrichtung der Schufa sinnvoll ist. Unter dem Schutz des Arguments "Datenschutz" soll niemand Betrügereien vornehmen können. Auf der anderen Seite können Verwechslungen und Falscheintragungen bei der Schufa zu viel Ärger, ja unter Umständen in kritischen ökonomischen Lebenssituationen zu einer existentiellen Gefahr führen. Gerade deshalb ist die Beachtung des Datenschutzes bei dieser Einrichtung fundamental. Da Fehler nie völlig vermeidbar sind, ist eine enge und vertrauensvolle Zusammenarbeit der Schufa-Geschäftsstellen mit den Aufsichtsbehörden notwendig. Beim konkreten Fall brachte diese auch eine schnelle Klärung.

Kurz nach dem Abschluß des Falles "Klaus Müller" wurde ich mit dem Fall "Beate Meier" konfrontiert, geb. am 2.2.1962 (Angaben geändert). Unter diesem Namen und dem Geburtsdatum wurden von der SCHUFA zwei Datensätze geführt. Aufgrund einer inhaltlich zutreffenden, aber eine andere Beate Meier betreffenden SCHUFA-Auskunft änderte die Bank einfach die gesamten Adreßangaben, mit der Folge, daß diese Bank ihre gesamte Korrespondenz mit der falschen "Beate Meier" führte. Erst nach knapp einem halben Jahr und unter Einschaltung meiner Dienststelle konnte sichergestellt werden, daß die Korrespondenz wieder korrekt verteilt wurde.

36. Auskunfteien

36.1 Datenklau durch Wirtschaftsauskunftei

Im April 1995 hatte ein Nachrichtenmagazin folgende Titelgeschichte: "Skandal: Größter Datenklau". Es wurde berichtet, daß sich eine Berliner Wirtschaftsauskunftei unter Vorspiegelung falscher Identitäten (z.B. als Polizei, Krankenhaus oder sogar als Betroffener selbst) bei datenverarbeitenden privaten wie öffentlichen Stellen in großem Umfang unzulässig Daten beschafft hat. Die Staatsanwaltschaft ermittelte und führte eine großangelegte Durchsuchung durch. Nach dem Pressebericht gehörten auch zwei große niedersächsische Versicherungen zu den Kunden der Wirtschaftsauskunftei. Auf Anfrage teilten diese mir übereinstimmend mit, sie hätten von den aggressiven Ermittlungsmethoden der Wirtschaftsauskunftei nichts gewußt. Die Aufträge seien von der Berliner Niederlassung, nicht von der Zentrale erteilt worden. Es sei um die Klärung von Bonitätsfragen im Zusammenhang mit Regreßforderungen aus Schadensfällen gegangen. Von den Bonitätsauskünften würde abhängig gemacht, ob es sinnvoll sei, bestehende Ansprüche rechtlich weiter zu verfolgen. Die Bonitätsauskünfte seien jeweils zur Schadenakte genommen worden und würden weder dateimäßig gespeichert noch anderweitig genutzt. Interessant an diesen Auskünften ist, daß negative Bonitätsangaben für die Betroffenen hier offensichtlich von Vorteil sind: Diese werden von Versicherungen wegen eines Schadens-Regresses nicht weiter behelligt. Dies rechtfertigt aber natürlich nicht eine illegale Datenbeschaffung. Schon die Presseberichte haben offensichtlich dazu geführt, daß dieser Auskunftei keine weiteren Aufträge erteilt werden.

36.2 Benachrichtigung nach § 33 BDSG als Wink mit dem Zaunpfahl

Auskunfteien betreiben geschäftsmäßige Datenverarbeitung zum Zweck der Übermittlung. Sie sind daher nach § 33 Abs. 1 Satz 2 BDSG verpflichtet, Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Eine große bundesweite Auskunftei-Organisation, deren Mitgliederfirmen zugleich als Inkassobüros arbeiten, hatte sich nun eine elegante Form der Benachrichtigung einfallen lassen: Beim Eintreiben der Forderungen teilten Sie dem mutmaßlichen Schuldner am Ende mit: "P.S.: Über Sie sind diese Daten gespeichert bei der Firma XX, Postfach, Ort YY". Damit wußte die Empfängerin bzw. der Empfänger, daß das Nichtbezahlen der fremden Forderung einer Auskunftei bekannt ist und unter Umständen bundesweit auf Anfrage mitgeteilt wird. Ein solches Wissen fördert natürlich die Zahlungsbereitschaft ungemein: Wer will schon bundesweit als unzuverlässiger Kunde dastehen? Abgesehen von diesem Wink mit

dem Zaunpfahl erfuhren die Betroffenen aber nichts: Postfachnummer, Adresse und Postleitzahl wurden ebenso wenig mitgeteilt wie der rechtliche Grund des PS-Vermerks. § 33 BDSG verlangt, daß die verarbeitende Stelle eindeutig bezeichnet wird. Die Regelung soll für mehr Transparenz sorgen und den Bürgerinnen und Bürgern die Wahrnehmung ihrer Rechte erleichtern. Eine unvollständige Postfachadresse genügt da unter keinen Umständen. So mußten für eine richtige Adressierung bei den Betroffenen zunächst Recherchen durchgeführt werden. Mangels Angabe der Hausadresse war eine persönliche Vorsprache noch schwieriger.

Da die unzureichende Benachrichtigung der Betroffenen eine Ordnungswidrigkeit darstellt (§ 44 Abs. 1 Nr. 3 BDSG), leitete ich gegen eine der Auskunfteien ein Bußgeldverfahren ein. Dieser Wink mit dem Zaunpfahl wurde von der Bundesorganisation der Auskunfteien offensichtlich sofort verstanden. Mir wurde mitgeteilt, daß binnen Monatsfrist die Benachrichtigung bundesweit auf folgenden Text umgestellt würde: "Benachrichtigung gemäß § 33 BDSG: Über Sie sind diese Daten gespeichert bei: Fa. XX KG, ZZ-Straße, Plz Ort YY". Tatsächlich wird inzwischen so verfahren. Da nun für die Zukunft eine datenschutzkonforme Praxis zu erwarten war, stellte ich das Bußgeldverfahren ein. Ich frage mich aber: Weshalb mußte hier erst mit einem Bußgeld gedroht werden?

36.3 Auskunfteirecherche über mißliebigen Journalisten?

Welche Bedeutung die Benachrichtigung nach § 33 BDSG hat, zeigt der Fall eines Journalisten, dem von einer Auskunftei mitgeteilt worden war, daß seine Daten erstmalig weitergegeben worden sind. Auf Nachfrage bei der Auskunftei erfuhr er, daß Anfragender eine süddeutsche Firma sei. Nähere Angaben wurden ihm verweigert. Nun hatte der Journalist aber seit Jahren keine geschäftlichen Kontakte nach Süddeutschland gehabt, die ein berechtigtes Abfrageinteresse hätten begründen können. Wohl aber hatte der Journalist über die "Machenschaften der Scientology-Sekte" und Zusammenhänge zu einem süddeutschen Unternehmen berichtet. Zunächst mußte ich gegenüber der Auskunftei beanstanden, daß ohne ersichtlichen Grund Angaben zur Ehefrau des Journalisten gespeichert und weitergegeben wurden. Auf meine Frage nach dem "berechtigten Interesse" mußte von der Auskunftei erst noch einmal nachgefragt werden. Die bayerische Firma behauptete darauf, sie habe den Journalisten als Referenten für ein Schulungsvorhaben von Führungskräften ansprechen wollen. Das Geschäft sei nicht zustande gekommen, so daß die Angelegenheit für erledigt angesehen werde. Die Antwort der bayerischen Firma endete mit den Worten: "Im übrigen dürfen wir Sie zukünftig bitten, von Nachfragen dieser Art Abstand zu nehmen, da wir nicht mehr bereit sein werden, über das übliche Maß hinaus unsere Geschäftsvorhaben bis ins Detail darzulegen". Da der Journalist im Bereich "Managementschulung" bisher nicht tätig war, mußte ich annehmen, daß hier eine Phantasiebegründung gewählt wurde und in Wirklichkeit ein ganz anderes Auskunftsinteresse verfolgt wurde. Aber selbst diese Phantasiebegründung rechtfertigte keine Datenweitergabe durch die Auskunftei. Ich erlegte daher der Auskunftei auf, der bayerischen Firma in Zukunft keine Auskünfte mehr zu erteilen.

37. Finanzwirtschaft

Die Zahl der Eingaben aus dem Finanzbereich nimmt ständig zu. Die Gründe dürften vielfältig sein: verstärkte Automation und erhöhtes Informationsinteresse bei den Unternehmen, aber auch erhöhte Sensibilität der Kundinnen und Kunden in Datenschutzfragen. Die Bandbreite der Probleme ist groß. Einige Stichworte: Ich konnte mangels rechtlicher Handhabe nicht erreichen, daß eine Bank ihre seit 25 Jahren praktizierte Übung, in der Kunden- bzw. Kontonummer das Geburtsdatum aufzunehmen, änderte. Wer einen Überweisungsauftrag ausfüllt, offenbart damit zwangsläufig seinen Geburtstag. Gegenüber der Postbank konnte ich zumindest teilweise erreichen, daß diese ihre Formulare zur Kontoverlängerung bzw. -änderung so umgestaltete, daß nicht erforderliche Daten nicht angegeben werden müssen. In einigen Banken wurde aus Sicherheitsgründen unter Zuhilfenahme der EC-Karten eine ausnahmslose Zugangskontrolle eingeführt. Mir wurde mitgeteilt, daß die dabei verarbeiteten Daten weder längerfristig gespeichert noch zu anderen als Sicherheitszwecken benutzt werden, so daß ich keine Veranlassung sah einzugreifen.

37.1 Wertpapierhandel: Freiwillige Beratung oder Zwangsangaben?

Mehrere Kunden einer Bank fragten bei mir irritiert wegen eines Fragebogens an, der ihnen von ihrem Geldinstitut zugesandt worden war. Unter Hinweis auf den seit 1. Januar 1995 geltenden § 31 Abs. 2 Wertpapierhandelsgesetz (WpHG) forderte die Bank ihre Depot-Kunden auf, bis zu einem festen Termin detaillierte Angaben zu machen über Beruf, Position, selbständige Tätigkeit, Güterstand, Anzahl der unterhaltsberechtigten Kinder, über das bisherige Anlageverhalten (Art, ausländisch-inländisch, seit wieviel Jahren, wie oft, in welcher Höhe, auf Kreditbasis), über Kreditrahmen, Vermögen, Verbindlichkeiten, Einkünfte, Ausgaben und Überschuß sowie über verfolgte Anlageziele. Ein Hinweis auf die Folgen einer Auskunftsverweigerung wurde nicht gegeben.

Statt der von mir geforderten Stellungnahme der betreffenden Bank erhielt ich ein Schreiben des Bundesverbandes deutscher Banken (BdB), der den Fragebogen als Mustertext erstellt und den Mitgliedsbanken empfohlen hatte. Mit dem Fragebogen werde das Ziel verfolgt, eine anleger- und anlagegerechte, d.h. eine ordnungsgemäße Anlageberatung sicherzustellen. Einige der an der Fragebogenaktion teilnehmenden Banken würden die erhaltenen Kundeninformationen EDV-technisch aufbereiten, um sie zum Zweck der Anlageberatung abrufbar zu halten. Meine Bedenken wollte der BdB nicht teilen. Derweil wurden von der betreffenden Bank die genannten Fragebögen weiter an

Kundinnen und Kunden versandt.

Mit dem Fragebogen sollen die Anlageberater in die Lage versetzt werden, die Schutzbedürftigkeit der Kundinnen und Kunden verläßlich einschätzen zu können. So kann beurteilt werden, ob die angestrebte Wertpapieranlageform für die jeweils Betroffenen finanziell verkraftbar und sinnvoll ist. § 31 Abs. 2 WpHG verpflichtet die Wertpapierdienstleistungsunternehmen, Angaben zu verlangen, nicht aber die Kundinnen und Kunden, die Angaben zu machen. Neben dem Kundenschutz ist es nur eine abgeleitete Zielsetzung, die Wertpapierdienstleistungsunternehmen vor unberechtigten Schadensersatzansprüchen wegen (angeblicher) Falschberatung zu schützen. Der Kundin bzw. dem Kunden muß es möglich sein, Angaben zu verweigern, auch auf die Gefahr hin, daß dadurch eine unvollständige Beratung und dadurch eine ungünstige Geldanlage erfolgt. Ich halte es also für unabdingbar, daß die Betroffenen auf die Freiwilligkeit ihrer Angaben hingewiesen werden (vgl. § 4 Abs. 2 Satz 1 BDSG).

§ 31 Abs. 2 WpHG begründet keine Pflicht zur Nacherhebung bei Altkunden. Bei Altkunden ist daher eine Erhebung nur sinnvoll, wenn neue Wertpapiere erworben werden sollen.

Die gestellten Fragen gingen viel zu sehr ins Detail. Nach der Art der geplanten Geldanlage muß differenziert werden. So besteht kein Bedürfnis nach einer Kundenbefragung, wenn ein einmaliger Erwerb eines relativ billigen und risikofreien Wertpapiers ansteht. Die Problematik anleger- und anlagegerechter Beratung verstärkt sich, je risikobehafteter, je umfangreicher und je mehr auf Dauer angelegt das Wertpapiergeschäft ist. Angaben über Beruf, Position, Güterstand, unterhaltsberechtigte Kinder, ziffernmäßige Angaben zu Vermögen, Verbindlichkeiten, Einkünften, Ausgaben und Überschuß halte ich ebensowenig für angebracht wie Angaben zu Kreditkarten, Versicherungen, Erbschaften oder dem Namen des Steuerberaters. Der mir vorliegende Anlageberatungsbogen des Niedersächsischen Sparkassen- und Giroverbandes ist geeigneter. Dort wird im Ankreuzverfahren allgemein nach speziellen Anlagezielen, Kenntnissen, Erfahrungen und nach der Risikobereitschaft gefragt. Die finanziellen Verhältnisse werden nur nach groben Kategorien erhoben. Für eine differenzierte Dokumentation besteht die Möglichkeit, als Freitext Bemerkungen einzutragen.

Der BdB hat zu Recht darauf hingewiesen, daß sich die Zweckbindung der Angaben aus der Zielsetzung bzw. dem Schutzzweck des § 31 Abs. 2 WpHG ergibt. Zur Zielerreichung ist nur die Dokumentation der Angaben erforderlich, nicht deren elektronische Speicherung in einem bankintern allgemein zugänglichen Informationssystem. Daher dürfen ausgefüllte Bögen lediglich in Papierform zur Kundenakte genommen werden. Für eine darüber hinausgehende Speicherung sehe ich keine Notwendigkeit. Die nach § 31 Abs. 2 WpHG vorgesehene Befragung muß zumindest in rudimentärer Form ohnehin anläßlich jedes neuen Vertragsabschlusses erfolgen, da sich seit dem letzten Vertragsabschluß die finanziellen Möglichkeiten und Wünsche geändert haben können. Eine elektronische Speicherung erhöht die Gefahr des unberechtigten

Zugriffs und das Risiko einer zweckwidrigen Nutzung, z.B. einer Auswertung der sehr sensiblen Angaben für Direktmarketingzwecke. Bei einer elektronischen Speicherung wäre eine schriftliche Einwilligung der Betroffenen erforderlich (§ 4 Abs. 2 Satz 2 BDSG).

Die Bank teilte mir mit, daß sie aufgrund meiner Intervention ihre Filialen angewiesen hat, keine Depotfragebögen mehr zu versenden und bei den Beratungsgesprächen auf die Freiwilligkeit der Angaben hinzuweisen.

37.2 Geldwäsche: Bisher fast nur weiße Westen!

Insbesondere Anfang 1995, aber auch noch bis zum Ende des Berichtszeitraumes, erreichten mich viele Beschwerden von teilweise langjährigen Kundinnen und Kunden von Kreditinstituten: Die Bank verlange eine persönliche Identifizierung anhand eines Personalausweises oder Reisepasses, der bei der Gelegenheit auch noch kopiert und abgeheftet wurde. Die Frage nach dem "Warum" wurde regelmäßig mit dem Schlagwort "Geldwäschegesetz" beschieden. Tatsächlich sieht das Ende 1993 in Kraft getretene Geldwäschegesetz (GwG) vor, daß bei Bargeldtransaktionen von 20.000 DM und mehr eine eindeutige Identifizierung der einzahlenden Person erfolgen muß. Erstaunlicherweise hatten jedoch alle, die sich an mich wandten, weniger als 20.000 DM eingezahlt und waren oft den Bediensteten am Schalter seit langem persönlich bekannt. Hilfsweise beriefen sich Banken auf § 154 Abs. 2 Abgabenordnung (AO). Dort werden Banken verpflichtet, sich über die Person des Verfügungsberechtigten eines Kontos zu vergewissern. Diese Identifikationspflicht verfolgt das Ziel der formalen Kontenwahrheit aus steuerlichen Gründen zugunsten des Fiskus und hat mit dem Ziel des GwG, Strafverfolgungsbehörden Anhaltspunkte für illegale Geldwäschetransaktionen zu verschaffen, nichts zu tun (so auch Urteil des BGH, DuD 1995, 363 ff.).

