Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

Postanschrift: Landesbeauftragte für den Datenschutz NRW
Postfach 20 04 44, 40102 Düsseldorf

Reichsstraße 43
40217 Düsseldorf
Telefon
(0211) 38 42 40
Telefax
(0211) 38 42 410
Auskunft erteilt:
Frau Gayk
(0211) 38 424 –92
Aktenzeichen
- 16.1 -

20.02.2001

An den
Präsidenten des Landtags
Nordrhein-Westfalen

40221 Düsseldorf

Betr.: Datenschutzbericht 1999/2000 der
Landesbeauftragten für den Datenschutz

Sehr geehrter Herr Präsident,

nach § 27 DSG NW lege ich dem Landtag den 15. Bericht über die Tätigkeit für die Zeit vom 1. Januar 1999 bis zum 31. Dezember 2000 vor.

Die für die Mitglieder des Landtags bestimmten Exemplare sind beigefügt.

Mit freundlichen Grüßen

Ihre

B. Sokol

(Sokol)

Datenschutzbericht 2001

Die Landesbeauftragte
für den Datenschutz
Nordrhein-Westfalen

Fünfzehnter Datenschutzbericht

der

Landesbeauftragten für den Datenschutz

Nordrhein-Westfalen

Bettina Sokol

für die Zeit vom 1. Januar 1999
bis zum 31. Dezember 2000

Herausgeberin:

Die Landesbeauftragte
für den Datenschutz
Nordrhein-Westfalen
Bettina Sokol
Reichsstraße 43

40217 Düsseldorf

Tel.: 0211/38424-0
Fax: 0211/3842410
E-mail: datenschutz@lfd.nrw.de

Diese Broschüre kann unter www.lfd.nrw.de oder
www.nordrhein-westfalen.datenschutz.de abgerufen werden.

ISSN: 0179-2431
Druck: toennes satz + druck GmbH
Erkrath 2001

Gedruckt auf chlorfrei gebleichtem Recyclingpapier

15. Datenschutzbericht

Inhaltsverzeichnis

		Seite
	Vorbemerkung	1
1.	**Zur Situation im Datenschutz - serviceorientiert "aus einer Hand"**	2
2.	**Technische und rechtliche Aspekte der Medienentwicklung**	8
2.1	Rund ums Internet	8
2.1.1	Vertraulichkeit im Internet - Verschlüsselung und Kryptopolitik	8
2.1.2	Rechtsverbindlichkeit im Internet - elektronische Signatur und Willenserklärung	9
2.1.3	Transparenz im Internet - Informationspflichten am Beispiel der Gestaltung von Webportalen	11
2.1.4	Beispiele aus der Internetpraxis	16
2.1.4.1	E-Mails	16
2.1.4.2	Der Weg ins Internet - Accessproviding	21
2.1.4.3	Interaktive Verwaltung	26
2.1.4.4	Die Nutzung von Internetdiensten auf Systemen zur Verarbeitung von Patientendaten - ein erhebliches Risiko für Datenschutz und Datensicherheit	30
2.2	Data Warehouse und Data Mining - Goldgräber im Informationszeitalter	37
2.2.1	Data-Warehouse	37
2.2.2	Data Mining - graben nach Erkenntnis	38
2.2.3	Datenschutzrechtliche Aspekte	39
2.3	Verzeichnisdienste - datenschutzrechtlich ambivalent	40

2.4	Common Criteria - neue Grundlagen zur Prüfung und Bewertung von IT-Sicherheit	43
2.5	Technischer Datenschutz - ein Schritt in die Zukunft	46
2.5.1	Innovative Technikregelungen	46
2.5.2	Sicherheitsziele	48
2.5.3	Sicherheitskonzept	49
2.5.4	Vorabkontrolle	51
2.6	Einzelfragen zur Datensicherheit	52
2.6.1	Wartung und Systembetreuung durch Externe	52
2.6.2	Löschen von PC-Festplatten	53
2.6.3	Unterlagenvernichtung	55
2.6.4	Outsourcing von Briefdruck-Service-Diensten	58
3.	**Videoüberwachung**	**60**
3.1	Videoüberwachung durch öffentliche Stellen ...	60
3.1.1	... eine kontrovers geführte Diskussion	60
3.1.2	Videoüberwachung nach dem Datenschutzgesetz	62
3.1.3	Videoüberwachung in einem Schwimmbad	62
3.1.4	Videoüberwachung nach dem Polizeigesetz	63
3.1.5	Pilotprojekt Bielefeld	64
3.2	Videoüberwachung durch Unternehmen oder Privatpersonen	64
3.2.1	Regelung im Bundesdatenschutzgesetz (BDSG) notwendig	64
3.2.2	Videoüberwachung zur Sicherung von Geschäfts- und Wohngebäuden	66
3.2.3	Videoüberwachung in öffentlichen Verkehrsmitteln	69
3.3	Web-Cams - nur eine andere Art der Werbung?	70
4.	**Polizei**	**72**

5.	**Telekommunikation - zwischen Grundrechtsschutz und Überwachung**	75
5.1	Telekommunikationsgesetz - Forderung nach einem Gesetz zur Sicherung der freien Telekommunikation	76
5.2	Telekommunikationsdatenschutzverordnung	77
5.3	Telekommunikationsüberwachungsverordnung	78
5.4	Zugriff auf Telekommunikationsdaten nach dem Fernmeldeanlagengesetz	78
5.5	Strenge Maßstäbe für die Einschränkung der Kommunikation	79
5.6	Immer mehr Telefonüberwachungen	81
6.	**Strafverfahren, Strafvollzug, Maßregelvollzug**	83
6.1	Datenschutz im Strafverfahren	83
6.2	Strafvollzug	84
6.2.1	Kontrolle der Gefangenenpost	84
6.2.2	Namensgleichheit und Postzustellung	85
6.2.3	Eine Weihnachtsfeier im Knast - und kein Geld	86
6.2.4	Installation einer Wächterschutz- und Kontrollanlage	86
6.3	Maßregelvollzugsgesetz	87
7.	**Verfassungsschutz**	89
8.	**Ausländerinnen und Ausländer**	90
8.1	"Ehe-TÜV" für binationale Paare	90
8.2	Ausschreibungen im Schengener Informationssystem (SIS) durch Ausländerbehörden	93
8.2.1	Ausschreibungen im SIS häufig ohne Rechtsgrundlage	94

8.2.2	Löschungsfristen nach Art. 112 SDÜ werden häufig missachtet	94
9.	**Kommunales**	96
9.1	Öffentliche Auslegung von Wählerverzeichnissen	96
9.2	Anschrift als Hinweis auf mangelnde Bonität	96
10.	**Sozialbereich**	98
10.1	Veraltete Formulare in den Sozialämtern	99
10.2	Verarbeitung von Sozialdaten im Auftrag	101
10.3	Neues Steuerungsmodell bei der Jugendhilfe	102
10.4	Gewährung von Akteneinsicht in Sozial- und Jugendämtern	103
10.5	Politisches Flugblatt in einer Sozialhilfeakte	105
10.6	Versorgungsverwaltung bietet "InfoLine für Gewaltopfer" an	105
11.	**Gesundheit**	107
11.1	Unverändert: Datenschutzgerechte Kostenerstattung bei Schwangerschaftsabbrüchen in besonderen Fällen nicht gewährleistet	109
11.2	Erstattung der Krankenhausrechnung nur gegen Vorlage des ärztlichen Entlassungsberichts?	110
11.3	Wenn Männer sich in frauenärztliche Behandlung begeben ...	110
11.4	Eine Bitte um Vertraulichkeit und ihre Erfüllung	111

12.	**Schule**	113
12.1	Schulen ans Netz	113
12.2	Datenverarbeitung auf häuslichen PCs der Lehrkräfte	113
12.3	Überprüfung der Verfassungstreue in Personalakten	114
13.	**Wissenschaft und Forschung**	116
13.1	Neues Hochschulgesetz	116
13.2	Internetnutzung durch die Hochschulen	116
13.3	Forschung in der Schule	117
13.3.1	Schule als Gegenstand der Forschung	117
13.3.2	Schule als Kontaktstelle für Forschung	118
13.4	Forschungsdaten in Kompetenznetzen	119
14.	**Statistik**	122
14.1	Wie gelangen statistische Erhebungsdaten in ein Verwaltungsgerichtsverfahren?	123
14.2	Abschottung eines Statistik-Bereichs datenschutzgerecht organisieren	124
15.	**Beschäftigte und Arbeitsorganisation**	126
15.1	Telearbeit: Datensicherheit auch hier an erster Stelle	127
15.2	Zuviel Transparenz in einem Beurteilungsverfahren	129
15.3	Ab in den Reißwolf - oder in die "Vorsteherneben-akte"?	130

16.	**Wirtschaft**	131
16.1	Umgang mit Schuldnerdaten in der Wirtschaft	131
16.1.1	Handel mit Schuldnerdaten	131
16.1.2	Schuldnerdaten zur Bonitätsprüfung	132
16.1.3	Schuldnerdaten im Internet	134
16.2	Führung von Guthabenkonten	135
16.3	Moderne Technik mangelhaft	135
16.4	Elektronischer Zahlungsverkehr	136
16.5	Das intelligente Verkehrsticket	138
16.6	Call Center	141
16.6.1	Telefonbanking	141
16.6.2	Call Center als externe Dienstleister	142
Anhang		144

Arbeitsergebnisse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Entschließungen der Datenschutzbeauftragten des Bundes und der Länder

Nr. 1 25./26. März 1999 - 57. Konferenz
Modernisierung des Datenschutzrechts jetzt - umfassende Novellierung des BDSG nicht aufschieben 144

Nr. 2 25./26. März 1999 - 57. Konferenz
Geplante erweiterte Speicherung von Verbindungsdaten in der Telekommunikation 145

Nr. 3 25./26. März 1999 - 57. Konferenz
Transparente Hard- und Software 146

Nr. 4 25./26. März 1999 - 57. Konferenz
Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL '98) 147

Nr. 5 17. Juni 1999 - Entschließung zwischen den Konferenzen
Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern 148

Nr. 6 25. August 1999 - Entschließung zwischen den Konferenzen 1999
Gesundheitsreform 149

Nr. 7 7./8. Oktober 1999 - 58. Konferenz
Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften 151

Nr. 8 7./8. Oktober 1999 - 58. Konferenz
Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation 151

Nr. 9 7./8. Oktober 1999 - 58. Konferenz
DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen 153

Nr. 10 7./8. Oktober 1999 - 58. Konferenz
Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union 154

Nr. 11 7./8. Oktober 1999 - 58. Konferenz
Patientenschutz durch Pseudonymisierung 154

Nr. 12 7./8. Oktober 1999 - 58. Konferenz
Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung 155

Nr. 13 7./8. Oktober 1999 - 58. Konferenz
"Täter-Opfer-Ausgleich und Datenschutz" 157

Nr. 14 14./15. März 2000 - 59. Konferenz
Risiken und Grenzen der Videoüberwachung 158

Nr. 15 14./15. März 2000 - 59. Konferenz
Für eine freie Telekommunikation in der freien Gesellschaft 160

Nr. 16 14./15. März 2000 - 59. Konferenz
Data Warehouse 164

Nr. 17 14./15. März 2000 - 59. Konferenz
Konsequenzen aus dem Urteil des Bundesverfassungs-
gerichts zu den Abhörmaßnahmen des BND 165

Nr. 18 14./15. März 2000 - 59. Konferenz
Strafverfahrensänderungsgesetz 1999 (StVÄG 1999) 167

Nr. 19 14./15. März 2000 - 59. Konferenz
Unzulässiger Speicherungsumfang in "INPOL-neu" geplant 168

Nr. 20 10. Oktober 2000
Auftragsdatenverarbeitung durch das Bundeskriminalamt 169

Nr. 21 12./13. Oktober 2000 - 60. Konferenz
Effektive parlamentarische Kontrolle von Lauschangriffen
durch aussagekräftige jährliche Berichte der Bundesregierung 170

Nr. 22 12./13. Oktober 2000 - 60. Konferenz
Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz
für eine serviceorientierte Verwaltung 171

Nr. 23 12./13. Oktober 2000 - 60. Konferenz
Novellierung des BDSG 172

Nr. 24 12./13. Oktober 2000 - 60. Konferenz
Datensparsamkeit bei der Rundfunkfinanzierung 173

Nr. 25 12./13. Oktober 2000 - 60. Konferenz
Datenschutzrechtliche Konsequenzen aus der Entschlüsselung
des menschlichen Genoms 174

Stichwortverzeichnis 177

Bestellformular Informationsmaterial

Vorbemerkung

Der Berichtszeitraum umfasst zwei außerordentlich turbulente Jahre für die Dienststelle. Die Bearbeitung einer weiter gestiegenen Zahl von Beschwerden, die intensiven Diskussionen mit dem Innenministerium um den Entwurf des seit etwa Mitte 2000 novellierten Landesdatenschutzgesetzes, der Ausbau der Beratungstätigkeit und nicht zuletzt die mit dem neuen Datenschutzgesetz übertragene Zuständigkeit auch für den Datenschutz in der gesamten Wirtschaft und bei anderen nicht-öffentlichen Stellen Nordrhein-Westfalens haben so manches mal die letzten Kraftreserven gefordert. Für ihren engagierten und unermüdlichen Einsatz sei daher allen meinen Mitarbeiterinnen und Mitarbeitern sehr herzlich gedankt.

Dass es trotz personeller Wechsel, Engpässe und Unterbesetzung möglich gemacht worden ist, begonnene Neuerungen kontinuierlich fortzusetzen, freut mich besonders. So konnte zum Beispiel die in Kooperation mit dem Institut für Informations-, Telekommunikations- und Medienrecht (ITM) der Universität Münster veranstaltete Tagungsreihe weiter fortgeführt werden. Wie positiv es allgemein gesehen wird, Grundsatzfragen des Datenschutzes mit Vertreterinnen und Vertretern aus Wissenschaft und Praxis in jedem Jahr einen Tag lang zu diskutieren, zeigt auch die große Nachfrage nach den Dokumentationen, die von den Tagungen erstellt werden. So ist zum Beispiel die Dokumentation des 1998 veranstalteten Symposiums "Neue Instrumente im Datenschutz" in Papierform bereits seit längerer Zeit vergriffen, unter www.lfd.nrw.de aber noch zum Download vorgehalten.

Die im November 1999 durchgeführte Tagung "Datenschutz und Anonymität" wurde in Kooperation mit noch weiteren Partnern veranstaltet, nämlich dem NRW Forschungsverbund Datensicherheit, der Siemens AG und der Ruhr-Universität Bochum. Auch die dort gehaltenen Vorträge sind unter www.lfd.nrw.de ins Netz eingestellt, aber auch in Papierform bestellbar. Gleiches gilt hoffentlich demnächst für die derzeit in Vorbereitung befindliche Dokumentation der wieder mit dem ITM und zusätzlich mit der Landesanstalt für Rundfunk NRW sowie dem WDR im November 2000 veranstalteten Tagung "Mediale (Selbst-)Darstellung und Datenschutz", die sich mit dem Wandel des gesellschaftlichen Verständnisses von Privatheit befasst.

Erwähnenswert ist außerdem das virtuelle Datenschutzbüro. Projektpartnerinnen und -partner sind Datenschutzinstitutionen aus Deutschland (meine Dienststelle ist dabei), den Niederlanden, der Schweiz und Kanada. Erreichbar unter www.datenschutz.de soll das virtuelle Datenschutzbüro zu einer Ansprechstelle für Datenschutzfragen im Internet werden.

1. Zur Situation im Datenschutz - serviceorientiert "aus einer Hand"

Dass es vor dem Hintergrund der rasanten technischen Entwicklung und der damit einhergehenden gesellschaftlichen Veränderungen neuer Datenschutzkonzepte bedarf, ist schon im 14. Datenschutzbericht 1999 unter 1. dargestellt worden. Die dortigen Ausführungen haben nach wie vor Gültigkeit: Benötigt werden datenschutzfreundliche Technologien, um beispielsweise auch auf der Ebene der System- und Verfahrensgestaltung bereits dazu beizutragen, dass es gar nicht erst zur Verarbeitung personenbezogener Daten kommt. Das Recht kann dafür Anreize schaffen, muss aber auch mit strengen Zweckbindungsregelungen und weitreichenden Rechten für die Betroffenen klare Aussagen darüber treffen, was erlaubt und was verboten ist, und zwar im Sinne einer Stärkung des **Rechts auf informationelle Selbstbestimmung**. Denn ohne effektiven Datenschutz und Datensicherheit ist die entstehende Informations- und Wissensgesellschaft demokratisch nicht zu verantworten.

Der nordrhein-westfälische Landtag hat am 9. Mai 2000 umfangreiche Änderungen des Landesdatenschutzgesetzes beschlossen, die in vielen Punkten den eben beschriebenen **Modernisierungsweg** einschlagen. Anlass für die Gesetzesnovelle war zwar die überfällige Umsetzung der europäischen Datenschutzrichtlinie in das Landesrecht, doch das neue Datenschutzgesetz beschränkt sich erfreulicherweise nicht auf die bloße Umsetzung der europäischen Vorgaben. Der Gesetzgeber hat vielmehr die Gelegenheit genutzt, das Datenschutzrecht insgesamt zu modernisieren und es damit zugleich auf die neuen Entwicklungen in der Informationstechnik einzustellen. Das neue **Landesdatenschutzgesetz** ist ein großer Schritt nach vorn zu einem technikorientierten und der Wahrung der Bürgerrechte verpflichteten Datenschutz.

Nur beispielhaft und nicht abschließend sind hier einige der wichtigsten Punkte zu benennen:

- Der Grundsatz der **Datenvermeidung** ist ausdrücklich aufgenommen worden. Schon immer durften und dürfen nur diejenigen personenbezogenen Daten verarbeitet werden, die für festgelegte Zwecke bei der Aufgabenerfüllung erforderlich sind. Der Grundsatz der Datenvermeidung ergänzt das Erforderlichkeitsprinzip allerdings in wesentlicher Hinsicht. Er setzt schon im technischen Vorfeld an. Bereits Planung, Gestaltung und Auswahl informationstechnischer Produkte und Verfahren haben sich danach an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben und weiter zu verarbeiten. Dies verpflichtet zur Berücksichtigung **datenschutzfreundlicher Technolo-**

gien. Ist die Datenschutzfreundlichkeit von Produkten und Verfahren gar in einem förmlichen **Auditierungsverfahren** festgestellt worden, sollen sie vorrangig berücksichtigt werden. Auch die öffentlichen Stellen selbst können in eine Art Wettbewerb um den besten Datenschutz treten und ihre Datenschutzkonzepte sowie ihre technischen Einrichtungen prüfen und bewerten lassen.

- Darauf, die Verarbeitung von Daten mit Personenbezug zu vermindern, zielt auch die neue Regelung über wissenschaftliche Forschung. Hier gilt es grundsätzlich, die Datenverarbeitung in **anonymisierter** oder zumindest **pseudonymisierter** Form zu betreiben.

- Die Aktenführung und die elektronische Datenverarbeitung sollen bei allen öffentlichen Stellen so organisiert sein, dass die **Trennung** der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. Damit soll erreicht werden, dass öffentlichen Stellen, aber auch Personen, die von ihrem Auskunfts- und Einsichtnahmeanspruch Gebrauch machen, im gegebenen Zusammenhang überflüssige Informationen über Dritte nicht zugänglich gemacht werden.

- Herzstück der bereits mehrfach als bundesweit vorbildlich innovativ gelobten technisch-organisatorischen Regelungen im neuen Landesdatenschutzgesetz ist **§ 10 DSG NRW.** Um die dort genannten Datenschutz- und Datensicherheitsziele zu verwirklichen, haben die öffentlichen Stellen eigene **Konzepte** zu erarbeiten (siehe dazu ausführlich unter 2.5). Sie haben vor der Entscheidung über den Einsatz oder eine wesentliche Änderung eines automatisierten Verfahrens jeweils eine **Vorabkontrolle** hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung der davon betroffenen Personen durchzuführen und im Konzept zu dokumentieren. Die im Konzept vorgesehenen Schutz- und Sicherheitsmaßnahmen müssen wirksam sein. Dies ist zu überprüfen. Ergeben sich Änderungsnotwendigkeiten, hat eine zeitnahe **Anpassung** zu erfolgen.

- Vor dem Hintergrund der gewachsenen Bedürfnisse - auch vieler Betroffener - nach dem Einsatz von **Chipkarten** in den vielfältigsten Verwendungszusammenhängen ist eine Bestimmung über mobile personenbezogene Datenverarbeitungssysteme in das Gesetz aufgenommen worden. Das neue Recht nimmt an dieser Stelle das Recht der Menschen auf informationelle Selbstbestimmung in vorbildlicher Weise ernst: Chipkarten und gegebenenfalls andere mobile Datenverarbeitungssysteme dürfen nur auf **freiwilliger Basis** ausgegeben werden. Die betroffenen Personen sind zunächst umfassend darüber zu informieren, was eigentlich mit und auf der Chipkarte passieren soll. Sind sie damit einverstanden oder auch nur mit einem Teil der angebotenen Verarbei-

tungsfunktionen, so müssen sie ihre ausdrückliche Einwilligung erteilen. Es kann also niemand dazu gezwungen werden, eine Chipkarte zu akzeptieren. Für die **Transparenz** der Datenverarbeitung gegenüber den Betroffenen sorgen weitere Detailregelungen.

- Auch für die **Videoüberwachung** zur Wahrnehmung des Hausrechts enthält das Datenschutzgesetz nunmehr eine Regelung (siehe ausführlich unter 3.1.2), die sich erfreulicherweise im Wesentlichen an den im 14. Datenschutzbericht 1999 unter 3.8.1 dargestellten Grundsätzen und Anforderungen orientiert.

- Eine Stärkung des Datenschutzes "vor Ort" verspricht die Pflicht zur Bestellung von in ihrer Funktion **weisungsfreien behördlichen Datenschutzbeauftragten.** Besitzen sie eine gewisse innere Unabhängigkeit, kann es ihnen auf Grund ihrer gesetzlich fixierten, starken Stellung gelingen, den Datenschutz maßgeblich voranzubringen. Sie haben Beratungs-, Schulungs- sowie Kontrollfunktionen, sind frühzeitig an der Erarbeitung datenschutzrelevanter Vorhaben zu beteiligen und führen die Vorabkontrollen durch. Als Serviceangebot ist eine Orientierungshilfe zur Arbeit behördlicher Datenschutzbeauftragter in Vorbereitung und in Kürze sowohl in Papierform als auch unter www.lfd.nrw.de erhältlich.

- Viel zu oft musste in der Vergangenheit eine Unterrichtung meiner Dienststelle - insbesondere bei Entwürfen für Rechts- und Verwaltungsvorschriften - erst angemahnt werden. Der Gesetzgeber hat insoweit deutliche Worte gefunden und eine unmissverständliche Klarstellung in das Gesetz aufgenommen. Der Text, der seit dem 31. Mai 2000 geltenden Vorschrift über die **frühzeitige Unterrichtung über Entwürfe für Rechts- oder Verwaltungsvorschriften**, die eine Verarbeitung personenbezogener Daten vorsehen, scheint jedoch noch nicht in allen Ministerien des Landes bekannt zu sein. Mit der Einhaltung der Bestimmung klappt es jedenfalls in manchen Fällen noch nicht.

- Last but not least ist im neuen Landesdatenschutzgesetz die **Zuständigkeit für die Datenschutzaufsicht im Bereich der privaten Wirtschaft** auf meine Dienststelle übertragen worden. Nordrhein-Westfalen ist mit dieser Grundentscheidung einer bürgerfreundlichen Bündelung der Datenschutzaufsicht "in einer Hand" dem Beispiel anderer Bundesländer gefolgt. Die dadurch notwendige Umorganisation der Dienststelle konnte angesichts der knappen personellen Kapazitäten bislang erst in Angriff genommen, aber noch nicht abgeschlossen werden. Um die frühere Zersplitterung der Datenschutzzuständigkeit für den öffentlichen und den nicht-öffentlichen Bereich tatsächlich vollständig zu beseitigen, ist organisatorisch die Umsetzung eines "Lebenssachverhaltskonzepts" angestrebt. Das bedeutet, dass beispielsweise in dem für die Polizei zu-

ständigen Referat auch die privaten Sicherheitsdienste angesiedelt sind, die Zuständigkeit für die öffentlichen Sparkassen um diejenige für die privaten Banken erweitert wird und die Kontrolle der Gesundheitsdatenflüsse zwischen öffentlichen Krankenhäusern und niedergelassenen Ärztinnen und Ärzten ebenfalls einheitlich in einem Referat stattfindet.

Wie im öffentlichen Bereich auch steht zunächst **Prävention** durch Beratung im Vordergrund, um es gar nicht erst zu Datenschutzverletzungen kommen zu lassen. Kontakte zu manchen Unternehmen und Verbänden sind bereits geknüpft, erste Gespräche geführt. Bei der Einzelkontrolle auf Grund von Beschwerden von Bürgerinnen und Bürgern werden allerdings in etlichen Fällen die Defizite des geltenden Bundesdatenschutzgesetzes deutlich, das keine wirklich wirksamen Eingriffsbefugnisse zur Beseitigung rechtswidriger Datenverarbeitungen enthält.

Der Mitte des Jahres 2000 vom Bundeskabinett beschlossene Gesetzentwurf zur Änderung des **Bundesdatenschutzgesetzes** beschränkt sich im Wesentlichen auf die Anpassung des Gesetzes an die Vorgaben der europäischen Datenschutzrichtlinie. Die Punkte, in denen darüber hinausgehende Ansätze zur Modernisierung des Datenschutzrechts gesehen werden können, zum Beispiel die Einführung eines Datenschutzaudits, werden leider bislang nicht alle vom Bundesrat unterstützt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die schon in ihrer Entschließung vom 25./26. März 1999 (Abdruck im Anhang, Nr. 1) erneut die Dringlichkeit der Modernisierung des Datenschutzrechts betont hatte, hat in einer weiteren Entschließung vom 12./13. Oktober 2000 (Abdruck im Anhang, Nr. 23) den Bundesrat aufgefordert, die Novelle nicht weiter zu blockieren. Eine grundlegende Reform des Datenschutzrechts soll in einer so genannten zweiten Stufe erfolgen, für die die Vorarbeiten bereits begonnen wurden.

Die weitere **Miniaturisierung** und **Vernetzung** haben nach wie vor maßgebliche Bedeutung für die technische Entwicklung und die damit verbundenen gesellschaftlichen Veränderungen. Computer nicht größer als Staubkörner (smart dust), so genannte Internet-Häuser, in denen die Kühlschränke die zentralen Schaltstellen bilden und Heizungen, Alarmanlagen sowie Einkäufe regeln und angeblich intelligente Kleidung, die nicht nur der Überwachung der eigenen Umgebung dienen soll, sind nur einige Beispiele, bei denen es sich teilweise schon gar nicht mehr um Zukunftsszenarien handelt. Ob wir das wirklich alles brauchen oder auch nur wollen, ist kritisch zu hinterfragen.

Die **Risiken der Internetnutzung** für den Schutz von Privatheit sind immer noch viel zu wenig bekannt. Die im Netz hinterlassenen Spuren dürfen nach

deutschem Recht nur unter strengen Voraussetzungen ausgewertet werden. Dass die geltenden gesetzlichen Regelungen - teils aus Unkenntnis - nicht immer eingehalten werden (siehe dazu unter 2.1.4.2), sollte allerdings nicht dazu verleiten, die Bestimmungen zum Nachteil der Nutzerinnen und Nutzer zu lockern. Dies darf unter anderem bei der anstehenden Novelle des Teledienstedatenschutzgesetzes nicht aus dem Blick verloren werden.

Daran, dass Menschen **gläsern** werden, sind mittlerweile viele interessiert. In den Vereinigten Staaten von Amerika ist eine regelrechte Branche entstanden, die ganz offen als Dienstleistung anbietet, Informationen über andere Leute "auszuspionieren" und gegen Entgelt zur Verfügung zu stellen. Mit der früheren Arbeit der aus Krimis so bekannten und beliebten Privatdetektivinnen und Privatdetektive hat dies allerdings nichts mehr gemein. Wer die Nachbarschaft, Geschäftspartnerinnen und -partner oder künftige Angestellte ausforschen lassen will, erhält unter Einsatz der heutigen technischen Möglichkeiten Informationen, die im Hinblick auf ihre Quantität und ihre Qualität früher mögliche Ergebnisse weit in den Schatten stellen.