Dies bedeutet: Ist die Identität der Person, die ein Konto innehat oder eröffnen möchte, der Bank bekannt, so muß und darf sie von dem Betroffenen keine weiteren Angaben verlangen. Ausweisart, Ausweisnummer und ausstellende Behörde haben die Bank bei einfachen Kontoeröffnungen nicht zu interessieren. Derartige Daten können aber auf freiwilliger Basis erhoben werden, so daß bei einer Kontoverfügung von mehr als 20.000 DM auf eine erneute Identifizierung verzichtet werden kann (§ 7 GwG). Darüber hinausgehende Verlautbarungen des Bundesaufsichtsamtes für das Kreditwesen (BAKred) berücksichtigen nicht den Datenschutz der Kundinnen und Kunden.

Alle identifizierungspflichtigen, d.h. über 20.000 DM hinausgehenden, Transaktionen werden in den Banken elektronisch aufgezeichnet und sechs Jahre gespeichert. Diese Daten dürfen nur zur Aufklärung geldwäscherelevanter Straftaten genutzt werden (§§ 9, 10 GwG). Bei einer Vielzahl von Gesprächen mit Vertretern der Banken und des BAKred erhärtete sich bei mir der Eindruck, daß diese gewaltigen Datenbestände praktisch nicht genutzt werden und auch nicht wirksam

genutzt werden können. Die Vermutung, daß diese "Datenfriedhöfe" ein unzulässige Vorrats-Datenverarbeitung darstellen, drängt sich auf.

Nicht nur die Speicherung der Transaktionen, auch die von den Banken vorzunehmenden Meldungen bei einem Geldwäscheverdacht brachten bisher nur wenig Erfolge bei der Bekämpfung von Geldwäschestraftaten. Gelegentlich wurde die Ansicht vertreten, die Rückmeldung des Verfahrensausgangs bei einer vorangegangenen Verdachtsmeldung an die Banken sei datenschutzrechtlich unzulässig. Richtig ist, daß § 11 Abs. 1 Satz 2 GwG nur vorsieht, daß die Staatsanwaltschaft dem Geldinstitut mitteilt, ob eine Transaktion trotz Anzeige durchgeführt werden kann. Andererseits hat aber das Institut ein legitimes Interesse zu erfahren, ob sein Verdacht erhärtet wurde und damit bei künftigen Transaktionen weiterhin eine Meldung erfolgen muß. Ich rege an, bei einer künftigen Gesetzesnovelle Klarheit zu schaffen.

In einem Gespräch mit einem Vertreter des BAKred, das für die Durchführung des GwG zuständig ist, zeigte dieser Verständnis für meine Einwände, die auch von anderen Datenschutzkontrollinstanzen sowohl im öffentlichen wie im privaten Bereich geteilt werden. Das aufwendige Kopieren der Ausweispapiere habe sich als wenig effektiv erwiesen. Ein Defizit des derzeitigen GwG sei, daß es auf illegale Bartransaktionen ziele und den massiv zunehmenden bargeldlosen Zahlungsverkehr vernachlässigt. Statt die Banken zu Hilfspersonen der Strafverfolgungsbehörden zu machen, sei es sinnvoller, die Banken im Eigeninteresse dazu zu bringen, jegliche Formen von Finanztransaktionen auf den Verdacht der Geldwäsche hin zu überprüfen. Es zeichnet sich ab, daß das GwG einer umfassenden Überarbeitung unterzogen wird. Dies wird von mir grundsätzlich begrüßt. So berechtigt das Anliegen der Verhinderung und der Aufklärung von Geldwäsche ist - so wichtig ist die Beachtung des Persönlichkeitsschutzes der Kundinnen und Kunden. Die bisher entstandenen großen Irritationen bei der GwG-Datenverarbeitung - und zwar bei allen Beteiligten - darf nicht fortgeschrieben werden. Verhindert werden muß insbesondere, daß mit dem Argument "Geldwäsche" eine verdachtsunabhängige Rasterfahndung auch bei alltäglichen Kleingeschäften erfolgt und daß es zu unbegründeten Stigmatisierungen von Bankkunden kommt.

37.3 Schüler hatte Zugriff auf den Kontostand der Nachbarn

Im Rahmen von Schülerbetriebspraktika werden Jugendliche auch in Banken und Sparkassen mit den dort von den Beschäftigten wahrzunehmenden Aufgaben vertraut gemacht. Immer wieder werde ich gefragt: Werden das Bankgeheimnis und der Datenschutz bei derartigen Praktika gewahrt? Eingaben zeigen, daß dies nicht immer der Fall ist. Besonders problematisch ist es, wenn die Praktikantinnen und Praktikanten im direkten Wohnumfeld oder im Heimatort eingesetzt werden und so Interessantes über die Finanzverhältnisse von Nachbarn und Bekannten erfahren.

Die betroffenen Banken sind durchgängig daran interessiert, hier nichts

falsch zu machen. Rechtlich gesehen erfolgt die Offenbarung von Kundendaten im Rahmen eines Praktikums auf der Grundlage von § 28 Abs. 1 Satz 1 Nr. 2 bzw. Abs. 2 Satz 1 Nr. 1 Buchst. a BDSG. Dabei ist jedoch jeweils zu beachten, daß kein Grund zu der Annahme besteht, daß schutzwürdige Interessen der Betroffenen entgegenstehen. Die Unterweisung von Schülerinnen und Schülern anläßlich der Durchführung von Betriebspraktika ist keine Ausbildung im eigentliche Sinne; sie liegt jedoch sowohl im betrieblichen, im allgemeinen wie im Schüler-Interesse. Wegen der hohen Sensibilität von Bankdaten muß deren Kenntnisgabe auf das unvermeidliche Maß beschränkt bleiben. Die Schülerinnen und Schüler müssen keinen uneingeschränkten Zugriff auf die automatisierte Datenverarbeitung im Unternehmen haben. Persönlichkeitsrechtlich heikle Bankvorgänge, wie z.B. Zahlungsverzug bei Kreditgeschäften, sollten von der Kenntniserlangung in Praktika ausgeschlossen werden. Ist eine Teilnahme an Beratungsgesprächen vorgesehen, so sollte die Bank die jeweilige Kundin bzw. den Kunden zunächst um das Einverständnis hierfür bitten. Ich rate den Banken dringend, dafür Sorge zu tragen, daß Praktikantinnen und Praktikanten nicht am Wohnort bzw. -bezirk einzusetzen. Selbstverständlich sollte sein, daß die Schülerinnen und Schüler eine Verpflichtungserklärung unterschreiben und mit einem Merkblatt zum Datenschutz über Geheimhaltungspflichten aufgeklärt werden.

38. Versicherungen: Der Trick mit der Allfinanz-Klausel

Innerhalb weniger Tage wurde ich Mitte 1995 mit einer Vielzahl von Eingaben konfrontiert, die sich alle gegen eine einseitige Veränderung von Vertragsbedingungen einer Versicherung wendeten. Hinzu kamen eine Vielzahl von Beschwerden, die bei anderen Datenschutzbeauftragten und beim Bundesaufsichtsamt für das Versicherungswesen eingegangen waren und von dort zuständigkeitshalber an mich abgegeben wurden. Die große Versicherung aus Hannover hatte nämlich ihren Versicherten ein "Merkblatt zur Datenverarbeitung" zugesandt, verbunden mit dem Zusatz zur bisherigen Datenschutz-Einwilligungserklärung: "Ohne Einfluß auf den Vertrag und jederzeit widerrufbar willige ich weiter ein, daß der Vermittler meine allgemeinen Antrags-, Vertrags- und Leistungsdaten darüber hinaus für die Beratung und Betreuung auch in sonstigen Finanzdienstleistungen nutzen darf". Außerdem teilte das Unternehmen folgendes mit: "Wir werden künftig von der Einwilligungserklärung in dem neuen Umfang Gebrauch machen und gehen davon aus, daß Sie damit einverstanden sind. Sollte dies nicht der Fall sein, bitten wir Sie um eine kurze Mitteilung". Teilweise wurde diese Vertragsänderung gemeinsam mit Werbematerial, teilweise mit einer Mitteilung über die "Wahl der Mitgliedergruppenvertreter" versandt.

Die Änderung der Vertragsbedingungen geht auf eine neue Entwicklung im Bereich der Finanzdienstleistungen zurück: Immer mehr Versicherungen, Banken, Bausparkassen und Vermögensberatungsunternehmen gehen dazu über, ihren Kundinnen und Kunden ein Komplettangebot zu unterbreiten. Da aber alle Dienstleistungen nicht von einem Unternehmen selbst angeboten werden, schließen sich Unternehmen zusammen, deren Leistungen sich gegenseitig ergänzen. Oftmals gehören diese Unternehmen einem gemeinsamen Konzern oder einer Unternehmens-Gruppe an. Außerdem bedienen sich Finanzdienstleister professioneller Vermittler, die wiederum in großen Vermittlerunternehmen zusammengeschlossen sind, insbesondere in den sog. Strukturvertrieben. Über die Änderung der Vertragsbedingungen soll es nun ermöglicht werden, daß die Daten aus einem Vertragsverhältnis dazu genutzt werden, für die anderen Finanzdienstleistungsprodukte zu werben und eine ganzheitliche Betreuung der Kundinnen und Kunden vorzunehmen. Zu diesem Zweck glaubt die Versicherungswirtschaft, auf einen umfangreichen Datenaustausch nicht verzichten zu können. Dies kann dazu führen, daß ein Versicherungsnehmer plötzlich von einem ihm völlig unbekannten Unternehmen mit einem Angebot konfrontiert wird, das offensichtlich auf einer genauen Kenntnis der Versicherungsdaten beruht. Ich kann sehr gut verstehen, daß viele Versicherte bei der Weitergabe teilweise

sehr sensibler Antragsdaten Unbehagen verspüren.

Daher verhandelte der Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) mit Vertretern der obersten Datenschutz-Aufsichtsbehörden, um eine praktikable, aber dennoch datenschutzgerechte Lösung durch Änderung der Vertragsbedingungen zu finden. Dabei erklärten sich die Aufsichtsbehörden letztendlich bereit, die oben genannte Neufassung der Einwilligungserklärung mit der Einräumung einer Widerspruchsmöglichkeit bei den sog. Altfällen zu akzeptieren. Die Unterrichtung sollte anläßlich des nächsten Anschreibens der Kundinnen und Kunden erfolgen. Daß die gefundene Einigung bei den Betroffenen zu Irritationen führt, hat sich anhand der Vielzahl der Eingaben bei mir gezeigt.

Angesichts der aktuellen gesetzlichen Lage ist es schwer, die Wirtschaft bei der Datenverarbeitung zu einem "mehr" an Transparenz und Wahlfreiheit zu veranlassen. Es wäre wünschenswert, wenn die Versicherten beim Vertragsabschluß durch Ankreuzen eine Wahlmöglichkeit bzgl. der Weitergabe ihrer Versichertendaten an befreundete Unternehmen bekämen, anstatt entsprechende Einwilligungen im Vertrag durchstreichen zu müssen. Im Bankenbereich zeichnet sich ab, daß zwar den Kundinnen und Kunden zwar keine Wahlmöglichkeit durch Ankreuzen eingeräumt wird, daß Ihnen aber auch keine Änderung der Vertragsbestimmungen untergeschoben wird.

Im Versicherungsbereich sind nun die Betroffenen selbst aufgefordert, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen. Dies kann dadurch erfolgen, daß bei Vertragsabschluß die sog. Allfinanzklausel in den Vertragsbedingungen einfach gestrichen wird. Da die Einwilligung in die Datenweitergabe an andere Finanzdienstleister kein notwendiger Vertragsbestandteil ist, sollte dies nicht dazu führen, daß der Abschluß durch die Versicherung verweigert wird. Da freiwillige Einwilligungen jederzeit widerrufbar sind, kann trotz einer zunächst erfolgten Unterschrift die entsprechende Einwilligung wieder zurückgezogen werden. In jedem Fall sollten die Betroffenen darauf achten, daß ihnen ein Merkblatt ausgehändigt wird, in dem die Datenverarbeitung innerhalb der Versicherung und der Finanzdienstleister beschrieben wird. Auf eine solche Kenntnis der Empfänger der Daten haben die Versicherten ebenso einen Anspruch wie auf eine jederzeit zu erteilende Auskunft über die jeweils gespeicherten Daten. Übermittelt werden dürfen übrigens nur die Daten der versicherten Person, nicht von Dritten, z.B. Angehörigen, Begünstigten usw. Will eine versicherte Person vermeiden, daß einem Versicherungsvermittler oder einer Vermittlungsgesellschaft die Vertragsdaten weitergegeben werden, so sollte der Versicherung der entsprechende Wunsch vorgetragen werden. Diese ist regelmäßig bereit, die Betreuung direkt durch die Zentrale oder eine Außenstelle ohne Zwischenschaltung eines Vermittlers vorzunehmen.

39. Wohnungswirtschaft: Unzulässige (Sozial-) Hilfeleistung des Vermieters

Eine gemeinnützige Baugesellschaft machte dem örtlich zuständigen Sozialamt monatlich Mitteilung über ihre Mieterinnen und Mieter, die mit zwei Monatsmieten in Rückstand geraten waren und denen daher eine Räumungsklage drohte. Die Betroffenen wurden sodann vom Sozialamt angeschrieben und gebeten, mit ihren Einkommensunterlagen zu einer Rücksprache zwecks eventueller Beantragung von Sozialhilfe in die Dienststelle zu kommen.

Die Unterrichtung des Sozialamtes bei Einleitung einer Räumungsklage wurde mit der Zweckbestimmung des Mietvertrags sowie mit einem berechtigten Interesse nach § 28 Abs. 1 BDSG begründet. Gegenstand des Mietvertrags ist aber nicht die Unterstützung bei der Beantragung von Sozialhilfe. Erfolgt eine Räumungsklage wegen Nichtbezahlens der Miete, so muß dies nicht an der Sozialhilfebedürftigkeit liegen, sondern kann auch auf mangelndem Zahlungswillen beruhen. In diesen Fällen ist die Datenübermittlung an das Sozialamt sinnlos.

Sicherlich hat die Gesellschaft an der Mietzahlung und an der Vermeidung von Räumungsklagen ein berechtigtes Interesse. Es erscheint mir aber sinnlos, über den eventuell Leistungsberechtigten hinweg den (potentiellen) Leistungsträger über eine Räumungsklage zu unterrichten. Nur im Einzelfall kommt eine solche Unterrichtung in Betracht, wenn die Mieterin bzw. der Mieter vom Vermieter auf die Möglichkeit der Inanspruchnahme von Sozialhilfe hingewiesen worden ist. Auch der Umstand, daß es sich bei einem Großteil der Mieter des Unternehmens um sozialschwache Personen handelte, konnte nach meinem Dafürhalten keine Rechtfertigung dafür sein, diesen die Möglichkeit zu nehmen, ihre sozialen Angelegenheiten selbst in die Hand zu nehmen. Der Umstand einer (anstehenden) Räumungsklage ist eine Information, deren Preisgabe prinzipiell schutzwürdige Interessen berührt. Ein Erfordernis der Aktion zur Wahrung öffentlicher Interessen konnte ich auch nicht erkennen, da die Betroffenen vom Vermieter darauf hingewiesen werden können, daß sie die Möglichkeit haben, Leistungen des Sozialamtes in Anspruch zu nehmen. Die von der Gesellschaft durchgeführte Datenübermittlung war rechtswidrig. Die Baugesellschaft wird künftig vor Einleitung einer Räumungsklage die betroffenen Mieterinnen und Mieter über die Möglichkeit des Sozialhilfebezugs informieren. Reagiert die angesprochene Person nicht, so habe ich keine durchgreifenden Bedenken, daß die Baugesellschaft sich im Einzelfall an das Sozialamt wendet. Dieses muß die übermittelten Daten aber sofort wieder löschen, wenn sich herausstellt, daß die Anspruchsvoraussetzungen für die Gewährung von Sozialhilfe nicht vorliegen.