Nicht die Informationsweitergabe ohne Wissen und Wollen der betroffenen Personen, sondern die **Kommerzialisierung** personenbezogener Daten unter **finanzieller Beteiligung** der Betroffenen ist ein weiterer Trend, der zu verzeichnen ist. Die immer stärkere Verbreitung findenden Payback-Cards sind eben gerade nicht mit den Rabattmarken und dem Rabattheftchen aus früheren Tagen vergleichbar. Der Preisnachlass von heute ist praktisch die Gegenleistung für die personenbezogene Erfassung, Speicherung und Auswertung des individuellen Kaufverhaltens. Im Internet zum Beispiel entstehen Firmen, deren alleiniger Geschäftszweck der Handel mit personenbezogenen Daten ist. Das wäre nichts Neues. Neu ist aber die prozentuale Umsatzbeteiligung derjenigen Personen, die freiwillig detaillierte Angaben über sich machen, ihr Kundenprofil also gleich selber liefern.

Ist der Datenschutz auf dem absteigenden Ast? Interessiert sich überhaupt noch jemand dafür angesichts der massenhaft präsenten Videoüberwachungskameras aller Orten, der zunehmenden Zahl von Web-Cams, mit denen sich Menschen in den eigenen vier Wänden von im wahrsten Sinne des Wortes "aller Welt" bei ihren Alltagsverrichtungen beobachten lassen? Ist mit dem Erfolg von den das Intimleben thematisierenden Talk-Shows und von "Big Brother" der freiwillige **Verlust der Privatheit** eingeläutet? Wohl eher nicht. Sonst gäbe es nicht die Empörung über die zahllosen versteckten Kameras, mit denen Aufnahmen beispielsweise aus Hotelzimmern, Umkleidekabinen, Solarien oder Duschräumen ohne Wissen der betroffenen Personen im Internet vermarktet werden. Es gäbe auch nicht die Empörung, die unter anderem in der auch in diesem Berichtszeitraum weiter angestiegenen

Zahl von Beschwerden zum Ausdruck kommt und die sich gegen die Erfassung und Speicherung personenbezogener Daten ohne Wissen und Wollen der Betroffenen richtet. Denn **Selbstbestimmung** heißt auch hier das Zauberwort. Und Selbstbestimmung bedeutet die Anerkennung eigener Maßstäbe und einer eigenen Definitionsmacht. Die Menschen wollen ihre Privatheit nicht verlieren, sie haben heute möglicherweise nur ein vielfältigeres Begriffsverständnis davon. Diesem **Wandel** gerecht zu werden, ist - neben der effizienten Aufklärung über die Risiken für die Selbstbestimmung - auch eine der wesentlichen Herausforderungen für den **Datenschutz der Zukunft.**

2. Technische und rechtliche Aspekte der Medienentwicklung

2.1 Rund ums Internet

Längst ist das Internet kein Medium nur für Insider und Technikfreaks mehr. Immer mehr Bürgerinnen und Bürger nutzen E-Mail, um Bekannten Nachrichten zu hinterlassen. Sie wollen ihre Kinder zum Kindergarten anmelden, über den neuen Volkshochschulkurs informiert werden, Verbrauchertipps abfragen und am liebsten am Wochenende im virtuellen Kaufhaus ganz ohne Gedränge einkaufen gehen, nachdem sie sich auf so genannten Webportalen über die besten Einkaufsadressen informiert haben. Patientinnen und Patienten holen sich seelischen Rat und Fürsprache über das Internet, tauschen sich mit ihrer Ärztin oder ihrem Arzt aus, wickeln ihre Bankgeschäfte ab und ordern ihr Essen beim Pizza-Versandservice um die Ecke.

Viele Bürgerinnen und Bürger wenden sich an meine Dienststelle, denn sie befürchten, bei den Transaktionen im Internet beobachtet zu werden, wollen sich nicht eine falsche oder sogar gefälschte Willenserklärung zurechnen lassen oder wissen nicht, wer was wann von wem speichert und haben die Sorge, ob der sichere Umgang mit ihren sensitiven Daten wie zum Beispiel ihren Krankendaten gewährleistet ist.

Erstmals haben im Berichtszeitraum das europäische Parlament und der europäische Rat Richtlinien - die so genannte Signaturrichtlinie und die Richtlinie über den elektronischen Geschäftsverkehr - im Anwendungsbereich des Internet verabschiedet. Auch der nationale Gesetzgeber hat sich der geschilderten Probleme des Internet im Berichtszeitraum in einer Reihe von weiteren Gesetzesvorhaben angenommen und bestehende Gesetze evaluiert.

2.1.1 Vertraulichkeit im Internet - Verschlüsselung und Kryptopolitik

Eine wirksame Möglichkeit Transaktionen im Netz vor der Beobachtung durch Dritte zu schützen, besteht darin, **Verschlüsselungsverfahren** einzusetzen. Immer wieder hat es allerdings Vorstöße gegeben, den Einsatz von Verschlüsselungsverfahren zu verbieten, denn sie machen eine Überwachung des Netzes auch zum Zwecke der Strafverfolgung unmöglich. In Deutschland besteht kein Verbot kryptographischer Verfahren. Im Gegenteil: Die **derzeitige Rechtslage verpflichtet** die Diensteanbieterinnen und -anbieter sogar dazu, durch technische und organisatorische Vorkehrungen

sicherzustellen, dass die Nutzerinnen und Nutzer Informations- und Kommunikationsdienste **gegen Kenntnisnahme Dritter geschützt** in Anspruch nehmen können, § 4 Abs. 2 Nr. 3 Teledienstedatenschutzgesetz (TDDSG) und § 13 Abs. 2 Nr. 3 Mediendienstestaatsvertrag (MDStV). Immer wieder wird allerdings ein Kryptoverbot oder aber eine gesetzlich verankerte Key-Recovery-Lösung, dass heißt ein Zugang zum Originaltext außerhalb der normalen Ver- und Entschlüsselung, diskutiert. In einem im Berichtszeitraum von der Bundesregierung veröffentlichten so genannten Eckpunktepapier zur Kryptopolitik (Pressemitteilung vom 02.06.1999) äußert sich die jetzige Bundesregierung nun allerdings eindeutig. Danach beabsichtigt sie nicht "die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland" einzuschränken. Vielmehr sieht sie "in der Anwendung sicherer Verschlüsselung eine entscheidende Voraussetzung für den Datenschutz der Bürgerinnen und Bürger, für die Entwicklung des elektronischen Geschäftsverkehrs sowie für den Schutz von Unternehmensgeheimnissen".

Die Position der Datenschutzbeauftragten zum Thema Verschlüsselung ist eindeutig: Die Datenschutzbeauftragten haben bereits 1996 in einer Entschließung gefordert, die Vertraulichkeit übertragener Daten durch geeignete Maßnahmen, zum Beispiel kryptographische Verfahren zu gewährleisten und dies mit einer weiteren Entschließung im Berichtszeitraum bekräftigt. Die Entschließungen sind abrufbar unter www.lfd.nrw.de.

2.1.2 Rechtsverbindlichkeit im Internet - elektronische Signatur und Willenserklärung

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

Wie schon im 14. Datenschutzbericht 1999 (unter 2.4.3.5) dargestellt, gibt es mit dem **Signaturgesetz** und der **Signaturverordnung** in Deutschland bereits Regelungen zur Ausgestaltung einer solchen Sicherungsinfrastruktur. Normiert sind unter anderem die Voraussetzungen für die Genehmigung von Zertifizierungsdiensteanbieterinnen für die Schlüsselzuordnung sowie die Anforderungen an die Tätigkeit und den Betrieb von Zertifizierungsdienste-

anbieterinnen. Mit der am 19. Januar 2000 in Kraft getretenen Europäischen Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen sollen nun einheitliche Regelungen für die Europäische Union geschaffen werden.

Erste **Entwürfe zur Umsetzung der Signaturrichtlinie** liegen bereits vor. Im Unterschied zur geltenden Rechtslage sollen die Zertifizierungsdiensteanbieterinnen künftig nach § 11 Signaturgesetz (SigG) verpflichtet werden, unter bestimmten Voraussetzungen für die Richtigkeit der Angaben in qualifizierten Zertifikaten zu haften. Nach dem Entwurf des Signaturgesetzes ist der Betrieb eines Zertifizierungsdienstes nun nicht mehr genehmigungspflichtig. Wer den Betrieb eines Zertifizierungsdienstes aufnimmt, hat dies der zuständigen Behörde aber anzuzeigen und unterliegt der Aufsicht der Regulierungsbehörde für Telekommunikation und Post. Neben der Anzeige des Betriebs sieht der Entwurf zum Signaturgesetz die freiwillige Akkreditierung von Zertifizierungsdiensteanbieterinnen vor und enthält somit die Möglichkeit, durch eine Vorabprüfung den Nachweis sicherer Verfahren zu führen.

Zu der nicht im Signaturgesetz behandelten Frage, in welcher **Form** künftig **Willenserklärungen** im Internet abgegeben werden dürfen und welche Rechtsfolgen damit verbunden sind, liegt ein Referentenentwurf des Bundesministeriums der Justiz vor. Der Entwurf strebt eine Überarbeitung der Formvorschriften des Zivilrechts und verschiedener prozessualer Gesetze an. Denn in den Fällen, in denen gesetzlich die Schriftform für die Abgabe von Willenserklärungen vorgesehen ist, und damit die eigenhändige Unterschrift erforderlich wird, können solche Erklärungen derzeit nicht in elektronischer Form abgegeben werden. Für eine Vielzahl von Regelungen möchte der Gesetzentwurf hier Abhilfe schaffen. Der Entwurf sieht als wesentlichste Änderungen in den §§ 126a und 126b BGB eine elektronische Form und eine Textform vor. Die elektronische Form erfordert eine qualifizierte elektronische Signierung des Dokumentes nach dem Signaturgesetz.

Ähnliches ist auch für den **öffentlichen Bereich** geplant. Eine entsprechende Entschließung verbunden mit der Aufforderung an die Bundesregierung, die elektronische Abwicklung von Verwaltungsdienstleistungen auch im Bereich der durch Bundesrecht vorgeschriebenen Formerfordernisse zuzulassen, hat der Bundesrat in seiner Sitzung am 09.06.2000 bereits angenommen (BR-Drs. 231/00; Beschluss). Einen **ersten Entwurf** hat die Konferenz **der Verwaltungsverfahrensrechtsreferentinnen und -referenten** im September beschlossen. Nach § 3a des Entwurfs kann eine durch Gesetz angeordnete Schriftform, soweit nicht Rechtsvorschriften etwas anderes bestimmen,

durch die mit einer qualifizierten elektronischen Signatur im Sinne des Signaturgesetzes verbundene elektronische Form ersetzt werden.

2.1.3 Transparenz im Internet - Informationspflichten am Beispiel der Gestaltung von Webportalen

Transparenz ist eine wichtige Voraussetzung für den Schutz des **Rechts auf informationelle Selbstbestimmung.** Nur wenn die Bürgerinnen und Bürger auch im World Wide Web wissen, wann von wem welche personenbezogenen Daten erhoben, gespeichert, verarbeitet und genutzt werden, können sie von ihrem Recht auf Selbstbestimmung Gebrauch machen. Welche Informationspflichten bestehen, soll am Beispiel der Gestaltung von Webportalen aufgezeigt werden. Die rechtlichen Vorgaben gelten jedoch generell für die Gestaltung von Internetseiten.

Was sind eigentlich Webportale? So schnell wie die Zahl der Internetnutzenden wächst, so schnell wächst auch das Angebot im World Wide Web. Für jede und jeden könnte die passende Information vorhanden sein, nur wie lässt sie sich in der neuen virtuellen Welt finden? Eine Hilfestellung wollen die so genannten Webportale geben, die sich in der Internetlandschaft immer mehr etablieren. Webportale sind Internetseiten, die eine breit gefächerte Themenpalette mit einem vorstrukturierten Themenangebot anbieten. Sie sind mehr als reine Homepages. Sie halten nicht nur Eigeninformationen bereit, sondern vermitteln auch an andere Internetanbieterinnen oder -anbieter weiter, mit denen kooperiert wird.

Neben der Frage, welche Inhalte in Webportale eingestellt werden dürfen, sind auch **datenschutzrechtliche Vorgaben für das Angebot von Informations- und Kommunikationsdiensten** zu beachten. Solche Vorgaben enthalten das **Teledienste- und das Teledienstedatenschutzgesetz** (TDG; TDDSG) **oder der Mediendienstestaatsvertrag** (MDStV), je nachdem, ob der jeweilige Informations- und Kommunikationsdienst als Teledienst für eine individuelle Nutzung von kombinierbaren Daten bestimmt ist oder ob er als Mediendienst an die Allgemeinheit gerichtet ist und redaktionell gestaltete Beiträge enthält. Welche Informationspflichten müssen nun realisiert werden?

Anbieterkennzeichnung

Die bunte Welt der Webportale, die den Nutzerinnen und Nutzern die Handhabung des Internet erleichtern will, ist bei genauem Hinsehen verwirrend. Wer verbirgt sich denn hinter dem Webportal, beispielsweise hinter dem Domainnamen der Stadt xy, der in das World Wide Web eingestellt ist? Betreibt die Stadtverwaltung das Webportal oder ist es eine Firma, die den Service anbietet? Die Anbieterkennzeichnung soll den Nutzerinnen und Nutzern ein Mindestmaß an Transparenz und Information ermöglichen. Nur mit ausreichender Anbieterkennzeichnung ist es möglich, den eigenen **datenschutzrechtlichen Auskunftsanspruch** nach § 7 TDDSG oder § 13 MDStV geltend zu machen. Auch die Datenschutzbeauftragten sind für eine effektive Kontrolle auf die umfassende und korrekte Kennzeichnung angewiesen.

Verbindlicher Mindestinhalt der Anbieterkennzeichnung:

- Name der Anbieterin oder des Anbieters (Firma, Rechtsform), Behörde
- Name der vertretungsberechtigten Person, Name der verantwortlichen Person
- Anschrift (Straße, Hausnummer, PLZ, Ort)
- Bei journalistisch gestalteten Texten:
  - Verantwortliche Person (Vorname, Nachname)
  - Anschrift (Straße, Hausnummer, PLZ, Ort)
  - Verantwortungsbereich

Nach **§ 6 TDG, § 6 Abs. 1 MDStV** haben Diensteanbieterinnen und -anbieter Namen und Anschrift sowie bei Personenvereinigungen und -gruppen auch Namen und Anschrift der vertretungsberechtigten Person anzugeben. Zusätzlich sind nach § 6 Abs. 2 MDStV noch die verantwortlichen Personen für den journalistischen Text mit Namen und Anschrift zu benennen. Empfehlenswert ist darüber hinaus die Angabe von Telefon- und Telefaxnummer, die eine Kontaktaufnahme erleichtern. Erfolgt die technische Abwicklung des Angebots durch ein Rechenzentrum oder andere Dritte, so sind diese dann in der Anbieterkennzeichnung ebenfalls aufzuführen.

Die am 8. Juni 2000 verabschiedete **Richtlinie** des Europäischen Parlaments und des Rates der Europäischen Union über den **elektronischen Geschäftsverkehr** enthält in ihren Artikeln 5 und 6 eine Reihe weiterer **Informationspflichten**, so unter anderem über die Handelsregistereintragung, die Mehrwertsteuernummer und die E-Mail-Adresse. Die Richtlinie ist bis zum 17. Januar 2002 in das jeweilige nationale Recht umzusetzen.

Während der **Inhalt** der Anbieterkennzeichnung zwar unmissverständlich normiert ist, fehlt es jedoch an einer Regelung der **Präsentation**. Sie ergibt

sich allerdings aus dem Zweck der Anbieterkennzeichnung. Die **Anbieterkennzeichnung** ist so zu plazieren und auszugestalten, dass sie **leicht auffindbar** und **gut lesbar** ist. Wer sich im Netz bewegt, weiß, dass dies leider oft nicht der Fall ist.

Die Anbieterkennzeichnung hat zumindest auf einer Seite des Webportals die vollständigen Angaben zu enthalten. Beim Aufrufen des Webportals sollte auf jeden Fall eine eindeutige Kurzbezeichnung (der Anbieterkennzeichnungsanker) und eine direkte Verweisung (Link) auf die vollständige Anbieterkennzeichnung vorhanden sein ("one click away"). Da im Internet nicht immer ein Einstieg über die Startseite des Webportals notwendig ist, ist zusätzlich zu gewährleisten, dass die Nutzerinnen und Nutzer auch von allen übrigen Seiten des Webportals direkt auf diejenige Seite gelangen können, von der aus auf die Anbieterkennzeichnung zugegriffen werden kann ("two clicks away"). Der Anbieterkennzeichnungsanker sollte ohne Schwierigkeiten gefunden werden können und eine bekannte und als solche eindeutig erkennbare Anbieterkurzbezeichnung gewählt werden. Auch farblich sowie hinsichtlich der Schriftart und -größe sollte eine gute Erkennbarkeit und Lesbarkeit sichergestellt werden. Daher ist es empfehlenswert, dass starke Kontraste in Farbe und Linienführung gewählt werden. Die Anbieterkennzeichnung ist so auszugestalten, dass sie problemfrei auszudrucken ist.

Anzeige der Weitervermittlung

Die Weitervermittlung an Kooperationspartnerinnen und -partner des Webportals oder an andere Dritte mittels eines Links ist nach **§ 4 Abs. 3 TDDSG, § 13 Abs. 3 MDStV** anzuzeigen. Auch hier steht der Gedanke der Transparenz im Vordergrund. Der Anzeige der Weitervermittlung kann beispielsweise durch einen unmissverständlichen Hinweis in Wortform Genüge getan werden oder durch Schaltung einer Zwischenseite, die auf die vermittelte Adresse hinweist und den Abbruch der Weiterschaltung ermöglicht. Auch sollte jederzeit erkennbar sein, wer für die aufgerufene Seite verantwortlich ist. Es kann irreführend sein, wenn zum Beispiel der Frame des Webportals einer Stadt bei einer nicht erkennbaren Weitervermittlung, etwa an die Stadtsparkasse noch vorhanden ist. Unter Umständen ist dann die Anbieterin oder der Anbieter des Webportals nach § 5 TDG und § 5 MDStV auch für den fremden Inhalt des Dritten verantwortlich.

Informationspflichten und elektronische Einwilligung

Damit Angebote für die Nutzerinnen und Nutzer schnell und unkompliziert abzurufen sind, werden oft so genannte Cookies verwendet. Cookies sind Datensätze, die von Internetservern auf die Rechner der Nutzerinnen und Nutzer übermittelt werden und dort in einer Datei auf der Festplatte abgelegt werden. Mit Hilfe von Cookies können Informationen über die Verweil-

dauer auf bestimmten Seiten, die Häufigkeit des Seitenaufrufs und dergleichen mehr ermittelt werden. **Cookies** dürfen - soweit sie personenbeziehbare Angaben ermitteln - nur mit **Einwilligung** der Nutzerinnen und Nutzer gesetzt werden. Nach **§ 3 Abs. 5 Satz 1 TDDSG, § 12 Abs. 6 Satz 1 MDStV** sind die Nutzerinnen und Nutzer vor Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten zu unterrichten. Da bei Cookies die Verarbeitung personenbezogener Daten erst zu einem späteren Zeitpunkt als dem ersten Aufruf der Seite erfolgt, verlangt **§ 3 Abs. 5 Satz 2 TDDSG**, dass die Nutzerinnen und Nutzer vor Beginn des automatisierten Verfahrens, welches eine spätere Identifizierung der Nutzerin und des Nutzers ermöglicht und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereitet, zu informieren sind.

Die Information zählt ebenso wie der Hinweis auf das jederzeitige Widerrufsrecht zu den notwendigen Voraussetzungen einer ausdrücklichen Willenserklärung, die unter Einhaltung der in § 3 Abs. 7 TDDSG normierten Anforderungen auch elektronisch abgegeben werden kann. Dafür bedarf es faktisch der Verwendung einer digitalen Signatur. Die Vollzugsdefizite in diesem Bereich sind jedoch unübersehbar. Nicht nur beim Setzen von Cookies, sondern auch in vielen anderen Fällen sind die Handlungsoptionen der Nutzerinnen und Nutzer darauf beschränkt, durch einen bloßen Mausclick die Anwendung zu akzeptieren oder abzulehnen.

Angesichts dieser Netzrealität ist es einerseits bedenklich, wenn der Entwurf zur Neuregelung des Teledienstedatenschutzgesetzes die Verwendung digitaler Signaturen nicht mehr als Bestandteil einer wirksamen elektronischen Einwilligung vorsieht. Andererseits könnte es aber unter dem Blickwinkel des unkomplizierten Abschlusses geringfügiger Rechtsgeschäfte möglicherweise unverhältnismäßig sein, dafür jeweils die Verwendung digitaler Signaturen zu verlangen. Es darf auch nicht aus dem Blick verloren werden, dass die digitale Signatur im Offline-Leben verglichen werden kann etwa mit der Vorlage des Personalausweises. Die zwei Anliegen, Datensicherheit zu gewährleisten und zugleich Datenvermeidung anzustreben, geraten damit in ein Spannungsverhältnis, das einer differenzierten Lösung bedürfte.

Auch **Programme** wie Active-X, JavaScript oder Plug-Ins können ebenso wie Cookies eine Nutzeridentifikation ermöglichen. Hier gelten ebenfalls die bereits im Zusammenhang mit Cookies beschriebenen Anforderungen. Die genannten **Programme stellen zusätzlich eine große Sicherheitsgefahr** dar, da sie den Nutzerrechner bei unzureichender Sicherheitseinstellung ausspähen können. Sie können beispielsweise Speicherinhalte lesen und Kreditkartennummern oder Passwörter ausforschen. Des weiteren kön-

nen diese Programme Viren enthalten und sie auf dem Nutzerrechner ablegen.

Transparenz durch Datenschutzpolicies

Wer es mit dem Respekt vor dem Selbstbestimmungsrecht der Nutzerinnen und Nutzer ernst meint, sollte darüber hinaus Datenschutzhinweise, auch bekannt als Datenschutzpolicies, auf dem Webportal plazieren. Damit wird offengelegt, wie mit automatisch anfallenden Daten - den Spuren im Netz – umgegangen wird und ob überhaupt Cookies oder aktive Inhalte verwendet werden. Sollen personenbezogene Daten erhoben werden, ist das nur aufgrund einer dies ausdrücklich erlaubenden Rechtsvorschrift zulässig, oder wenn eine wirksam erteilte Einwilligung vorliegt. Auch wenn keine personenbezogenen Daten direkt bei den Nutzerinnen und Nutzern erhoben werden, wird bei jeder Internetnutzung auf dem Portal zwangsläufig die IP-Adresse der Kommunikationsverbindung bekannt. Zwar ist es nicht so, dass diese Adresse immer personenbeziehbar ist, da im Regelfall Nutzerinnen und Nutzern über Accessprovider dynamische IP-Adressen zugeordnet werden. Aus Gründen der Transparenz empfiehlt es sich jedoch, darauf hinzuweisen, in welcher Form welche Datensätze gespeichert werden. Und schließlich rundet der Hinweis, dass auf Cookies und aktive Programme verzichtet wird, die Datenschutzpolicy ab.

Inhalt einer Datenschutzpolicy:
Mit dem Zugriff auf die Web-Site werden die um die letzte Stelle der letzten Zahl verkürzte IP-Adresse und weitere Angaben (Datum, Uhrzeit, letzte betrachtete Seite) auf dem Internetserver zu Zwecken der Datensicherheit und statistischen Zwecken für eine bestimmte Zeit (Angabe der Zeitdauer) gespeichert. Durch die Verkürzung der IP-Adresse ist ein Bezug der gespeicherten Daten zu Ihnen ausgeschlossen.
Auf die Verwendung von Cookies und aktive Inhalte wird verzichtet.

Individuelle Informationspflichten - elektronische Auskunft

Das Recht, wissen zu können, wer was über die eigene Person weiß, hat auch im Internet seinen Niederschlag gefunden. **§ 7 TDDSG** und **§ 16 Abs. 1 MDStV** normieren das Auskunftsrecht jeder Nutzerin und jedes Nutzers über die zur eigenen Person oder auch zum Pseudonym gespeicherten Daten. Die Einsichtnahme hat unentgeltlich zu erfolgen und ist auf Wunsch auch elektronisch zu erteilen.

2.1.4 Beispiele aus der Internetpraxis

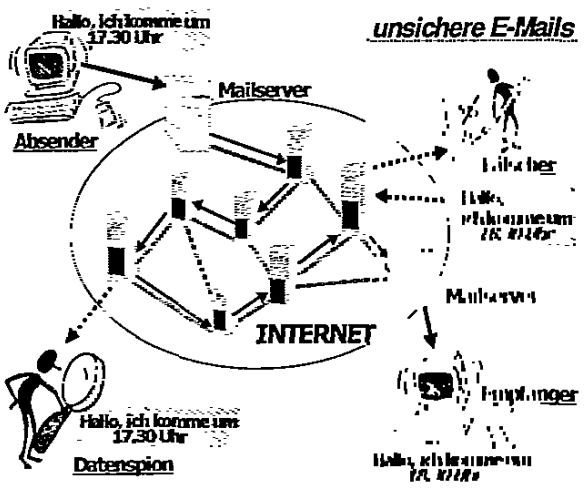
2.1.4.1 E-Mails

Elektronische Post, oder auch E-Mails, werden von immer mehr Menschen genutzt. Ob privat oder geschäftlich, E-Mails sind schnell geschrieben und auch schnell versandt. E-Mails sind aber unsicher. Zu den Risiken, Gefahren und Schutzmöglichkeiten sogleich mehr. Nicht alles was machbar ist, ist allerdings erlaubt. Deshalb nach den Risiken, Gefahren und technischen Schutzmöglichkeiten von E-Mails einige rechtliche Aspekte zum Thema E-Mail.

Risiken, Gefahren und Schutzmöglichkeiten
Ist man sich bei der Postkarte noch bewusst, dass zumindest die Briefträgerin die Urlaubsgrüße lesen kann, sind die Risiken bei E-Mails viel höher. E-Mails müssen auf ihrem Weg durch das weltweite Internet viele Stationen passieren, an denen sie abgefangen, mitgelesen oder auch verändert werden können. Außerdem kann niemand sicher sein, dass eine E-Mail von derjenigen Person stammt, deren Name und E-Mail-Adresse vom Mailprogramm angezeigt wird.

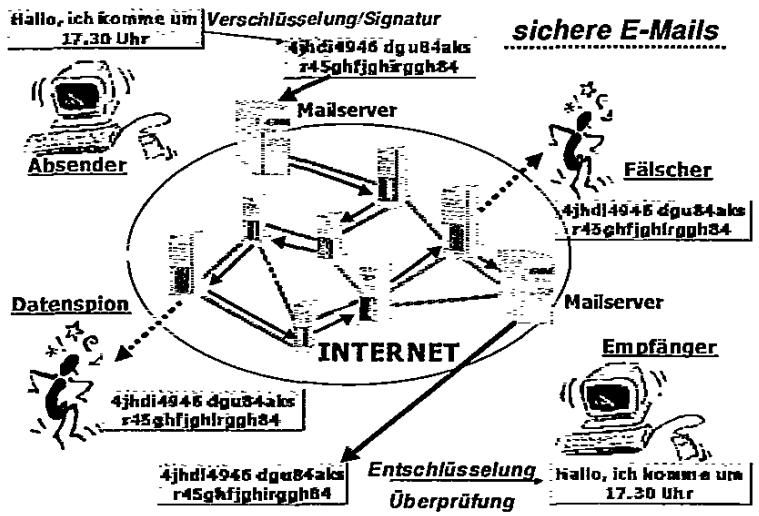
Es gibt aber Möglichkeiten, sich mit einfachen Mitteln vor solchen Risiken zu schützen. Um E-Mails vertraulich zu machen, sollten sie verschlüsselt werden. Nur so kann verhindert werden, dass sie von Unbefugten gelesen werden. Wird eine E-Mail zusätzlich mit einer elektronischen Signatur unterschrieben, kann man sicher sein, dass sie auch wirklich von der Absenderin oder dem Absender stammt und unverändert eingegangen ist.

Um sich der **Gefahren** beim **Versand von E-Mails** bewusst zu werden, muss man sich vergegenwärtigen, dass E-Mails selbst nur Textdaten enthalten, die mit unterschiedlichen Texteditoren erstellt und gelesen werden können. Soll eine Datei - zum Beispiel ein Word-Dokument oder ein Bild - verschickt werden, wird diese an die E-Mail angehängt (Attachment/ Anhang). Weiter erhält man üblicherweise keine Bestätigung, dass eine E-Mail angekommen ist oder gelesen wurde.



Auf ihrem Übertragungsweg durchläuft eine E-Mail verschiedene Computer des Internet, die in der Regel unterschiedlichen Betreibern (beispielsweise AOL, T-Online, Compuserve) zuzuordnen sind. Eine Kopie der E-Mail bleibt übrigens auf jedem der verschiedenen Server, die sie durchlaufen hat, so lange gespeichert, bis sie mangels Speicherplatz durch andere Nachrichten überschrieben werden muss. Damit existieren von einer E-Mail eine Vielzahl von Kopien auf den Servern des Internet. Durch diese Zwischenspeicherung der E-Mails auf den verschiedenen Servern, ist es leicht möglich, dass sie auch von Unbefugten gelesen werden. Dies können alle, die entsprechende Zugriffsrechte besitzen oder denen es gelingt, sie sich zu verschaffen.

Neben dem Mitlesen von E-Mails auf Mailservern ist die Vertraulichkeit der Nachrichten durch die systematische Überwachung von Übertragungswegen zwischen den am E-Mail Versand beteiligten Computern gefährdet. Nach einer Studie einer Arbeitsgruppe des Europäischen Parlaments (STOA) überwacht das staatliche US-System ECHELON systematisch weltweit alle E-Mail Verbindungen, durchsucht die E-Mails mit Verfahren der künstlichen Intelligenz nach bestimmten Schlüsselwörtern und führt interessant erscheinende E-Mails weiteren Auswertungen zu. Neben solchen, mit großem technischen Aufwand betriebenen Abhörsystemen werden E-Mails auch aus ökonomischen Gründen mitgelesen: E-Mails machen Wirtschaftsspionage furchtbar einfach. Sensible oder vertrauliche Geschäftsinformationen können ganz schnell bei der Konkurrenz landen, wenn sie ungeschützt übermittelt werden. Experten schätzen die Schäden durch das illegale Ausspähen, Manipulieren oder Zerstören von Daten jährlich in Milliardenhöhe. Wer eine E-Mail erhält, kann nicht sicher sein, dass der Inhalt der E-Mail unverfälscht eingegangen ist. Wer die Möglichkeit hat, fremde E-Mails auf den Servern zu lesen, ist auch in der Lage, die Inhalte der E-Mails zu verändern.



Aber nicht nur der Text einer E-Mail kann verfälscht werden. Viel leichter ist die **Fälschung der Absenderangaben.** Der Absender, den das Mailprogramm zu einer eingegangenen E-Mail anzeigt, muss nicht der wirkliche Absender sein. Wird eine E-Mail verschickt, sendet das Mailprogramm

automatisch einen Namen und eine E-Mail-Adresse als Absender mit. Diese Angaben müssen von den Benutzerinnen und Benutzern des Programms in den Konfigurationsdaten eingetragen werden. Welcher Name und welche E-Mail-Adresse eingetragen ist, ist dem Programm völlig egal, und kann auch jederzeit wieder geändert werden. Auch durch eine Überprüfung des Übertragungsweges auf die angegebene Adresse des ersten sendenden Mailservers und der Absenderangabe in der E-Mail gibt es hier keine Sicherheit. Mit einem einfachen Terminalprogramm ist es möglich, einen beliebigen Mailserver im Internet zu veranlassen, eine E-Mail auf die Reise zum Empfänger zu schicken. Dieser E-Mail kann zudem eine beliebige E-Mail-Adresse als Absenderkennung mitgegeben werden. Um E-Mail Fälschungen vorzubeugen, gibt es nur das Mittel der digitalen Signatur. Sie stellt sicher, dass eine E-Mail ihrer Urheberin oder ihrem Urheber zugeordnet werden kann. Unabhängig von den manipulierbaren Absenderangaben kann geprüft werden, wer die E-Mail wirklich aufgegeben hat. Gleichzeitig kann mit der Signaturprüfung festgestellt werden, ob der Inhalt der E-Mail unverändert angekommen ist. Ein weiteres Problem ist das unerkannte Löschen oder der Verlust von E-Mails. Man kann sich nicht darauf verlassen, dass eine E-Mail wirklich den Empfänger erreicht - sie könnte irgendwo im Internet aufgrund technischer Probleme bei der Übertragung oder aufgrund eines Hackerangriffs auf einen Mailserver verschollen gehen. Sie könnte aber auch von jemandem absichtlich auf einem Mailserver gelöscht werden. Fälle nicht angekommener E-Mails gibt es immer wieder. Gegen solche Gefahren hilft auch eine Verschlüsselung oder digitale Signatur nicht weiter. Es kann aber beispielsweise vereinbart werden, dass innerhalb einer gewissen Zeitspanne eine kurze "Quittungs-E-Mail" gesandt wird, in welcher der Empfang der E-Mail bestätigt wird. Um sicher zu sein, sollte diese Nachricht auch signiert sein.

Risiken von E-Mails	**Schutzmöglichkeiten**
Mitlesen durch Unbefugte	Verschlüsselung
Verfälschung von Inhalt oder Absender	Digitale Signatur
Löschen oder Verlust	Quittungsverfahren
Viren und Trojanische Pferde	Anti-Virenprogramme

Viren und Trojanische Pferde sind auch bei der E-Mail Kommunikation eine Gefahr. Sowohl bei Viren als auch bei Trojanischen Pferden handelt es sich um ausführbare Programmcodes. Sie können nur aktiviert werden und damit ihre Schadensfunktionen entfalten, wenn sie in ein Programm eingebettet sind. Anders sieht dies bei einer besonderen Virenart aus, den so genannten

Makro-Viren. Makro-Viren können sich in normalen Dateien befinden, wie in einer Textdatei, die mit einem Textverarbeitungsprogramm erstellt wurde oder in einer Tabelle, die von einem Tabellenkalkulationsprogramm stammt.

Um sich vor Viren und Trojanischen Pferden zu schützen, sollten alle Attachments, die als Anhänge einer Mail mitgeschickt werden, unbedingt vor dem Öffnen mit einem Anti-Virenprogramm überprüft werden. Erst wenn das Anti-Virenprogramm keine Viren oder Trojanische Pferde gefunden hat, sollte das in einem Attachment mitgesandte Programm auf dem Computer gestartet oder die Datei geöffnet werden. Attachments von Unbekannten sollten gleich gelöscht werden. Hierdurch ist auch ein Schutz vor so genannten Mail-Bomben möglich. Dies sind Attachments, die beim Öffnen eine Unmenge von Unterverzeichnissen erzeugen oder sehr viel Festplattenplatz beanspruchen. Mail-Bomben werden von Anti-Virenprogrammen nicht erkannt. Erhält man ein verschlüsseltes Attachment, muss dies vor der Virenprüfung zunächst entschlüsselt werden. Ansonsten kann das Anti-Virenprogramm nichts finden.

Soviel zu den Risiken, Gefahren und Schutzmöglichkeiten. Da nicht alles, was möglich ist, auch erlaubt ist, nun einige rechtliche Aspekte zum Thema E-Mail.

Rechtliche Aspekte

Die Kommunikation per E-Mail wirft auch etliche Rechtsfragen auf. Welche rechtlichen Vorgaben im Einzelnen im Zusammenhang mit E-Mails zu beachten sind, lässt sich nicht allgemein beantworten, sondern ist davon abhängig, ob es sich um **Pflichten einer Mailboxbetreiberin**, um etwaige Pflichten der Empfängerin oder des Empfängers einer E-Mail - zum Beispiel **eines E-Commerce-Unternehmens** - oder um die Frage handelt, inwieweit auch **Arbeitgeber** etwa gegenüber ihren Arbeitnehmerinnen und Arbeitnehmern zur Beachtung des prinzipiell geltenden Fernmeldegeheimnisses verpflichtet sind.

Pflichten der Mailboxbetreiberin

Welche rechtlichen Pflichten treffen eine Mailboxbetreiberin? Die **Mailboxbetreiberin** ist Diensteanbieterin im Sinne des **Teledienstegesetzes**, denn es handelt sich um ein Angebot im Bereich der Individualkommunikation nach **§ 2 Abs. 2 Nr. 1 TDG.** Das bedeutet, dass die Mailboxbetreiberin als Teleddiensteanbieterin vor allem die bei den Providern (siehe unter 2.1.4.2) beschriebenen Pflichten zu beachten hat.

Personenbezogene Daten dürfen nach § 3 Abs. 1 TDDSG zur Durchführung von Telediensten nur erhoben, verarbeitet und genutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder die Nutzerinnen und Nutzer eingewilligt haben. Das bedeutet, dass beispielsweise **keine Profile** etwa über die Häufigkeit der Inanspruchnahme der Nutzung des Dienstes gebildet werden dürfen. Ob und **wie lange** Mailboxbetreiberinnen ihre vertraglich angebotene Leistung - zur Verfügung stellen von Mailboxen mitsamt der darin enthaltenen E-Mails - vorzuhalten haben und damit personenbezogene Daten ihrer Kundinnen und Kunden speichern dürfen, richtet sich nach dem zu Grunde liegenden **Vertragsverhältnis.** Darüber hinaus muss die Mailboxbetreiberin das in Art. 10 Grundgesetz und § 85 Abs. 1 Telekommunikationsgesetz (TKG) normierte **Fernmeldegeheimnis** beachten. Zwar handelt es sich bei E-Mail um einen Teledienst; das Fernmeldegeheimnis gilt aber auch für die Anbieterinnen von Telediensten. Sowohl das Teledienstegesetz als auch das Teledienstedatenschutzgesetz enthalten an mehreren Stellen Hinweise auf das Fernmeldegeheimnis (§ 5 Abs. 4 TDG; § 6 Abs. 4 Satz 2 TDDSG) und gehen damit von der Geltung des Fernmeldegeheimnisses aus. Mailboxbetreiberinnen dürfen daher außerhalb der gesetzlich normierten Eingriffsbefugnisse **weder sich noch anderen** über das für die Erbringung des Dienstes erforderliche Maß hinaus **Kenntnis vom Inhalt oder den näheren Umständen der Versendung einer E-Mail verschaffen.**

Verpflichtungen der Nutzerinnen und Nutzer

Treffen auch die Empfängerin einer E-Mail datenschutzrechtliche Pflichten, sofern es sich beispielsweise um ein **Unternehmen** handelt? Für die Frage, ob und wie lange eine Firma die mittels E-Mail transportierten Informationen etwa im Postkorb speichern darf, gilt nichts anderes als für das Medium Papier. Die Empfängerinnen einer E-Mail sind nicht Anbieterinnen des Informations- und Kommunikationsdienstes E-Mail, da sie den Teledienst nicht zur Nutzung bereit halten, sondern **selber Nutzerinnen** sind. Die Speicherung von personenbezogenen Daten durch ein E-Commerce-Unternehmen, bei dem **mittels E-Mail Waren bestellt** werden können, wäre also etwa nach **§ 28 Abs. 1 Nr. 1 BDSG** im Rahmen der Zweckbestimmung eines Vertragsverhältnisses zulässig. Nach § 13 DSG NRW können **öffentliche Stellen** personenbezogenen Daten solange speichern, wie es für ihre rechtmäßige Aufgabenerfüllung erforderlich ist.

Reichweite des Fernmeldegeheimnisses am Arbeitsplatz

Dürfen die Vorgesetzten auf E-Mails zugreifen? Die Antwort ist davon abhängig, ob es sich um private oder dienstliche E-Mails handelt. Der Versand und Empfang einer **privaten E-Mail** am Arbeitsplatz wird durch das **Fern-**

meldegeheimnis in § 85 Abs. 1 Telekommunikationsgesetz (TKG) geschützt. Ebenso wie beim Briefgeheimnis darf damit zunächst niemand den privaten E-Mail-Verkehr einfach so - ohne gesetzliche Grundlage - überwachen. Ob der Arbeitgeber die private Nutzung des Internetanschlusses überhaupt gestatten will, obliegt allein ihm. Wird die private Nutzung von E-Mail zugelassen, sollten auf jeden Fall verschiedene E-Mail-Adressen für die dienstliche und die private Post zugewiesen werden.

Dienstliche E-Mail unterliegen gegenüber dem Arbeitgeber ebenso wenig wie die geschäftliche Briefpost **dem Fernmeldegeheimnis.** Nach § 85 Abs. 2 Satz 1 TKG ist zur Wahrung des Fernmeldegeheimnisses verpflichtet, wer geschäftsmäßig Telekommunikationsdienste erbringt. Ein geschäftsmäßiges Erbringen von Telekommunikationsdiensten liegt nach § 3 Nr. 5 TKG aber nur bei dem Angebot von Telekommunikation für Dritte vor. Die Beschäftigten sind im Verhältnis zu ihren Arbeitgebern im Rahmen der dienstlichen E-Mail-Kommunikation nicht als Dritte anzusehen. Im Rahmen ihrer dienstlichen Aufgaben sind sie ja für ihre Arbeitgeber tätig. Wie bei der herkömmlichen Briefpost können Vorgesetzte sich dienstliche E-Mails vorlegen oder sich einen Zugang hierzu einräumen lassen. Zudem dürfen Arbeitgeber aus Sicherheitsgründen ein- und ausgehende E-Mails dienstlicher und privater Natur auf Virenbefall kontrollieren, wenn die Kontrolle automatisch erfolgt.

2.1.4.2 Der Weg ins Internet - Accessproviding

Um das Internet nutzen zu können, benötigt man einen **Zugang.** Ein solcher Internet-Zugang wird von den so genannten Accessprovidern vermittelt. Die Accessprovider sind eine Schnittstelle in der Organisationsstruktur des Internet. Die Accessprovider betreiben einen Internetserver (Point of Presence - POP), der mittels einer festen Datenleitung an das Internet angebunden ist und über den die Nutzerin oder der Nutzer mit Hilfe einer Wählverbindung ins World Wide Web kommt. Diesen Service lassen sich die Provider von den Nutzerinnen und Nutzern bezahlen, entweder über einen festen Vertrag oder Internet by Call. Dabei können personenbezogene Daten anfallen, die von den Providern gespeichert und verarbeitet werden. Die Accessprovider erhalten alle technischen Daten über die Internetnutzung.

Die Accessprovider sind nach **§ 3 Abs. 1 Nr. 1 TDG** Diensteanbieterinnen, da sie den Zugang zur Nutzung von **Telediensten** vermitteln. Sie agieren auf der so genannten Diensteebene, die durch das Teledienstegesetz geregelt wird. Die Diensteebene betrifft alle Handlungen, die mit der Vertragserfüllung verbunden sind, vom Speichern der Kundendaten bis zur Abrechnung.

Grundsätzlich besteht auch hier für die Datenerhebung, -verarbeitung und -nutzung ein Verbot mit Erlaubnisvorbehalt. Daten dürfen also nur dann erhoben werden, wenn die Nutzerin und der Nutzer darin eingewilligt haben oder wenn eine Rechtsvorschrift dies vorsieht. Solche Rechtsvorschriften enthält das **Teledienstedatenschutzgesetz (TDDSG).**

Nach der Übertragung der Zuständigkeit für den Datenschutz auch im nichtöffentlichen Bereich Mitte 2000 konnten erste Erfahrungen mit der Einhaltung des TDDSG durch gewerbliche Provider gemacht werden. Bei einigen Providern fanden Beratungs- und Kontrollbesuche mit im Wesentlichen folgenden Ergebnissen statt:

Verpflichtung zur Datenvermeidung
Provider sind nach den im TDDSG niedergelegten Grundsätzen für die Verarbeitung personenbezogener Daten zur Datenvermeidung verpflichtet. Das bedeutet unter anderem, dass sich nach § 3 Abs. 4 TDDSG schon die Gestaltung und Auswahl technischer Einrichtungen für Teledienste an dem Ziel auszurichten haben, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.

In der Praxis ist festzustellen, dass die Datenvermeidung eng im Zusammenhang mit der technischen Ausgestaltung des Internetzuganges steht. Bietet der Accessprovider auch Telekommunikationsdienste an, so werden Bestands- und Nutzungsdaten meistens nach gleichen Regeln wie die Telefondaten verarbeitet. Neben den Daten, die für den Internetaccess erforderlich sind werden auch die Vermittlungsdaten und die Telefonnummern gespeichert. Accessprovider, die lediglich einen POP betreiben und alle anderen technischen Internet-Anbindungen wie beispielsweise Proxy, E-Mail-Dienst und Web-Hosting durch Drittfirmen vornehmen lassen, kommen dem Prinzip der Datenvermeidung näher. In diesem Fall besitzt der Accessprovider die Bestandsdaten, alle anderen Daten fallen lediglich unter einer Benutzerkennung bei den Drittfirmen an. Der Provider hat somit keine Kenntnis von den IP-Adressen seiner Kundinnen und Kunden und dem gesamten Internet-Traffic. Da jedoch die Drittfirma keinerlei Bestandsdaten hat, kann keine Zusammenführung von Nutzungsdaten und Bestandsdaten zur Auswertung des Internetverhaltens erfolgen.

Zum Prinzip der Datenvermeidung gehört auch, dass die Provider den Nutzerinnen und Nutzern im Rahmen ihrer technischen Möglichkeiten ermöglichen sollen, anonym oder unter Pseudonym ins Internet zu kommen und auch die Bezahlung anonym oder unter Pseudonym durchzuführen, **§ 4 Abs. 1 TDDSG.** Beratungs- und Kontrollbesuche ergaben, dass eine anonyme Nutzung des Internet derzeit wegen des Vertragsverhältnisses zwi-

schen Providern und Nutzenden nicht möglich ist. Denkbar wäre eine anonyme Nutzung des Internet über Prepaid-Karten, wie sie für Mobiltelefone angeboten werden. Eine vollkommen anonyme Nutzung des Internet ist in Internet-Cafes möglich, da man dort ohne Benutzerkennung ins Netz kommt und lediglich die tatsächliche Surfzeit bezahlt. Auch eine pseudonyme Bereitstellung des Internetzuganges ist unter bestimmten technischen Konstellationen durchaus möglich. Wenn jedoch der Accessprovider gleichzeitig Telekommunikationsanbieter ist, dann ist die pseudonyme Inanspruchnahme des Internet nicht ohne weiteres machbar. Eine pseudonyme Bezahlung des Internetzuganges wird von keinem der besuchten Provider angeboten.

Verpflichtung zur Anbieterkennzeichnung
Die Praxis zeigt, dass der Verpflichtung zur Transparenz, die schon unter 2.1.3 dargestellt wurde, zum Teil nur ungenügend Rechnung getragen wird. Die in Nordrhein-Westfalen besuchten Provider haben zwar auf ihren Internetseiten irgendwo ihre Adresse und auch die verantwortlichen Personen angegeben, jedoch nicht immer mit einem eindeutigen Anbieterkennzeichnungsanker versehen. Die vollständigen Daten sind oft in der Rubrik "Unternehmen" und dann in der Unterrubrik "Unternehmensdaten" aufgeführt. Dies allein bedeutet schon, dass die Nutzerinnen und Nutzer nach den gemäß **§ 6 TDDSG** erforderlichen Daten förmlich fahnden müssen. Ein allgemeiner Datenschutzhinweis wird bislang von keinem Accessprovider gegeben. Ebenso wenig wird auf die Verwendung von Skripten und Cookies hingewiesen.

Bestands-, Nutzungs- und Abrechungsdaten
Damit ein Providervertrag zustande kommt, erhebt der Provider die personenbezogenen Daten seiner Kundinnen und Kunden, wie unter anderem Name, Adresse und Bankverbindung. Diese Daten sind **Bestandsdaten**. Sie können nach **§ 5 TDDSG** nur erhoben, verarbeitet und genutzt werden, wenn sie für die Begründung, inhaltliche Ausgestaltung oder Änderung des Vertragsverhältnisses zwischen Nutzerin oder Nutzer und Provider erforderlich sind. Bei Kontrollbesuchen und Kontrollen im Internet ergab sich, dass auch nicht erforderliche Bestandsdaten wie das Geburtsdatum und der Beruf gespeichert wurden. Außerdem ließen sich einige Accessprovider damit, dass auch Bestandsdaten nach Beendigung eines Vertragsverhältnisses zu löschen sind, unzulässigerweise bis zu zwei Jahren Zeit.

Während die Nutzerin oder der Nutzer im Internet verweilt, entstehen zudem **Nutzungsdaten.** Nutzungsdaten sind nach § 6 Abs. 2 Nr. 1 TDDSG frühestmöglich zu löschen, spätestens unmittelbar nach Ende der jeweiligen Nutzung. Nur diejenigen Nutzungsdaten, die für Abrechnungszwecke erforderlich sind, können gespeichert bleiben. Diese Nutzungsdaten werden dann

zu **Abrechnungsdaten**. Auch Abrechnungsdaten sind zu löschen, wenn sie für die Abrechnungszwecke nicht mehr benötigt werden. Nach § 6 Abs. 2 Nr. 2 TDDSG sind Abrechnungsdaten spätestens 80 Tage nach Versendung der Rechnung zu löschen, es sei denn, über die Rechnungsforderung wird gestritten. Es konnte nicht festgestellt werden, dass die 80-Tage-Frist etwa zu kurz wäre. In der Praxis besteht daher offenbar gar kein Bedarf für die - im Gesetzentwurf zur Änderung des Teledienstedatenschutzgesetzes - vorgesehene Ausdehnung der zulässigen Speicherfrist auf sechs Monate. Auch im Hinblick auf den Grundsatz der Datenvermeidung sollte auf eine derart lange Speicherfrist verzichtet werden.

Als Nutzungsdaten erfasst werden beispielsweise die Nutzeridentifikation, die Vermittlungsdauer, das Volumen der übertragenen Daten und ein Identifizierungsmerkmal (beispielsweise die Telefonnummer) für das Einwahlverfahren (Internet by Call oder Festvertrag). Die temporäre IP-Adresse wird aus Gründen der Nachweisbarkeit für Abrechnungszwecke in einer Protokolldatei gespeichert und zyklisch überschrieben. Die Überschreibungszyklen sind bei den Providern unterschiedlich angelegt, im Allgemeinen liegen sie bei drei Monaten nach Nutzung, was in der Regel unterhalb der möglichen Speicherfrist für Abrechnungsdaten von 80 Tagen nach Rechnungslegung liegt.

Nutzungsdaten, die nicht zur Abrechnung dienen, werden beispielsweise dann erfasst, wenn der Internetzugang über einen sicheren Proxyserver realisiert wird. Der Proxyserver ermöglicht eine pseudonyme Bewegung im Internet, da individuelle Nutzungsdaten nicht ins Netz gelangen. Allerdings protokollieren die Provider aus technischen Gründen die IP-Adressen der Nutzerinnen und Nutzer und die von ihnen angewählten IP-Adressen. Auf diesen Proxyservern fällt deshalb eine sehr große Datenmenge an. Bei den besuchten Providern wird die Datei alle drei bis sieben Tage aus Kapazitätsgründen überschrieben. Da diese Daten das genaue Nutzungsverhalten abbilden, ist darauf zu achten, dass die Provider die Speicherdauer auf das Notwendige minimieren.

Ist der Internetzugang unentgeltlich, können keine Abrechnungsdaten entstehen. Die Nutzungsdaten sind daher sofort vollständig zu löschen. Gleiches gilt für so genannte **Flatrates**, also Pauschalverträge zwischen Nutzerinnen und Nutzern und den Providern. Da der Provider ja nicht die Leistung abzurechnen braucht, ist auch eine Speicherung der Nutzungsdaten nicht erforderlich. In der Praxis werden allerdings sehr wohl auch bei Flatrateverträgen Nutzungsdaten wie etwa die Verweildauer und die Datenmenge gespeichert. Einige Provider führen ein so genanntes Monitoring durch, um die Wirtschaftlichkeit ihrer Flatrateangebote zu überprüfen. Ein Monitoring des

Nutzungsverhaltens bei einem Flatratevertrag ist jedoch nur mit vorheriger Einwilligung der Nutzerin oder des Nutzers möglich.

Verpflichtung zur Unterrichtung
Vor Erhebung von Bestands-, Nutzungs- und Abrechnungsdaten hat der Provider die Nutzerinnen und Nutzer über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung zu unterrichten, **§ 3 Abs. 5 TDDSG.** Der Entwurf zur Änderung des sich in der **Evaluation befindlichen TDDSG** sieht nun vor, dass nur noch über den Ort der Datenverarbeitung informiert werden muss, wenn die Datenverarbeitung in einem Drittstaat außerhalb der europäischen Union stattfindet. Die Unterrichtung muss jederzeit abrufbar sein und ist zu protokollieren. Auf die Unterrichtung kann verzichtet werden, der Verzicht muss jedoch ebenfalls protokolliert werden. Der Änderungsentwurf zum TDDSG sieht einen Ordnungswidrigkeitentatbestand für die nicht richtige, vollständige oder rechtzeitige Unterrichtung der Nutzerinnen und Nutzer vor. Zurzeit werden die gesetzlichen Vorgaben für die ausführliche Unterrichtung leider so gut wie nicht eingehalten. Die meisten Provider beschränken sich auf einen kurzen, unzureichenden Hinweis in ihren Allgemeinen Geschäftsbedingungen, dass die gesetzlichen Bestimmungen zum Datenschutz beachtet werden.

Bieten Provider eine Anmeldung zu ihrem Dienst über das Netz an, sollten sie nicht nur ebenfalls im Netz die für die Unterrichtung erforderlichen Angaben vorhalten, sondern sich deren Kenntnisnahme auch mit der Anmeldung bestätigen lassen.

Verpflichtung zur Auskunft
Die kontrollierten Accessprovider bieten alle eine schriftliche Auskunft über die zur eigenen Person oder zum eigenen Pseudonym gespeicherten Daten an. Manche bieten den besonderen Service der Online-Kontenabfrage an, wobei sich die Kundinnen und Kunden mit ihrer Registriernummer authentisieren müssen, um an die gewünschten Informationen zu kommen. Keiner der kontrollierten Provider bietet eine Auskunft via E-Mail an.

Resümee
Die Kontrollbesuche ergaben, dass die Provider das seit 1997 bestehende Informations- und Kommunikationsdienstegesetz, insbesondere das Teledienstegesetz und das Teledienstedatenschutzgesetz - zum Teil aus Unkenntnis - nicht im erforderlichen Maße einhalten. Die Vollzugsdefizite bestehen vor allem bei dem Transparenzgebot, der Unterrichtungspflicht und den Löschungfristen der Daten.

2.1.4.3 Interaktive Verwaltung

Neben den allgemeinen Informationsangeboten und der Bereitstellung von Antragsunterlagen im Internet wollen die Verwaltungen zunehmend auch interaktive Kommunikation mit den Bürgerinnen und Bürgern im Internet etwa in Form von elektronisch ausfüllbaren Formularen anbieten. Aufbauend auf den Ausführungen im 14. Datenschutzbericht 1999 zu "Homepages öffentlicher Stellen" (2.4.3.6) und "Antragstellung per Mausclick" (2.4.3.7) sind bei der Gestaltung solcher interaktiver Angebote unter anderem folgende Gesichtspunkte zu berücksichtigen :

Müssen die **Verwaltungen Verschlüsselungsverfahren** anbieten?
Anders als bei der Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem Informations- und Kommunikationsdienst E-Mail sind die Verwaltungen Diensteanbieterinnen, wenn sie die Bürgerinnen und Bürger zu einer internetbasierten Kommunikation etwa im Rahmen einer Homepage einladen. Nach **§ 4 Abs. 2 Nr. 3 TDDSG** hat die Diensteanbieterin durch technische und organisatorische Vorkehrungen sicherzustellen, dass Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch genommen werden können. Für die Bürgerinnen und Bürger muss also die Möglichkeit - nicht die Verpflichtung - bestehen, sich durch technische Maßnahmen gegen unbefugte Kenntnisnahme und Verfälschung ihrer Kommunikation zu schützen. Die abstrakte Verpflichtung nach § 4 Abs. 2 Nr. 3 TDDSG regelt allerdings nicht, welcher Art die Anforderungen an die Verfahren zur Gewährleistung vertraulicher Kommunikation zu sein haben. Praktisch bedeutet das jedoch, dass die Verwaltungen Verschlüsselungsverfahren anzubieten haben. Ein Warnhinweis auf die Risiken unverschlüsselter Datenübertragung - wie ihn manche Verwaltungen verwenden - ist zwar ein erster Schritt, genügt aber nicht. Einen wirksamen Schutz, wie er als technische oder organisatorische Maßnahme von den Diensteanbieterinnen nach dem Teledienstedatenschutzgesetz gefordert ist, stellt der Warnhinweis nämlich nicht dar, weil er keine vor der Kenntnisnahme Dritter geschützte Kommunikation sicherstellen kann. Die Auswahl des konkreten Verschlüsselungsverfahrens richtet sich nach den allgemeinen Datenschutzgrundsätzen. Danach hat die Verwaltung diejenigen Verschlüsselungsverfahren anzubieten oder zu verwenden, die erforderlich sind, um die Vertraulichkeit zu gewährleisten.