40. Privates Gesundheitswesen: Arztdaten als Objekt eines Beziehungsclinchs

Ein Arzt schilderte mir folgenden Fall: Er lebte mit einer Partnerin zusammen, die ihn in der Praxis unterstützte und außerdem ein Kosmetikstudio betrieb. Die Partnerin führte die Kundendatei ihres Kosmetikstudios im ärztlichen Praxisprogramm auf einem sehr leistungsfähigen PC. Der Arzt, ein Gynäkologe, der auch Psychotherapien durchführt, speicherte auf der Festplatte des PC in komprimierter Form die Daten von ca. 7.000 Patientinnen, darunter auch Daten über Psycho- und Sexualtherapien und Vergewaltigungsgutachten, die auch Kinder und Jugendliche betreffen. Wie das Leben nun einmal spielt: Der Arzt und seine Partnerin trennten sich im Unfrieden. Mehrere Wochen nach der Trennung ließ die frühere Freundin das Haus durch den Schlüsseldienst öffnen und nahm den Computer an sich. Der Arzt erstattete deshalb Strafanzeige, was zur Sicherstellung des Computers durch die Kriminalpolizei führte. Die Ex-Freundin ließ sich jedoch dahingehend ein, der Computer sei ihr von dem Arzt geschenkt worden. Da hier Aussage gegen Aussage stand, stellte die Staatsanwaltschaft das Strafverfahren ein und gab den PC der Ex-Freundin wieder zurück. Die Aufregung des Arztes war für mich nachvollziehbar: Ärztliche Daten mit hochsensiblen, teilweise aus den intimsten Bereichen stammenden Angaben befanden sich bei einer Person, die dies alles nichts anging.

Die Klärung des Falles erwies sich als äußerst schwierig und langwierig. Die zivilrechtliche Frage, wem der Computer gehört, konnte auch ich nicht beantworten. Die Eigentumsfrage ist aber von der Frage der Verfügungsberechtigung über die auf dem PC gespeicherten Patientendaten zu trennen. Unstreitig war, daß der Ex-Freundin kein Zugriff auf die ärztlichen Daten zustand. Die unbefugte Speicherung nicht offenkundiger Daten erfüllt den objektiven Straftatbestand des § 43 Abs. 1 Nr. 1 BDSG. Die Freundin hätte sich nun der datenschutzrechtlichen Verantwortlichkeit durch Datenlöschung entledigen können. Dies hätte jedoch zur Folge gehabt, daß die Interessen des Arztes verletzt worden wären: Nach § 11 Abs. 2 der Ärztlichen Berufsordnung ist er verpflichtet, die ärztlichen Aufzeichnungen mindestens 10 Jahre nach Behandlungsabschluß aufzubewahren. Angeblich gab es für viele der gespeicherten Unterlagen keinen weiteren Aktenrückhalt. Einer Löschung standen somit Drittinteressen entgegen (§ 35 Abs. 3 Nr. 3 BDSG); sie hätte u.U. Schadenersatzansprüche ausgelöst. Da der Rechner von älterem Baujahr ist und die Daten in komprimierter Form abgelegt sind, wäre es mit einem hohen technischen Aufwand verbunden gewesen, die Daten auf einen anderen Datenträger zu überspielen und diese auf dem zurückzugebenden PC zu löschen. Eine entsprechende Vorgehensweise hätte ich nach § 38 Abs. 5 BDSG gegenüber der Beteiligten anordnen

können. Letztlich war es dann jedoch möglich, die frühere Freundin zu veranlassen, den PC wieder herauszugeben. Der Konflikt hatte offensichtlich kaum einen materiellen, sondern einen privaten Hintergrund. Da mir für einen Mißbrauch der Patientendaten keine Anhaltspunkte vorlagen, betrachtete ich nach der Rückgabe des Computers die Angelegenheit als erledigt.

Anlagen Materialien zum Datenschutz

Anlage 1
Checkliste des Düsseldorfer Kreises zum Datenschutz beim grenzüberschreitenden Datenverkehr mit personenbezogenen Daten im nicht-öffentlichen Bereich

Anlagen 2 bis 26
Entschließungen, Beschlüsse und Stellungnahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Anlage 2
9./10. März 1995: Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen

Anlage 3
9./10. März 1995: Datenschutz bei elektronischen Mitteilungssystemen

Anlage 4
9./10. März 1995: Automatische Erhebung von Straßennutzungsgebühren

Anlage 5
9./10. März 1995: Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz) (Bundesrats-Drucksache 94/95)

Anlage 6
9./10. März 1995: Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Anlage 7
9./10. März 1995: Anforderungen an den Persönlichkeitsschutz im Medienbereich

Anlage 8
9./10. März 1995: Maßhalten beim vorbeugenden personellen Sabotageschutz

Anlage 9
9./10. März 1995: Sozialgesetzbuch VII (Unfallversicherung)

Anlage 10
9./10. März 1995: Datenschutz bei Wahlen

Anlage 11
13. Oktober 1995: Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen

Anlage 12
9./10. November 1995: Weiterentwicklung des Datenschutzes in der Europäischen Union

Anlage 13
9./10. November 1995: Planungen für ein Korruptionsbekämpfungsgesetz

Anlage 14
9./10. November 1995: Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

Anlage 15
9./10. November 1995: Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Anlage 16
9./10. November 1995: Datenschutz bei der Neuordnung der Telekommunikation (Postreform III)

Anlage 17
14./15. März 1996: Transplantationsgesetz

Anlage 18
14./15. März 1996: Grundsätze für die öffentliche Fahndung im Strafverfahren

Anlage 19
14./15. März 1996: Modernisierung und europäische Harmonisierung des Datenschutzrechts

Anlage 20
29. April 1996: Eckpunkte für die datenschutzrechtliche Regelung von Mediendiensten

Anlage 21
9. Mai 1996: Forderung zur sicheren Übertragung elektronisch

gespeicherter personenbezogener Daten

Anlage 22
22./23. Oktober 1996: Datenschutz durch Technik

Anlage 23
22./23. Oktober 1996: Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Anlage 24
Anlage des Arbeitskreises Medien: Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Anlage 25
22./23. Oktober 1996: Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Anlage 26
22./23. Oktober 1996: Automatisierte Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen

---

Anlagen

Stand 14.11.1996

Anlage 1

Checkliste des Düsseldorfer Kreises zum Datenschutz beim grenzüberschreitenden Datenverkehr mit personenbezogenen Daten im nicht-öffentlichen Bereich

I. Rechtliche Ausgangslage

Rechtsgrundlagen für Datenübermittlungen ins Ausland sind derzeit die §§ 28 Abs. 1 und 2 sowie § 29 Abs. 2 BDSG, soweit nicht bereichsspezifische Regelungen vorgehen. Der Tatsache, daß Datenübermittlungen in Länder stattfinden, die kein ausreichendes Datenschutzniveau haben, ist dabei bei sämtlichen Alternativen der genannten Vorschriften durch eine Abwägung mit den schutzwürdigen Interessen des Betroffenen Rechnung zu tragen; lediglich § 28 Abs. 1 Satz 1 Nr. 1 BDSG sieht eine solche Abwägung nicht ausdrücklich vor, da hier von einer jedenfalls konkludenten Einwilligung des Betroffenen ausgegangen werden kann. Vereinbarungen zwischen inländischen Datenübermittlern und ausländischen Datenempfängern mit dem Ziel, die Rechte der Betroffenen zu sichern, haben zum jetzigen Zeitpunkt

also insofern Bedeutung, als sie als ein Abwägungselement in diese allgemein formulierten Abwägungsklauseln eingestellt werden können. Solche Vereinbarungen kommen vor allem dann in Betracht, wenn Datenübermittlungen durchgeführt werden sollen, für die keine entsprechende Einwilligung vorliegt und die auch nicht zur Erfüllung eines Vertrages mit dem Betroffenen erforderlich sind.

Für die Beurteilung der Zulässigkeit einer derartigen Datenübermittlung kann die nachfolgende flexibel zu handhabende Checkliste herangezogen werden, durch die der Wirtschaft ein Instrumentarium zur eigenständigen Beurteilung von Datenübermittlungen an die Hand gegeben werden soll. Eine derartige Checkliste, aus der nach den Umständen des Einzelfalls die Vertragsbestandteile eigenverantwortlich zusammengesetzt werden können, kann dazu beitragen, in einigen Bereichen den Schutz der inländischen Betroffenen zu verstärken. Dies ist vor allem erforderlich, wenn Datenschutzdefizite im Land des Datenempfängers bestehen. Mit der Checkliste soll kein Modellvertrag entworfen werden. Es geht vielmehr darum, durch zusätzliche Datenschutzmaßnahmen das Risiko für den Betroffenen bei grenzüberschreitenden Datenübermittlungen zu mindern.

II. Inhalt der Checkliste

1. Kooperation der Beteiligten

Die übermittelnde Stelle soll die den Datenschutz betreffende Rechtslage im Empfängerland ermitteln; dabei bieten sich Kontaktaufnahmen zu den zuständigen Behörden im Empfängerland und zum Datenempfänger an. Ob ein Land ein ausreichendes Datenschutzniveau hat, beurteilt sich anhand sämtlicher Umstände des Einzelfalls (Art der Daten, Zweckbestimmung, Verwendungszusammenhang, Dauer der geplanten Verarbeitung, allgemeine oder sektorale gesetzliche Bestimmungen im Empfängerland, Standesregeln im Empfängerland). Führt die übermittelnde Stelle trotz unklarer Datenschutzlage im Empfängerland keine Recherchen durch oder bleibt die Datenschutzlage im Empfängerland trotz derartiger Recherchen unklar, so ist im Zweifel davon auszugehen, daß das Empfängerland kein angemessenes Datenschutzniveau bietet.

2. Verwendungszusammenhang

Der Zweck der Datenverwendung sollte im Vertrag möglichst präzise und verbindlich fixiert sein. Übermittelnde Stelle und Datenempfänger sollten im Vertrag ein Verbot zweckwidriger Verwendung der Daten vereinbaren. Gegebenenfalls können bestimmte unzulässige Verwendungen beispielhaft zur Klarstellung verboten werden.

3. Auskunftsrechte

Im Interesse einer größtmöglichen Transparenz sollte der Betroffene

Auskunftsansprüche sowohl gegen den ausländischen Datenempfänger als auch gegen den inländischen Übermittler haben. Dieses Ziel ist effektiv jedoch nur dann zu erreichen, wenn der Datenempfänger vertraglich verpflichtet wird, der übermittelnden Stelle entsprechende Auskünfte zu erteilen, da letztere anderenfalls kaum in der Lage wäre, dem Betroffenen die verlangten Informationen zu geben.

4. Berichtigung, Sperrung, Löschung

Auch diese Rechte sollte der Betroffene in bezug auf den ausländischen Datenbestand wahlweise gegenüber dem ausländischen Empfänger wie auch gegenüber dem inländischen Übermittler geltend machen können. Soweit der Anspruch des Betroffenen gegenüber der übermittelnden Stelle geltend gemacht wird, richtet sich dieser Anspruch auf deren Mitwirkung bei der Erfüllung der Pflichten des Datenempfängers. Dies setzt voraus, daß sich der Datenübermittler gegenüber dem Datenempfänger einen Anspruch auf Berichtigung, Sperrung und Löschung einräumen läßt.

5. Benachrichtungspflicht

Von besonderer Bedeutung ist, daß sich die übermittelnde Stelle verpflichtet, den Betroffenen - über die gesetzliche Regelung des § 33 DSG hinausgehend - über die Datenübermittlung ins Ausland zu benachrichtigen. Dabei ist der Betroffene insbesondere auch über die ihm durch die vertragliche Vereinbarung zwischen übermittelnder Stelle und Datenempfänger eingeräumten Rechte zu informieren.

6. Datensicherung

Maßnahmen zur Datensicherung sollten dem Datenempfänger vertraglich auferlegt werden. Als Grundsatz sollte gelten, daß sich das Sicherheitsniveau vorrangig an der Sensibilität der Daten orientiert. Als Anhaltspunkt kann insoweit § 9 BDSG einschließlich Anlage gelten.

7. Vereinbarung zur Verminderung bestehender Kontrolldefizite im Ausland

Die Umsetzung unter anderem auch der o.g. vertraglichen Vereinbarungen muß durch die übermittelnde Stelle überwacht werden können. Zu denken ist hier insbesondere an Auskunfts- und Einsichtsrechte sowie gegebenenfalls Besichtigungsrechte der übermittelnde Stelle. Auch die Einsetzung eines Beauftragten kommt in Betracht.

8. Vertragsstrafe

Der Datenempfänger sollte zur Zahlung einer Vertragsstrafe an die übermittelnde Stelle für den Fall verpflichtet werden, daß er seine vertraglichen Verpflichtungen nicht einhält. Auch dadurch kann beim Datenempfänger die Bereitschaft zur Wahrung der Rechte des

Betroffenen gestärkt werden.

9. Haftung

Die Interessen des Betroffenen würden eine gesteigerte Berücksichtigung erfahren, wenn übermittelnde Stelle und Datenempfänger dem Betroffenen gegenüber gesamtschuldnerisch haften würden. Zu denken wäre an eine gemeinsame Verpflichtungserklärung zwischen übermittelnder Stelle und Datenempfänger, wobei der Betroffene über diesen Vertragsinhalt zu informieren wäre, da er sonst aus Unkenntnis seine erworbenen Ansprüche nicht geltend machen könnte. Im Falle der Übermittlung besonders sensibler Daten kann auch die Vereinbarung einer verschuldensunabhängigen Haftung erwogen werden.

Anlage 2

Entschließung der 49. Konferenz der Datenschutzbeauftragtendes Bundes und der Länder vom 9./10. März 1995 zum **eingeschränkten Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen**

Die gesetzlichen Krankenkassen schließen sich zunehmend zu landesweiten oder überreagionalen gesetzlichen Krankenkassen zusammen. Es stellt sich daher verstärkt die Frage, welche bzw. wiewiele Geschäftsstellen solcher Krankenkassen umfassend auf alle gespeicherten Daten eines Versicherten zugreifen können.

Die Datenschutzbeauftragten halten nur folgendes für vertretbar:

1. Geschäftsstellen einer Krankenkasse können ohne schriftliches Einverständnis des Versicherten nur auf einen "Stammdatensatz" zugreifen. Dieser "Stammdatensatz" darf nur den Namen, das Geburtsdatum, die Anschrift, die Krankenversichertennummer und die betreuende Geschäftsstelle des Versicherten umfassen.

2. Lediglich eine Geschäftsstelle kann umfassend auf den Datensatz eines Versicherten zugreifen, sofern der Versicherte nicht ausdrücklich und eindeutig schriftlich in derartige Zugriffsmöglichkeiten durch weitere Geschäftsstellen eingewilligt hat.

3. Vor der Einwilligung ist der Betroffene umfassend aufzuklären. Die Daten dürfen nur zweckgebunden verwendet werden.

Anlage 3

Entschließung der 49. Konferenz der Datenschutzbeauftragtendes Bundes und der Länder vom 9./10. März 1995 zum **Datenschutz bei elektronischen**

Mitteilungssystemen

Es ist damit zu rechnen, daß in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche bedeutsame Informationen und insbesondere personenbezogene Daten über Netze ausgetauscht werden.

Die zunehmende Nutzung von elektronischen Mitteilungssystemen (Electronic-Mail, Dokumentenaustausch über Datenfernübertragung, Message Handling Systems MHS/X.400) hat zur Folge, daß Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit verschärft werden, weil Unbefugte Zugriffe auf Daten und Programme erhalten können und die Übertragungswege vom Kommunikationspartner nicht sicher zu kontrollieren sind. Deshalb ist beim Einsatz solcher Systeme das Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In diesem Zusammenhang gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information durch eine Vielzahl umfassender aufeinander abgestimmter Sicherheitsmaßnahmen an Bedeutung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, daß den folgenden Sicherheitsaspekten beim Einsatz von elektronischen Mitteilungssystemen Rechnung getragen wird:

Es ist damit zu rechnen, daß in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche bedeutsame Informationen und insbesondere personenbezogene Daten über Netze ausgetauscht werden.

Die zunehmende Nutzung von elektronischen Mitteilungssystemen (Electronic-Mail, Dokumentenaustausch über Datenfernübertragung, Message Handling Systems MHS/X.400) hat zur Folge, daß Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit verschärft werden, weil Unbefugte Zugriffe auf Daten und Programme erhalten können und die Übertragungswege vom Kommunikationspartner nicht sicher zu kontrollieren sind. Deshalb ist beim Einsatz solcher Systeme das Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In diesem Zusammenhang gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information durch eine Vielzahl umfassender aufeinander abgestimmter Sicherheitsmaßnahmen an Bedeutung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, daß den folgenden Sicherheitsaspekten beim Einsatz von elektronischen Mitteilungssystemen Rechnung getragen wird:

1. Authentizität von Benutzern, Nachrichten und Systemmeldungen

Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit

bestehen, anhand bestimmter Kriterien die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen (z. B. Empfangs- und Weiterleitungsbestätigungen, Sendeanforderungen, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

2. Vertraulichkeit von übertragenen Daten

Für alle Arten von Daten in elektronischen Mitteilungssystemen - Nachrichten sowie Verkehrs- und Verbindungsdaten - muß die Vertraulichkeit gewahrt bleiben. Sie ist durch geeignete Maßnahmen, z.B. kryptografische Verfahren, sicherzustellen.

3. Integrität von Nachrichten und Meldungen

Es ist zu gewährleisten, daß bei Speicherung und Weiterleitung von Daten keine unbefugte, unerkannte Veränderung erfolgen kann.

4. Fälschungssichere Kommunikationsnachweise

Die für die Anerkennung einer elektronischen Kommunikation erforderlichen fälschungssicheren Sende-, Empfangs- und Übertragungsnachweise müssen dem Anwender auf Wunsch zur Verfügung stehen.

5. Ausschluß von Kommunikationsprofilen

Die Erstellung von Kommunikationsprofilen muß verhindert werden. Gespeicherte Protokollierungsdaten dürfen nur zu Zwecken des Datenschutzes und der Datensicherung (§§ 14 Abs. 4, 31 BDSG bzw. landesgesetzliche Regelungen) verwendet werden.

Empfehlungen zum Einsatz von elektronischen Mitteilungssystemen:

Zum sicheren Einsatz von elektronischen Mitteilungssystemen sind als Grundschutzmaßnahmen folgende Empfehlungen zu beachten.

1. Grundsätzlich sind nur solche Produkte einzusetzen, die die Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahre 1988 erfüllen. Vorhandene Systeme - insbesondere solche, die noch auf Empfehlungen von 1984 basieren -, sollen künftig durch geeignete Zusatzprodukte hinsichtlich ihrer Sicherheit verbessert oder durch neuere Softwareversionen ersetzt werden.

2. Bei Übertragung von personenbezogenen Daten ist eine Verschlüsselung vorzusehen. Die Verschlüsselung der Daten muß mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgen. Neben der Auswahl eines effektiven Verschlüsselungsalgorithmus (z. B. DES, IDEA) muß dabei insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein. Verschlüsselungskomponenten sind durch technische, bauliche und

organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.

3. Zur Absicherung der Integrität der Daten sollte auf Verfahren der "elektronischen Unterschrift" zurückgegriffen werden.

4. Nach Möglichkeit ist die Funktion des Systemverwalters von der des Netzwerkverwalters - insbesondere der Verwaltung des elektronischen Mitteilungssystems - aus Sicherheitsgründen zu trennen.

5. Es ist grundsätzlich separat administrierbare Hard- oder Software - z. B. in Form eines Kommunikationsservers - für das elektronische Mitteilungssystem vorzusehen.

6. Bei Verwendungen von öffentlichen Übertragungswegen, sind die vorhandenen Sicherheitsmechanismen dieser Netze z. B. geschlossene Benutzergruppen, Rufnummernidentifikation, Teilnehmerzeichengabe und automatische Rückruffunktion zur Abwehr des Zugriffs durch externe zu nutzen.

7. Zur Beweissicherung einer stattgefunden Kommunikation sollte die eingesetzte Software folgende Funktionen beinhalten:

- Zustellung/Empfangsnachweise

- Sende/Empfangsübergabenachweise.

Anlage 4

Entschließung der 49. Konferenz der Datenschutzbeauftragtendes Bundes und der Länder vom 9./10. März 1995 zur **automatischen Erhebung von**

Straßennutzungsgebühren

Gegenwärtig werden Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren in mehreren Versuchsfeldern erprobt. Sie können im Rahmen der weiteren Entwicklung zu zentralen Komponenten umfassender Verkehrstelematiksysteme (z.B. Verkehrsinformation und -leitung) werden.

Mit der Einführung derartiger Verkehrstelematiksysteme besteht die Gefahr, daß personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern, erhoben und verarbeitet werden. Exakte Bewegungsprofile können dadurch erstellt werden. Damit wären technische Voraussetzungen geschaffen, daß Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil das Grundrecht auf freie Entfaltung der Persönlichkeit auch das Recht umfaßt, sich möglichst frei und unbeobachtet zu bewegen. Vor diesem Hintergrund ist es besonders wichtig,

elektronische Mautsysteme datenschutzgerecht auszugestalten. Bei den anstehenden Entscheidungen sind andere Verfahren wie z. B. die Vignette einzubeziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, daß der Grundsatz der datenschutzgerechten Ausgestaltung von Systemen zur automatischen Erhebung von Straßenbenutzungsgebühren von allen Beteiligten am Feldversuch auf der BAB A 555 akzeptiert wird. Zur Umsetzung dieses Grundsatzes fordern die Datenschutzbeauftragten:

- Der Grundsatz der "datenfreien Fahrt" muß auch künftig gewährleistet sein. Über Verkehrsteilnehmer, die ordnungsgemäß bezahlen, dürfen keine Daten erhoben oder verarbeitet werden, die die Herstellung eines Personenbezugs ermöglichen. Es sind ausschließlich solche Zahlungsverfahren anzuwenden, bei denen die Abrechnungsdaten nur dezentral beim Verkehrsteilnehmer gespeichert werden. Die Verkehrsteilnehmer dürfen jedoch nicht gezwungen werden, einen lückenlosen Nachweis über ihre Bewegungen zu führen.

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Möglichkeit einer flächendeckenden Kontrolle ist von vornherein technisch und rechtlich auszuschließen. Die Gebührenkontrolle ist so zu gestalten, daß die Identität des Verkehrsteilnehmers nur dann aufgedeckt wird, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Gebühren nicht entrichtet worden sind.

- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Verkehrsteilnehmer durchschaubar sein. Der Verkehrsteilnehmer muß jederzeit über sein Guthaben, die Abbuchung und den eventuellen Kontrollvorgang informiert sein.

- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, daß sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

Die hierbei anzuwendenden Verfahren wären gesetzlich abschließend vorzugeben. Dabei ist sicherzustellen, daß anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen. Ferner ist zu gewährleisten, daß Betreiber derartiger Systeme - unabhängig von ihrer Rechtsform - einer Datenschutzkontrolle nach einheitlichen Kriterien unterliegen. Die Bundesregierung wird aufgefordert, bei der anstehenden internationalen Normierung elektronischer Mautsysteme die datenschutzrechtlichen Anforderungen durchzusetzen.

Anlage 5

Entschließung der 49. Konferenz der Datenschutzbeauftragtendes Bundes und der Länder vom 9./10. März 1995 zum **Entwurf eines**

Gesetzes über das Bundeskriminalamt (BKA-Gesetz) (Bundesrats-Drucksache 94/95)

Zu den Beratungen des Entwurfs für ein Gesetz über das Bundeskriminalamt erklären die Datenschutzbeauftragten des Bundes und der Länder:

Auch aus Sicht des Datenschutzes ist es zu begrüßen, daß die seit langem überfälligen bereichspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung insbesondere im polizeilichen Informationssystem (INPOL) nunmehr in das Gesetzgebungsverfahren eingebracht werden. Der Gesetzentwurf enthält im Vergleich zu den Vorentwürfen eine Reihe von Vorschriften, die datenschutzrechtlich positiv zu werten sind. Hierzu gehören:

- der Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sog. "Feststellung des Anfangsverdachts";

- das Erfordernis der Einwilligung für die Speicherung von Daten über Zeugen und mögliche Opfer;

- Übermittlungsverbote bei überwiegenden schutzwürdigen Interessen der Betroffenen oder bei entgegenstehenden gesetzlichen Verwendungsregelungen;

- die Beachtung landesgesetzlicher Löschungsfristen.

Andererseits begegnet der Gesetzentwurf jedoch nach wie vor gewichtigen Bedenken, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht, deren Voraussetzungen und Reichweite unklar oder nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt sind. Dies gilt insbesondere für

- die Verwendung des Begriffs der Straftaten von erheblicher Bedeutung ohne Definition, um welche Tatbestände es sich handelt, weil damit nicht mehr voraussehbar ist, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind;

- die Befugnisse der Zentralstelle zu selbständigen Datenerhebungen und Übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Einvernehmen mit den jeweils verantwortlichen Länderpolizeien;

- die unklare Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Befugnisse zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie die fehlende klare Zweckbindungs- und Zweckänderungsregelung;

- die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne

eindeutige Begrenzung auf den Schutz gefährdeter Ermittler.

Die Datenschutzbeauftragten fordern den Gesetzgeber auf, die Schwachstellen des Entwurfs auszuräumen. Insbesondere fordern sie klare verfassungskonforme Regelungen zur Auskunftserteilung an Betroffene und der Prüfrechte für INPOL-Daten dahingehend, daß die Datenschutzkontrollrechte bei der datenschutzrechtlichen Verantwortung der Stellen anknüpfen, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen.

Anlage 6

Entschließung der 49. Konferenz der Datenschutzbeauftragtendes Bundes und der Länder vom 9./10. März 1995 zu
Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z.B. die bislang bekannt gewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesver fassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.

Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu ver einfachen und zu verkürzen. Soweit geboten sind Verkürzungen vorzunehmen.

3. Die derzeit geltende generelle 30-jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte - abweichend von der bisherigen Praxis, nach der es auf die Weglegung der Akte ankommt - regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

Ergeht keine rechtskraftfähige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.

5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.

6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.

7. Für die Daten von Nebenbeteiligten (z.B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die voll ständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.

8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

Anlage 7

Entschließung der 49. Konferenz der Datenschutzbeauftragtendes Bundes und der Länder vom 9./10. März 1995 zu **Anforderungen an den Persönlichkeitsschutz im Medienbereich**

Die unabhängige und unzensierte Berichterstattung durch Presse, Rundfunk und Film (Art. 5 Abs. 1 Satz 2 GG) dient der freien individuellen und öffentlichen Meinungsbildung. Das Bundesverfassungsgericht hat die freie Meinungsbildung als

Voraussetzung sowohl der Persönlichkeitsentfaltung als auch der demokratischen Ordnung bezeichnet. Insofern besteht ein enger Zusammenhang zwischen der Selbstbestimmung des Einzelnen und der Medienfreiheit.

Die rasante Entwicklung der Medientechnik, die Zunahme interaktiver Teledienste und die verstärkte kommerzielle Nutzung von Pressedatenbanken eröffnen einerseits neue Informationsmöglichkeiten für den Bürger, verschärfen aber die Gefährdungen des Rechts auf informationelle Selbstbestimmung. Diesen Gefährdungen muß der Datenschutz auf rechtlicher und technisch-organisatorischer Ebene angemessen begegnen.

- Electronic Publishing und Medienarchive

Neue Formen der Verbreitung von Informationen über Netze und auf elektronischen Datenträgern führen in bisher unbekanntem Maß zu großen Informationsbeständen, in denen potentiell jedermann gezielt auf personenbezogene Daten zugreifen kann. Zudem öffnen Medienarchive, die bislang ausschließlich für journalistische Zwecke genutzt wurden, riesige Datensammlungen für medienfremde Nutzer. In Persönlichkeitsrechte wird dann besonders tief eingegriffen, wenn auch lange zurückliegende Publikationen praktisch von jedermann recherchiert werden können. Damit droht das in verschiedenen Rechtsbereichen vorgesehene ZRecht auf VergessenZ wirkungslos zu werden, das z.B. durch die Löschungsvorschriften für das Bundeszentralregister gewährleistet werden soll.

Angesichts dieser Entwicklungen muß die Reichweite der datenschutzrechtlichen Sonderstellung der Medien (ZMedienprivilegZ) neu bestimmt werden. Es ist zumindest gesetzlich klarzustellen, daß die geschäftsmäßige Verwendung personenbezogener Daten außerhalb des eigenen Medienbereichs, insbesondere durch kommerzielle Pressedatenbanken, nicht unter das "Medienprivileg" fällt.

- Interaktive Dienste und Mediennutzungsprofile

Auch beim Ausbau neuer digitaler Kommunikationsformen (interaktive Dienste wie z.B. Video on Demand) müssen die Persönlichkeitsrechte der Nutzer gewahrt werden. Dabei ist stärker als bisher von vornherein Wert darauf zu legen, daß datenschutzfreundliche Techniken entwickelt werden und zum Einsatz kommen, bei denen personenbezogene Verbindungs - und Nutzungsdaten erst gar nicht entstehen. Von besonderer Bedeutung sind hier anonyme Zahlverfahren, z.B. Prepaid - Karten, auf denen Informationen über die Nutzung ausschließlich dezentral gespeichert werden.

Entsprechend den Bestimmungen im Bildschirmtextstaatsvertrag und in den neueren Mediengesetzen ist sicherzustellen, daß sich die Erhebung und die Aufzeichnung von Verbindungs - und Abrechnungsdaten auf das erforderliche Maß beschränken. Dieser strikte Verarbeitungsrahmen darf auch nicht dadurch ausgeweitet werden, daß die Nutzung eines Dienstes

von der Einwilligung in eine zweckfremde Verwendung der Daten abhängig gemacht wird. Die Länder sollten entsprechende einheitliche Regelungen für alle interaktiven Dienste treffen.

Da es sich bei den angesprochenen Diensten um Bestandteile einer entstehenden globalen Informationsinfrastruktur handelt, wird die Bundesregierung aufgefordert, sich auf internationaler Ebene für entsprechende Regelungen einzusetzen.

- Rechte der Betroffenen gegenüber den Medien

Während die von der Berichterstattung Betroffenen - neben dem für alle Bereiche geltenden Gegendarstellungsrecht - gegenüber den öffentlich-rechtlichen und privaten Rundfunkveranstaltern inzwischen weitere elementare Datenschutzrechte besitzen, gibt es gegenüber der Presse keine vergleichbaren Regelungen.

So kann derjenige, der durch die Berichterstattung der Rundfunkveranstalter in seinem Persönlichkeitsrecht beeinträchtigt wird, in den meisten Fällen nach der Publikation Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Gegenüber der Presse hat er kein entsprechendes Auskunftsrecht. Die meisten Rundfunkveranstalter sind - anders als die Presse - zudem verpflichtet, etwaige Gegendarstellungen zu den gespeicherten Daten zu nehmen, auf die sie sich beziehen (Mitspeicherungspflicht). Ein sachlicher Grund für diese Unterscheidungen ist nicht erkennbar.

Das Presserecht sollte insofern der Rechtslage nach dem Rundfunkrecht (z.B. § 41 Abs. 3 BDSG und Art. 17 Abs. 2 ZDF-Staatsvertrag) angeglichen werden.

Gegenüber Pressedatenbanken, die nicht nur dem eigenen internen Gebrauch dienen, sollte der Betroffene darüber hinaus ein Auskunftsrecht bezüglich des zu seiner Person gespeicherten veröffentlichen Materials haben.

- Öffentlichkeitsarbeit der Behörden

Personenbezogene Veröffentlichungen von Behörden können das Recht auf informationelle Selbstbestimmung erheblich beeinträchtigen. Das gilt für die Personen, auf die die Aktivitäten der Behörde unmittelbar gerichtet sind, wie auch für andere Verfahrensbeteiligte (wie z. B. Einwender, Opfer von Straftaten, Zeugen) und im besonderen Maße für unbeteiligte Personen aus dem sozialen Umfeld des Betroffenen. Deshalb ist bei der Weitergabe von Daten aus Strafermittlungsverfahren an die Medien besonders zurückhaltend zu verfahren.

Für den Umfang des Anspruchs der Medien auf Weitergabe personenbezogener Daten in Form von Presseerklärungen und Auskünften gibt es keine konkreten gesetzlichen Festlegungen. Die

Datenschutzbeauftragten des Bundes und der Länder halten es daher für geboten, daß der Gesetzgeber Kriterien für die Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und der Freiheit der Berichterstattung durch Rundfunk und Presse deutlicher als bisher festlegt. Dafür kommen die Vorschriften des Landespresserechts, in besonders sensiblen Bereichen aber auch spezialgesetzliche Regelungen wie etwa die Strafprozeßordnung in Betracht.