Ist der Einsatz von **Signierverfahren erforderlich**?
Zum Schutz von Authentizität und Integrität der Kommunikation ist der Einsatz von Signierverfahren zu empfehlen. Nach § 10 Abs. 2 Nr. 2 und 4 Datenschutzgesetz Nordrhein-Westfalen sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass personenbezogene Daten während der

Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität) und jederzeit ihrem Ursprung zugeordnet werden können (Authentizität). Eine technische Maßnahme zur Umsetzung dieser Verpflichtung kann der Einsatz von Signierverfahren sein. Manchmal erweist sich die Verwendung von Signierverfahren auch aus anderen Erwägungen als sinnvoll. Die Signatur eines Dokumentes als obligatorische Voraussetzung etwa für eine elektronische Bestellung der Sperrmüllabfuhr kann notwendig sein, um die Identität der Betroffenen zweifelsfrei sicherzustellen und einer Verbreitung unrichtiger Daten über die Betroffenen, wie etwa bei scherzhaften Massenbestellungen unter einem falschen Namen vorzubeugen. Zwar ist dies auch derzeit per Telefon möglich. Die unsichere Identifizierung der anrufenden Person ist jedoch auch der angerufenen Person bekannt. Demgegenüber lässt sich im Internet der tausendfache Versand einer E-Mail unter einer Scheinidentität mit wenigen Mausclicks initiieren.

Welche technischen und organisatorischen Maßnahmen sind für die Ausgestaltung des Verfahrens denkbar? Die nachfolgende Tabelle soll einer ersten Orientierung über den Umfang der erforderlichen technischen und organisatorischen Maßnahmen dienen. Sie weist auf den Zusammenhang hin, der je nach der konkreten Datenverarbeitungssituation im aktuellen Verwendungszusammenhang entsprechend der unterschiedlichen Sensitivität der Daten unterschiedliche technische und organisatorische Maßnahmen fordert. Die Anwendung der Tabelle darf nicht schematisch erfolgen.

Kategorien personenbezogene Daten	Technische und organisatorische Maßnahmen	Technische Umsetzung
Kategorie 1: Personenbezogene Daten oder Verwendungszusammenhänge, die wegen ihrer Sensitivität in dem konkreten Datenverarbeitungszusammenhang einen besonderen Datenschutz erfahren müssen. Dieses Schutzniveau ist i. d. R. insbesondere bei Berufs- und Amtsgeheimnissen (z.B. Sozialdaten) und bei personenbezogenen Daten, die nach Art. 8 der EG-Datenschutzrichtlinie als besondere Kategorie eingestuft worden sind (z.B. Daten über die Gesundheit) zu fordern. Ferner personenbezogene Daten oder Verwendungszusammenhänge, deren Missbrauch zu einer Beeinträchtigung von weiteren Grundrechten oder in der Folge zu sonstigen besonders schwerwiegenden Nachteilen führen kann.	Es ist sicher zu stellen, dass nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können (Wahrung der Vertraulichkeit). Erforderlich sind außerdem Maßnahmen, die geeignet sind, dass personenbezogene Daten während der Verarbeitung unversehrt und vollständig bleiben (Integrität) sowie jederzeit ihrem Ursprung zugeordnet werden können (Authentizität).	Die Kommunikationspartnerinnen und Kommunikationspartner müssen eine hinreichende Verschlüsselung der Daten vornehmen und eine digitale Signatur einsetzen, die auf dem Signaturgesetz i.V.m. der Signaturverordnung basiert.
Kategorie 2: Personenbezogene Daten, deren Missbrauch in ihrem Verwendungszusammenhang geeignet ist, die Betroffenen in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen nicht besonders gewichtig zu beeinträchtigen.	Es sind grundsätzlich die gleichen Maßnahmen wie in Kategorie 1 erforderlich. Allerdings sind an die Ausgestaltung der Sicherungsinfrastruktur keine besonderen (über einen geregelten RZ-Betrieb hinausgehenden) Anforderungen zu stellen. Betroffene und öffentliche Stellen können Zertifikate oder vergleichbare Authentifizierungsmaßnahmen nach eigenen festgesetzten Regeln verwenden.	Eine Umsetzungsmöglichkeit besteht darin, allgemein verbreitete Verschlüsselungs- und Signatursoftware einzusetzen. Notwendige Voraussetzung für einen vertrauenswürdigen Umgang mit einem derartigen Produkt ist die Einrichtung von Zertifizierungsstellen, bei denen die Bürgerinnen und Bürger ihren öffentlichen Schlüssel hinterlegen und digital bestätigen, also zertifizieren lassen können.
Kategorie 3: Personenbezogene Daten, die den Kategorien 1 und 2 nicht zugeordnet werden können.	Es sind Schutzmaßnahmen zu treffen, die einen sicheren Übertragungskanal zwischen den beteiligten Endsystemen mit ausreichender Verschlüsselung ermöglichen. Zusätzliche Maßnahmen sind dann erforderlich, wenn der Verwendungszusammenhang dies erfordert.	Eine Möglichkeit der Kommunikation öffentlicher Stellen mit Bürgerinnen und Bürgern über einen „sicheren Kanal" besteht darin, Secure Socket Layer einzusetzen. Secure Socket Layer (SSL) legt, wie der Name andeutet, eine zusätzliche Schicht zwischen die Transport-Ebene TCP/IP und die Anwendungsebene (HTTP, Telnet, FTP,...) einer Datenübertragung. Von "oben" gesehen ist sie transparent, d.h. die Anwendungsprogramme können ohne große Modifikation auf eine sichere Übertragung zugreifen.

Die Einordnung der einzelnen Daten hängt entscheidend von dem Sachzusammenhang ab, in dem diese Daten verarbeitet werden. Wegen der Kontextabhängigkeit der Sensitivität von Daten müssen besondere Risiken individuell berücksichtigt werden. Sind die Daten eines Datensatzes unterschiedlichen Stufen zuzuordnen, so sind jeweils für den genannten Datensatz die Anforderungen der höchsten Stufe für das einzelne Datum zu wählen. Ebenso wenig darf die Tabelle genutzt werden, um sich der Verpflichtung zu entziehen, ein ausreichendes Sicherheitskonzept zu erstellen.

Leider wurden die **beschriebenen Standards** in der **Praxis nicht immer umgesetzt.** Einige öffentliche Stellen sind erste Schritte in Richtung interaktiver Verwaltung mit ersten Anwendungsbeispielen gegangen – Meldung einer Fundsache, Antrag auf Erteilung eines Anwohnerparkausweises, Anmeldung eines Kindes zum Kindergarten. Teilweise wurden solche Anwendungen realisiert, **ohne** dass sichergestellt wurde, dass die Bürgerinnen und Bürger Kommunikation **gegen Kenntnisnahme Dritter geschützt** in Anspruch nehmen können.

Auch die in unterschiedlichen Planungs- und Entwicklungsstufen befindlichen "gläsernen Rathäuser" und "virtuellen Verwaltungen" werden sich im Interesse der Bürgerinnen und Bürger, nicht zuletzt aber auch im eigenen Interesse Datenschutz- und Datensicherheitsmaßnahmen überlegen müssen. Erste Hinweise für eine datenschutzgerechte Gestaltung derartiger Vorhaben finden sich in der Broschüre "Vom Bürgerbüro zum Internet", die im Berichtszeitraum von einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder unter Federführung von Nordrhein-Westfalen erarbeitet wurde. Die Broschüre ist in Papierform erhältlich, kann aber auch unter www.lfd.nrw.de auf- und abgerufen werden.

Eine Bezirksregierung nahm im Berichtszeitraum eine Online-Antragstellung für Bewerbungen im Lehrereinstellungsverfahren in Angriff: Mit Hilfe des Webbrowsers und eines Moduls "Multiweb" können die Bewerberinnen und Bewerber einen Teil der Daten selbst eingeben und in verbindlicher Form einreichen. Als Zertifizierungsdiensteanbieterin fungiert das Landesrechenzentrum. Die von uns beschriebenen Standards - Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Authentizität einer elektronischen Information - wurden hier erstmals komplett in die Praxis umgesetzt.

2.1.4.4 Die Nutzung von Internetdiensten auf Systemen zur Verarbeitung von Patientendaten - ein erhebliches Risiko für Datenschutz und Datensicherheit

Auch im Gesundheitswesen wächst verständlicherweise der Wunsch, das vielfältige Informationsangebot des Internet zu nutzen. Das Internet wurde allerdings als offenes System entwickelt, Sicherheitsüberlegungen spielten dabei keine oder nur eine untergeordnete Rolle. Patientendaten verarbeitende Systeme hingegen unterliegen aber wegen der Sensibilität der Daten einem hohen Schutzbedarf und sind aus diesem Grunde als geschlossene Systeme angelegt. Mit der Öffnung medizinischer Systeme gegenüber dem Internet geht zwangsläufig eine Öffnung gegenüber den mit der Internettechnologie inhärent verbundenen Sicherheitsrisiken einher.

Den geläufigen Gefahren bei der Nutzung des Internet, wie der offenen Übertragung von Daten und Angriffen von Hackern, kann durch Datenverschlüsselung und Einrichtung von Firewallsystemen begegnet werden. Diese Schutzmechanismen sind bereits im 14. Datenschutzbericht 1999 unter 2.2.2 und 2.3 ausführlich dargestellt worden. Es gibt aber Bedrohungen, die meist unterschätzt werden und geeignet sind, selbst die Schutzmechanismen von Firewallsystemen zu unterlaufen oder von diesen gar nicht abgefangen werden können. Hierin liegt eine oft unterschätzte Gefahr für Patientendaten verarbeitende Systeme. Die Ursache für diese Bedrohungen ist darin begründet, dass die Informationen im Internet nicht in Form von reinen Texten vorliegen, sondern in Formaten, die gerade die Multimediafähigkeit des Internet ermöglichen. Auf diese Problematik soll im Folgenden näher eingegangen werden. Dabei werden für die wichtigsten Internetdienste die spezifischen Risiken betrachtet.

Risiken der Internet-Dienste

➢ **Der WWW-Dienst:**

Der WWW-Dienst ist ein Informationsdienst des Internet, der auf der Hypertext-Technologie basiert. Diese ermöglicht die Verknüpfung von Informationen durch so genannte Hyperlinks. WWW-Seiten werden definiert in HTML (Hypertext-Markup-Language) und mittels des HTTP-Protokolls (Hypertext-Transfer-Protokoll) zwischen Client und Server übertragen. Die Darstellung von WWW-Seiten auf dem Client erfolgt durch so genannte Browser.

Die ursprünglichen Möglichkeiten von HTML waren ziemlich eingeschränkt. Durch die Einführung von so genannten aktiven Inhalten wurde HTML zu einem flexibleren Instrument, das eine dynamische und benutzer-

orientierte Präsentation von Informationen bietet. Aktive Inhalte sind Programmcodes, die auf den Client-Systemen zum Ablauf gebracht werden und eine nahezu unbegrenzte Funktionsvielfalt bieten. Genau darin liegt aber das Sicherheitsproblem. Wenn aktive Inhalte den Zugriff auf die Ressourcen des Client-Systems haben, entstehen Risiken für die Vertraulichkeit, Integrität und Verfügbarkeit der dort gespeicherten und verarbeiteten Daten.

Im Wesentlichen sind die folgenden Formen aktiver Inhalte von Bedeutung:

ActiveX

ActiveX steht für eine Reihe von Technologien, die es ermöglichen, WWW-Seiten um eine Vielzahl von multimedialen Effekten, unterschiedlichen Layouts und ausführbaren Applikationen, die über das Internet geladen werden, zu erweitern. Die folgenden ActiveX-Komponenten sind dabei relevant:

- ActiveX-Controls sind kleine Programme, die in WWW-Seiten eingebunden oder als eigene Programme ausgeführt werden können.
- ActiveX-Documents ermöglichen die Darstellung von Nicht-HTML-Dokumenten (wie Word und Excel) innerhalb des Browsers.
- ActiveX-Scripting ermöglicht die Integration von Scripts (VBScripts und JScripts) in WWW-Seiten. Scripts sind Programmcodes, die gewisse Interaktionsmöglichkeiten der Nutzerinnen und Nutzer unterstützen.

ActiveX-Komponenten unterliegen keinerlei Einschränkungen auf dem Client-System. Insofern stellen sie ein immenses Sicherheitsrisiko dar.

Folgende Sicherheitsrisiken sind bisher bekannt:

- Ausforschen von Nutzern und Computersystemen: Durch entsprechende ActiveX-Komponenten kann auf beliebige Nutzer- und Systeminformationen zugegriffen werden. Diese Informationen können unbemerkt an Dritte übermittelt werden (zum Beispiel per E-Mail oder Dateitransfer).
- Infektion durch Viren und Trojanische Pferde: ActiveX-Komponenten können beliebige Viren und Trojanische Pferde ins System einschleusen und installieren.
- Beschädigung von Systemressourcen: ActiveX-Komponenten können beliebige Systemressourcen verändern (zum Beispiel Löschen der Festplatte oder Verändern oder Auswerten von bestimmten Daten).

- Überlasten des Systems: ActiveX-Komponenten können durch massiven Verbrauch von Systemressourcen das System überlasten und gegebenenfalls zum Absturz bringen.

JavaScript

JavaScript ist eine Scriptsprache. Sie wird direkt in WWW-Seiten eingebunden und über einen in die Browser integrierten Interpreter ausgeführt. JavaScript wurde in seinem Funktionsumfang restriktiv konzipiert, um Zugriffe auf Ressourcen der Client-Systeme zu verhindern. Die Praxis zeigt aber immer wieder, dass durch Design- und Implementierungsfehler der Browser Sicherheitslücken entstehen.

Hier eine - kleine - Auswahl der in der Vergangenheit entdeckten Sicherheitslücken:

- Ein Fehler in der Browser-Implementierung ermöglichte den Zugriff auf die Festplatten von Client-Systemen. Dabei konnten Festplattenverzeichnisse, der Browser-Cache und die Browser-Konfigurationsdatei ausgelesen werden. Die Konfigurationsdatei enthält häufig die E-Mail-Adresse und das Mail-Passwort. Die ausgelesen Daten konnten an einen beliebigen Server übertragen werden.
- Ebenso war es durch eine Sicherheitslücke möglich Dateiinhalte von Dateien mit bekanntem Pfad von der Festplatte des Client-Systems auszulesen und an einen beliebigen Server im Internet zu übertragen. Dieselbe Lücke erlaubte auch das Auslesen der Verzeichnisstruktur. Auf diese Weise konnte dann der Pfad einer Datei ermittelt werden, deren Inhalt ausgelesen werden sollte.
- Ein weiterer Implementierungsfehler ließ das Auslesen der so genannten Legende des Browsers zu, das heißt die besuchten WWW-Seiten konnten ermittelt und an einen beliebigen Rechner im Netz verschickt werden.
- Eine andere Lücke konnte ausgenutzt werden, um unbemerkt das Client-System zum Senden einer E-Mail zu veranlassen. Dadurch konnten E-Mail-Adressen ausgeforscht werden.

Java

Java ist eine objektorientierte Programmiersprache. Sie bietet die Möglichkeit Anwendungen für das WWW (Java-Applets) zu schreiben. Java-Applets können in HTML-Seiten integriert, über das Internet geladen und auf einem beliebigen Rechner durch die virtuelle Java Maschine ausgeführt werden. Java bietet ein integriertes Sicherheitsmodell, die so genannte Java-

Sandbox. Damit soll sichergestellt werden, dass Java-Applets nur unter einer strengen Sicherheitskontrolle ablaufen. Applets, die über das Internet geladen werden unterliegen damit den folgenden Einschränkungen:

- Das Lesen und Schreiben von Dateien auf dem Client ist nicht möglich.
- Netzwerkverbindungen zu anderen Rechnern sind nicht erlaubt, außer zu dem Rechner, von dem das Applet geladen wurde.
- Das Starten von Programmen auf dem Client ist nicht möglich.
- Ein Aufruf von Systemfunktionen wird verhindert.

Trotz der Sicherheitsmechanismen, die Java bietet, wurden Risiken bekannt, die zurückzuführen sind auf fehlerhafte Implementierungen der komplexen Java-Ablaufumgebung. Hierzu gehörten:

- Angriffe, die das System oder seine Ressourcen modifizierten, mit den Konsequenzen, dass Daten verändert oder gelöscht werden konnten oder das System abstürzte.
- Angriffe, die eine weitere Benutzung des Systems verhinderten, indem Applets massiv Systemressourcen (Speicher, Prozessorzeit) verbrauchten, um das System zu überlasten.
- Angriffe, die spezifische Dateien auf dem Client-System auslesen und sie zu einem Server übermitteln oder eine E-Mail vom Client-System aus verschicken und die Dateien als Attachments anhängen.
- Angriffe, die ein Client-System durch Installation eines Applets zu einem Datei-Server machen, der lokale Dateien an jeden beliebigen als Angreifer fungierenden Rechner im Internet überträgt.

Ebenso ist Java wegen seiner Plattformunabhängigkeit als Implementierungssprache für Viren geradezu prädestiniert. Die Wirksamkeit von Virenangriffen wird zwar durch das Sandbox-Modell in hohem Maße eingeschränkt, dennoch sollten die Gefahren durch Java-Viren keinesfalls als gering eingeschätzt werden. In diesem Zusammenhang ist erwähnenswert, dass es Experten gibt, die der Meinung sind, die Sicherheitsarchitektur von Java weise sowohl strukturelle als auch technische Schwächen auf. Ein weiteres Gefahrenpotential ergibt sich dadurch, dass Java-Applets direkt JavaScripts und JavaScripts direkt Java-Applets aufrufen können.

Festzuhalten ist, dass aktive Inhalte eine erhebliche Bedrohung der Vertraulichkeit, Integrität und Verfügbarkeit der lokal gespeicherten Daten darstellen. Das Bundesamt für Sicherheit in der Informationstechnik hat bereits 1999 empfohlen: "Da sich der Internet-Nutzer einem kaum einschätzbaren

Schadenspotential aussetzt, rät das BSI dringend, bei der Nutzung des Internet auf aktive Inhalte zu verzichten."

Nun stellt sich aber die Frage, wie man dieser Empfehlung nachkommen kann. Die gängigen WWW-Browser bieten zwar die Möglichkeit aktive Inhalte durch entsprechende Browser-Konfigurationen abzuschalten. Diese Abschaltmechanismen haben sich aber als nicht ausreichend sicher erwiesen. Außerdem können alle, die eine Zugriffsberechtigung für den Browser haben, die Sicherheitseinstellungen jederzeit verändern. Insofern ist diese Vorgehensweise keine Lösung in Bereichen, in denen hoch sensible Daten verarbeitet werden und zudem eine Vielzahl von nicht technisch versierten Nutzerinnen und Nutzern Zugriff auf ein und dasselbe System haben. Dies dürfte aber in der medizinischen Datenverarbeitung, wie etwa im Klinikbereich, der Regelfall sein. Außerdem kann ein Blockieren von aktiven Inhalten dazu führen, dass bestimmte Informationen auf WWW-Seiten nur noch eingeschränkt oder gar nicht mehr genutzt werden können. Da sich die Verwendung aktiver Inhalte auf WWW-Seiten aber einer wachsenden Beliebtheit erfreut, würde sich bei einem Anhalten dieses Trends die grundsätzliche Frage nach dem Nutzen eines Internet-Anschlusses stellen.

Eine weitere Alternative könnte nun darin bestehen, an zentraler Stelle, nämlich an der Firewall, aktive Inhalte mit schädigender Wirkung zu filtern. Die Erkennung von AktivX-Controls, Java-Applets oder Scripting-Programmen mit einer Schadensfunktion ist allerdings ein schwierig zu lösendes Problem. Es existieren zur Zeit keine brauchbaren Programme, die eine ähnlich wirksame Erkennung ermöglichen, wie es bei Virenscannern der Fall ist. Selbst falls zukünftig solche Programme entwickelt werden können, wird immer eine gewisse Zeit zwischen dem bekannt werden eines schädigenden aktiven Inhalts und der Aktualisierung der Filtersoftware durch die Hersteller vergehen. Dieses Zeitintervall der Schutzlosigkeit kann bei Patientendaten verarbeitenden Systemen aber nicht hingenommen werden. Eine Filterung ist sowieso in den Fällen kein probates Mittel, in denen eine gesicherte HTTPS-Verbindung genutzt wird, da die übertragenen Daten dann verschlüsselt sind.

➢ Der FTP-Dienst:

Der FTP-Dienst (File Transfer Protokoll) ermöglicht den komfortablen Zugriff auf Dateien über Netzwerke hinweg. Mit FTP können beliebige Dateien, die im Internet auf einem Server bereitgestellt werden, auf den lokalen Client heruntergeladen werden. Damit entsteht ein erhebliches Sicherheitsrisiko, da die Dateien Trojanische Pferde, Viren (File-Viren, Boot-Viren, Makro-Viren) und Würmer enthalten können, also Programme mit schädigenden Funktionen. Diese Risiken sind ebenso bei einem Datei-Download über

HTTP gegeben, der über den Browser angestoßen werden kann. Die Bedrohungslage verschärft sich noch durch die Möglichkeit, heruntergeladene Dateien direkt der Applikation zuzuführen, die das Dateiformat verarbeiten kann. Damit wird zum Beispiel für eine Word-Datei das Word-Textverarbeitungsprogramm gestartet. Dieser Automatismus hat zur Folge, dass ein in einer Datei enthaltenes Programm mit schädigenden Funktionen sofort seine Wirkung entfalten kann.

➢ **Der E-Mail-Dienst:**

Der E-Mail-Dienst ist wohl der beliebteste Internet-Dienst. Er ist aber auch gleichzeitig der Dienst, der mit den größten Risiken für den Datenschutz und die Datensicherheit behaftet ist. Da an eine E-Mail beliebige Dateien (Attachments) angehängt werden können, entsteht dieselbe Gefährdungssituation durch Trojanische Pferde, Viren und Würmer wie beim FTP-Dienst.

Ein weiteres, meist nicht beachtetes Risiko, entsteht dadurch, dass die neueren E-Mail-Programme es erlauben, den E-Mail-Inhalt (Body Part) im HTML-Format zu erstellen. Damit ergeben sich dieselben Risiken, die für den WWW-Dienst in Zusammenhang mit aktiven Inhalten beschrieben wurden. Beim Anschauen einer HTML-E-Mail werden die darin enthaltenen aktiven Inhalte automatisch ausgeführt. Darüber hinaus kann ein solcher HTML-Body-Part auch einen Hyperlink enthalten, der bei Aktivierung (anklicken) durch die Nutzerin oder den Nutzer einen Datei-Download anstößt. Dieser Mechanismus führt dann wiederum zu den bereits beschrieben Bedrohungen durch Trojaner, Viren und Würmer.

Manche meinen, die Bedrohungen durch schädigende Programmcodes adäquat durch den Einsatz von Virenscannern an zentraler Stelle (Firewall) abwehren zu können. Bei dieser Vorgehensweise verbleibt aber ein Restrisiko, das bei hoch sensiblen Daten, wie es im medizinischen Bereich der Fall ist, nicht toleriert werden kann. Neu auftretende Trojaner, Viren oder Würmer können von Virenscannern erst erkannt werden, wenn die Scannerhersteller eine neue Virendefinition bereitstellen und diese dann auch installiert ist. Dabei vergeht aber eine Zeitspanne der Schutzlosigkeit, in der bereits ein schädigendes Ereignis eintreten kann. Erinnert sei hier nur an den Melissa- und den Loveletter-Virus, die in kürzester Zeit, weltweit großen Schaden angerichtet haben. Werden Daten verschlüsselt übertragen ist ein Virenscannen sowieso nicht möglich.

Resümee

Aufgrund der hohen Sensibilität der Daten, die in medizinischen Systemen verarbeitet und gespeichert werden, können Datenschutz und Datensicherheit nach dem heutigen Stand der Technik nur gewährleistet werden, wenn die folgenden Voraussetzungen erfüllt sind:

Internet-Dienste (WWW, FTP, E-Mail) dürfen nur auf Rechnersystemen zur Ausführung gebracht werden, die keine patientenbezogenen Daten verarbeiten oder speichern und die nicht in ein Netzwerk eingebunden sind, in dem sich ein Rechnersystem befindet, das patientenbezogene Daten verarbeitet.

Lösungsvorschläge für eine nach heutigem Erkenntnisstand hinreichend sichere Internetanbindung

Die restriktiven Anforderungen, die an eine Internetanbindung für Patientendaten verarbeitende Systeme zu stellen sind, bedeuten nicht, dass prinzipiell kein Internetzugang möglich wäre. Es ist allerdings ein erhöhter technischer Aufwand zu betreiben, der auch mit höheren Kosten verbunden ist. Daran darf im Sinne der Patienten und des medizinischen Personals aber nicht gespart werden, wenn die Notwendigkeit für einen Internetzugang unabdingbar gegeben ist.

Die folgenden technischen Alternativen sind als Lösungsvorschläge zu verstehen und nicht abschließend zu sehen:

1. Wird die Notwendigkeit gesehen alle oder auch nur viele Arbeitsplätze mit einem Internetzugang auszustatten, bietet sich der Aufbau eines separaten Netzes an, das über eine zentrale Firewall mit dem Internet verbunden wird. Damit müsste jeder Arbeitsplatz mit zwei Rechnern ausgestattet werden. Ein Rechner, der mit dem internen Netz verbunden ist und ein Rechner, der an das Netz mit Internetzugang angeschlossen ist. Monitor, Tastatur und Maus könnten mittels eines Umschalters mit beiden Rechnern gekoppelt werden.

2. Falls nur an einigen wenigen Arbeitsplätzen ein Internetzugang erforderlich ist, könnten stand-alone Rechner mit einem Internetzugriff ausgestattet werden.

3. Eine weitere, unkonventionelle aber kostengünstige Lösungsalternative stellt das Konzept der so genannten grafischen Firewall dar. Dabei werden VNC-Server (VNC steht für Virtual Network Computing) eingerichtet, die dem internen Netz vorgelagert sind. Die VNC-Server haben eine Verbindung zum Internet und zum internen Netz. Die Arbeitsplätze des internen Netzes sind die Clients der VNC-Server. Das VNC-Konzept basiert nun darauf, dass zwischen einem VNC-Server und seinen VNC-Clients, auf denen ein so genannter VNC-Viewer installiert ist, ausschließlich Grafik- Tastatur- und Mausinformationen übertragen werden. Damit können Internet-Dienste dem internen Netz vorgelagert werden. Sämtliche Ressourcen (Prozesse und Daten), die mit der Ausführung von Internet-Diensten zu tun haben, befinden sich ausschließlich auf den VNC-Servern. Auf den VNC-Clients, also auf den Arbeits-

plätzen der Internet-Nutzer, findet lediglich die Präsentation statt. Den VNC-Servern und dem internen Netz wird eine Firewall zwischengeschaltet, die nur das spezifische VNC-Protokoll passieren lässt. Zwischen dem Internet und den VNC-Servern befindet sich eine Firewall mit den üblichen Sicherheitskonfigurationen. VNC liegt im Quellcode vor und unterliegt der GNU Public License. VNC ist im Internet unter http://www.uk.research.att.com/vnc/index.html zu finden.

2.2 Data Warehouse und Data Mining - Goldgräber im Informationszeitalter

2.2.1 Data Warehouse

Elektronisch gespeicherte Informationsbasen wachsen mit exponentiellen Raten. Dieser Prozess wird durch die Einführung elektronischer Kassen- und Abrechnungssysteme oder aber durch die Speicherung von Daten, die implizit durch die Erbringung einer Dienstleistung im Rahmen von Tele- oder anderen Kommunikationsdiensten anfallen, beschleunigt.

Das führte in der jüngeren Vergangenheit dazu, dass Unternehmen mit großen Datenmengen und mehreren Geschäftsbereichen den Überblick über ihre eigenen Daten zu verlieren drohten. Es existierten parallel diverse operative Datenbestände auf womöglich heterogenen Systemen. So lagern beispielsweise in den Datenbanken des Verkaufs die Umsatzzahlen, die dazugehörigen Kundendaten dagegen separat in einer anderen Datenbank. Die Qualität strategischer Entscheidungen hängt jedoch unmittelbar von der Qualität der zugrundeliegenden Informationen ab. Abhilfe sollte eine "strategische" Datenbank schaffen, in der die operativen Daten aus allen Geschäftsbereichen der Unternehmen unter Management-Gesichtspunkten zusammengeführt werden konnten, ein "**Datenlager**". Die Warehouse-Management-Software sammelt also in einer von den operativen Systemen getrennten Datenbank regelmäßig Einträge aus den verschiedensten Geschäftsbereichen, ordnet und verdichtet sie und versieht sie mit beschreibenden Zusatzattributen, den so genannten Metadaten.