- Gerichtsfernsehen

Die Datenschutzbeauftragten des Bundes und der Länder treten den in jüngster Zeit zunehmend erhobenen Forderungen nach einer Aufhebung des Verbots der Hörfunk- und Fernsehberichterstattung aus Gerichtsverhandlungen entgegen. Insbesondere bei Strafprozessen vor laufenden Mikrofonen und Kameras würde es unweigerlich zu einer gravierenden Beeinträchtigung des Persönlichkeitsrechts der Angeklagten, der Opfer, der Zeugen und ihrer Angehörigen kommen. Selbst mit Einwilligung aller Prozeßbeteiligten darf die Hörfunk- und Fernsehberichterstattung nicht zugelassen werden.

Die Gerichtsverhandlung darf nicht zu einem masssenmedial vermittelten "modernen Pranger" werden.

Anlage 8

Entschließung der 49. Konferenz der Datenschutzbeauftragtendes Bundes und der Länder vom 9./10. März 1995**: Maßhalten beim vorbeugenden personellen Sabotageschutz**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, bei Sicherheitsüberprüfungen zum personellen Sabotageschutz Augenmaß zu bewahren. Bei diesen Sicherheitsüberprüfungen werden sensible Daten, z. B. über politische Anschauungen oder Alkoholkonsum, vorbeugend erhoben, also ohne daß der Betroffene dazu Anlaß geboten hätte. Polizei und Verfassungsschutz sind routinemäßig beteiligt. Schon wenn der Betroffene im Verlauf der Überprüfung auch nur in den Verdacht der Unzuverlässigkeit gerät, kann dies bereits erheblichen Einfluß zumindest auf das berufliche Fortkommen nehmen.

Gegenwärtig sind solche Überprüfungen spezialgesetzlich für den Atombereich und für Flughäfen vorgesehen. Das Bundesministerium des Innern will jetzt klären, inwieweit Beschäftigte in anderen Einrichtungen überprüft werden sollen.

Unstreitig können solche Überprüfungen unbescholtener Bürger nur zum Schutz von "lebens- und verteidigungswichtigen Einrichtungen" angemessen sein und nur Personen betreffen, die dort an "sicherheitsempfindlichen Stellen" tätig sind. Als "lebenswichtig" sehen die Innenminister und -senatoren aber bereits Stellen an, "die für das Funktionieren des Gemeinwesens unverzichtbar sind". Damit könnten

Beschäftigte in weiten Bereichen des öffentlichen Dienstes und der Wirtschaft mit Sicherheitsüberprüfungen überzogen werden.

Die Datenschutzbeauftragten meinen, daß das Persönlichkeitsrecht hier größere Zurückhaltung gebietet. Die Sicherheitsüberprüfungen müssen auf Bereiche beschränkt bleiben, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß.

Soweit in solchen Bereichen Sicherheitsüberprüfungen durchgeführt werden sollen, bedarf es einer ebenso klaren gesetzlichen Grundlage, wie bisher im Atomgesetz und im Luftverkehrsgesetz. Die zu schützenden Arten lebens- und verteidigungswichtiger Einrichtungen müssen durch Rechtsvorschrift abschließend festgelegt sein. Dabei sind für die jeweiligen Bereiche angemessene Regelungen zu treffen, die mit Rücksicht auf die Interessen Betroffener folgende allgemeine Grundsätze beachten:

- möglichst klare Vorgaben zur "Sicherheitsempfindlichkeit" in der Vorschrift und exakte Festlegung dieser Stellen durch die zuständige Behörde nach Anhörung der Personalvertretung der einzelnen Einrichtung,

- Zustimmung des Betroffenen als Verfahrensvoraussetzung,

- abschließender Katalog der regelmäßig durchzuführenden Maßnahmen, dabei Beschränkung auf vorhandene Erkenntnisse, keine Ausforschungsermittlungen,

- strenge Zweckbindung und angemessene organisatorische Vorkehrungen zu deren Gewährleistung, insbesondere Trennung von Personalakte,

- eigene Verfahrensrechte des Betroffenen, insbesondere rechtliches Gehör vor ablehnender Entscheidung und aktenkundige Gegendarstellung,

- angemessener Auskunftsanspruch, einschließlich Akteneinsicht,

- effektive Datenschutzkontrolle, auch zur Datenverarbeitung in Akten bei nicht-öffentlichen Stellen.

Im Regelfall muß zusätzlich gelten:

- Überprüfung durch die zuständige Aufsichtsbehörde selbst, nicht durch Verfassungsschutzbehörden,

- keine Einbeziehung weiterer Personen (wie Ehegatten usw.).

Ausnahmetatbestände wären - auch zum Verfahren - präzise zu fassen.

Die Praxis der Sicherheitsüberprüfungen zum personellen Sabotageschutz steht in Bund und Ländern vor einer wichtigen Weichenstellung. Sie muß klar und angemessen sein.

Anlage 9

Entschließung der 49. Konferenz der Datenschutzbeauftragtendes Bundes und der Länder vom 9./10. März 1995 zum **Sozialgesetzbuch VII**

Verfassungsgemäßer Datenschutz für Unfallversicherte erforderlich

Durch die Träger der gesetzlichen Unfallversicherung werden oft Daten der Versicherten hinter deren Rücken oder zumindest ohne deren konkrete Kenntnis erhoben und weitergegeben. Der vorliegende Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz - SGB-VII sieht dazu keine Änderungen vor.

Aus dem Recht auf informationelle Selbstbestimmung der Versicherten, insbesondere auf Transparenz der einzelnen Verfahrensschritte, ergeben sich mehrere grundlegende Forderungen, die bei einer Überarbeitung des Referentenentwurfes berücksichtigt werden müssen:

1. Auskunftspflicht behandelnder Ärzte gegenüber Unfallversicherungsträgern

Für behandelnde Ärzte sollte eine gesetzliche Auskunftspflicht gegenüber Unfallversicherungsträgern nur festgelegt werden, soweit dies erforderlich ist für eine sachgerechte und schnelle Heilung (§§ 557 Abs. 2 RVO - § 34 Referentenentwurf SGB VII). Die gesetzliche Auskunftspflicht ist daher auf Angaben über die Behandlung und den Zustand des Verletzten zu beschränken. Danach dürfen Vorerkrankungen, die aus Sicht des Arztes mit dem aktuellen Status in keinem Zusammenhang stehen oder keine Bedeutung im Zusammenhang mit dem Arbeitsunfall oder der Berufskrankheit haben, nicht übermittelt werden (Beispiel: Handverletzung und Salmonellenvergiftung).

2. Datenerhebung, -verarbeitung und -nutzung durch Durchgangsärzte und Berufskrankheitenärzte

Soweit von den Unfallversicherungsträgern bestellte Durchgangsärzte personenbezogene Daten über den Unfallverletzten erheben und Unfallversicherungsträgern und anderen Stellen mitteilen, muß dies auf eine normenklare gesetzliche Grundlage gestellt werden; die bisherige Regelung in dem zwischen den Verbänden der Kassenärzte und der Unfallversicherungsträger geschlossenen "Ärzteabkommen" reicht für die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen nicht aus. Entsprechendes gilt für die geplante Einführung eines Berufskrankheitenarztes.

3. Mitteilung personenbezogener Patientendaten durch Unfallversicherungsträger an ärztliche Gutachter

Im Hinblick auf das Recht der Betroffenen, der Bestellung eines bestimmten Gutachters im Einzelfall aus wichtigem Grund - z. B. wegen möglicher Befangenheit - zu widersprechen, haben die Betroffenen ein besonderes berechtigtes Interesse an der Transparenz dieser Datenübermittlungen.

Gesetzlich festzulegen ist daher, daß dem Betroffenen vor Übermittlung seiner Daten an einen Gutachter der Zweck des Gutachtens und die Person des Gutachters unter Hinweis auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X mitzuteilen sind.

4. Eingriffe der Unfallversicherungsträger und ihrer Verbände in das Recht auf informationelle Selbstbestimmung

Aufgaben der Unfallversicherungsträger und ihrer Verbände und ihre Befugnisse zur Datenerhebung, -verarbeitung und nutzung - einschließlich der Aufbewahrungsfristen - sind differenziert in der verfassungsrechtlich gebotenen Klarheit gesetzlich zu regeln. Der vorliegende Referentenentwurf erscheint in diesem Punkt weitgehend unzureichend. So werden undifferenziert Unfallversicherungsträger und ihre Verbände behandelt, die Fachaufgaben dieser Stellen nicht oder nicht hinreichend deutlich genannt und andererseits Selbstverständlichkeiten wie das Führen von Dateien über erforderliche Daten aufgeführt. Außerdem beschränkt sich die Regelung auf die Datenverarbeitung in Dateien und übergeht die gerade im Bereich der Berufsgenossenschaften mit Gutachten und ähnlichen Unterlagen stark ausgeprägte Datenverarbeitung in Akten.

Die Zuweisung von Aufgaben und Befugnissen an Verbände der gesetzlichen Unfallversicherung muß zudem wie bei allen anderen Verbänden von Leistungsträgern durch die Einrichtung einer staatlichen Aufsicht ergänzt werden.

Soweit Vorschriften der Unfallversicherungsträger und ihrer Verbände (z. B. Unfallverhütungsvorschriften) durch Regelungen über die Erhebung, Verarbeitung und Nutzung sensibler medizinischer Daten in das Recht auf informationelle Selbstbestimmung eingreifen, sind diese Eingriffe gesetzlich zu regeln.

5. Anzeige eines Berufsunfalls und einer Berufskrankheit

Bei Datenschutzkontrollen der bisherigen Anzeigen von Berufsunfällen und - krankheiten hat sich gezeigt, daß der Umfang der an die verschiedenen Stellen übermittelten Daten zum Teil dem Grundsatz der Verhältnismäßigkeit, insbesondere der Erforderlichkeit nicht Rechnung trägt. Der Inhalt dieser Anzeigen muß an diesen Grundsätzen gemessen neu festgelegt werden.

6. Zentraldateien mehrerer Unfallversicherungsträger oder ihrer Verbände

Zweck und Inhalt zentral geführter Dateien sind in angemessenem Umfang gesetzlich präzise zu regeln. Dasselbe gilt für die Datenverarbeitung und - nutzung sowie die Festlegung der jeweils speichernden Stelle.

Die rechtzeitige Beteiligung des jeweils zuständigen Bundes- oder Landesbeauftragten für den Datenschutz vor Einrichtung einer Zentraldatei ist vorzusehen.

7. Anforderung medizinischer Unterlagen bei anderen Sozialleistungsträgern

Der in § 76 Abs. 2 SGB X vorgesehene Hinweis auf das Widerspruchsrecht gegen die Übermittlung medizinischer Daten geht stets dann ins Leere, wenn bei der speichernden bzw. übermittelnden Stelle kein Verwaltungsverfahren läuft

Es ist daher festzulegen, daß ein Unfallversicherungsträger vor der Anforderung von Sozialdaten im Sinne des § 76 SGB X bei anderen Sozialleistungsträgern den Versicherten auf dessen Widerspruchsrecht nach § 76 Abs. 2 SGB X gegenüber der übermittelnden Stelle hinzuweisen hat.

8. Akteneinsichtsrecht der Versicherten

Hinsichtlich des gesetzlichen Akteneinsichtsrechts nach § 25 SGB X treten in der Praxis seitens der Unfallversicherungsträger Unsicherheiten auf, ob zum Schutz von Betriebs- und Geschäftsgeheimnissen oder Urheberrechten das Einsichtsrecht beschränkt werden muß. Hierzu ist eine gesetzliche Klarstellung geboten, daß diese Rechte dem Akteneinsichtsrecht nicht entgegenstehen.

Anlage 10

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zum **Datenschutz bei Wahlen**

Bei der Durchführung von Wahlen haben sich Probleme bei der Verarbeitung personenbezogener Daten ergeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die folgende Entschließung gefaßt:

1. Durchführung von Wahlstatistiken

Diejenigen Wahlberechtigten, in deren Wahlbezirk eine repräsentative

Wahlstatistik durchgeführt werden soll, sind bereits mit der Wahlbenachrichtigung hierüber zu informieren. In allgemeiner Form ist auch im Wahllokal ein gut sichtbarer Hinweis auf die Einbeziehung in die Wahlstatistik anzubringen.

Die Statistik sollte nur in solchen Wahlbezirken durchgeführt werden, in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt. Das Kriterium ist vom Landeswahlleiter vor der Festlegung der Auswahlbezirke zu prüfen. Gegebenenfalls sind ungeeignete Wahlbezirke auszutauschen.

Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse sollte durch den Wahlvorstand erfolgen, während die statistische Auszählung der Stimmzettel durch die jeweils für die Durchführung der Statistik zuständige Stelle vorzunehmen ist.

Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- und personenbezogen zusammengeführt werden, gefährden das Wahlgeheimnis und sind daher unzulässig.

2. Auslegung von Wählerverzeichnissen

Durch die Einsicht in das Wählerverzeichnis besteht nach der jetzigen Rechtslage die Gefahr, daß Daten sowohl von Bürgern, über die in Melderegistern eine Auskunftssperre eingetragen ist, als auch von Bürgern, die in einer speziellen sozialen Situation leben (z. B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Kliniken, Obdachlose), offenbart werden.

Um einerseits die Kontrollmöglichkeit durch die Öffentlichkeit im Vorfeld einer Wahl weiterhin zu gewährleisten, andererseits die datenschutzrechtlichen Belange der genannten Betroffenen zu wahren und dem Mißbrauch einer Adreßrecherche vorzubeugen, fordern die Datenschutzbeauftragten des Bundes und der Länder, daß bei allen Wahlen

- entweder in den öffentlich ausliegenden Wählerverzeichnissen nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgeführt werden

- oder aber bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden, wenn er vorher die Adresse dieser Person angegeben hat.

Im übrigen sind Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht zu veröffentlichen.

3. Gewinnung von Wahlhelfern

Bei der Gewinnung von Wahlhelfern sind folgende Grundsätze zu beachten:

Es dürfen nur die zur Bestellung erforderlichen Daten, wie Name, Vorname und Wohnanschrift, erhoben werden. Die Betroffenen sind über den Zweck der Datenerhebung und die weitere Datenverarbeitung umfassend zu unterrichten.

Über die Abwicklung der jeweiligen Wahl hinaus dürfen die Daten der Wahlhelfer, soweit sie nicht ausdrücklich widersprochen haben, in einer Wahlhelferdatei nur gespeichert werden, wenn sie dieser Speicherung nicht widersprochen haben. Die Wahlhelfer sind auf ihr Widerspruchsrecht hinzuweisen.

Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zuläßt. Im Falle der Freiwilligkeit muß es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben. Nach Gründen, die einer Übernahme des Ehrenamtes entgegenstehen, darf erst im förmlichen Verfahren durch die Wahlbehörde gefragt werden.

4. Erteilung von Wahlscheinen

Die in den Wahlordnungen des Bundes und der Länder enthaltene Regelung, nach der die Antragstellung für die Erteilung eines Wahlscheines auf einem Vordruck zu begründen ist und der Grund gegenüber der Gemeinde glaubhaft gemacht werden muß, ist aus datenschutzrechtlicher Sicht unverhältnismäßig. Da sich aus der geforderten Differenzierung der Begründung keine unterschiedlichen Rechtsfolgen ableiten, ist diese entbehrlich. Es genügt in der Antragstellung eine Erklärung des Wahlberechtigten, daß er am Tag der Wahl aus wichtigem Grund das für ihn zuständige Wahllokal nicht aufsuchen kann.

Anlage 11

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. Oktober 1995 zum **Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen**

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, daß bei kartengestützten Zahlungssystemen, die zunehmend in Konkurrenz zum Bargeld treten, datenschutzfreundliche Verfahren eingesetzt werden. Dabei bietet es sich an, vor allem Guthabenkarten zu verwenden. Es sollten nur solche Clearingverfahren eingesetzt werden, die weder eine individuelle Kartennummer benutzen noch einen anderen Bezug zum Karteninhaber herstellen.

Sowohl im öffentlichen Personennahverkehr als auch bei der Deutschen Bank AG können Fahrscheine bargeldlos erworben werden. Auch Autofahrer können auf Bargeld verzichten: Beim Parken, beim Tanken, künftig auch bei der Benutzung von Autobahnen wird verstärkt auf elektronisches Bezahlen zurückgegriffen. Immer mehr Telefone und Warenautomaten werden auf bargeldlose Zahlungsverfahren umgestellt, so daß viele Artikel des täglichen Bedarfs elektronisch bezahlt werden können. Von Kreditinstituten wird die Kombination verschiedener Anwendungen auf einer Karte angestrebt, z.B. mit einer Kombination der Bezahlung für den öffentlichen Nahverkehr, Parkgebühren und Benutzungsentgelte für öffentliche Einrichtungen.

Zum elektronischen Bezahlen werden entweder Kreditkarten, Debitkarten oderGuthabenkarten eingesetzt. Bei Kredit- und Debitkarten werden sämtliche Zahlungsbeträge verbucht, dem Käufer in Rechnung gestellt, auf den Kontoauszügen ausgedruckt und für mindestens 6 Jahre gespeichert. Dagegen wird bei Guthabenkarten im voraus ein Guthaben eingezahlt und bei jeder einzelnen Zahlung das Guthaben entsprechend herabgesetzt; die Zahlungsbeträge müssen keinem Käufer zugeordnet werden.

Beim elektronischen Bezahlen entstehen sehr unterschiedliche Datenschutzrisiken. Bei Kredit- und Debitkarten besteht die Gefahr, daß die aus Abrechnungsgründen gespeicherten personenbezogenen Daten ausgewertet und zweckentfremdet genutzt werden: Informationen über den Kauf von Fahrscheinen oder über die Nutzung von Autobahnen können zu Bewegungsprofilen verdichtet werden. Das Konsumverhalten des einzelnen wird bis ins Detail nachvollziehbar, falls auch Kleineinkäufe am Kiosk nachträglich abgerechnet werden. Durch den Datenverkauf für Werbung und Marketing können sich weitere Risiken ergeben. Demgegenüber kann bei der Verwendung von Guthabenkarten auf das Speichern personen- oder kartenbezogener Daten aus erfolgten Zahlungen verzichtet werden.

Vor allem im Kleingeldbereich ist die Nutzung von Debit- und Kreditkarten entbehrlich, da fälschungssichere Guthabenkarten auf der Basis von Chipkarten mit integriertem Verschlüsselungsbaustein zur Verfügung stehen. Falls größere Geldbeträge nachträglich per Kredit- oder Debitkarten bezahlt werden, ist darauf zu achten, daß die Abrechnung zunächst über Konten erfolgt, deren Inhaber dem Zahlungsempfänger nicht namhaft gemacht wird. Erst bei Zahlungsunregelmäßigkeiten ist es notwendig, den Bezug zum Kontoinhaber herzustellen.

Angesichts der Risiken, aber auch der von Chipkarten ausgehenden Chancen, fordern die Datenschutzbeauftragten die Kartenherausgeber und die Kreditwirtschaft dazu auf, kartengestützte Zahlungssysteme zu entwickeln, die möglichst ohne personenbezogene Daten auskommen, und deren Anwendung so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt. Der Gesetzgeber muß sicherstellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher anonym zu

bleiben.

Anlage 12

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zur
Weiterentwicklung des Datenschutzes in der Europäischen Union

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 8.9.1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenomen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehenen Instanzen sichergestellt wird.

- Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10.2.1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der u.a. folgende Aussagen enthält: "Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens ... wird gewährleistet".

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28.4.1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild anderer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17.2.1993 und 9./10.3.1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht

umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie von öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikations-Netze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einem in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

-Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden.

- Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau.

- Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte.

- Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.

- Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entgegengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

- Materielle Datenschutzregelungen

Mit der kürzlich verabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

- Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedstaaten einschließlich ihrer Datenschutzkontrolle der

Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.

- Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch, wie derzeit zu befürchten, in unzureichender Form verabschiedet werden.

- Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.

- Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.

- In den Bereichen Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.

- Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes in den Staaten der EU.

- Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z.B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist.

Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

- Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26.5.1994, 8.9.1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25.8.1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutzbeauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EU-Organe und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollte ein solcher Europäischer Datenschutzbeauftragter nicht mit der Funktion des Bürgerbeauftragten nach den EG-Verträgen vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die europäische Union institutionell abgesichert

wird.

- Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EUV derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Verantwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereichen Justiz und Inneres muß daher eine lückenlose parlamentarische und gerichtliche nationale Kontrolle sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

Anlage 13

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zu **Planungen für ein Korruptionsbekämpfungsgesetz**

Derzeit gibt es Vorschläge, die Bekämpfung der Korruption durch Verschärfungen des Strafrechts und des Strafprozeßrechts mit weiteren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu organisieren. Ein Beispiel dafür ist der Beschluß des Bundesrates vom 3. November 1995 zur Einbringung eines Korruptionsbekämpfungsgesetzes.

Nach dem vom Bundesrat beschlossenen Gesetzentwurf sollen Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden, bei deren Verdacht die Überwachung des Fernmeldeverkehrs und der Einsatz technischer Mittel ohne Wissen des Betroffenen (§§ 100a, 100c StPO) angeordnet werden dürfen.

Die Datenschutzbeauftragten weisen demgegenüber darauf hin, daß es vorrangig um Prävention, nicht um Repression geht. Die Datenschutzbeauftragten treten für eine entschlossene und wirksame Bekämpfung der Korruption mit rechtsstaatlichen Mitteln unter strikter Beachtung der Freiheitsrechte ein.

Sie wenden sich zugleich gegen eine Rechtspolitik, welche - noch bevor sie sich darüber im klaren ist, was die bisherigen Verschärfungen und Eingriffe an Vorteilen und an Nachteilten gebracht haben - auf weitere Verschärfungen und Eingriffe setzt. Gerade gegenüber der Korruption gibt es Möglichkeiten, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger nicht antasten:

- Rotation derjenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, deren Position und Aufgaben erfahrungsgemäß für Bestechungsversuche in Betracht kommen;

- Vier- und Sechsaugenprinzip bei bestimmten Entscheidungen;

- Trennung von Planung, Überwachung und Ausführung, von Ausschreibung und Vergabe;

- Prüfverfahren und Innenrevision;

- Codes of Conduct (formalisierte "Ethikprogramme") im Bereich der Wirtschaft;

- verbesserte Transparenz von Entscheidungsprozessen in der Verwaltung.

Die in den Gesetzentwürfen vorgesehene weitere Einschränkung von Grundrechten, die mit einer abermaligen Erweiterung der Telefonüberwachung verbunden wäre, ist nur vertretbar, wenn sie nach einer sorgfältigen Güter- und Risikoabwägung zusätzlich zu den o.g. Verfahrens- und Verhaltensmaßregeln als geeignet und unbedingt erforderlich anzusehen wäre.

Die Datenschutzbeauftragten verlangen, daß vor einer zusätzlichen Aufnahme von Straftatbeständen in den Katalog der Abhörvorschrift des § 100a StPO diese Abwägung durchgeführt wird.

Die Datenschutzbeauftragten fordern weiterhin, daß eine Erweiterung des genannten Straftatenkataloges nur befristet vorgenommen wird, damit sich vor einer Verlängerung die Notwendigkeit stellt, auf der Grundlage einer sorgfältigen Erfolgs- und Effektivitätskontrolle erneut die Erforderlichkeit und Verhältnismäßigkeit einer solchen Erweiterung des Grundrechtseingriffs zu überprüfen.

Die Datenschutzbeauftragten verlangen, daß der Gesetzgeber vor weiteren Eingriffen in Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Schließlich gibt die anstehende erneute Erweiterung des Katalogs von § 100a StPO Veranlassung, den Umfang der darin genannten Straftaten so bald wie möglich grundlegend zu überprüfen.

Anlage 14

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zu **Forderungen**

an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

1. Für die Übermittlung von personenbezogenen Daten durch Justiz und Polizei an die Medien sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

2. Die Übermittlung personenbezogener Daten an die Medien ist nur ausnahmsweise gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

3. Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange des Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten/Angeklagten und deren Angehörige sowie die Schwere, die Umstände und die Folgen des Delikts.

Bei der Übermittlung von personenbezogenen Daten über Beschuldigte/Angeklagte sind auch der Grad des Tatverdachts und der Stand des Verfahrens zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines "überwiegenden Interesses" der Öffentlichkeit anzulegen.

Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. Akteneinsicht durch Medienvertreter kommt nicht in Betracht.

4. Grundsätzlich sind in Auskünfte und Erklärungen über das Ermittlungs- und Strafverfahren keine Namen und sonstige personenbezogene Angaben, die Opfer von Straftaten, Zeugen, Beschuldigte und Angeklagte bestimmbar machen, aufzunehmen. Vor allem bei Hinweisen auf den Wohnort, das Alter, den Beruf und die familiären Verhältnisse oder sonstigen Bindungen (z.B. Partei- oder Vereinsmitgliedschaft) ist zu prüfen, inwieweit dadurch eine Identifizierung des Betroffenen möglich wird.

5. Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

6. Ist die Bekanntgabe der Person des Beschuldigten oder Angeklagten wegen des überwiegenden öffentlichen Interesses gerechtfertigt, muß auch bei der Übermittlung sonstiger personenbezogener Daten

abgewogen werden, ob diese Informationen für die Berichterstattung über die Tat selbst oder die Hintergründe, die zu der Tat geführt haben, erforderlich sind, und in welchem Umfang der Betroffene dadurch in seinem Persönlichkeitsrecht beeinträchtigt wird.

7. Die Bekanntgabe von Vorstrafen ist nur ausnahmsweise zulässig. Sie setzt voraus, daß die frühere Verurteilung im Bundeszentralregister noch nicht getilgt und ihre Kenntnis für eine nachvollziehbare Berichterstattung über eine schwerwiegende Straftat - auch unter Berücksichtigung des Persönlichkeitsrechts des Betroffenen und des Resozialisierungsgedankens - erforderlich ist. Besondere Zurückhaltung ist bei Auskünften und Erklärungen über Sachverhalte geboten, die der früheren Verurteilung zugrunde liegen.

8. Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren gegen diesen Personenkreis besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren.

9. Opfer, Zeugen und Familienangehörige haben in der Regel keine Veranlassung gegeben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekannt gemacht werden. Die Übermittlung personenbezogener Daten über diesen Personenkreis an die Medien kommt deshalb grundsätzlich nicht in Betracht.

10. Bildveröffentlichungen greifen wegen der damit verbundenen sozialen Prangerwirkung besonders tief in das Persönlichkeitsrecht des Betroffenen ein. Eine Bildherausgabe kommt daher für Zwecke der Medienberichterstattung nicht in Betracht.

Anlage 15

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zu
datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 9./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z.B. Vital-Card der AOK Leipzig,

Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)

- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z.B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.

- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.

- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalshafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

- ob Daten auf einer Chipkarte gespeichert werden,

- welche der Gesundheitsdaten auf die Karte aufgenommen werden,

- welche Daten auf der Karte wieder gelöscht werden,

- ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und

- welche Daten im Einzelfall zugänglich gemacht werden.

Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungs-Nr., gespeichert werden, da andernfalls - zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad - die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen

oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z.B. durch Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z.B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht duch eine Chipkarten-vermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte - z.B. mit Hilfe von Schlüsselbegriffen - dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z.B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine "Einwilligung" in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor "billigen Gesundheitskarten" ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der

Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib-/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung, ..., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neue zentralen medizinischen Datensammlungen

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten - einschließlich der Sicherungskopien - übertragen oder nicht.

7. Leserecht des Karteninhabers

Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Anlage 16

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zum **Datenschutz bei der Neuordnung der Telekommunikation** (Postreform III)

Mit der Postreform III soll die Neugestaltung des Telekommunikationssektors in Deutschland nach den Vorgaben des Liberalisierungskonzepts der Europäischen Union abgeschlossen werden. Entstehen wird ein riesiger Markt mit einer Vielzahl von großen und kleinen, teilweise auch grenzüberschreitend tätigen Netzbetreibern und Diensteanbietern. Die Akteure auf diesem Telekommunikationsmarkt werden zum größeren Teil als Privatunternehmen operieren, es werden aber auch öffentliche Stellen ihre Leistungen anbieten. Der gesetzgeberische Abschuß der Liberalisierung und der Privatisierung des TK-Sektors wird die rechtliche Grundlage bilden für den endgültigen Eintritt in das Zeitalter von weltweiter Vernetzung, Multimedia und interaktiven Diensten und damit für den rapiden Anstieg des Konsums von Angeboten der Telekommunikation, des interaktiven Rundfunks und der Datenverarbeitung.

Die Konsequenzen sind absehbar: Gegenüber der heutigen Situation werden unvergleichlich mehr personenbezogene Daten durch mehr Stellen registriert und ausgewertet werden. Betroffen sind alle, die fernsehen, telefonieren, fernkopieren, Texte und Dokumente über Datenleitungen schicken oder Telebanking oder Teleshopping betreiben. Die Risiken für den einzelnen durch die vermehrten Möglichkeiten der Verhaltens- und Umfeldkontrolle oder der Ausforschung persönlicher Lebensgewohnheiten und Eigenschaften vergrößern sich entsprechend.

Der vom Bundesministerium für Post und Telekommunikation vorgelegte Referentenentwurf für ein Telekommunikationsgesetz (TKG-E, Stand: 6. Oktober 1995) macht es erforderlich, erneut die Realisierung der grundlegenden Rahmenbedingungen für eine datenschutzgerechte Gestaltung der künftigen Telekommunikationslandschaft - soweit die Gesetzgebungskompetenz des Bundes betroffen ist - anzumahnen.

Ein wirksamer Datenschutz muß - wie bereits jetzt gesetzlich fixiert - auch künftig gleichberechtigtes Regulierungsziel neben z.B. der Sicherstellung der flächendeckenden Grundversorgung mit Telekommunikationsdienstleistungen bleiben.

Kundenwünsche nach variablerer und komfortablerer Nutzung der technischen Möglichkeiten werden zunehmen. Gerade deshalb müssen die Prinzipien der Datenvermeidung und der strikten Begrenzung der Datenverarbeitung auf das erforderliche Ausmaß ihren Vorrang bei der Ausgestaltung der kommunikationstechnischen Infrastruktur behalten. Netzbetreiber und Diensteanbieter sollten verpflichtet werden, überall dort, wo dies technisch möglich ist, auch anonyme Zugangs- und Nutzungsformen für ihre Leistungen bereitzustellen. Für eine sichere Datenübertragung sind ohne prohibitive Zusatzkosten wirksame Verschlüsselungsverfahren bereitzustellen.

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis müssen für alle Netzbetreiber und Diensteanbieter ungeachtet ihrer Rechtsform und ihrer Kundenstruktur (z.B. sog. Corporate Networks) einheitlich auf einem hohen Niveau gesichert werden. Der bisherige Schutzstandard darf keinesfalls unter den durch die Postreform II erreichten Stand gesenkt werden. Ein hohes Datenschutzniveau ist als Grundversorgung unabdingbar; seine Gewährleistung sollte deshalb Teil der Universaldienstleistung sein. Die in Grundrechte eingreifenden Regelungen sind im Telekommunikationsgesetz selbst und nicht in Verordnungen zu treffen. Die untergesetzlichen, den Datenschutz betreffenden Normen gehören in eine einzige, nicht verstreut in mehrere Verordnungen.

Entscheidend für die Wirksamkeit des Grundrechtsschutzes ist die strikte Einhaltung der Zweckbindung der Verbindungs- und Rechnungsdaten. Das "Feststellen mißbräuchlicher Inanspruchnahme" oder die "bedarfsgerechte Gestaltung" von TK-Leistungen dürfen nicht als Anlaß für eine umfassende Auswertung dieser Angaben oder sogar der Nachrichteninhalte herangezogen werden.

Für den Kunden bzw. Teilnehmer ist es von größter Bedeutung, die Verarbeitungsvorgänge im TK-Bereich überschauen zu können. Er muß auch künftig über die Nutzungsrisiken bestimmter Kommunikationstechniken (z.B. Mobilfunk) ebenso wie über seine Widerspruchsmöglichkeiten umfassend aufgeklärt werden. Keinesfalls darf die Einwilligung des Betroffenen mißbraucht werden, um bereichsspezifische Schutznormen oder effiziente Datensicherungsvorkehrungen zu umgehen.

Um auch und gerade für das besonders schutzwürdige Fernmeldegeheimnis einen durchgängig hohen Schutzstandard zu sichern, braucht es eine unabhängige Kontrolle nach bundesweit einheitlichen Kriterien. Die Zuweisung dieser Überwachungsaufgabe an die im TKG-Entwurf vorgesehene Regulierungsbehörde ist wegen deren mangelhafter Unabhängigkeit und der von ihr wahrzunehmenden Regulierungsaufgaben, die mit Interessenkonflikten verbunden sein werden, nicht akzeptabel.