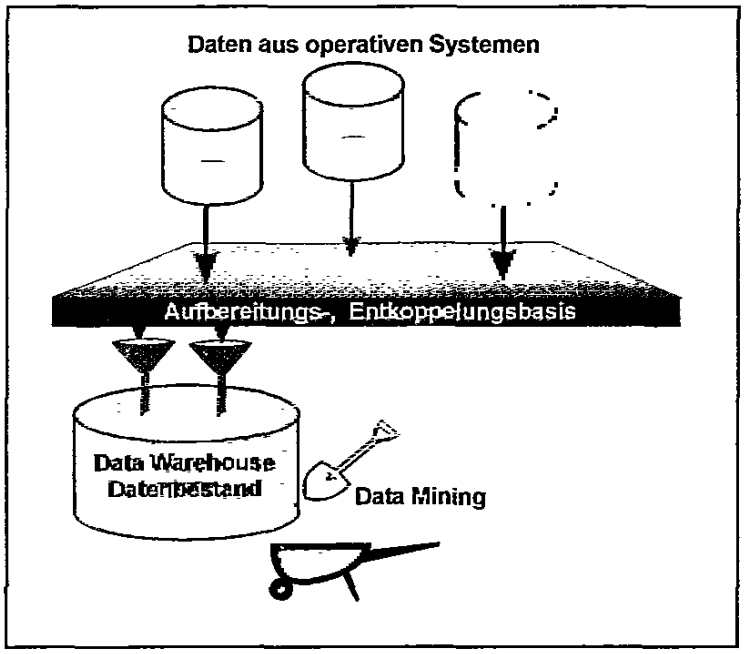
Die beschreibenden Merkmale eines Data Warehouse lassen sich wie folgt zusammenfassen:

- Ein Data Warehouse integriert Daten aus unterschiedlichen Quellen zu einem homogenen Datenbestand.
- Ein Data Warehouse sammelt nicht möglichst viele Informationen, sondern setzt eine genaue Analyse des Informationsbedarfs voraus.

- Ein Data Warehouse enthält neben aktuellen Informationen auch ältere Daten aus demselben Kontext sowie solche für zukünftige Planungen.

Die Daten und Strukturen eines Data Warehouse stehen über einen längeren Zeitraum zur Verfügung. Abfragen können deshalb beliebig oft wiederholt werden.

Ziel eines Data Warehouse ist es nicht, einzelne Datensätze zu untersuchen. Im Gegenteil: Von einzelnen Daten soll abstrahiert, kumuliert, aggregiert werden, um Zusammenhänge größerer Ordnung zu erkennen. Dazu ist es häufig nötig, die Speicherdauer extrem zu verlängern, da relevante Zusammenhänge oft erst nach Monaten oder Jahren erkannt werden können.



Um nun wirksam die so entstandene Datenmenge auswerten zu können, bedarf es weiterer Werkzeuge: Hier ist in datenschutzrechtlicher Sicht insbesondere das Data Mining relevant.

2.2.2 Data Mining - graben nach Erkenntnis

Den Kern von Data Mining bilden Verfahren, die selbständig Annahmen generieren, diese prüfen und den Auswertenden relevante Ergebnisse in verständlicher Form präsentieren. Der Begriff beinhaltet eine Reihe von Technologien, mit deren Hilfe Unternehmen entscheidungsrelevante Informationen aus Datenbanken extrahieren können. Es werden bereits bekannte Lösungsansätze aus dem Bereich der künstlichen Intelligenz wie neuronale Netze als nicht lineare Prognoseverfahren, die biologischen Informationsverarbeitungen nachempfunden werden und "selbständig lernen", sowie herkömmliche statistische Verfahren berücksichtigt. Data Mining steht also

nicht für eine bestimmte Analyse, sondern für eine ganze Reihe von Verfahren. Sie ermöglichen die Analyse und Prognose von Verhaltensweisen und Trends. Data Mining liefert Erkenntnisse und Zusammenhänge, die bisher in der Masse der Daten untergegangen sind oder für die kein analysierbarer Zusammenhang erkannt wurde.

Ein gern zitiertes Beispiel für den Effekt von Data Mining liefert eine Handelskette, die einen Anstieg des Verkaufs von Bier und Windeln in den frühen Abendstunden entdeckte: Offensichtlich kauften viele Väter nach Feierabend noch schnell Windeln für den Nachwuchs und gönnten sich zur Belohnung für diese schweißtreibende und verantwortungsvolle Aufgabe diverse Bierchen. Das Handelsunternehmen zog aus dieser Erkenntnis Konsequenzen: Beide Produkte wurden nebeneinander platziert. Ob der Bierumsatz insgesamt durch diese Maßnahme gesteigert wurde, ist nicht bekannt.

2.2.3 Datenschutzrechtliche Aspekte

Für den dargestellten Fall oder ähnliche Zusammenhänge sind personenbezogene Daten nicht relevant. Die eine Einzelperson repräsentierenden Daten werden als simple Zahl zu einer Summe addiert. Der Focus von Auswertungen ist die Aufdeckung von Einsparpotentialen oder Strukturmängeln. Problematisch wurde die Situation, als das Marketing das Potential der Data Warehouse-Technologie für die Auswertung von Kundenmerkmalen entdeckte. Je mehr der einzelne Kunde in der Verkaufsphilosophie der Unternehmen in den Mittelpunkt rückte (One-to-One Marketing), desto lauter wurde der Ruf nach der Erstellung von Kundenprofilen, in denen demographische und verhaltensorientierte Daten verarbeitet werden können.

Solange dabei die Analyse anhand anonymisierten Datenmaterials vorgenommen wird, so dass eine Rückführung auf einzelne Personen oder Personengruppen nicht möglich ist, bestehen aus datenschutzrechtlicher Sicht keine Einschränkungen. Häufig wird allerdings mit der Analyse der Wunsch verbunden, die Ergebnisse auch kundenbezogen auswerten zu können. Das bedeutet nichts anderes als das Konsumverhalten der einzelnen Kundinnen und Kunden personenbezogen zu erfassen, auf beispielsweise Präferenzen oder die Zahlungsfreudigkeit hin auszuwerten und Prognosen über das künftige Verhalten aufzustellen.

Ohne Einwilligung der betroffenen Personen steht das geltende Recht einer derart weitreichenden Datenverarbeitung entgegen. Noch ungeklärt ist allerdings, ob in eine solche Datenverarbeitung überhaupt wirksam eingewilligt werden kann. Dafür wäre es zunächst erforderlich, den Zweck der Datenver-

arbeitung hinreichend spezifizieren zu können. Eine detailgenaue und umfassende Profilbildung kann die betroffenen Personen zudem ab einer bestimmten Qualität derart "gläsern" werden lassen, dass trotz ihrer Einwilligung die Grenze des rechtlich Zulässigen überschritten werden kann. Da das Recht auf Löschung personenbezogener Daten nach den gesetzlichen Vorschriften nicht abbedungen werden kann, ist außerdem fraglich, ob und wie weitgehend eine Einwilligung in die Datenverarbeitung in einem Data Warehouse erteilt werden kann.

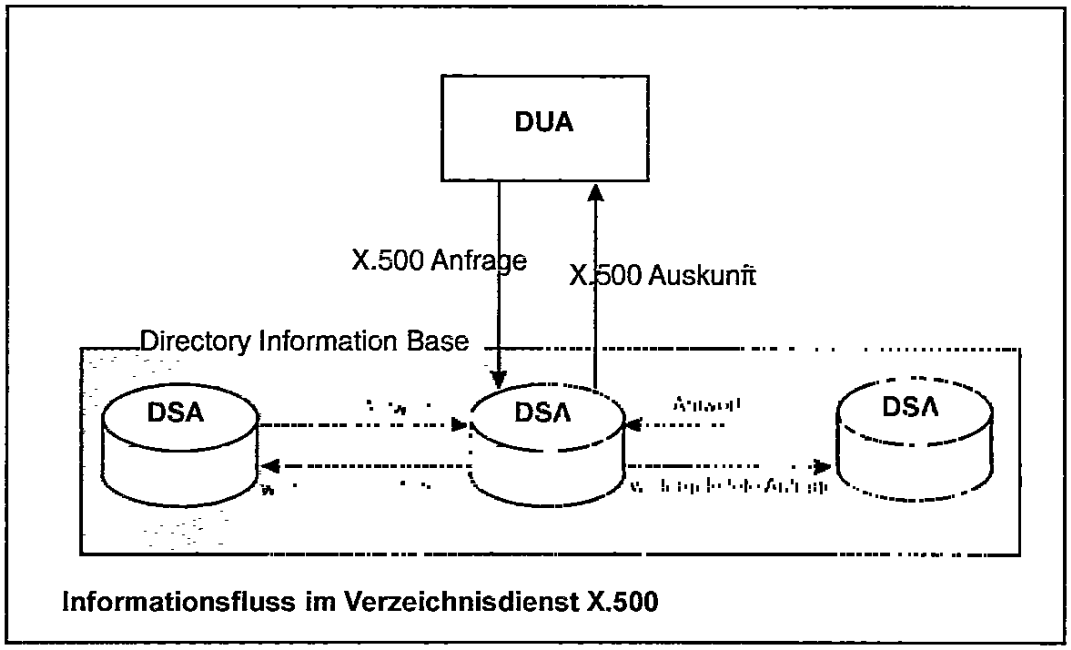
Für den Bereich der öffentlichen Verwaltungen ist die Rechtslage demgegenüber klarer: Da sich die personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse vom ursprünglichen Verwendungszweck entfernt, stellt sie ohne Einwilligung der betroffenen Personen eine unzulässige Speicherung auf Vorrat ohne Zweckbindung dar.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich in ihrer Entschließung vom 14./15. März 2000 kritisch mit Data Warehouse-Systemen und Data Mining-Verfahren auseinandergesetzt (Abdruck im Anhang, Nr. 16). Als datenschutzrechtliche Risiken und Gefahren werden darin benannt: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Datenspeicherungen. Dabei geht es nicht darum, derartige Technologien etwa zu verteufeln, sondern Verfahren so einzusetzen, dass die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermieden wird.

2.3 Verzeichnisdienste - datenschutzrechtlich ambivalent

Es ist inzwischen selbstverständlich mittels E-Mail oder ähnlicher Dienste weltweit miteinander zu kommunizieren. Doch wie erfährt man die Adresse eines Kommunikationspartners? Bei der herkömmlichen Kommunikation genügte ein Blick ins Telefonbuch oder ein Anruf bei der Auskunft. Ein Medium wie E-Mail bietet jedoch ein weltumspannendes Netz mit Millionen Adressen, die sich ständig ändern. Manche wünschen sich daher ein ständig aktuelles "elektronisches Adressbuch", das möglichst weltweit Auskunft zu Kommunikationsadressen von Einrichtungen und Personen liefern kann. Die Beschreibung eines solchen Dienstes wurde 1988 in Form eines Referenzmodells der Internationalen Organisation für Standardisierung (ISO) geschaffen und als X.500-Verzeichnisdienst eingeführt. X.500 ist ein Standard im OSI/ISO Schichten Modell und wurde dort in die Anwendungsschicht eingebunden. Anhand dieses Modells soll im Folgenden grob die Funktionsweise eines Verzeichnisdienstes skizziert werden.

Der X.500-Verzeichnisdienst ist ein verteiltes System, lokale Daten liegen in einzelnen Teilsystemen, den Directory System Agents (DSA). Die Gesamtheit aller DSA-Daten bildet die Directory Information Base (DIB) und stellt sich den Clients, auch Directory User Agents (DUA) genannt, als ein homogenes logisches System dar. Jeder DSA verfügt nur über die dort gespeicherten Daten. Sollte ein Eintrag nicht bekannt sein, wird die Anfrage des Client an andere Datenbanken (DSA) weitergeleitet. Dieser Mechanismus wird solange wiederholt bis die Information gefunden ist.



Informationsfluss im Verzeichnisdienst X.500

In der logischen Struktur von X.500 werden Informationen zu Objekten (Rechnern, Personen) in Form von Einträgen zusammengefasst. Diese Einträge sind in einer baumartigen Hierarchie angeordnet, die auch Directory Information Tree (DIT) genannt wird. Um die Einträge im DIT einheitlich zu strukturieren, werden jedem Eintrag bestimmte Objektklassen zugeordnet. Die Klasse beschreibt die jeweilige Art des Objektes, wie zum Beispiel Land, Organisation, Person. Die Objekte selbst bestehen aus Attributen. Ein Attribut wiederum besteht aus einem Attributtyp und einem oder mehreren Attributwerten. Jeder Eintrag im Directory wird durch einen eindeutigen Namen, den Distinguished Name (DN), referenziert.

Bisher dienten Verzeichnisdienste vornehmlich der Benutzerverwaltung. Verzeichnisdienste nach dem X.500 Standard ermöglichen durch ein standardisiertes Protokoll die Speicherung nahezu beliebiger Objekte. Alle Informationen über einen Anwender, also auch Schlüsselzertifikate, können in einem einzigen zentralen Verzeichnis abgelegt sein, auf das alle anderen

Systeme zugreifen. Als weiterer Schritt können Informationen über andere Objekte wie Rechner, Netze und Peripheriegeräte hinzugefügt werden.

Der Zugriff auf Daten des Directory erfolgt über ein eigens dafür entwickeltes Protokoll, das Directory Access Protocol (DAP). In der Praxis wird häufig auch eine abgespeckte Variante, das Leightweight Directory Access Protocol (LDAP) auf der Client Seite eingesetzt. Es bietet die Möglichkeit, eine Authentifizierung des Benutzers gegenüber dem Directory zu implementieren. Diese Authentifizierung kann schwach (Name/Passwort) oder stark (asymmetrisches Kryptosystem) ausfallen.

Diese Mechanismen sind im Standard **X.509** beschrieben: Berechtigungen für bestimmte Daten und die Art des Zugriffs werden in Zugriffskontrolllisten niedergelegt. Ein weiterer, wichtiger Mechanismus ist der des Schlüsselmanagements. Es wurde festgelegt, wie ein Schlüsselzertifikat abgespeichert wird und global von einer Applikation wiedergefunden werden kann, also die Voraussetzung zum Aufbau einer PKI (Public Key Infrastructur) geschaffen.

Die Rolle von Verzeichnisdiensten im Datenschutz ist durchaus ambivalent: Auf der einen Seite gewährleisten sie durch die Möglichkeit zentraler Verwaltung von beliebigen Objekten auf verteilten Systemen Verfügbarkeit und Transparenz, auf der anderen Seite sind beispielsweise System- oder Benutzerverwalter in der Lage, sämtliche über eine Person gespeicherten Daten einzusehen. Dies birgt Missbrauchsrisiken in sich. Es gilt also wie immer die Devise restriktiver Datensparsamkeit. Dem Versuch durch Nutzerinnen und Nutzer, sich unbefugt Zugriffsrechte zu beschaffen, ist mit starker Authentifizierung und mit konsequenter Nutzung der Zugriffskontrollmechanismen zu begegnen. Ein weiterer Aspekt ist die Möglichkeit der Verteilung. Eine sehr fein granulare Verteilung erfordert die vermehrte Replikation von Daten und gefährdet dadurch die Konsistenz und Aktualität der Daten, während eine sehr grob granulare Verteilung die bekannten Risiken der zentralen Speicherung von Daten birgt.

Es gilt hier einen geeigneten Kompromiss zu finden und die beschriebenen Sicherheitsmechanismen konsequent zu implementieren. Dann bieten Verzeichnisdienste eine benutzerfreundliche Plattform, Daten weltweit zur Verfügung berechtigter Personen zu stellen.

2.4 Common Criteria - neue Grundlagen zur Prüfung und Bewertung von IT-Sicherheit

Die Common Criteria (CC) sind ein neuer Weg, die bislang weltweit unterschiedlichen Bestimmungen zur Beschreibung, Bewertung und Evaluierung von informationstechnischen Produkten und Systemen zu harmonisieren. Aus der Sicht des Datenschutzes sind hierbei besonders die Möglichkeit der Beschreibung von Anforderungskatalogen sowie die Einbringung zusätzlicher funktionaler Sicherheitsaspekte zur Kommunikation, Kryptografie und Privatsphäre von Bedeutung.

Mit der Überarbeitung der "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik / Common Criteria for Information Technology Security Evaluation, Version 2.0" erfolgte 1997 eine Weiterentwicklung und Harmonisierung der europäischen "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (**ITSEC**)", des "Orange-Book (**TCSEC**)" der USA und der kanadischen Kriterien (**CTCPEC**). Die Verfeinerung und Ergänzung der CC wird fortgeschrieben. Nach den Vorstellungen der Entwickler der CC soll dieses "Regelwerk zur Beschreibung von IT-Techniken" eine Grundlage sowohl für Anwender sein, ihre Wünsche und Anforderungen zu definieren, als auch für Hersteller und Entwickler, um ihre Produktbeschreibungen und Konzepte zu dokumentieren.

- Die Anwenderinnen und Anwender spezifizieren ihre Funktions- und Sicherheitsanforderungen (Angebotsanfrage) an Produkte oder Systeme durch die Erstellung von Protection Profiles (PP).
- Die Entwicklung erklärt und beschreibt ihre produktspezifische Umsetzung von Anforderungen in den Security Targets (ST).

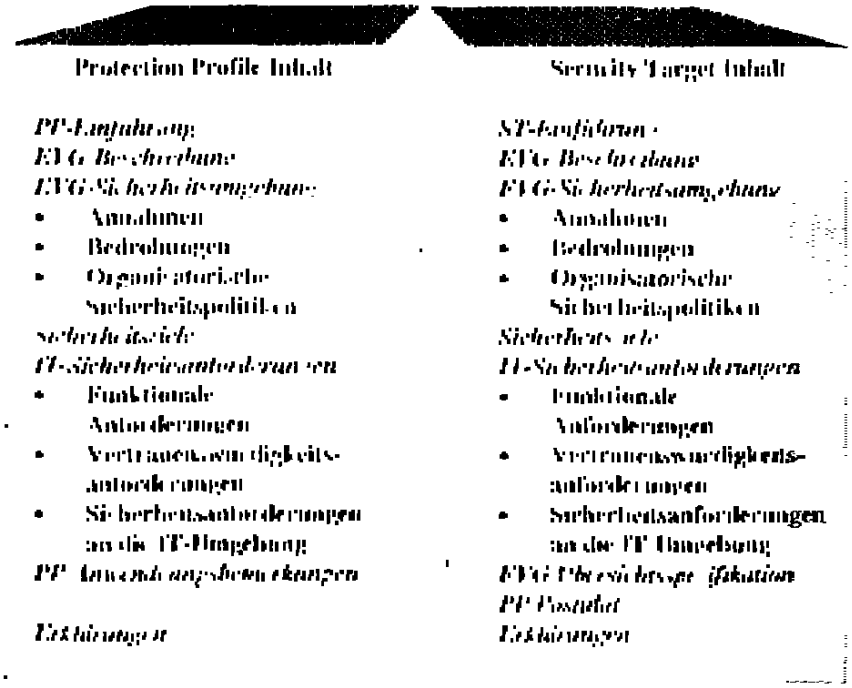
Beide Beschreibungen dienen der Prüfungsinstanz (Evaluator) zur Bewertung und Einstufung der Produkte.

Die CC Dokumentation gliedert sich in drei Teile :

Teil 1: Einführung und Allgemeines Modell
Teil 2 : Funktionale Sicherheitsanforderungen
Teil 3: Anforderungen an die Vertraulichkeit

Unter Datenschutzaspekten sind die funktionalen Sicherheitsanforderungen (Teil 2) und die Anforderungen an die Vertraulichkeit (Teil 3) von hohem Interesse.

Der Aufbau der Protection Profiles (PP) und Security Targets (ST) erfolgt in verschiedenen Abschnitten, die sowohl die Umgebung, die Gefährdungen, die Annahmen und allgemeine Anforderungen an die zu entwickelnden und zu prüfenden IT-Komponenten, den so genannten Evaluierungsgegenstand (EVG), beschreiben.



Es gibt umfangreiche Kataloge mit bereits entwickelten Modulen, die bei der Erstellung von neuen Protection Profiles und Security Targets übernommen oder je nach Erfordernis angepasst werden können. Hierbei werden Abhängigkeiten, Bezüge und Optionen zu weiteren Anforderungen und die Verkettung von Funktionsbausteinen aufgezeigt.

Bei der Erarbeitung der CC wurden neben den Standard-Sicherheitsanforderungen (beispielsweise die Identifizierung und Authentisierung, Zugriffskontrolle) auch moderne Anforderungen an die IT-Sicherheit berücksichtigt, die im Besonderen auch die Belange des Datenschutzes betreffen. Ein Teil dieser besonderen funktionellen Sicherheitsanforderungen finden sich unter den Begriffen:

Kommunikation

- Nichtabstreitbarkeit der Urheberschaft von übertragenen Daten
- Nichtabstreitbarkeit des Empfangs von übertragenen Daten

Kryptografische Unterstützung

- Kryptografisches Schlüsselmanagement
- Kryptografischer Betrieb

Privatsphäre

- Unbeobachtbarkeit (die Benutzung bestimmter Dienste bleibt anderen Benutzerinnen und Benutzern verborgen)
- Anonymität (die Benutzung bestimmter Dienste ist vollständig verborgen)
- Pseudonymität (die Benutzung bestimmter Dienste ist bedingt sichtbar, beispielsweise für die Gebührenabrechnung)
- Unverkettbarkeit (die Sichtbarkeit der Benutzung bestimmter Dienste ist eingeschränkt)

Die CC sind auf alle IT-Sicherheitsprodukte und -systeme anwendbar. Es kann Hardware und Software nach den CC evaluiert werden, wobei der Schwerpunkt bei der Software liegt.

Eine Gruppe des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder hat sich mit den Möglichkeiten und der Methodik der CC beschäftigt. Es wurde untersucht in welcher Form der Einsatz und die Nutzung der CC für die Beschreibung, Vorgabe und Bewertung von datenschutztechnischen Anforderungen verwendet werden kann.

Bei der Erstellung eines PP "Datenschutz- und Datensicherheitsmodul" wurde die Erfahrung gemacht, dass bei einer den CC konformen Bearbeitung der PP/ST eine Vielzahl von Abhängigkeiten bei Anforderungen und Funktionen zu berücksichtigen sind. Dies bedeutet, dass bei den Beschreibungen sehr konkrete Aussagen erforderlich sind. Es müssen detaillierte Kenntnisse über organisatorische Anforderungen und Verpflichtungen, Einsatz- und Umgebungsbedingungen wie auch über technische Realisierungsmöglichkeiten vorhanden sein. Hier zeigen sich aber auch die Grenzen der CC. Für viele Anwenderinnen und Anwender sind die eigenen Kenntnisse nicht mehr ausreichend, um die Feinheiten in den Anforderungen oder den Funktionen festzulegen und die komplexen Zusammenhänge zu beschreiben. Hieraus ergibt sich das Erfordernis einer projektorientierten Vorgehensweise unter Beteiligung von Entwicklern und Expertinnen. In einem interaktiven Prozess sind die Spezifikationen immer weiter zu verfeinern, bis alle aufgestellten Forderungen erfüllt sind.

Für die Interessen des Datenschutzes bieten die CC insgesamt folgende Möglichkeiten:

- Die Beschreibungen nach den Strukturen der CC lassen die Vergleichbarkeit von Anforderungen und Funktionen zu.
- Die Nutzung der Module der CC kann zu einer systematischen Betrachtung aller Teilaspekte genutzt werden.
- Das Prinzip, jeder Sicherheitsfunktion eine Bedrohung entgegenzustellen, entspricht den Forderungen eines Sicherheitskonzepts.
- Die Berücksichtigung der eingebrachten funktionellen Sicherheitsanforderungen zum Datenschutz und zur Datensicherheit erhöht die Qualität der Anforderungen in den PP und Produktspezifikationen in den ST.

Die Grenzen aus Anwendungssicht liegen in der vorgesehenen Umsetzungstiefe der Beschreibungsgegenstände. Eine vollständige Erstellung von PP oder ST ist deshalb nur in einem Projektteam mit Unterstützung der erforderlichen Fachleute möglich. Voraussetzung ist weiter, dass eine fachkundige Einweisung und Schulung erfolgt ist.

2.5 Technischer Datenschutz – ein Schritt in die Zukunft

2.5.1 Innovative Technikregelungen

Mit der neuen Fassung des nordrhein-westfälischen Datenschutzgesetzes wurde nach intensiven Diskussionen mit dem Innenministerium § 10 DSG NRW grundlegend überarbeitet. Dies war aufgrund der technischen Entwicklung im IT-Bereich dringend notwendig. Die bis zur Gesetzesnovellierung geltenden Regelungen zu den technischen und organisatorischen Maßnahmen, die so genannten "10 Gebote", hatten ihren Ursprung in den 70er Jahren und orientierten sich an der damaligen Technologie und Infrastruktur der Datenverarbeitung. Geprägt war diese Zeit von zentral organisierten Rechenzentren. Telekommunikation und Vernetzungen spielten nur eine untergeordnete Rolle. Die Datensicherheitsüberlegungen waren ausgerichtet auf eine monolithische Großrechnerwelt und primär verbunden mit dem Schutz der Rechner, die in hermetisch abgeschlossenen Rechenzentren betrieben wurden. In einer Zeit, in der Datenverarbeitung zunehmend dezentral in weltumspannenden Rechnernetzen betrieben wird, sind solche Regelungen nur noch bedingt oder gar nicht mehr wirksam. Die nachfolgenden Beispiele sollen dies verdeutlichen:

- **Zugangskontrolle**: Unbefugten sollte mit dieser Maßnahme der physische Zugang zu Räumen verwehrt werden, in denen sich Datenverar-

beitungsanlagen befinden. Heute stehen Rechner aber nicht mehr ausschließlich in besonders gesicherten Räumen eines Rechenzentrums, sondern nahezu jede Mitarbeiterin und jeder Mitarbeiter hat einen Personalcomputer auf dem Schreibtisch. Zugangskontrollen der herkömmlichen Art sind damit nicht mehr praktikabel, aber auch nicht mehr ausreichend.

- **Datenträgerkontrolle:** Die Datenträgerkontrolle konnte in Zeiten der Großrechner durch die Einrichtung von zentralen Datenträgerarchiven realisiert werden. Heute müssen jedoch Datenträger für eine große Zahl von Nutzerinnen und Nutzern dezentral verfügbar sein. Außerdem sind die verschiedenen Formen der Datenträger weitaus vielfältiger geworden (wie etwa Festplatten, Disketten, CD-ROMs, DVDs, Bildplatten, Chipkarten, Bänder). Das Ziel der Regelung, ein unbefugtes Auswerten, Verändern und Entfernen der Daten auf Datenträgern zu verhindern, ist auf dem Wege der konventionellen Datenträgerkontrolle nicht mehr erreichbar.

- **Speicherkontrolle:** Die unbefugte Eingabe von Daten sowie deren Kenntnisnahme, Veränderung und Löschung ist nicht mehr nur über die Konsole im Rechenzentrum möglich und beschränkt sich nicht mehr nur auf Speichermedien als Träger von Daten, sondern ist in einer vernetzten DV-Landschaft von jedem Endgerät aus möglich unter Einbeziehung der verbindenden lokalen Netzwerke (LAN) oder der Weitverkehrsnetze (WAN) selbst. Die frühere Regelung bliebe daher heute weitgehend wirkungslos.

- **Benutzerkontrolle:** Die Benutzung eines Datenverarbeitungssystems mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte sollte hierdurch verhindert werden. Die Nutzung von Mechanismen zur Datenfernübertragung sind heute keine Besonderheit mehr, sondern der Regelfall. Insofern bedarf es keiner Regelung, die dies besonders hervorhebt. Allgemein muss sichergestellt werden, dass die Benutzerinnen und Benutzer eines Datenverarbeitungssystems nur im Rahmen ihrer Berechtigungen personenbezogene Daten verarbeiten können, mit welchen technischen Einrichtungen ist dabei ohne Belang.

- **Zugriffskontrolle:** Die Zugriffskontrolle sollte sicherstellen, dass Benutzer und Benutzerinnen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Damit beinhaltete die Zugriffskontrolle die Benutzerkontrolle. Die Benutzerkontrolle war also eine redundante Regelung.

- **Übermittlungs- und Eingabekontrolle:** Mit der Übermittlungskontrolle und der Eingabekontrolle wurden zwei Maßnahmen definiert, die beide auf die Revisionsfähigkeit abzielen. Beide Maßnahmen griffen

aber zu kurz, da sie nur die Verarbeitungsschritte Eingabe und Übermittlung erfassten. Alle übrigen Phasen der Datenverarbeitung wurden nicht berücksichtigt und wären so einer Revision nicht zugänglich gewesen.