Deshalb sollte aufgrund seiner langjährigen fachlichen Erfahrung bei der Kontrolle der Telekom und seiner umfassenden Querschnittskenntnisse im TK-Bereich der Bundesbeauftragte für den Datenschutz eine zentrale Funktion für die Kontrolle im Telekommunikationsbereich erhalten. Die Aufgaben, die die Landesbeauftragten für den Datenschutz und die Aufsichtsbehörden im Rahmen ihrer Zuständigkeiten erfüllen, sind gesetzlich klar zu regeln.

Die Akzeptanz der Informationsgesellschaft der Zukunft hängt wesentlich ab von der Sicherung des Grundrechts auf unbeobachtete Kommunikation. Das Telekommunikationsgesetz wird einen entscheidenden Baustein für die rechtliche Ausgestaltung der künftigen TK-Infrastruktur bilden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordern daher dazu auf, die von ihr

vorgeschlagenen Regelungen im weiteren Gesetzgebungsverfahren zu berücksichtigen und sich für ihre Umsetzung auch auf der europäischen Ebene (z.B. in der ISDN-Richtlinie) einzusetzen.

Anlage 17

Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 - **Transplantationsgesetz**

Bei der anstehenden gesetzlichen Regelung, unter welchen Voraussetzungen die Entnahme von Organen zur Transplantation zulässig sein soll, werden untrennbar mit der Ausformung des Rechts auf Selbstbestimmung auch Bedingungen des Rechts auf informationelle Selbstbestimmung festgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont hierzu, daß von den im Gesetzgebungsverfahren diskutierten Modellen die "enge Zustimmungslösung" - also eine ausdrückliche Zustimmung des Organspenders - den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung beinhaltet. Sie zwingt niemanden, eine Ablehnung zu dokumentieren. Sie setzt auch kein Organspenderregister voraus.

Mit einer engen Zustimmungslösung ist auch vereinbar, daß der Organspender seine Entscheidung z.B. einem nahen Angehörigen überträgt.

Anlage 18

Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 - **Grundsätze für die öffentliche Fahndung im Strafverfahren**

Bei den an die Öffentlichkeit gerichteten Fahndungsmaßnahmen nach Personen (Beschuldigten, Verurteilten, Strafgefangenen und Zeugen) wird stets das Recht des Betroffenen auf informationelle Selbstbestimmung eingeschränkt. Es bedarf daher nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15.12.1983 für alle Maßnahmen der öffentlichen Fahndung nach Personen einer normenklaren und dem Grundsatz der Verhältnismäßigkeit entsprechenden gesetzlichen Regelung, die bisher fehlt.

1. Der Gesetzgeber hat zunächst die Voraussetzungen der öffentlichen Fahndung zu regeln und dabei einen sachgerechten Ausgleich zwischen dem öffentlichen Strafverfolgungsinteresse und dem Recht auf informationelle Selbstbestimmung des Betroffenen zu treffen.

Die öffentliche Fahndung sollte nur bei Verfahren wegen Verletzung bestimmter vom Gesetzgeber zu bezeichnender Straftatbestände und

bei Straftaten, die aufgrund der Art der Begehung oder des verursachten Schadens ein vergleichbares Gewicht haben, zugelassen werden.

Sie soll nur stattfinden, wenn weniger intensive Fahndungsmaßnahmen keinen hinreichenden Erfolg versprechen.

Der Grundsatz der Erforderlichkeit mit der gebotenen Beschränkung des Verbreitungsgebiets ist auch bei der Auswahl des Mediums zu berücksichtigen.

2. Bei der öffentlichen Fahnung nach unbekannten Tatverdächtigen, Beschuldigten, Angeschuldigten, Angeklagten einerseits und Zeugen andererseits erscheint es geboten, die Entscheidung, ob und in welcher Weise gefahndet werden darf, grundsätzlich dem Richter vorzubehalten; dies gilt nicht bei der öffentlichen Fahndung zum Zwecke der Straf- oder Maßregelvollstreckung gegenüber Erwachsenen.

Bei Gefahr in Verzug kann eine Eilkompetenz der Staatsanwaltschaft vorgesehen werden; dies gilt nicht bei der öffentlichen Fahndung nach Zeugen. In diesem Falle ist unverzüglich die richterliche Bestätitung der Maßnahme einzuholen.

Die öffentliche Fahndung nach Beschuldigten setzt voraus, daß ein Haftbefehl oder Unterbringungsbefehl vorliegt bzw. dessen Erlaß nicht ohne Gefährdung des Fahndungserfolges abgewartet werden kann.

3. Eine besonders eingehende Prüfung der Verhältnismäßigkeit hat bei der Fahndung nach Zeugen stattzufinden.

Eine öffentliche Fahndung nach Zeugen darf nach Art und Umfang nicht außer Verhältnis zur Bedeutung der Zeugenaussage für die Aufklärung der Straftat stehen. Hat ein Zeuge bei früherer Vernehmung bereits von seinem gesetzlichen Zeugnis- oder Auskunftsverweigerungsrecht Gebrauch gemacht, so soll von Maßnahmen der öffentlichen Fahndung abgesehen werden.

4. In Unterbringungssachen darf eine öffentliche Fahndung mit Rücksicht auf den Grundsatz der Verhältnismäßigkeit nur unter angemessener Berücksichtigung des gesetzlichen Zwecks der freiheitsentziehenden Maßregel, insbesondere der Therapieaussichten und des Schutzes der Allgemeinheit angeordnet werden.

5. Die öffentliche Fahndung zur Sicherung der Strafvollstreckung sollte zur Voraussetzung haben, daß

- eine Verurteilung wegen einer Straftat von erheblicher Bedeutung vorliegt und

- der Verurteilte, der sich der Strafvollstreckung entzieht, (noch) eine

Restfreiheitsstrafe von in der Regel mindestens einem Jahr zu verbüßen hat, oder ein besonderes öffentliches Interesse, etwa tatsächliche Anhaltspunkte für die Begehung weiterer Straftaten von erheblicher Bedeutung, an der alsbaldigen Ergreifung des Verurteilten besteht.

6. Besondere Zurückhaltung ist bei internationaler öffentlicher Fahndung geboten. Dies gilt sowohl für Ersuchen deutscher Stellen um Fahndung im Ausland als auch für Fahndung auf Ersuchen ausländischer Stellen im Inland.

7. Öffentliche Fahndung unter Beteiligung der Medien sollte in den Katalog anderer entschädigungspflichtiger Strafverfolgungsmaßnahmen des § 2 Abs. 2 StrEG aufgenommen werden.

Durch Ergänzung des § 7 StrEG sollte in solchen Fällen auch der immaterielle Schaden als entschädigungspflichtig anerkannt werden.

Der Gesetzgeber sollte vorsehen, daß auf Antrag des Betroffenen die Entscheidung über die Entschädigungspflicht öffentlich bekanntzumachen ist.

Anlage 19

Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 - **Modernisierung und europäische Harmonisierung des Datenschutzrechts**

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: "Die Datenverarbeitungssysteme stehen im Dienste des Menschen".

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, bespielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten.

2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung.

3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz.

4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität.

5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen.

6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung.

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung.

8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist.

9. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren.

10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z.B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten.

11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung alle Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen.

12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung.

13. Verstärkung des Schutzes gegenüber Adressenhandel und

Direktmarketing.

14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau.

Anlage 20

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29. April 1996 zu **Eckpunkten für die datenschutzrechtliche Regelung von Mediendiensten**

In letzter Zeit finden Online-Dienste und Multimedia-Anwendungen zunehmend Verbreitung. Mit den - häufig multimedialen - Angeboten, auf die interaktiv über Telekommunikationsnetze zugegriffen werden kann, sind besondere Risiken für das Recht auf informationelle Selbstbestimmung der Teilnehmer verbunden; hinzuweisen ist insbesondere auf die Gefahr, daß das Nutzerverhalten unbemerkt registriert und zu Verhaltensprofilen zusammengeführt wird. Das allgemeine Datenschutzrecht reicht nicht aus, die mit den neuen technischen Möglichkeiten und Nutzungsformen verbundenen Risiken wirkungsvoll zu beherrschen.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, durch bereichsspezifische Regelungen technische und rechtliche Gestaltungsanforderungen für die elektronischen Dienste zu formulieren, die den Datenschutz sicherstellen. Leitlinie sollte hierbei der Grundsatz der Datenvermeidung bzw. -minimierung sein. Die Datenschutzbeauftragten haben dazu in einer Entschließung vom 14./15. März 1996 zur Modernisierung und zur europäischen Harmonisierung des Datenschutzrechts vorgeschlagen, daß die informationelle Selbstbestimmung bei Multimediadiensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsverfahren anzubieten, durch den Schutz vor übereilter Einwilligung, z.B. durch ein Widerspruchsrecht, und durch strenge Zweckbindung für die bei der Verbindung, Nutzung und Abrechnung anfallenden Daten sichergestellt. wird.

Die Datenschutzbeauftragten weisen darauf hin, daß auch mit Inhalten, die durch Mediendienste verbreitet werden, datenschutzrechtliche Probleme verbunden sein können. Auf diese Probleme wird im folgenden jedoch - ebenso wie auf die Datenschutzaspekte der Telekommunikation - nicht näher eingegangen. Bei den datenschutzrechtlichen Eckpunkten wird ferner bewußt darauf verzichtet, den Regelungsort - etwa einen Länder-Staatsvertrag oder ein Bundesgesetz - anzugeben. Die Datenschutzbeauftragten appellieren an die Gesetzgeber in Bund und Ländern, eine angemessene datenschutzgerechte Regulierung der neuen Dienste nicht an Kompetenzstreitigkeiten scheitern zu lassen.

1. Anonyme bzw. datensparsame Nutzung:

Die Dienste und Multimedia-Einrichtungen sollten so gestaltet werden, daß keine oder möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden; deshalb sind auch anonyme Nutzungs- und Zahlungsformen anzubieten. Auch zur Aufrechterhaltung und zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen (Systempflege) sind soweit wie möglich anonymisierte Daten zu verwenden. Soweit eine vollständig anonyme Nutzung nicht realisiert werden kann, muß jeweils geprüft werden, ob durch andere Verfahren, z.B. die Verwendung von Pseudonymen, ein unmittelbarer Personenbezog vermieden werden kann. Die Herstellung des Personenbezugs sollte bei diesen Nutzungsformen nur dann erfolgen, wenn hieran ein begründetes rechtliches Interesse besteht.

2. Bestandsdaten:

Bestandsdaten dürfen nur in dem Maße erhoben, verarbeitet und genutzt werden, soweit sie für die Begründung und Abwicklung eines Vertragsverhältnisses sowie für die Systempflege erforderlich sind. Die Bestandsdaten dürfen zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen sowie zur Werbung und Marktforschung genutzt werden, soweit der Betroffene dem nicht widersprochen hat. Für die Werbung und Marktforschung durch Dritte dürfen Bestandsdaten nur mit der ausdrücklichen Einwilligung des Betroffenen verarbeitet werden.

3. Verbindungs- und Abrechnungsdaten:

Verbindungs- und Abrechnungsdaten dürfen nur für Zwecke der Vermittlung von Angeboten und für Abrechnungszwecke erhoben, gespeichert und genutzt werden. Sie sind zu löschen, wenn sie für die Erbringung der Dienstleistung oder für Abrechnungszwecke nicht mehr erforderlich sind. Soweit Verbindungsdaten ausschließlich zur Vermittlung einer Dienstleistung gespeichert werden, sind sie spätestens nach Beendigung der Verbindung zu löschen. Die Speicherung der Abrechnungsdaten darf den Zeitpunkt, die Dauer, die Art, den Inhalt und die Häufigkeit bestimmter von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennen lassen, es sei denn, der Teilnehmer beantragt eine dahingehende Speicherung. Verbindungs- und Abrechnungsdaten sind einer strikten Zweckbindung zu unterwerfen. Sie dürfen über den hier genannten Umfang hinaus nur mit der ausdrücklichen Einwilligung des Betroffenen erhoben, verarbeitet und genutzt werden. Unberührt hiervon bleibt die Speicherung von Daten von Verantwortlichen für Angebote im Zusammenhang mit Impressumspflichten.

4. Interaktionsdaten:

Werden im Rahmen von interaktiven Dienstleistungen darüber hinaus personenbezogene Daten erhoben, die nachweisen, welche Eingaben der Teilnehmer während der Nutzung des Angebots zur Beeinflussung des Ablaufs vorgenommen hat (Interaktionsdaten; hierzu gehören z.B. Daten, die bei lexikalischen Abfragen, in interaktive Suchsysteme - etwa elektronische Fahrpläne und Telefonverzeichnisse - und bei Online-

Spielen eingegeben werden), darf dies nur in Kenntnis und mit ausdrücklicher Einwilligung des Betroffenen geschehen. Interaktionsdaten dürfen nur unter Beachtung einer strikten Zweckbindung verarbeitet und genutzt werden. Sie sind grundsätzlich zu löschen, wenn der Zweck, zu dem sie erhoben wurden, erreicht wurde (so müssen Daten über die interaktive Suche von Angeboten unmittelbar nach Beendigung des Suchprozesses gelöscht werden). Eine weitergehende Verarbeitung dieser Daten ist nur auf Grundlage einer ausdrücklichen Einwilligung des Betroffenen zulässig.

5. Einwilligung:

Der Abschluß oder die Erfüllung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, daß der Betroffene in die Verarbeitung oder Nutzung seiner Daten außerhalb der zulässigen Zweckbestimmung eingewilligt hat. Soweit Daten aufgrund einer Einwilligung erhoben werden, muß diese jederzeit widerrufen werden können. Für die Form und Dokumentation elektronisch abgegebener Einwilligungen und sonstiger Willenserklärungen ist ein Mindeststandard zu definieren, der einen fälschungssicheren Nachweis über die Tatsache, den Zeitpunkt und den Gegenstand gewährleistet. Dabei ist sicherzustellen, daß der Teilnehmer bereits vor der Einwilligung soweit wie möglich über den Inhalt und die Folgen seiner Einwilligung und über sein Widerrufsrecht informiert ist. Deshalb müssen die Betroffenen sowohl vor als auch nach Eingabe der Erklärung die Möglichkeit haben, auf Einwilligungen, Verträge und sonstige Informationen über die Bedingungen der Nutzung von Diensten, Multimedia-Einrichungen und Dienstleistungen zuzugreifen und diese auch in schriftlicher Form zu erhalten. Da Verträge oder andere rechtswirksame Erklärungen, die in einer Fremdsprache verfaßt sind, unter Umständen juristische Fachbegriffe enthalten, die nur vor dem Hintergrund der jeweiligen Rechtsordnung zu verstehen sind, sollten zumindest diejenigen Dienste, die eine deutschsprachige Benutzeroberfläche anbieten, derartige Unterlagen auch in deutscher Sprache bereitstellen.

6. Transparenz der Dienste und Steuerung der Datenübertragung durch die Teilnehmer:

Die automatische Übermittlung von Daten durch die beim Betroffenen eingesetzte Datenverarbeitungsanlage ist auf das technisch für die Vertragsabwicklung notwendige Maß zu beschränken. Eine darüber hinausgehende Übermittlung ist nur aufgrund einer besonderen Einwilligung zulässig. Im Hinblick darauf, daß die Teilnehmer bei der eingesetzten Technik nicht erkennen können, in welchem Dienst sie sich befinden und welche Daten bei der Nutzung von elektronischen Diensten bzw. bei der Erbringungen von Dienstleistungen automatisiert übertragen und gespeichert werden, ist sicherzustellen, daß die Teilnehmer vor Beginn der Datenübertragung hierüber informiert werden und die Möglichkeit haben, den Prozeß jederzeit abzubrechen. Die zur Nutzung vom Anbieter oder Netzbetreiber bereitgestellte Software muß eine vom Nutzer aktivierbare Möglichkeit enthalten, den gesamten Strom der ein- und ausgehenden Daten vollständig zu

protokollieren. Bei einer Durchschaltung zu einem anderen Dienst bzw. zu einer anderen Multimedia-Einrichtung müssen die Teilnehmer über die Durchschaltung und damit mögliche Datenübertragungen informiert werden. Diensteanbieter haben zu gewährleisten, daß sie keine erkennbar unsicheren Netze für die Übertragen personenbezogener Daten nutzen bzw. den Schutz dieser Daten durch angemessene Maßnahmen sicherstellen. Entsprechend dem Stand der Technik sind geeignete (z.B. kryptographische) Verfahren anzuwenden, um die Vertraulichkeit und Integrität der übertragenen Daten sowie eine sichere Identifizierung und Authentifikation zwischen Teilnehmern und Anbietern zu gewährleisten.

7. Rechte von Betroffenen:

Die Rechte von Betroffenen auf Auskunft, Sperrung, Berichtigung und Löschung sind auch bei multimedialen und sonstigen elektronischen Diensten zu gewährleisten. Soweit personenbezogene Daten im Rahmen eines elektronischen Dienstes veröffentlicht wurden, der dem Medienprivileg unterliegt, ist das Gegendarstellungsrecht der von der Veröffentlichung Betroffenen sicherzustellen.

8. Datenschutzkontrolle:

Eine effektive, unabhängige und nicht anlaßgebundene Datenschutzaufsicht ist zu gewährleisten. Den für die Kontrolle des Datenschutzes zuständigen Behörden ist ein jederzeitiger kostenfreier elektronischer Zugriff auf die Dienste und Dienstleistungen und der Zugang zu den eingesetzten technischen Einrichtungen zu ermöglichen. Bei elektronischen Diensten, für die das Medienprivileg gilt, ist die externe Datenschutzkontrolle entsprechend zu beschränken.

9. Geltungsbereich:

Der Geltungsbereich der jeweiligen Regelungen ist eindeutig festzulegen. Es ist sicherzustellen, daß die Datenschutzbestimmungen auch gelten, sofern personenbezogene Daten nicht in Dateien verarbeitet werden.

10. Internationale Datenschutzregelung:

Im Hinblick auf die zunehmende Bedeutung grenzüberschreitender elektronischer Dienste und Dienstleistungen ist eine Fortentwicklung der europäischen und internationelen Rechtsordnung dringend erforderlich, die auch bei ausländischen Diensten, Dienstleistungen und Multimedia-Angeboten ein angemessenes Datenschutzniveau gewährleistet. Die Verabschiedung der sog. ISDN-Datenschutzrichtlinie mit einem europaweiten hohen Schutzstandard ist überfällig. Kurzfristig ist es notwendig, den Betroffenen angemessene Mittel zur Durchsetzung ihrer Datenschutzrechte gegenüber ausländischen Betreibern und Dienstleistern in die Hand zu geben. Die in Deutschland aktiven Dienste aus Nicht-EG-Staaten haben im Sinne der EG-Datenschutzrichtlinie

(95/46/EG) vom 24.10.1995 einen verantwortlichen inländischen Vertreter zu benennen.

Anlage 21

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996 - **Forderung zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten**

Der Schutz personenbezogener Daten ist während der Übertragung oder anderer Formen des Transportes nicht immer gewährleistet. Elektronisch gespeicherte, personenbezogene Daten können sowohl auf leitungsgebundenen oder drahtlosen Übertragungswegen als auch auf maschinell lesbaren Datenträgern weitergegeben werden. Oft sind die Eigenschaften des Transportweges dem Absender und dem Empfänger weder bekannt noch durch sie beeinflußbar. Vor allem die Vertraulichkeit, die Integrität (Unversehrtheit) und die Zurechenbarkeit der Daten (Authentizität) sind nicht sichergestellt, solange Manipulationen, unbefugte Kenntnisnahme und Fehler während des Transportes nicht ausgeschlossen werden können. Die Verletzung der Vertraulichkeit ist möglich, ohne daß Spuren hinterlassen werden.

Zahlreiche Rechtsvorschriften gebieten, das Grundrecht auf informationelle Selbstbestimmung auch während der automatisierten Verarbeitung personenbezogener Daten zu sichern (z.B. § 78 a SGB X mit Anlage, § 10 Abs. 8 Btx-Staatsvertrag, § 9 BDSG nebst Anlage und entsprechende landesgesetzliche Regelungen).

Kryptographische Verfahren (z.B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können in vielen Anwendungsfällen mit vertretbarem Aufwand eingesetzt werden.

Angesichts der beschriebenen Situation und der vorhandenen technischen Möglichkeiten fordern die Datenschutzbeauftragten des Bundes und der Länder, geeignete, sichere krypographische Verfahren beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwürdigkeit anzuwenden.

Anlage 22

Kurzbericht zum "**Datenschutz durch Technik**" für die 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 22./23. Oktober 1996

Datensparsamkeit durch moderne Informationstechnik - Datenvermeidung, Anonymisierung und Pseudonymisierung

Die zunehmende Verbreitung, Nutzung und Verknüpfbarkeit von Informations- und Kommunikationstechnik bringt mit sich, daß jeder Benutzer immer mehr elektronische Spuren hinterläßt. Das wird dazu führen, daß er über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der vielen über ihn gespeicherten Daten keine Kontrolle mehr hat, so daß die Gefahr des Mißbrauchs und der Zusammenführung zu komplexen Persönlichkeitsprofilen ständig zunimmt.

Dieser Gefahr kann begegnet werden, wenn in Zukunft die Frage nach der Erforderlichkeit personenbezogener Daten im Vordergrund steht, wobei Datensparsamkeit bis hin zur Datenvermeidung angestrebt werden muß. Durch die Nutzung neuer Möglichkeiten der modernen Informations- und Kommunikationstechnik (IuK-Technik) ist es in vielen Anwendungsfällen möglich, den Umgang mit personenbezogenen Daten zu reduzieren bis hin zur vollständigen Vermeidung. Auf diese Weise kann das Prinzip "Datenschutz durch Technik" umgesetzt werden. Datensparsamkeit und Datenvermeidung werden sich dabei auch zunehmend als Wettbewerbsvorteil erweisen.

Ausgehend von einer Untersuchung des niederländischen Datenschutzbeauftragten und des Datenschutzbeauftragten von Ontario/Kanada zum sogenannten Identity Protector beschäftigen sich derzeit die Datenschutzbeauftragten des Bundes und der Länder intensiv mit der Formulierung von Anforderungen zur datenschutzfreundlichen Ausgestaltung von IuK-Technik. Schon die Sommerakademie in Kiel zeigte unter dem Motto "Datenschutz durch Technik - Technik im Dienste der Grundrechte" Wege zur Wahrung der Persönlichkeitsrechte der Bürger auf. Einige datenvermeidende Technologien wie die anonyme, vorausbezahlte Telefonkarte, sind bereits seit längerer Zeit allgemein akzeptiert. Erste Ansätze der Datenvermeidung auf gesetzgeberischer Ebene sind in den Entwürfen zum Teledienstegesetz und zum Mediendienste-Staatsvertrag enthalten.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" erarbeitet im Auftrag der Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Bericht mit Vorschlägen und Empfehlungen, wie unter Nutzung der modernen Datenschutztechnik das Prinzip der Datenvermeidung umgesetzt werden kann. Neben der Entwicklung entsprechender Hard- und Software werden Anonymisierung und Pseudonymisierung eine zentrale Rolle spielen. Bei der Erarbeitung des Berichtes werden Experten aus Wissenschaft und Forschung hinzugezogen, um die technische Entwicklung berücksichtigen zu können. Auch Vertreter der Wirtschaft als Entwickler und Anwender werden einbezogen, damit die Umsetzung der Vorschläge der Datenschutzbeauftragten als zukünftiger Wettbewerbsvorteil erkannt wird.

Anlage 23

Entschließung der 52. Konferenz der Datenschutzbeauftragten des

Bundes und der Länder vom 22./23. Oktober 1996 zum **Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen**

Mit der Markteinführung des digitalen Fernsehens eröffnen sich für die Anbieter - neben einem deutlich ausgeweiteten Programmvolumen - neue Möglichkeiten für die Vermittlung und Abrechnung von Sendungen. Hinzuweisen ist in erster Linie auf Systeme, bei denen die Kunden für die einzelnen empfangenen Sendungen bezahlen müssen. Dort entsteht die Gefahr, daß die individuellen Vorlieben, Interessen und Sehgewohnheiten registriert und damit Mediennutzungsprofile einzelner Zuschauer erstellt werden. Die zur Vermittlung und zur Abrechnung verfügbaren technischen Verfahren können die Privatsphäre des Zuschauers in unterschiedlicher Weise beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter und Programmlieferanten auf, den Nutzern zumindest alternativ auch solche Lösungen anzubieten, bei denen die Nutzung der einzelnen Programmangebote nicht personenbezogen registriert werden kann, wie es der Entwurf des Mediendienste-Staatsvertrages bereits vorsieht. Die technischen Voraussetzungen für derartige Lösungen sind gegeben.

Die technischen Verfahren sind so zu gestalten, daß möglichst keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden (Prinzip der Datensparsamkeit). Verfahren, die im voraus bezahlte Wertkarten - Chipkarten - nutzen, um die mit entsprechenden Entgeltinformationen ausgestrahlten Sendungen zu empfangen und zu entschlüsseln, entsprechen weitgehend dieser Forderung. Allerdings setzt eine anonyme Nutzung voraus, daß beim Zuschauer gespeicherte Informationen über die gesehenen Sendungen nicht durch den Anbieter abgerufen werden können.

Die Datenschutzbeauftragten sprechen sich außerdem dafür aus, daß für die Verfahren auf europäischer Ebene Vorgaben für eine einheitliche Architektur mit gleichwertigen Datenschutzvorkehrungen entwickelt werden.

Anlage 24

Anlage zur Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, vorgelegt vom Arbeitskreis Medien: **Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen**

Grundsätzlich werden auch Pay-per-View-Programme - wie das traditionelle Abonnenten-Fernsehen - verschlüsselt übertragen. Der Kunde braucht einen Decoder, um die Programme empfangen zu können (die sog. "Set-Top-Box"). Die Sendesignale werden von dem Decoder nur entschlüsselt, wenn er "freigeschaltet" wurde. Die Freischaltung kann mit verschiedenen technischen Verfahren realisiert werden:

1. Zentrale Freischaltung aus dem Netz

Mit dem Sendesignal gekoppelt werden die Benutzernummern sämtlicher Kunden übertragen, die eine bestimmte Sendung sehen wollen. Der Decoder wird auf diese Weise aus dem Netz nur für die betreffende Sendung "freigeschaltet". Dieses Verfahren setzt voraus, daß die Kunden entweder telefonisch oder über einen Rückkanal beim Sender die Freischaltung für eine Sendung verlangen. Damit wird das vom Kunden gewünschte Programmangebot grundsätzlich zunächst registriert.

Zudem werden mit dem über Kabel oder Satellit verteilten Signal für die Sendung auch die Nutzernummern der Interessenten - unverschlüsselt - übertragen, deren Decoder freigeschaltet werden soll; sie können im gesamten Netz mit verhältnismäßig geringem Aufwand mitgelesen und ausgewertet werden. Im Unterschied zur periodischen Freischaltung von Decodern im Abonnenten-Fernsehen ist damit eine sendungsspezifische Registrierung des Nutzungsverhaltens möglich.

Nur durch zusätzliche organisatorische Maßnahmen - etwa die Einschaltung eines neutralen Dritten, der die Freischaltung im Auftrag des Anbieters übernimmt, jedoch keinen direkten Kundenkontakt hat - läßt sich bei diesem Verfahren eine direkt personenbezogene Speicherung des Nutzungsverhaltens vermeiden.

2. Lokale Freischaltung durch den Nutzer

Jede Sendung wird mit einer elektronischen Entgeltinformation (Token) versehen. Die Kunden, die das Programmangebot sehen wollen, teilen dies per Fernbedienung dem Decoder mit. Das Guthaben auf der Chipkarte, die in den Decoder eingeführt ist, wird entsprechend verringert und der Decoder lokal freigeschaltet.

Das Token-System läßt sich mit vorhandener Technik so gestalten, daß beim Anbieter keinerlei personenbezogene Informationen über die Inanspruchnahme einzelner Sendungen entstehen. Eine vollständig anonyme Nutzung kann insbesondere durch den Einsatz von Wertkarten realisiert werden. Selbst bei Einsatz personalisierter wiederaufladbarer Wertkarten besteht die Möglichkeit, daß lediglich der Ladevorgang (z.B. durch Einzahlung eines Guthabens an einem Automaten oder bei Aufladung aus dem Netz), nicht jedoch die einzelne Programmnutzung durch den Anbieter oder einen zwischengeschalteten Dritten registriert wird.

Allerdings besteht die Gefahr, daß auch bei Token-Verfahren auf der Chipkarte Informationen über die einzelnen Programmabrufe gespeichert und - per Rückkanal - an den Anbieter für Zwecke seiner Abrechnung mit Programmlieferanten übermittelt bzw. von diesem abgerufen werden.

Dem datenschutzrechtlichen Gebot, technische Verfahren so zu

gestalten, daß möglichst wenige personenbezogene Daten entstehen und auch eine anonyme Nutzung gewährleistet ist, kann durch das Token-Verfahren bei Pay-per-View besser entsprochen werden als durch Verfahren mit individueller zentral gesteuerter Freischaltung. Eine anonyme Nutzung ist jedoch auch bei dem Token-Verfahren nur dann zu gewährleisten, wenn der Abruf der Daten über die einzelnen gesehenen Sendungen durch den Anbieter unterbleibt.

Anlage 25

Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996 über
Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Die Entwicklung moderner Informations- und Telekommunikationstechniken führt zu einem grundlegend veränderten Kommunikationsverhalten der Bürger.

Die Privatisierung der Netze und die weite Verbreitung des Mobilfunks gehen einher mit einer weitreichenden Digitalisierung der Kommunikation. Mailboxen und das Internet prägen die Informationsgewinnung und -verbreitung von Privatleuten, von Unternehmen und öffentlichen Institutionen gleichermaßen.

Neue Dienste wie Tele-Working, Tele-Banking, Tele-Shopping, digitale Videodienste und Rundfunk im Internet sind einfach überwachbar, weil personenbezogene Daten der Nutzer in digitaler Form vorliegen. Die herkömmlichen Befugnisse zur Überwachung des Fernmeldeverkehrs erhalten eine neue Dimension; weil immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, können sie mit geringem Aufwand kontrolliert und ausgewertet werden. Demgegenüber stehen jedoch auch Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken. Die Datenschutzbeauftragten erkennen an, daß die Strafverfolgungsbehörden in die Lage versetzt werden müssen, solchen mißbräuchlichen Nutzungen der neuen Techniken zu kriminellen Zwecken wirksam zu begegnen.

Sie betonen jedoch, daß die herkömmlichen weitreichenden Eingriffsbefugnisse auch unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können. Die zum Schutz der Persönlichkeitsrechte des einzelnen gezogenen Grenzen müssen auch unter den geänderten tatsächlichen Bedingungen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährleistet werden. Eine Wahrheitsfindung um jeden Preis darf es auch insoweit nicht geben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher Thesen zur Bewältigung dieses Spannungsverhältnisses entwickelt.

Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunkationssysteme müssen mit personenbezogenen Daten

möglichst sparsam umgehen. Daher verdienen solche Systeme und Technologien Vorrang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten, ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z.B. Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht.

Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwendet werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, z.B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen - insbesondere im weltweiten Datenverkehr - ohnehin leicht zu umgehen und kaum kontrollierbar wären.

Anlage 26

Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996 zur **automatisierten Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen**

Der in dem Schiedsspruch vom 20. Februar 1995 für die Abrechnung festgelegte Umfang der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen erfüllt nicht die Anforderungen des Sozialgesetzbuches an diesen Datenaustausch. § 295 SGB V fordert, daß Daten nur im erforderlichen Umfang und nicht versichertenbezogen übermittelt werden dürfen.

Die Datenschutzbeauftragten begrüßen es deshalb, daß der größte Teil

der gesetzlichen Krankenkassen in "Protokollnotizen" - Stand 22. März 1996 - den Umfang der zu übermittelnden Daten reduziert hat. Das Risiko der Identifizierbarkeit des Versicherten wurde dadurch deutlich verringert. Zum letztlich erforderlichen Umfang haben die Spitzenverbände der gesetzlichen Krankenkassen erklärt, daß genauere Begründungen für die Erforderlichkeit der Daten erst gegeben werden könnten, wenn das DV-Projekt für das Abrechnungsverfahren auf Kassenseite weit genug entwickelt sei.

Der Verband der Angestellten-Ersatzkassen (VdAK) hat bisher als einziger Spitzenverband der gesetzlichen Krankenkassen diese Datenreduzierungen nicht mitgetragen. Die Datenschutzbeauftragten fordern den VdAK auf, sich in der Frage der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen der einheitlichen Linie anzuschließen. Dies liegt im gesetzlich geschützten Interesse der Versicherten.

Die besonderen Vorgaben des Sozialgesetzbuches für die Prüfung der Wirtschaftlichkeit der ärztlichen Abrechnungen werden dadurch nicht berührt.