Die "10 Gebote" definierten **Sicherheitsmaßnahmen** (worauf schon der Begriff Kontrolle hindeutet) und hatten im Wesentlichen **die technischen Komponenten** von IT-Systemen zum Gegenstand. Einerseits waren sie dadurch stark technologieabhängig und hätten ständig neueren Entwicklungen angepasst werden müssen. Andererseits sind **Sicherheitsmaßnahmen** individueller Natur und abhängig von dem Schutzbedarf der zu verarbeitenden Daten, der konkreten Bedrohungslage, dem Stand der Technik, der Architektur der zu betrachtenden IT-Systeme und den DV-Verfahren, die auf diesen Systemen ablaufen sollen. Die Festlegung der Maßnahmen, die zur Sicherung eines konkreten Systems erforderlich sind, kann aber erst das Ergebnis einer individuellen Sicherheitsanalyse auf der Grundlage eines Sicherheitskonzepts sein und lässt sich nicht in einer gesetzlichen Regelung abschließend definieren. Insofern waren die bisherigen Regelungen des § 10 DSG NRW zwangsläufig unvollständig. Selbst wenn alle "10 Gebote" eingehalten wurden, konnte nicht notwendigerweise von einem sicheren System ausgegangen werden.

2.5.2 Sicherheitsziele

Nicht zuletzt bedingt durch die rasante Entwicklung der Informationstechnologie vollzieht sich ein Paradigmenwechsel im Datenschutz. Die bisherige primäre Ausrichtung des Schutzes auf die bei der Datenverarbeitung eingesetzten technischen Komponenten ist heute nicht mehr haltbar, da nicht mehr eine zentral ausgerichtete Datenverarbeitung im Vordergrund steht, sondern dezentralisierte und verteilte Strukturen vernetzter multimedialer Systeme. Heute schwirren die Daten über Datenautobahnen und es existieren vielfältige Möglichkeiten auf diese Datenautobahnen zu gelangen, um an der globalen elektronischen Kommunikation teilzunehmen. Die möglichen Formen der Datenverarbeitung von morgen sind zudem nicht absehbar. Die Innovationszyklen in der Informationstechnologie werden immer kürzer, Entwicklungen immer dynamischer und die Technik immer komplexer.

Damit erhält der Datenschutz eine neue Qualität. Datenschutz ist nicht mehr nur an technischen Anlagen festzumachen, sondern primär - im eigentlichen Sinne des Wortes - an den Daten selbst. Attribute wie vertraulich, integer, verfügbar und authentisch sind als Eigenschaften der Daten anzusehen, die unabhängig vom aktuellen Aufenthaltsort der Daten, der Art und dem Stadi-

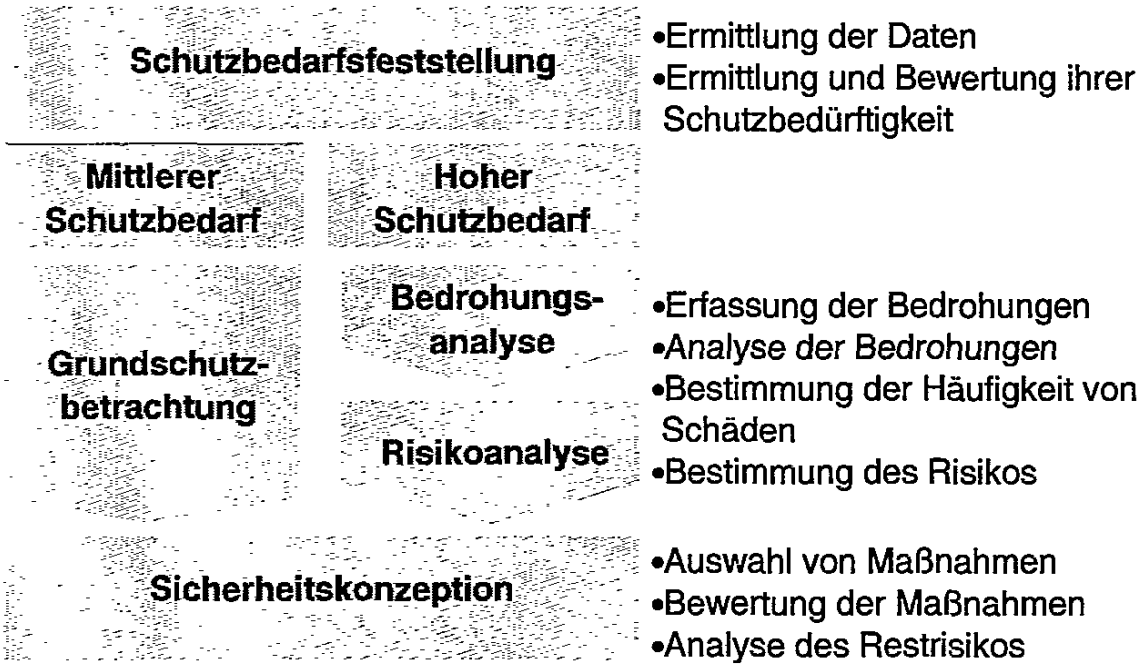
um ihrer Verarbeitung und den technischen Verarbeitungskomponenten gesichert werden müssen.

Daraus resultiert, dass für die Formulierung neuer Regelungen methodisch ein anderer Ansatz zu wählen ist. Es sind nicht mehr an der Technik orientierte **Sicherheitsmaßnahmen**, sondern auf einem abstrakteren Niveau primär an den Daten ausgerichtete **Sicherheitsziele** zu definieren. Die Zieldefinition muss gegenüber technischen Entwicklungen unempfindlich sein und allgemeingültige Anforderungen an eine sichere Datenverarbeitung beschreiben.

Die novellierte Fassung des § 10 DSG NRW trägt diesen Entwicklungen Rechnung. Nach § 10 Abs. 2 DSG NRW sind durch geeignete technische und organisatorische Maßnahmen unter anderem die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten zu gewährleisten. Diese Sicherheitsziele sind die klassischen Anforderungen der IT-Sicherheit. Sie zielen auf die **Verlässlichkeit** der Datenverarbeitungssysteme ab. Dies ist aber nur eine Seite der Medaille. Ein IT-System kann nur als sicher bezeichnet werden, wenn es auch **beherrschbar** ist. Damit ist gemeint, dass die schutzwürdigen Belange der Betroffenen durch die Nutzung von IT-Systemen nicht unzulässig beeinträchtigt werden dürfen. Die in § 10 Abs. 2 DSG NRW definierten Sicherheitsziele der Authentizität, Revisionsfähigkeit und Transparenz haben zum Ziel, dass IT-Systeme derart konstruiert und betrieben werden, dass sie beherrschbar sind. Erst diese duale Sichtweise gewährleistet eine Sicherheit im Sinne des Datenschutzes.

2.5.3 Sicherheitskonzept

Die Ermittlung der technischen und organisatorischen Maßnahmen, die zur Gewährleistung der in § 10 Abs. 2 DSG NRW angeführten Sicherheitsziele zu treffen sind, hat nach § 10 Abs. 3 DSG NRW auf der Grundlage eines Sicherheitskonzepts zu erfolgen.



Vorgehen bei der Erstellung eines Sicherheitskonzepts

Beim Prozess der Sicherheitskonzeption werden in der ersten Phase die schutzbedürftigen Daten ermittelt. Abhängig vom Grad der Sensibilität der Daten steigt ihre Schutzbedürftigkeit. Auch die Verarbeitungszwecke und die konkreten Verwendungszusammenhänge beeinflussen die Intensität der Schutzbedürftigkeit. Einzubeziehen sind auch die Bedeutung und die Schwere der Folgen eines Datenmissbrauchs für die Betroffenen. Bei Daten mit einem erhöhten Schutzbedarf schließt sich in der zweiten Phase die Bedrohung- und Risikoanalyse an. Hier werden zunächst alle Bedrohungen ermittelt und analysiert. Für jede Bedrohung werden die damit verbundenen Risiken bestimmt. In der dritten Phase werden für jede Bedrohung die technischen und organisatorischen Maßnahmen ermittelt, die zur Abwehr der Bedrohung geeignet sind und das verbleibende Restrisiko entsprechend dem Schutzbedarf vertretbar machen. Da es zur Abwehr ein und derselben Bedrohung möglicherweise mehrere Maßnahmenalternativen gibt, werden mittels einer Kosten/Nutzen-Analyse die angemessenen Maßnahmen bestimmt. Für Daten bis zu einem mittleren Schutzbedarf kann in der zweiten Phase der Sicherheitskonzeption die individuelle Bedrohungs- und Risikoanalyse durch die verallgemeinerte Grundschutzbetrachtung nach dem IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik ersetzt werden.

Die Entwicklung einer Sicherheitskonzeption ist kein einmaliger, sondern ein permanenter Prozess. Die Wirksamkeit der getroffenen Sicherheitsmaß-

nahmen ist fortlaufend mit Blick auf sich wandelnde Bedrohungen, veränderte Rahmenbedingungen der Datenverarbeitung und Entwicklungen der Technik zu überprüfen. Ergibt sich dabei ein Anpassungsbedarf, sind die notwendigen Änderungen zeitnah umzusetzen.

2.5.4 Vorabkontrolle

Die ebenfalls in § 10 Abs. 3 DSG NRW geforderte Vorabkontrolle zielt ab auf die mit der jeweils spezifischen Form der Datenverarbeitung eventuell verbundenen Gefahren für das in § 1 DSG NRW geschützte Recht auf informationelle Selbstbestimmung. Sie ist eine Art "kleine Technikfolgenabschätzung". Insofern ist vor der Entscheidung für den Einsatz oder für eine wesentliche Änderung eines automatisierten Verfahrens zu prüfen, ob von dem konkreten Verfahren Gefahren für das Recht auf informationelle Selbstbestimmung ausgehen.

Im Rahmen der Vorabkontrolle sind ohne Anspruch auf Vollständigkeit insbesondere folgende Kriterien zu prüfen:

- Kann das Verfahren die Zulässigkeit der Datenverarbeitung nach § 4 Abs. 1 DSG NRW gewährleisten?
- Kann mit dem Verfahren der Grundsatz der Datensparsamkeit nach § 4 Abs. 2 Satz 1 DSG NRW erfüllt werden oder gibt es alternative Verfahren, die mit weniger personenbezogenen Daten auskommen und das gleiche Ziel erreichen?
- Gibt es alternative Verfahren, für die bereits ein Datenschutzaudit nach § 4 Abs. 2 Satz 2 DSG NRW durchgeführt wurde? Dieser Aspekt wird natürlich erst relevant, wenn die gesetzlichen Voraussetzungen nach § 10a Satz 3 DSG NRW geschaffen sind.
- Berücksichtigt das Verfahren die besonderen Voraussetzungen der Verarbeitung personenbezogener Daten nach § 4 Abs. 3 DSG NRW ?
- Können die in § 4 Abs. 4 DSG NRW angeführten Rechte der Betroffenen gewährleistet werden?
- Gewährleistet das Verfahren den Betroffenen die Geltendmachung schutzwürdiger besonderer persönlicher Interessen nach § 4 Abs. 5 DSG NRW.
- Ermöglicht das Verfahren die Trennung personenbezogener Daten nach den Vorschriften des § 4 Abs. 6 DSG NRW?
- Sind gegebenenfalls die Anforderungen nach § 4a DSG NRW erfüllt?

- Kann das Verfahren die Rechte der Betroffenen auf Auskunft, Einsichtnahme, Widerspruch, Unterrichtung, Berichtigung, Sperrung und Löschung nach § 5 DSG NRW gewährleisten?
- Ist sichergestellt, dass Betroffene ihre Rechte ohne unvertretbaren Aufwand geltend machen können?
- Gewährleistet das Verfahren die Anforderungen an die Datenerhebung nach § 12 DSG NRW?
- Sichert das Verfahren die Zweckbestimmung nach § 13 DSG NRW?
- Gewährleistet das Verfahren gegebenenfalls die Übermittlungsgrundsätze nach §§ 14 bis 17 DSG NRW?

Die Prüfungsergebnisse der Vorabkontrolle werden zusammen mit dem Sicherheitskonzept dokumentiert.

2.6 Einzelfragen zur Datensicherheit

2.6.1 Wartung und Systembetreuung durch Externe

Arbeiten zur Wartung und Systembetreuung von DV-Anlagen beinhalten ein hohes Risiko des unbefugten Zugriffs auf personenbezogene Daten. In der Regel werden zur Durchführung der Arbeiten zwar keine personenbezogenen Daten benötigt, ihre Offenbarung kann jedoch im Störungsfall unvermeidlich sein. Wartungs- und Systembetreuungsarbeiten dürfen nur aufgrund schriftlicher Vereinbarungen erfolgen. Die veranlassten und vereinbarten technischen und organisatorischen Maßnahmen sind festzulegen. Die mit den Arbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.

Das neugefasste Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) beinhaltet nunmehr auch Regelungen zur Wartung und Systembetreuung von Einrichtungen zur automatisierten Datenverarbeitung durch Externe. Nach § 11 Abs. 4 DSG NRW unterliegen diese Arbeiten den Regelungen der Datenverarbeitung im Auftrag. Aufgrund der im Allgemeinen für diese Arbeiten erforderlichen umfangreichen Zugriffsrechte haben Auftraggeber vor Beginn der Arbeiten sicherzustellen, dass Auftragnehmer personenbezogene Daten nur zur Kenntnis nehmen können, soweit dies unvermeidlich ist. Auftragnehmer müssen ihnen zugegangene personenbezogene Daten der Auftraggeber nach Erledigung der Arbeiten unverzüglich löschen. Es wird somit verlangt, alle Möglichkeiten auszuschöpfen, um die Offenbarung personenbezogener Daten bei der Wartung und Systembetreuung durch Externe

zu verhindern. Bei der Auftragsvergabe ist denjenigen Konzepten der Vorzug zu geben, die den Zugriff auf personenbezogene Daten ausschließen.

Besonders kritisch zu betrachten ist die Möglichkeit, Wartungs- und Systembetreuungsarbeiten im Wege der Datenfernverarbeitung durchzuführen, weil hierbei Daten unmittelbar an den Auftragnehmer übermittelt werden. Um die Risiken bei diesen Arbeiten zu minimieren, ist sicherzustellen, dass

- nur dafür autorisiertes Personal die Arbeiten vornehmen kann und eine hinreichende Authentifikation erfolgt,
- alle Arbeiten nur mit Wissen und Wollen der speichernden und damit verantwortlichen Stelle erfolgen können,
- Daten nur verschlüsselt übertragen werden,
- alle Arbeiten während der Durchführung beim Auftraggeber maschinell protokolliert werden, so dass sie zu Revisionszwecken nachvollzogen werden können. Die Protokolle sind entsprechend dem Datenschutzgesetz drei Jahre aufzubewahren.
- Zugriffsrechte auf das unbedingt notwendige Maß beschränkt sind,
- bei den Arbeiten keine Programme aufgerufen werden können, die nicht benötigt werden,
- nach den Arbeiten vor Aufnahme des Echtbetriebs ein Funktionstest erfolgt, in dem überprüft wird, dass die DV-Systeme entsprechend den Vorgaben nicht unbefugt verändert worden sind.

2.6.2 Löschen von PC-Festplatten

Rasant wachsende Anforderungen führen zu immer schnelleren Austauschzyklen der PCs in Betrieben und Behörden. Doch wie steht es mit den auf ihnen gespeicherten Daten? Werden sie nicht sorgfältig gelöscht, können sie Unbefugten leicht zur Kenntnis gelangen. Es ist deshalb ein besonderes Augenmerk darauf zu richten, dass vor der Entsorgung oder Weitergabe von PCs die auf den Festplatten gespeicherten personenbezogenen Daten irreversibel gelöscht werden. Der Prozess der Löschung oder Vernichtung der Daten auf Festplatten ist insgesamt organisatorisch festzulegen. Wegen der unterschiedlichen Beschaffenheit der jeweiligen Speichermedien - beispielsweise optische Datenträger - sind Eigenheiten durch gesonderte Maßnahmen zu berücksichtigen.

Da PCs bei der Ausmusterung in der Regel noch funktionsfähig sind, wird häufig das Prinzip "Wiederverwertung vor Entsorgung und Recycling" an-

gewendet. In vielen Fällen werden die PCs einschließlich der Festplatten an Entsorgungsunternehmen oder als Spende weitergegeben. Auch ist es üblich ausgemusterte Rechner innerhalb von Behörden oder Firmen in anderen Abteilungen einzusetzen. Sind die auf den Festplatten gespeicherten Daten verschlüsselt oder hinreichend sicher gelöscht, entstehen in der Regel keine gravierenden datenschutzrechtlichen Probleme. Doch häufig werden beim Verkauf oder der Weitergabe die Festplatten nicht oder nur unzureichend gelöscht, so dass die Daten von unbefugten Dritten gelesen oder wiederhergestellt werden können. In Unkenntnis und auch mangels vorhandener leistungsfähiger Löschprogramme werden die Daten mit Kommandos wie beispielsweise Papierkorb leeren, entfernen oder formatieren vermeintlich gelöscht. Auch bei der High-Level-Formatierung (beispielsweise mit dem DOS Format-Befehl) werden Festplatten nur logisch gelöscht, so dass die Daten mit marktgängigen Tools leicht wiederhergestellt werden können. In einem Fall wurde meine Dienststelle durch ein Weiterverwertungsunternehmen darauf aufmerksam gemacht, dass PCs in größeren Zahlen von Betrieben ausgemustert wurden, ohne dass vorab eine Löschung der Daten auf den Festplatten erfolgte. Hierdurch gelangten Daten von Kundinnen und Kunden in die Hände des Unternehmens. Im Schriftwechsel mit den Auftraggeberinnen wurden die Mängel aufgezeigt und empfohlen, die Festplatten mit einem sicherem Verfahren (siehe unten) zu löschen, sowie durch ergänzende organisatorische Maßnahmen eine ordnungsgemäße Durchführung des gesamten Entsorgungsprozesses sicherzustellen. Datenschutzrechtlich gelten gespeicherte personenbezogene Daten erst dann als gelöscht, wenn sie unkenntlich sind (§ 3 Abs. 2 Nr. 6 DSG NRW und § 3 Abs. 5 Nr. 5 BDSG). Unkenntlichmachen bedeutet, dass eine Information nicht länger aus gespeicherten Daten gewonnen werden kann.

Als Verfahren für die Löschung von Daten auf Festplatten kommen in Betracht:

Low-Level-Formatierung

Bei einer Low-Level-Formatierung (LL-Formatierung) werden Spuren und Sektoren einer Festplatte physikalisch neu angelegt und die Sektoren mit einem einheitlichen Bitmuster überschrieben. Bei der LL-Formatierung sollte man auf herstellereigene Formatierungssoftware zurückgreifen. Auf einer LL-formatierten Festplatte, die mit einem einheitlichen Bitmuster nur einmal überschrieben wurde, können Restmagnetspuren nachgewiesen werden. Eine teilweise Wiederherstellung der Daten mit Hilfe spezieller Analoglesegeräte ist daher nicht auszuschließen, so dass besser eines der folgenden Verfahren angewendet wird.

Überschreiben
Bei dieser Methode wird die Festplatte komplett überschrieben. Auf dem Markt werden zahlreiche Löschprogramme angeboten, die mit dieser Methode arbeiten. Zu empfehlen sind solche Tools, die ein Mehrfachüberschreiben mit unterschiedlichen Bitmustern zulassen. Eine Rekonstruktion von Daten ist nach mehrmaligen Wiederbeschreiben mit unterschiedlichen Bitmustern laut Auskunft von Firmen, die sich auf die Wiederherstellung von Daten spezialisiert haben, nicht mehr möglich.

Behandlung mit Magnetlöschgeräten
Mit Hilfe geeigneter Magnetlöschgeräte, die die notwendigen magnetischen Feldstärken erzeugen, kann ein Wiederherstellen der Daten mit der heute zur Verfügung stehenden Technik fast ausgeschlossen werden. Dieses Verfahren hat den Vorteil, dass auch Platten, die nicht mehr funktionsfähig sind, sicher gelöscht werden können.

Zerstörung
Eine gängige Methode ist die Vernichtung der Festplatten durch Zerkleinerung (Schreddern). Hier kann die DIN 32757 Teil 1 als Vergleichsgrundlage für die Auswahl geeigneter Geräte herangezogen werden, da sie neben den Anforderungen für die Vernichtung von Papier, Filmen und Kunststoffen auch die für Metall festlegt. Auf Grund der hohen Speicherdichte der Festplatten ist das Risiko einer Rekonstruktion aus den Streifen oder Partikeln nicht unerheblich. Zu empfehlen wäre eine Kombination des Schredderns der Festplatte und eine anschließende Behandlung mit starken Magneten nach DIN 33858, insbesondere dann, wenn die Festplatten nicht mehr funktionsfähig sind.

2.6.3 Unterlagenvernichtung

Leider immer noch viel zu häufig werden ausgesonderte und zu vernichtende Unterlagen mit personenbezogenen Daten an öffentlichen Orten aufgefunden.

Um eine sichere Aussonderung und Vernichtung von Unterlagen zu erreichen, sind alle Schritte von der Zwischenlagerung in Papierkörben oder dem Sammeln der Unterlagen am Arbeitsplatz über den Transport bis hin zur zentralen Deponierung und zum eigentlichen Vernichtungsverfahren unter Sicherheitsaspekten zu betrachten. Unterlagen gelten dann als vernichtet, wenn ihre Reproduktion nur mit sehr hohem Aufwand möglich ist.

Allgemeine Anforderungen
Soweit keine spezialgesetzlichen Vorschriften einschlägig sind, unterliegt die Vernichtung von Unterlagen mit personenbezogenen Daten in den öffentlichen Stellen des Landes Nordrhein-Westfalen dem Datenschutzgesetz Nordrhein-Westfalen (DSG NRW). Bei den nicht-öffentlichen Stellen ist das Bundesdatenschutzgesetz (BDSG) dann anzuwenden, wenn es sich bei den Unterlagen um personenbezogene Daten aus Dateien handelt.

Grundsätzlich gilt, dass Unternehmen und öffentliche Stellen für die Sicherheit der Daten in Unterlagen, die vernichtet werden sollen, solange verantwortlich sind, bis die in den Unterlagen enthaltenen personenbezogenen Daten als gelöscht gelten können, die Vernichtung also abgeschlossen ist. Dies bedeutet, dass sie über alle Unterlagen mit personenbezogenen Daten bis zu deren Vernichtung die uneingeschränkte Verfügungsgewalt besitzen müssen. Insbesondere dürfen zu vernichtende Unterlagen mit personenbezogenen Daten vor Abschluss der Vernichtung nicht in das Eigentum Dritter übergehen.

Der Zustand, in dem die Unterlagen als vernichtet gelten können, ist festzulegen. Als Orientierung kann hierzu die Norm DIN 32757 (Vernichten von Informationsträgern) herangezogen werden. Hiernach ist eine Informationsträgervernichtung dann ausreichend, wenn die Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter sehr hohem Aufwand an Personen, Hilfsmitteln oder Zeit möglich ist (Sicherheitsstufe 3).

Auch für die Vernichtung von Unterlagen gilt, dass durch regelmäßige Kontrollen die ordnungsgemäße Durchführung der Vernichtung zu überprüfen ist. Daraus folgt, dass insbesondere dann, wenn die Vernichtung als Auftrag nach außerhalb vergeben wurde, der gesamte technische Vorgang oder das Verfahren bekannt sein muss. Mit der Kontrolle der Vernichtung von Unterlagen sollte eine Person oder Organisationseinheit schriftlich beauftragt werden.

Vernichten von Unterlagen in Eigenregie
Aus Gründen der Datensicherheit sollten die Unterlagen möglichst umgehend vor Ort vernichtet werden. Zwischenlagerungen - womöglich nacheinander an mehreren Orten - erhöhen das Risiko fehlerhaften Handelns und erfordern genaue Regelungen und Kontrollen. Insofern ist eine unmittelbare Unterlagenvernichtung durch die zuständige Sachbearbeitung ein wirksamer Datenschutz. In jedem Fall sollte schriftlich geregelt sein, wie Mitarbeiterinnen und Mitarbeiter die Vernichtung ihrer Unterlagen durchzuführen

haben. Daneben sind sie zu verpflichten, die Unterlagen bis zu deren Vernichtung sicher zu verwahren.

Werden Unterlagen zentral vernichtet, ist der gesamte Ablauf schriftlich zu regeln. Dies gilt beispielsweise für zentrale, besonders zu sichernde Sammelstellen, wie auch für den Transport zur Sammelstelle. Die Sicherheit der zu vernichtenden Unterlagen ist ebenfalls bis zu deren Ablieferung bei der Sammelstelle zu gewährleisten. Falls die Unterlagen durch einen zentralen Dienst eingesammelt werden, ist auch diese Phase unter Sicherheitsaspekten zu betrachten. Die Vernichtung der Unterlagen ist in geeigneter Weise zu protokollieren.

Vernichten von Unterlagen durch externe Stellen
Sollen Unterlagen durch externe Dritte vernichtet werden, so sind die Regelungen der Datenverarbeitung im Auftrag (beispielsweise § 11 DSG NRW oder § 11 BDSG) einzuhalten. Voraussetzung für eine Auftragserteilung ist, dass das zu beauftragende Unternehmen die nach den Datenschutzgesetzen notwendigen technischen und organisatorischen Maßnahmen gewährleisten kann. Die gesamte Handhabung und Sicherung der Unterlagen zwischen der Übergabe und dem Abschluss der Vernichtung einschließlich etwaiger Unterauftragsverhältnisse ist vertraglich festzulegen. Insbesondere müssen der Transport, eine eventuell erforderliche Zwischenlagerung, der Vernichtungsort und der höchstzulässige Zeitraum zwischen der Übergabe der Unterlagen sowie dem Abschluss der Vernichtung geregelt sein. Weiter ist schriftlich festzulegen, in welchem Zustand sich die Unterlagen zu befinden haben, um als vernichtet gelten zu können. Durch das beauftragte Unternehmen ist zu gewährleisten, dass Unbefugte keine Kenntnis der in den Unterlagen gespeicherten Daten erhalten können. Die Übergabe von Unterlagen an das Auftragsunternehmen sollte quittiert werden und die Durchführung jeder Vernichtungsaktion sollte schriftlich bestätigt werden. Generell gilt, dass die Erteilung von Unterauftragsverhältnissen möglichst ausgeschlossen werden sollte. Wenn das beauftragte Unternehmen keine öffentliche Stelle ist, sind die für die Unterlagenvernichtung zuständigen Beschäftigten bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.

Die auftraggebende Stelle muss über ihre Unterlagen bis zum Abschluss der Vernichtung uneingeschränkt verfügen können. Die Unterlagen müssen deshalb bis zum Abschluss der Vernichtung in ihrem Eigentum bleiben. Dies bedeutet außerdem, dass sie vor ihrer Vernichtung nicht mit fremden Unterlagen vermischt werden dürfen. Es ist deshalb auch mit dem beauftragten Unternehmen zu vereinbaren, dass die auftraggebende Stelle bis zum Abschluss der Vernichtung zu Kontrollen berechtigt ist. Sollen Sozialdaten oder ärztliche Unterlagen vernichtet werden, sind die spezialgesetzlichen

Regelungen zu beachten - beispielsweise im Sozialgesetzbuch oder im Gesundheitsdatenschutzgesetz NRW.

2.6.4 Outsourcing von Briefdruck-Service-Diensten

Unter anderem aus Kostengründen verlagern zunehmend mehr öffentliche und private Stellen ihre bisher in Eigenregie geführte Brieferstellung auf Dritte (Briefdruck, Kuvertierung, Frankierung sowie Übergabe an Postdienstunternehmen). Soll der Datenschutz hierbei nicht zu kurz kommen, ist besonders auf die Sensibilität und Anlieferung der Daten sowie auf das Vertragsverhältnis und die Kompetenz der Auftragnehmerin zu achten.

Alle Anfragen, die meine Dienststelle bisher aus dem öffentlichen Bereich erreichten, galten der Nutzung des seit 1994 eingeführten elektronischen Briefservices der Deutschen Post AG (ePost - nicht zu verwechseln mit dem seit Juni 2000 von der Deutschen Post AG angebotenen kostenlosen Internet-E-Mail-Service). Vertragsgegenstand hierbei ist die Übernahme von elektronischen Daten des Auftraggebers, die Übermittlung innerhalb des ePost-Systems, der Druck der Daten, die Produktion körperlicher Sendungen und die Übergabe der Sendungen an die Briefpost der Deutschen Post AG. Die Kunden können ihre Geschäftspost auf Datenträgern oder auf elektronischem Weg (Internet, X.25, SNA, ISDN) im ePost-Language-Format (EPL-Format) an die jeweilige ePost-Station übergeben.

Werden beim ePost-Verfahren oder bei Briefdruck-Service-Diensten anderer Anbieter personenbezogene Daten verarbeitet, ist das Kerngeschäft datenschutzrechtlich als Datenverarbeitung im Auftrag nach § 11 DSG NRW für öffentliche Stellen des Landes NRW und nicht als Postdienstleistung im Sinne des § 4 Abs. 1 PostG zu werten. Vor Anwendung des § 11 DSG NRW ist allerdings zu prüfen, ob nicht bereichsspezifische Rechtsvorschriften (wie § 80 SGB X, § 7 GDSG NW, § 30 AO) existieren, die diese Art der Datenverarbeitung regeln. Bei nicht-öffentlichen Auftraggebern gelten entsprechend die Bestimmungen des § 11 BDSG.

Bei der Auslieferung der gedruckten Schreiben an die Adressatinnen und Adressaten durch die Briefpost handelt es sich um einen Postdienst nach § 4 PostG, so dass dieses Gesetz und die Verordnung über den Datenschutz für Unternehmen, die Postdienstleistungen erbringen (Postdienstunternehmendatenschutzverordnung - PDSV), einschlägig sind.

Bei der Auftragsvergabe des Briefdruck-Services sollten neben den in § 11 DSG NRW bzw. § 11 BDSG einzuhaltenden gesetzlichen Verpflichtungen

durch den Auftraggeber auch zusätzliche Sicherheitsmaßnahmen für die Gewährleistung des Datenschutzes vertraglich fixiert werden. Beispielsweise sollte sowohl der elektronische Transport der Daten vom Auftraggeber zum Briefdruck-Service-Unternehmen als auch die elektronische Weiterleitung zu den verschiedenen Produktionsstätten des Auftragnehmers verschlüsselt erfolgen. Weitere Hinweise für die inhaltliche Vertragsgestaltung bei der Auftragsdatenverarbeitung können dem vorhergehenden Abschnitt Unterlagenvernichtung entnommen werden.

Bei Berücksichtigung der dargestellten Grundsätze begegnet es letztlich keinen datenschutzrechtlichen Bedenken, personenbezogene Daten im Rahmen der Auftragsvergabe durch Briefdruck-Service-Anbieter verarbeiten zu lassen. Werden jedoch personenbezogene Daten verarbeitet, die wegen ihrer hohen Sensibilität oder auf Grund besonderer Rechts- oder Geheimhaltungsvorschriften besonders schutzbedürftig sind, sollte wegen der prinzipiellen Möglichkeit einer Kenntnisnahme durch Mitarbeiterinnen oder Mitarbeiter des beauftragten Unternehmens - etwa durch die Systemverwaltung oder bei Stichprobenprüfungen oder bei Störfällen während der Briefproduktion - auf eine Auslagerung des Briefdruck-Services verzichtet werden.

3. Videoüberwachung

3.1 Videoüberwachung durch öffentliche Stellen ...

Jede Videoüberwachung durch öffentliche Stellen ist ein Eingriff in das Recht auf informationelle Selbstbestimmung und bedarf deshalb stets einer gesetzlichen Grundlage, die dem Verhältnismäßigkeitsgrundsatz entspricht.

3.1.1 ... eine kontrovers geführte Diskussion

Schon der 14. Datenschutzbericht 1999 thematisierte unter 3.8.1 die Videoüberwachung. Auch im jüngsten Berichtszeitraum wurde sie immer wieder intensiv diskutiert, wobei die befürwortenden und die ablehnenden Stimmen etwa gleich verteilt waren. Im Rahmen der Schaffung zweier gesetzlicher Grundlagen für die Videoüberwachung haben sich Mitglieder aller Landtagsfraktionen zu Gunsten des Datenschutzes gegen "britische Verhältnisse" ausgesprochen, also gegen eine lückenlose, flächendeckende Überwachung ganzer Straßenzüge.

Der Einsatz von Videokameras wird in der öffentlichen Diskussion oftmals als Mittel zur Verbesserung der Sicherheit genannt. Dabei wird in der Regel ein Einsatz an Orten vorgeschlagen, an denen sich häufig Drogenkranke oder Obdachlose aufhalten oder an Orten, die wegen ihrer baulichen Gegebenheiten ein Unsicherheitsgefühl bei einigen Bürgerinnen und Bürgern verursachen. Die Frage, ob die Kriminalität an diesen Orten objektiv höher ist als an anderen Orten oder ob die Videoüberwachung als Mittel gegen ein Gefühl der Unsicherheit eingesetzt werden soll, wird dabei oft nicht differenziert beurteilt. Ein Mittel, das erheblich in die Grundrechte von Bürgerinnen und Bürgern eingreifen kann, darf aber nicht zur Beseitigung einer lediglich subjektiv empfundenen bedrohlichen Lage eingesetzt werden. Videoüberwachung kann zwar dazu dienen, im Fall einer Gefahr durch Aufzeichnung Bildmaterial zu gewinnen, das für die Ahndung von Ordnungswidrigkeiten oder Straftaten oder zur Durchsetzung zivilrechtlicher Ansprüche hilfreich sein kann. Dennoch wird die Sicherheit des Ortes, der mittels Videokamera beobachtet wird, nicht erhöht, wenn keine Person "vor Ort" ist, die im Falle einer Gefährdung von Menschen oder Sachen eingreifen könnte.

Der Einsatz von Videokameras berührt immer dann datenschutzrechtliche Belange, wenn Personen auf den Bildern erkennbar sind oder mittels spezieller Techniken erkennbar gemacht werden können. Dabei ist zwischen **Beobachtung** und **Aufzeichnung** durch Videokameras zu unterscheiden.

Schon das Beobachten von Personen durch eine Videokamera stellt eine Datenerhebung dar. Diese Technik erlaubt es einer Person, mehrere Orte gleichzeitig zu beobachten, wodurch eine andere Qualität der Überwachung erreicht wird als durch den Einsatz von tatsächlich am zu beobachtenden Ort anwesenden Personen. Außerdem bleiben die Personen, die sich im Beobachtungsbereich einer Kamera befinden, darüber im Ungewissen, ob sie gerade beobachtet werden.

Vor diesem Hintergrund bestehen aus datenschutzrechtlicher Sicht folgende Mindestanforderungen an die Videoüberwachung:

- Der Einsatz von Videokameras braucht eine **normenklare gesetzliche Grundlage** und kann nicht auf allgemein gehaltene Generalklauseln gestützt werden. Dabei müssen Regelungen, die eine Aufzeichnung von Bildern erlauben sollen, restriktiver sein als die Regelungen, die eine bloße Beobachtung zulassen.
- Vor einem Einsatz von Videoüberwachung muss der Zweck der Maßnahme klar definiert und die **Geeignetheit** und **Erforderlichkeit** geprüft werden. Die Videoüberwachung darf die beobachteten Personen **nicht unverhältnismäßig** beeinträchtigen.
- Alle Personen sollten stets die Möglichkeit haben, den Ort, den sie aufsuchen wollen, zu erreichen, **ohne eine videoüberwachte Zone durchqueren** zu müssen.
- Es müssen organisatorische Vorkehrungen getroffen werden, die bei konkreten Gefahren ein **Eingreifen** zum Schutz von Personen ermöglichen.
- Es ist klar zu regeln, ob und zu welchen Zwecken Bilder aufgezeichnet werden dürfen, wobei grundsätzlich der **Zweckbindungsgrundsatz** gilt, das heißt, die Bilder dürfen nur für die Zwecke benutzt werden, für die sie aufgezeichnet wurden.
- Bilder, die nicht mehr für die im Voraus festgelegten Zwecke benötigt werden, sind unverzüglich zu **löschen.**
- Die Tatsache, dass ein Ort videoüberwacht wird, muss für die betroffenen Personen stets **erkennbar** sein. Das kann durch das Aufstellen entsprechender Hinweisschilder, die zum Beispiel ein Piktogramm und Angaben zur überwachenden Stelle enthalten, erreicht werden.
- Ferner ist sicherzustellen, dass die Personen, die auf aufgezeichneten Bildern erkannt werden, **benachrichtigt** werden, damit sie die Gelegenheit haben, die Rechtmäßigkeit des ihre Person betreffenden Grundrechtseingriffs überprüfen zu lassen.

- In regelmäßigen Abständen ist neu zu beurteilen, ob und inwieweit die Videoüberwachung noch erforderlich ist.

3.1.2 Videoüberwachung nach dem Datenschutzgesetz

Im Rahmen der Novellierung des Datenschutzgesetzes ist eine Vorschrift eingefügt worden, die öffentlichen Stellen unter bestimmten Voraussetzungen die Videoüberwachung gestattet. Dabei wurde zwischen **Beobachtung** und **Aufzeichnung** unterschieden und für letztere eine Benachrichtigungspflicht festgeschrieben. Außerdem muss die Tatsache, dass ein Gebäude videoüberwacht wird, für die betroffenen Personen erkennbar sein.

Nach § 29b DSG NRW (Optisch-elektronische Überwachung) ist die Beobachtung mittels Videokamera zulässig, soweit dies der Wahrnehmung des **Hausrechts** dient und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen betroffener Personen überwiegen. Danach setzt der Einsatz von Videokameras stets eine Abwägung zwischen den Interessen der öffentliche Stelle und den Interessen der betroffenen Personen voraus. Die Videoüberwachung kann daher nicht ohne weiteres bei allen Behörden zum Einsatz kommen.

Diese Vorschrift ermöglicht insbesondere die Videoüberwachung von Hauseingängen und -einfahrten. Diese kann sinnvoll sein, wenn die genannten Bereiche aufgrund der räumlichen Gegebenheiten nicht direkt durch eine Person beobachtet werden können. Die Regelung erlaubt aber grundsätzlich nicht die Videoüberwachung öffentlicher Straßen und Plätze. Eine **Speicherung** von Bildern ist **nur bei einer konkreten Gefahr** zu Beweiszwecken zulässig, wenn dies zum Erreichen der verfolgten Zwecke unverzichtbar ist. Das heißt, dass eine Aufzeichnung nur anlassbezogen erfolgen kann, nämlich dann, wenn erkennbar ist, dass Ordnungswidrigkeiten oder Straftaten begangen werden oder unmittelbar bevorstehen. Außerdem müssen die Aufzeichnungen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind. In den Fällen, in denen eine Aufzeichnung erfolgt ist, sind die betroffenen Personen grundsätzlich zu benachrichtigen.

3.1.3 Videoüberwachung in einem Schwimmbad

Kein Freizeitvergnügen ohne Überwachung? Videokameras halten immer mehr Einzug auch in Bereiche, wo sie eigentlich niemand bislang vermutet hat. Mit einer Videokamera wurden nach Belieben der Kassiererin weibliche und männliche Gäste beim Aus- und Ankleiden beobachtet.

Diese Erfahrung musste ein Bürger machen, der einem Freizeitvergnügen nachgehen wollte und zu diesem Zweck ein städtisches Schwimmbad aufsuchte. Dort befanden sich insgesamt elf Videokameras, davon jeweils eine Kamera in der Herren- und Damensammelumkleidekabine.

Die Videoüberwachung stellt - da auf den Bildern einzelne Personen erkennbar sind - einen Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung dar. Dieser Eingriff ist bezogen auf die Sammelumkleidekabinen deshalb besonders schwerwiegend, weil der Intimbereich der Besucherinnen und Besucher, die zumindest mit der Möglichkeit rechnen müssen, beim An- oder Auskleiden beobachtet zu werden, erheblich tangiert wird. Alle Kameras dienen der Wahrnehmung des Hausrechts. In den Sammelumkleidekabinen tritt das Hausrecht jedoch hinter die schutzwürdigen Interessen der sich dort aufhaltenden Personen zurück. Damit ist eine Videoüberwachung von Umkleidekabinen unzulässig.

Die Stadt hat die Empfehlung befolgt, die Videokameras in den Sammelumkleidekabinen zu entfernen.

3.1.4 Videoüberwachung nach dem Polizeigesetz

Im Zusammenhang mit der Novellierung des Datenschutzgesetzes wurde auch eine Regelung in das Polizeigesetz Nordrhein-Westfalen (PolG NRW) aufgenommen, die der Polizei unter strengen Voraussetzungen die Videoüberwachung von einzelnen öffentlich zugänglichen Orten erlaubt, § 15a PolG NRW. Die Videoüberwachung einzelner öffentlicher Orte ist danach nur zulässig, wenn dort wiederholt Straftaten von erheblicher Bedeutung begangen wurden und nur solange Tatsachen die Annahme rechtfertigen, dass dort weitere Straftaten von erheblicher Bedeutung begangen werden. Die Videoüberwachung muss offen erfolgen. Sofern die Beobachtung nicht offenkundig ist, ist sie durch geeignete Maßnahmen erkennbar zu machen.

Die Aufzeichnung kann nur anlassbezogen geschehen. Erst dann, wenn sich durch die Beobachtung der Verdacht einer begonnenen oder unmittelbar bevorstehenden Straftat ergibt, kann aufgezeichnet werden. Außerdem ist eine strenge **Zweckbindung** vorgesehen, die keine Ausnahmen zulässt. Die aufgezeichneten Daten sind unverzüglich zu löschen, wenn sie nicht mehr benötigt werden. Zudem besteht die Pflicht zur Benachrichtigung betroffener Personen.

Nach Inkrafttreten der Gesetzesänderung haben sich mehrere Polizeipräsidenten in der Öffentlichkeit skeptisch über den Nutzen von Videoüberwa-

chungen geäußert. Ein Polizeipräsidium plant, die Videoüberwachung jedoch mit einem Pilotprojekt zu erproben.

3.1.5 Pilotprojekt Bielefeld

In Bielefeld sollen der Ravensberger und der Rochdale Park videoüberwacht werden. Dort befinden sich unter anderem die Volkshochschule, ein Museum, die alte Hechelei, die für Großveranstaltungen genutzt wird, ein Biergarten und das Ordnungsamt.

Wie sich aus der Begründung zu § 15a PolG NRW ergibt, wollte der Gesetzgeber den Einsatz von Videoüberwachungsmaßnahmen auf Kriminalitätsbrennpunkte begrenzen (LT-Drs. 12/4780, S. 65). Der polizeilichen Auflistung von Straftaten in den von der Videoüberwachung erfassten Bereichen ist nicht zu entnehmen, dass der Ravensberger und der Rochdale Park als Kriminalitätsbrennpunkt einzuordnen wären. Im Jahr 1999 sind in 21 Fällen Ermittlungsverfahren wegen Straftaten von erheblicher Bedeutung aufgenommen worden, in den ersten sieben Monaten des Jahres 2000 in fünf Fällen. Ohne die Lage in den Bielefelder Parks zu bagatellisieren ist nicht feststellbar, dass die Kriminalitätsbelastung dort in herausstechender Weise hoch wäre. Auch fehlt es an zusätzlichen Tatsachen, die die Annahme rechtfertigen könnten, es entstehe dort ein Kriminalitätsbrennpunkt. Somit liegen die gesetzlichen Voraussetzungen für eine Videoüberwachung nicht vor.

Unter Beibehaltung dieser Rechtsauffassung habe ich zusätzlich angeregt, wenigstens überwachungsfreie Zonen in räumlicher und zeitlicher Hinsicht zu erhalten. Dies könnte die Belastung für die Betroffenen zumindest mildern.

3.2 Videoüberwachung durch Unternehmen oder Privatpersonen

3.2.1 Regelung im Bundesdatenschutzgesetz (BDSG) notwendig

Wer sich bislang gegen die Videoüberwachung in Kaufhäusern, an Tankstellen oder gar durch den Nachbarn oder Nachbarin wehren wollte, konnte im Bundesdatenschutzgesetz keine rechte Hilfe finden. Um es nicht beim alleinigen Schutz durch den zivilrechtlichen Unterlassungsanspruch zu belassen, ist eine klare Norm im Bundesdatenschutzgesetz erforderlich, die die Anforderungen an die Zulässigkeit einer Videoüberwachung festlegt und

dem "Wildwuchs" in diesem Bereich damit Grenzen zieht. Dem wird die im Gesetzentwurf für ein geändertes Bundesdatenschutzgesetz vorgesehene Bestimmung bedauerlicherweise nicht gerecht. Danach soll eine Videoüberwachung schon erlaubt sein, wenn sie zur Wahrnehmung des Hausrechts oder zur Erfüllung eigener Geschäftszwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Denn auch ein Eingriff in das Allgemeine Persönlichkeitsrecht kann nur hingenommen werden, wenn die unter 3.1.1 für das Recht auf informationelle Selbstbestimmung genannten datenschutzrechtlichen Anforderungen beachtet werden, die im Wesentlichen auch für eine Videoüberwachung öffentlich zugänglicher Bereiche durch Private erfüllt sein müssen (siehe Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 - Abdruck im Anhang, Nr. 14). Es sind folgende Gesichtspunkte hervorzuheben:

- Eine **Beobachtung** öffentlich zugänglicher Bereiche mit Videokameras ist nur zulässig, wenn sie der Gewährleistung der Sicherheit dient und zur Erreichung dieses Zweckes **erforderlich** ist. Sie ist zudem unverhältnismäßig, soweit schutzwürdige Interessen betroffener Personen das individuelle Interesse der Beobachtenden überwiegen. Ist eine Beobachtung mit Eingriffen in schutzwürdige Interessen Betroffener verbunden, muss der Schutz gewichtiger privater Rechte entgegenstehen, der auch nicht auf andere zumutbare Weise erreicht werden könnte. Außerdem darf eine Beobachtung **nicht flächendeckend** sein. In der Regel darf ein Videoeinsatz auch nicht dazu führen, dass Personen keine Möglichkeit mehr haben, etwa ihre Wohnung oder ihren Arbeitsplatz aufzusuchen, ohne videoüberwachte Zonen durchqueren zu müssen.

- Bevor eine **Aufzeichnung** von Bildern erfolgt, muss zusätzlich geprüft werden, ob die Speicherung der Bilder für die Erreichung des mit der Videoüberwachung verfolgten Zweckes **unerlässlich** ist. Gegenüber der bloßen Beobachtung stellt die Aufzeichnung einen stärkeren Eingriff in das Allgemeine Persönlichkeitsrecht der betroffenen Personen dar, weil sie dem privaten Beobachter zusätzliche Möglichkeiten der Verarbeitung von Bilddaten eröffnet. Im nicht-öffentlichen Bereich besteht auch die Gefahr einer zweckfremden Verwendung der gespeicherten Bilder, so dass besondere Vorkehrungen (etwa verbindliche Festlegung des bestimmten Zweckes, Zugriffsbefugnis und am Zweck orientierte Speicherdauer) getroffen sein müssen.

- Im Hinblick auf die Videoaufzeichnung durch Privatpersonen ist ferner die oben genannte **Benachrichtigungspflicht** unverzichtbar, wenn die aufgezeichneten Bilder einer bestimmten Person zugeordnet werden,

also eine Identifizierung erfolgt. Nur so kann sichergestellt werden, dass sich die betroffene Person wehren kann, indem sie ihren Anspruch auf **Löschung** geltend macht.

- Zur Durchführung der Kontrolle durch die Aufsichtsbehörde im nicht-öffentlichen Bereich ist eine **Anzeigepflicht** der Videoüberwachung durch private Personen oder Stellen nicht nur notwendig, um präventiv prüfen zu können, ob der Videoeinsatz unbedenklich ist. Es kann damit auch eine Übersicht über die Überwachungseinrichtungen gewonnen sowie eine bessere Unterrichtung der Parlamente und der Öffentlichkeit ermöglicht werden.

Soweit demgegenüber Videoüberwachung in **nicht öffentlich zugänglichen** Bereichen durch die Eigentümerin oder den Eigentümer stattfindet und auf das Hausrecht gestützt wird, ist der Einsatz von Videokameras weitgehend zulässig. Allerdings sind unzulässige Eingriffe in die Rechte Dritter - etwa der Mieterinnen und Mieter - denkbar, wie etwa durch verdeckte Aufnahmen oder eine Beobachtung in besonders geschützten Bereichen (siehe auch unter 3.2.2). Der Schutz vor solchen Eingriffen ist durch das Allgemeine Persönlichkeitsrecht gewährleistet.

3.2.2 Videoüberwachung zur Sicherung von Geschäfts- und Wohngebäuden

Die Überwachung erfolgt meist außen an den Häuserfronten in den Eingangsbereichen und wird auf die Wahrnehmung des Hausrechts gestützt. Teils wird aber die Überwachung exzessiv in den öffentlichen Verkehrsraum ausgedehnt, teils werden die betroffenen Personen in verschiedenen Lebenssituationen beeinträchtigt.

Die Sicherung einer **Sparkasse** durch Videoüberwachung sollte im Falle eines Banküberfalls nicht nur Kenntnis darüber verschaffen, mit welchem PKW die Täter an den Tatort gekommen waren, sondern auch über den nach dem Überfall eingeschlagenen Fluchtweg Auskunft geben, um der Polizei die Strafverfolgung zu erleichtern. Dazu sollten Videokameras an den Laternenmasten auf den gegenüberliegenden Straßenseiten zweier stark befahrener Ausfallstraßen angebracht werden und den gesamten Straßensektor wie auch einen vor der Sparkasse liegenden Parkplatz erfassen. Beabsichtigt war eine so genannte Ringspeicherung, bei der die Bilder permanent aufgezeichnet, aber nach 15 Minuten durch Überschreiben mit neuen Bildern wieder gelöscht werden. Im Alarmfall sollte alles gespeichert bleiben.

Wenn auch das Überwachungsanliegen verständlich und nachvollziehbar ist, ist es gleichwohl rechtlich nicht zulässig. Die Straßenzüge und der Parkplatz sind öffentliche Verkehrsflächen, die grundsätzlich nicht unter Berufung auf das Hausrecht überwacht werden dürfen. Nur wenn es lage- oder situationsbedingt unvermeidbar ist, öffentlichen Grund mit in die Überwachung einzubeziehen, kann dies im Ausnahmefall gerechtfertigt sein, ist aber auf das zwingend erforderliche Ausmaß zu beschränken. Bei einer solchen Prüfung sind die schutzwürdigen Belange der von der Überwachung betroffenen Personen zudem von besonderem Gewicht. Sie mit personenscharfen Aufnahmen zu erfassen, hätte die vielen Menschen, die sich auf den beiden Straßen und dem Parkplatz bewegen, einer Kontrolle und Registrierung ausgesetzt, die sie in ihren Rechten unverhältnismäßig beeinträchtigt hätte. Aufgrund dieser Rechtslage hat die Sparkasse Abstand von ihrem Vorhaben genommen.

Anders ist der Einsatz von Videokameras am **Gebäude einer Versicherung** zu bewerten. Dort dienen sechs an der Gebäudeaußenfront installierte Beobachtungskameras der Kontrolle der Tiefgarageneinfahrt sowie dem Schutz vor Einbruch und Verunreinigung der Fassaden. Die Kameras erfassen außer der Gebäudefront selbst noch einen schmalen Streifen des Bürgersteigs. Die aufgenommenen Bilder werden auf Bildmonitore übertragen. Eine Aufzeichnung erfolgt nicht, obwohl sie wegen eines angeschlossenen Aufzeichnungsgerätes technisch möglich ist. Solange durch die Kameras nur in geringem Umfang öffentlich zugänglicher Raum in nur beobachtender Weise erfasst wird und die passierenden Personen die auffällig montierten Kameras erkennen und ihnen ausweichen können, werden schutzwürdige Interessen nicht unverhältnismäßig beeinträchtigt. Um unbefugten Gebrauch zu vermeiden, habe ich allerdings sicherheitshalber empfohlen, das Aufzeichnungsgerät zu entfernen.

Bedenken begegnet allerdings beispielsweise eine Videoüberwachungseinrichtung, mit der der Eigentümer einer **Wohnanlage** eine Tiefgarage und teils private, aber öffentlich zugängliche, teils öffentliche Verkehrsflächen unter Berufung auf sein Hausrecht beobachten lässt. Die installierten Kameras übertragen die Bilder in einen mit Monitoren ausgestatteten Raum, in dem die Abläufe rund um die Uhr beobachtet werden können. Aufgezeichnet werden die Bilder nicht.

Die **Tiefgarage** wird im Wesentlichen von Personen benutzt, die einen festen Stellplatz gemietet haben. Gegen eine Überwachung bestehen grundsätzlich dann keine durchgreifenden datenschutzrechtlichen Bedenken, wenn sie ausschließlich dem Zweck dient, die sichere Benutzung der Garage zu gewährleisten, und zudem im Mietvertrag vereinbart ist. Zusätzlich müs-

sen etwaige Begleitpersonen, Besucherinnen und Besucher durch deutlich sichtbare Hinweisschilder auf die Videobeobachtung aufmerksam gemacht werden.

Anders ist die Situation im **Außenbereich**, der allgemein öffentlich zugänglich ist. Wie oben festgestellt wurde, dürfen öffentliche Verkehrsflächen grundsätzlich nicht unter Berufung auf das Hausrecht überwacht werden; allenfalls in besonders gelagerten Einzelfälle kann eine solche Überwachung ausnahmsweise gerechtfertigt sein.

Im vorliegenden Fall sind im Außenbereich zwei starre Kameras installiert, von denen die eine auf einen Wendehammer und die andere auf einen Abstellplatz für einen LKW gerichtet ist. Außerdem gibt es eine schwenkbare, mit einem Zoom-Objektiv ausgestattete Kamera, die auf einem Mast moniert ist. Die auf den - auf privatem Grund befindlichen - Abstellplatz gerichtete Kamera soll dem Schutz eines LKWs dienen. Personen, die den relativ eingeschränkten Beobachtungsraum passieren, werden nur sehr kurzfristig von der Kamera erfasst. Die Beeinträchtigung des Persönlichkeitsrechts der beobachteten Personen in diesem relativ geringen Umfang erscheint noch hinnehmbar. Demgegenüber erfasst die auf den Wendehammer gerichtete Kamera einen wesentlichen größeren Beobachtungsraum, unter anderem nicht nur den Zugang zu einem öffentlichen Kinderspielplatz und Weg, sondern auch einen der gegenüberliegenden Hauseingänge. Ziel dieser Überwachungsmaßnahme ist es, die freie Zufahrt zur Wohnanlage und zur Tiefgarage zu sichern. Eine außergewöhnliche Situation, die die Beobachtung der öffentlichen Verkehrsfläche in diesem Umfang ausnahmsweise rechtfertigen würde, ist nicht gegeben; die Überwachung ist deshalb unzulässig.

Datenschutzrechtliche Bedenken bestehen schließlich auch hinsichtlich der umfassenden Beobachtungsmöglichkeiten mit der schwenkbaren Kamera. Durch das Schwenken der Kamera ist es technisch möglich, einen großflächigen Bereich von 359° um den Montagemast herum einzusehen; mit dem Zoom-Objektiv können sogar die Kennzeichen von Fahrzeugen und die Gesichter von Personen aus 200 Meter Entfernung erkannt werden. Der Beobachtungsradius und die Detailgenauigkeit sind für die Erreichung des angestrebten Zweckes - die Wahrung der Sicherheit der Anlage - nicht erforderlich. Da für die betroffenen Personen ein Passieren des kameraüberwachten Bereichs unvermeidbar ist, stellt diese umfassende Beobachtungsmöglichkeit eine unverhältnismäßige Beeinträchtigung ihres Persönlichkeitsrechtes dar. Es muss daher durch geeignete Vorkehrungen gewährleistet sein, dass nur ein anlassbezogener Einsatz erfolgt, der auf das erforderliche Maß reduziert wird. So ließe sich etwa durch technische Veränderungen der

Schwenkbereich der Kamera eingrenzen und das Zoom-Objektiv durch ein anderes, nur den Nahbereich erfassendes Objektiv ersetzen.

Soweit der Eigentümer der Wohnanlage eine **andere Person** mit der Beobachtung **beauftragt**, muss zuvor verbindlich festgelegt werden, unter welchen Voraussetzungen die Beobachtung erfolgen darf.

Grundsätzlich ist jede Videoüberwachung öffentlicher Verkehrsflächen durch private Personen unzulässig. Ob eine Beobachtung mit einer Videokamera, die auch Teile einer solchen Fläche erfasst, ausnahmsweise hingenommen werden kann, muss in jedem Einzelfall sorgfältig geprüft werden.

3.2.3 Videoüberwachung in öffentlichen Verkehrsmitteln

Videoüberwachung macht vor U-Bahnen und Bussen nicht halt. Der Einbau solcher Überwachungsinstrumente wird mit öffentlichen Mitteln gefördert und allgemein als besondere Serviceleistung zur Sicherung der Fahrgäste vermarktet. Beobachtung und Aufzeichnung stellen allerdings nicht unerhebliche Beeinträchtigungen der Fahrgäste dar.

Geplant - und zum Teil auch schon realisiert - sind Ausstattung mit Videotechnik und Durchführung der Überwachung nach folgendem Standard: Vier Minikameras pro Wagen sollen installiert und die Standbilder in kurzem Wechsel auf einen Monitor bei der Fahrerin oder beim Fahrer übertragen werden. Daneben soll eine permanente Aufzeichnung auf einem digitalen Aufzeichnungsgerät mit einer Speicherkapazität von 24 Stunden erfolgen. Ereignet sich in dieser Zeit kein Vorfall, der entweder direkt im Wagen bemerkt oder später durch das Fahrpersonal als Schadensfall festgestellt wird, so werden die gespeicherten Bilder neu überschrieben, die alten Bilder damit gelöscht. Bei einem Vorfall wird auf die Meldung des Fahrpersonals hin von der Sicherheitsleitstelle oder einer speziell im Verkehrsunternehmen bestimmten Person der Datenträger (beispielsweise Festplatte, Diskette) oder die Videokassette dem verschlossenen Aufnahmegerät entnommen und ausgewertet. Die benötigten Bilder werden überspielt und als Beweismaterial zur Verfügung gestellt, während die übrige Aufzeichnung gelöscht wird.

Auf Initiative des Verbandes Deutscher Verkehrsunternehmen wurde erstmals in einer gemeinsamen Gesprächsrunde versucht, generelle Regeln für den Videoeinsatz in öffentlichen Verkehrsmitteln zu entwickeln, die den Verkehrsunternehmen zur Beachtung empfohlen werden sollen. Ziel ist dabei, in einer Art vorbeugendem Datenschutz bereits vor der Entscheidung

durch das jeweilige Verkehrsunternehmen Kriterien für den Einsatz von Videotechnik zu finden. Konsensfähige Kriterien könnten sein:

- Der Videoeinsatz in Bussen und Bahnen dient nur der sicheren Beförderung der Fahrgäste oder der Verhinderung von Eigentumsstörungen, muss zu diesem Zweck auch erforderlich sein und darf die Persönlichkeitsrechte der Fahrgäste nicht unverhältnismäßig beeinträchtigen.
- Eine Beobachtung ist in der Regel verhältnismäßig, soweit in den Verkehrsmitteln Zonen verbleiben, die nicht von Kameras erfasst sind, damit den Fahrgästen eine unbeobachtete Fahrt möglich ist.
- Mit der Beobachtung werden zugleich Vorkehrungen für konkrete Gefahrenlagen getroffen, damit zur Sicherheit der Fahrgäste eingegriffen werden kann.
- Eine Aufzeichnung erfolgt, wenn ein Anlass dazu besteht, etwa weil Ereignisse festgestellt werden, die die Gewährleistung der Sicherheit beeinträchtigen.
- Die Auswertung aufgezeichneter Bilder wird nur zweckentsprechend und nur durch die dazu befugte Person vorgenommen. Nicht benötigte Bilder werden unverzüglich gelöscht.
- Auf Beobachtung und Aufzeichnung sowie die verantwortliche Stelle (unter Angabe der Telefonnummer) wird deutlich sichtbar hingewiesen. Bei einer personenbezogenen Auswertung wird die betroffene Person grundsätzlich benachrichtigt.
- Die notwendigen Sicherheitsmaßnahmen sind in einer Betriebsanweisung festgelegt. Es wird in regelmäßigen Abständen überprüft, ob der Videoeinsatz noch erforderlich ist oder die Datenschutzvorkehrungen neu zu bewerten sind.

3.3 Web-Cams - nur eine andere Art der Werbung?

Öffentliche Einrichtungen - Museen, Rathäuser oder Universitäten - und private Unternehmen - Ladenpassagen oder Internetcafés - wollen auch im weltweiten Medium vertreten sein und werbend auf sich aufmerksam machen. Zu diesem Zweck setzen sie Web-Cams ein. Dabei übersehen viele zunächst, dass sie die Rechte der Menschen missachten, die sich im Bannkreis der Web-Cams aufhalten. Schon allein die Abbildung einer bestimmten Person kann eine Beeinträchtigung ihres Persönlichkeitsrechtes bewirken. Unabhängig davon verletzt jedenfalls die Verbreitung einer Aufnahme über Internet dieses Recht, soweit keine Einwilligung der betroffenen Person

vorliegt. Das unbefugte Verbreiten von Bildaufzeichnungen ist nach dem Kunsturhebergesetz zudem strafbar.

Werden Bilder in das Internet eingestellt, auf denen eine Person oder eine personenbeziehbare Angabe, etwa das amtliche Kennzeichen eines Kraftfahrzeuges oder eine auf einem Fahrzeug angebrachte Aufschrift eindeutig erkennbar ist, hat dies als **öffentliches Verbreiten personenbezogener Daten** datenschutzrechtliche Relevanz. Oft reagieren die Verantwortlichen mit dem Hinweis, es würden keine personenbezogenen Daten ins Netz gestellt. Trotz der Tatsache, dass heute auch mit zoomfähigen Web-Cams aufgenommen wird, sind sie der Überzeugung, nur Übersichtsaufnahmen gemacht zu haben, auf denen keine Personen zu erkennen sind. Dann wäre gegen solche Bilder im Internet auch nichts einzuwenden. Bei Überprüfungen stellt sich aber leider häufig heraus, dass auf den heruntergeladenen und ausgedruckten Bildern einzelne Personen zu erkennen und - jedenfalls mit Zusatzwissen - auch zu identifizieren sind. Installieren **öffentliche Stellen** Web-Cams, die Personen auf öffentlichen Plätzen oder in öffentlich zugänglichen Räumen erfassen, so übermitteln sie damit zudem unerlaubt personenbeziehbare Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs. Eine Stadt beispielsweise stellte fortlaufend Bilder vom Marktplatz ins Internet ein. Da sie diese unzulässige Praxis trotz ausführlicher Empfehlungen fortzusetzen beabsichtigte, war ihr Verhalten sogar förmlich zu beanstanden.

Weil es keine Rechtsgrundlage für eine zulässige Einstellung von Personenaufnahmen ins Internet gibt, kann sie nur auf der Grundlage einer **Einwilligung** der betroffenen Personen gerechtfertigt sein. Eine wirksame Einwilligung setzt die freiwillige Entscheidung nach umfassender Unterrichtung über die bildliche Erfassung und die Verbreitung über Internet voraus. Jede Person muss wählen können, ob Daten über sie verbreitet werden sollen - es ist zwar nur ein Bild, aber eine Aufnahme sagt über die abgebildete Person viel aus, etwa über ihre Stimmung, über ihre Tätigkeit und beispielsweise die Tatsache, dass sie sich zu einem bestimmten Zeitpunkt an einem bestimmten Ort aufgehalten hat. Wer nicht aufgenommen werden will, muss sich auch der Aufnahme entziehen können. Erkennbarkeit der Web-Cam und Wahlfreiheit hinsichtlich der Aufnahme sind deshalb unbedingte Voraussetzungen.

4. Polizei

Im Berichtszeitraum haben sich viele Bürgerinnen und Bürger an die Dienststelle gewandt und um Überprüfung der **Speicherpraxis der Polizeibehörden** gebeten. Dabei war leider festzustellen, dass für Daten, die in einem strafrechtlichen Ermittlungsverfahren erhoben wurden, oftmals ohne weiteres eine Speicherdauer von 10 Jahren vorgesehen wird. Diese - in Richtlinien vorgesehene Höchstfrist - wird häufig, unabhängig von der Schwere des Tatvorwurfs und ohne den Ausgang strafrechtlicher Ermittlungsverfahren abgefragt zu haben, festgelegt.

Wenn das Ermittlungsverfahren eingestellt wird oder ein Freispruch erfolgt, ist aber eine weitere Speicherung der Daten nur ausnahmsweise zulässig. Maßgeblich für die Zulässigkeit der Speicherung sind die Bedeutung der Straftat und die Gründe, die zur Verfahrenseinstellung oder zum Freispruch geführt haben; Letzteres nachzuhalten ist Aufgabe der für die Speicherung verantwortlichen Stelle, der Polizei. In zahlreichen Fällen mussten Akten teilweise vernichtet und Daten gelöscht oder die Speicherfristen verkürzt werden. Außerdem ist endlich **die die Führung kriminalpolizeilicher personenbezogener Sammlungen regelnde Richtlinie** (KpS-Richtlinie; siehe dazu unter 8. im 13. Datenschutzbericht 1995/96) überarbeitet worden. Insgesamt sieht die Richtlinie nun eine deutlich datenschutzgerechtere Praxis beim Umgang mit KpS vor.

Nicht die Führung einer KpS, sondern eine bedenkliche Datenerhebung eines Polizeipräsidiums im Zusammenhang mit der Abhaltung von Pressekonferenzen, gab Anlass zu einer Empfehlung. Durch das Beschwerdeschreiben eines Journalisten wurde bekannt, dass ein Polizeipräsidium bei Pressekonferenzen stets eine **namentliche Eintragung von Journalistinnen und Journalisten in ausliegende Anwesenheitslisten** verlangte; das bloße Vorzeigen des Presseausweises war nicht ausreichend. Wer sich selbst nicht eintrug, wurde handschriftlich eingetragen. Eine solche Datenerhebung mag der Polizei zwar dienlich oder nützlich sein, um zu wissen, wer auf den konkreten Fall angesprochen werden kann, erforderlich ist sie jedoch nicht. Damit müssen sowohl die eigenhändige Eintragung als auch die Eintragung durch andere Personen auf freiwilliger Basis erfolgen.

Anlässlich der Fußball-Europameisterschaft 2000 war die **Verbunddatei Gewalttäter Sport**, die der Polizei bei der Gefahrenabwehr im Zusammenhang mit Sportveranstaltungen dient, wieder einmal Thema (siehe 11. Datenschutzbericht 1991/92 unter 5.7.2). Nach einer Richtlinie des Innenministeriums NRW werden dort Personen gespeichert, die entweder strafrechtlich in Erscheinung getreten sind oder die Adressaten einer polizeilichen

Maßnahme, wie Personalienfeststellung, Platzverweis oder Ingewahrsamnahme waren, wenn zu befürchten ist, dass die betroffenen Personen sich in Zukunft an anlassbezogenen Straftaten beteiligen werden. Die Polizeibehörden orientieren sich dabei an der Richtlinie. Diese ist aus datenschutzrechtlicher Sicht insoweit zu weitgehend, als Adressaten von präventiv polizeilichen Maßnahmen bis hin zur Personalienfeststellung, die anders als im strafrechtlichen Ermittlungsverfahren nicht zwingend einer gerichtlichen Kontrolle unterliegen, in die Datei aufgenommen werden. Die Erfassung von Maßnahmen zur Gefahrenabwehr ohne strafrechtlichen Vorwurf ist nicht akzeptabel. Die gleichzeitig geforderte Prognose, dass die von der Maßnahme betroffene Person sich künftig an anlassbezogenen Straftaten beteiligen wird, ist auf der Basis einer bloßen Feststellung der Personalien nicht sachgerecht vorzunehmen. Auf Grund der Prüfung etlicher Einzelfälle ist festzustellen, dass zahlreiche Personen in der Datei Gewalttäter Sport gespeichert worden sind, ohne dass sie eine Straftat begangen haben. Die Antwort des Innenministeriums auf die Empfehlung, die Richtlinie so zu ändern, dass eine Eintragung in diese Datei nur dann erfolgt, wenn gegen die betreffende Person ein Ermittlungsverfahren eingeleitet worden ist, steht noch aus.

Im Rahmen der **INPOL-Neukonzeption** (14. Datenschutzbericht 1999 unter 3.7.3. und Entschließungen der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 und vom 10. Oktober 2000 - Abdruck im Anhang, Nr. 19 und Nr. 20) sollen die Datenbestände zahlreicher Bundesländer zukünftig beim Bundeskriminalamt (BKA) verwaltet werden. Die Verlagerung wesentlicher Teile der Landesdatenbestände zum BKA ist in dem jetzt geplanten Ausmaß nicht von den gesetzlichen Grundlagen gedeckt. Der Gesetzgeber wollte mit der Änderung des Bundeskriminalamtgesetzes (BKAG), die am 01.07.1998 in Kraft getreten ist, die Verwaltung von Länderdaten durch das BKA in Einzelfällen, aber keinesfalls flächendeckend ermöglichen. Die Auslagerung der Landesdatenhaltung auf das BKA könnte dazu führen, dass die letztlich verfassungsrechtlich bedingte Kompetenz- und Aufgabentrennung zwischen Landespolizeien und Zentralstelle faktisch schrittweise unterlaufen werden könnte.

Als Übergangslösung war zunächst eine zeitlich befristete Verlagerung der Datenbestände vorgesehen. Das Innenministerium ist jedoch an dem Angebot des BKA, die Datenverarbeitung für das Land dauerhaft zu übernehmen, sehr interessiert. Es existieren bis jetzt einige Entwürfe einer Rahmenvereinbarung, die zwischen Bund und dem jeweiligen Land geschlossen werden soll. In dieser Rahmenvereinbarung muss aus datenschutzrechtlicher Sicht klar beschrieben sein, welche Daten ausgelagert werden und nach welchen Kriterien diese durch das BKA verarbeitet werden. Dabei muss deutlich werden, dass die Verarbeitung von Landesdaten nach Landesrecht zu erfol-

gen hat und nicht nach den Vorschriften des BKAG. Das Innenministerium bleibt außerdem aufgerufen, die Voraussetzung für eine eigene Landesdatenhaltung zu schaffen. Bezeichnend ist, dass auch mehrere Jahre nach Beginn der INPOL-Neukonzeption kaum ein Land einschätzen kann, welches Datenvolumen und welche Datenbestände in die Auftragsdatenhaltung eingebracht werden sollen. Auch ein Sicherheitskonzept ist bisher noch nicht erstellt worden.

5. Telekommunikation - zwischen Grundrechtsschutz und Überwachung

Bereits im 14. Datenschutzbericht 1999 wurde unter 2.4.2.2 über die **verstärkten Überwachungstendenzen** auf Kosten des Datenschutzes berichtet. An der steigenden Tendenz hat sich in den letzten zwei Jahren allerdings leider nicht sehr viel geändert. Aufgrund der Digitalisierung der Telekommunikationsnetze hinterlässt jede Nutzung personenbezogene Spuren, die für die Dauer ihrer Speicherung ausgewertet werden können. In den gegenwärtig existierenden Mobilfunknetzen können die Teilnehmerinnen und Teilnehmer geortet werden. Die Möglichkeiten der Ausforschbarkeit werden sich noch um ein Vielfaches dann erhöhen, wenn zukünftige Mobilfunknetze (UMTS) und Handys ortsunabhängige und leistungsfähige Dienste anbieten und die bereits heute im Internet vorhandenen Recherchemöglichkeiten auch noch durch eine Ortung der Teilnehmerinnen und Teilnehmer ausgeweitet werden können.

Doch nicht nur die technische Entwicklung begünstigt die Überwachungsmöglichkeiten. Die intensivierte Zusammenarbeit auf europäischer Ebene findet auch im Bereich der Telekommunikationsüberwachung statt. Die unter der Abkürzung **Enfopol** - für Enforcement Police - stattfindende Diskussion in der Europäischen Union wird unter anderem um die Übermittlung von Überwachungsanordnungen von einem Staat an einen anderen Staat geführt. Das von den europäischen Justiz- und Innenministern im Mai 2000 unterzeichnete Europäische Rechtshilfeabkommen enthält zudem bereits Bestimmungen über die **grenzüberschreitende Überwachung** der Telekommunikation. Die Tendenz einer verstärkten internationalen Zusammenarbeit betrifft im Übrigen auch die Überwachung des Internet. So existiert zum Beispiel der Entwurf eines Übereinkommens des Europarates über Datennetzkriminalität. Die - auch auf europäischer Ebene - immer wieder erhobene Forderung nach der Verpflichtung von Internet Service-Providern zur routinemäßigen Aufbewahrung von Verkehrs-, also Nutzungsdaten hat die europäische Datenschutzkonferenz mit Beschluss vom 6./7. April 2000 als eine unzulässige Beeinträchtigung von Grundrechten zurückgewiesen.

Eine bei manchen europäischen Staaten eher Empörung hervorrufende Behauptung hat sich im Berichtszeitraum zunehmend verifiziert: Von den Vereinigten Staaten von Amerika selbst wurde mittlerweile öffentlich bestätigt, dass deren National Security Agency (NSA) in Zusammenarbeit mit dem britischen Geheimdienst und den Diensten anderer englisch-sprachiger Staaten (Australien, Neuseeland, Kanada) ein weltumspannendes Abhörsystem betreibt. Mit dem satellitengestützten System **ECHELON**, in das auch eine Station auf deutschem Boden in Bad Aibling eingebunden sein

soll, soll es möglich sein, den weltweiten Telekommunikationsverkehr unter Einsatz von Sprachdatenbanken und Spracherkennungssoftware zu überwachen. Wer E-Mails an Empfängerinnen oder Empfänger in den Vereinigten Staaten schickt oder wessen elektronische Post über Stationen in den USA geleitet wird, könnte zudem ins Visier der US-Bundespolizei FBI geraten. Dem FBI steht nämlich ein Überwachungssystem mit Namen "Carnivore" zur Verfügung, mit dem das FBI auf richterliche Anordnung hin schnell und von den Betroffenen unbemerkt Kopfinformationen von E-Mails prüfen kann.

5.1 Telekommunikationsgesetz - Forderung nach einem Gesetz zur Sicherung der freien Telekommunikation

Mit Hilfe von Ausnahmeregelungen auf Verordnungsebene ist den überschießenden gesetzlichen Überwachungsbefugnissen nicht wirklich wirksam beizukommen. Die Datenschutzbeauftragten haben sich bereits in der Vergangenheit dafür stark gemacht, dass das Telekommunikationsgesetz (TKG) selbst geändert wird. Anlass könnte bald der vorliegende Kommissionsentwurf einer Richtlinie des europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation sein. Mit dem Entwurf sollen die bisherigen Bestimmungen an neue und vorhersehbare Entwicklungen auf dem Gebiet elektronischer Kommunikationsdienste und -technologien angepasst werden. So enthält der **Kommissionsentwurf** zum Beispiel einen Regelungsvorschlag auch in Bezug auf Standortdaten, der der Tatsache Rechnung tragen soll, dass über zellulare und satellitengestützte Netze ein neuer Dienst verfügbar ist, bei dem sich die Endgeräte von mobilen Nutzerinnen und Nutzern genau lokalisieren lassen. Diese Daten, die den geografischen Standort des Endgeräts von Nutzerinnen und Nutzern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben, sollen künftig nur mit Einwilligung der Teilnehmerinnen und Teilnehmer verwendet werden dürfen. Und es soll möglich werden, die Verarbeitung der Standortdaten auf genauso einfache Weise zeitweise unterdrücken zu können, wie das für die Anzeige der Rufnummer der Fall ist.

Das **Telekommunikationsgesetz** verpflichtet alle, die geschäftsmäßig Telekommunikationsdienste anbieten, also zum Beispiel **jedes Unternehmen**, das eigene Netze oder Nebenstellenanlagen betreibt, **Kundinnen- und Kundendateien** zu führen, auf die die Sicherheitsbehörden jederzeit online und unbemerkt zurückgreifen können. Bereits im 14. Datenschutzbericht 1999 wurde unter 2.4.2.2 darauf hingewiesen, dass § 90 TKG Anbieterinnen und Anbieter von Telekommunikationsdiensten nicht verpflichtet, perso-

nenbezogene Daten von Kundinnen und Kunden zu erheben, wenn diese von den Unternehmen selbst gar nicht benötigt werden. Diese Auslegung des § 90 TKG wurde durch das Verwaltungsgericht Köln bestätigt: Die Unternehmen sind nach dem Urteil nicht gehalten, im Rahmen des Vertriebs von Prepaid-Produkten Daten von Kundinnen und Kunden zu erheben, zu überprüfen und eine Kundenidentifizierung vorzunehmen, auch wenn die Regulierungsbehörde dies zunächst verlangt hatte. Das Urteil ist allerdings nicht rechtskräftig.

Wenn die Informationsgesellschaft in Deutschland eine demokratisch und rechtsstaatlich verantwortbare Zukunft haben soll, muss der drohenden Erosion des Telekommunikationsgeheimnisses Einhalt geboten werden. Mit anderen Datenschutzbeauftragten gemeinsam habe ich mich daher für eine Sicherung der **freien Telekommunikation** in unserer Gesellschaft eingesetzt. Dafür ist insbesondere notwendig:

- Alle Telekommunikationsanbieterinnen und Telekommunikationsanbieter sind zu Datensparsamkeit und Datenvermeidung zu verpflichten. Optionen für anonyme und pseudonyme Nutzungen sind zur Verfügung zu stellen.
- Verschlüsselung ist als kostenlose Standardleistung anzubieten.
- Die Mitwirkungspflichten bei Abhörmaßnahmen sind auf lizenzpflichtige Unternehmen (wie zum Beispiel Telefongesellschaften) zu begrenzen. Nebenstellenanlagen in Hotels, Betrieben und Krankenhäusern sind auszunehmen. Die Anwendung der Überwachungsbefugnisse muss regelmäßig von unabhängiger Seite evaluiert werden.
- Datenschutzfreundliche Techniken sind zu fördern. Sie müssen erforscht, entwickelt sowie kundenfreundlich auf dem Markt angeboten werden.
- Berufliche Schweigepflichten zum Beispiel von Ärztinnen und Ärzten oder Anwältinnen und Anwälten sind besonders wirksam zu schützen.

In diese Richtung zielt auch eine **Entschließung** der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 (Abdruck im Anhang, Nr.15).

5.2 Telekommunikationsdatenschutzverordnung

Seit In-Kraft-Treten des Telekommunikationsgesetzes ist die Neufassung der Telekommunikationsdatenschutzverordnung (TDSV) überfällig gewesen. Der Bundesrat hat nun einer novellierten Fassung zugestimmt, die das

Datenschutzniveau senkt. Entgegen der Forderung der Datenschutzbeauftragten des Bundes und der Länder und der Empfehlung des Wirtschaftsausschusses können nun **Verbindungsdaten** unter Kürzung der Zielnummer bis zu **6 Monate** nach Versendung der Rechnung gespeichert werden. Im Ergebnis wird damit die Menge der Daten vergrößert, auf die Sicherheitsbehörden im Bedarfsfall zugreifen können. Das Gleiche gilt, wenn die Daten dazu dienen sollen, unberechtigt in Anspruch genommenen Leistungen auf die Spur zu kommen. Hier wurde der Zeitraum, aus dem der Gesamtbestand der Daten gebildet werden kann, von einem auf ebenfalls sechs Monate ausgeweitet.

5.3 Telekommunikationsüberwachungsverordnung

Der erste Entwurf einer Telekommunikationsüberwachungsverordnung, die die veraltete Fernmeldeüberwachungsverordnung ersetzen sollte, stand bereits im letzten Berichtszeitraum zur Debatte. Der jetzt vorliegende Referentenentwurf für eine **Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation** (Telekommunikationsüberwachungsvorordnung, TKÜV) begrenzt mit verschiedenen Regelungsinstrumenten den Umfang der Überwachungsverpflichtungen. So sollen nun im Grundsatz **vor allem die Telefongesellschaften** zum Vorhalten technischer Schnittstellen verpflichtet werden. Außerdem sind **umfangreiche Ausnahmeregelungen** vorgesehen. So sind etwa solche Telekommunikationsanlagen vom Vorhalten technischer Schnittstellen ausgenommen, mittels derer nicht mehr als 250 Endnutzerinnen und Endnutzern die Möglichkeit einer Individualkommunikation angeboten wird. Betreiberinnen und Betreiber, die keine Telekommunikationsdienstleistungen für die Öffentlichkeit anbieten, haben nach dem Entwurf allerdings auch ihrer **gesetzlichen Verpflichtung** gemäß der im **Einzelfall mit den berechtigten Stellen zu treffenden Absprachen** nachzukommen. Was immer das dann heißen mag.

5.4 Zugriff auf Telekommunikationsdaten nach dem Fernmeldeanlagengesetz

Mit einer speziellen Programmkomponente, die beispielsweise bei der Deutschen Telekom AG seit 1997 im Einsatz ist, kann eine **Zielwahl-Suche** durchgeführt werden. Durch den Abgleich von Datensätzen werden so Verbindungsdaten ermittelt. Im Jahre 1999 sind im Bereich der Deutschen Telekom AG mehr als 3000 Telefonnummern im Wege der Zielwahl-Suche

mit den Kommunikationsdatensätzen aller übrigen Anschlussinhaberinnen und -inhaber abglichen worden.

Mit richterlichem Beschluss oder bei Gefahr im Verzuge auch allein durch die Staatsanwaltschaft kann nach § 12 Abs. 1 Fernmeldeanlagengesetz (FAG) Auskunft über die Telekommunikation verlangt werden. Das betrifft sowohl den Zugriff auf **Verbindungsdaten**, die erkennen lassen, wer wann von wo aus mit wem telefoniert hat, als auch die Auskunft über den **Standort** oder das **Bewegungsprofil** eines mobilen Telefonanschlusses. Umstritten ist allerdings die Reichweite des Auskunftsanspruchs. Tendierte die Rechtsprechung in einzelnen Entscheidungen früher durchaus dazu, die Auskunft über Daten aus der Vergangenheit wie über künftig erst anfallende Daten für zulässig zu erachten, so hat sich inzwischen mehrheitlich durchgesetzt, dass dem insoweit klaren Wortlaut der Bestimmung entsprechend nur die in der Vergangenheit entstandenen Daten mitgeteilt werden dürfen.

Die Norm steht zudem seit langem in der **Kritik**. Sie sieht keine Einschränkungen hinsichtlich der Schwere der Tat vor, die es aufzuklären gilt. Vielmehr erlaubt sie auch Zugriffe wegen unbedeutender Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Auch hinsichtlich des Verdachtsgrades und der Subsidiarität ihrer Anwendbarkeit - etwa ob der angestrebte Zweck auch auf andere Weise erreichbar wäre - lässt die Bestimmung ausdrückliche Begrenzungen vermissen. In der heutigen Zeit, die von Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen gekennzeichnet ist, sind Zweifel an der Verfassungsmäßigkeit von § 12 Abs. 1 FAG angebracht. Die Datenschutzbeauftragten des Bundes und der Länder sehen mit der Bestimmung den Verhältnismäßigkeitsgrundsatz verletzt und haben sich in ihrer **Entschließung** vom 7./8. Oktober 1999 (Abdruck im Anhang, Nr. 8) gegen die - dann im Dezember 1999 beschlossene - Verlängerung der Geltungsdauer von § 12 FAG ausgesprochen.

5.5 Strenge Maßstäbe für die Einschränkung der Kommunikationsfreiheit

"Die Befürchtung einer Überwachung mit der Gefahr einer Aufzeichnung, späteren Auswertung, etwaigen Übermittlung und weiteren Verwendung durch andere Behörden kann schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen, hier insbesondere zur Vermeidung bestimmter Gesprächsinhalte oder Termini, führen. Dabei ist nicht nur die individuelle Beeinträchtigung einer Vielzahl einzelner Grund-

> rechtsträger zu berücksichtigen. Vielmehr betrifft die heimliche Überwachung des Fernmeldeverkehrs auch die Kommunikation der Gesellschaft insgesamt." (BVerfGE 100, 313/381)

Das Bundesverfassungsgericht hatte über mehrere Verfassungsbeschwerden aus dem Bereich von Presse und Wissenschaft zu entscheiden. Die Beschwerden richteten sich gegen die 1994 durch das so genannte Verbrechensbekämpfungsgesetz erweiterten **Befugnisse** des Bundesnachrichtendienstes (BND) bei der **Telefonüberwachung**. Die in der öffentlichen Diskussion vielfach als "verdachtslose Rasterfahndung" und "Staubsaugermethode" kritisierte Praxis, anhand von Suchworten die satellitengestützte Telekommunikation mit dem Ausland zu durchforsten, sah das Bundesverfassungsgericht als eine Methode an, die wegen ihrer Verdachtslosigkeit und Streubreite das Fernmeldegeheimnis aus Artikel 10 GG besonders nachhaltig berührt.

Die grundrechtlichen Bindungen und Maßgaben, die das Gericht in der Volkszählungsentscheidung an Hand des Rechts auf informationelle Selbstbestimmung entwickelt hatte, hat das Gericht mit der Entscheidung auch auf das Fernmeldegeheimnis aus Artikel 10 GG übertragen. Außerdem ist klargestellt, das Artikel 10 GG nicht nur Telefonate, sondern **jedwede Kommunikation** per Datenübertragung schützt und dass sich dieser Schutz auf den **gesamten Verarbeitungsprozess** von Telekommunikationsdaten erstreckt. Erforderlich sind danach klar definierte Zwecksetzungen für die Datenverarbeitung und die strikte Bindung an diese bestimmten Zwecke. Das Gericht hat die Möglichkeiten der **Weitergabe** von personenbezogenen Daten durch den BND an andere Behörden deutlich **eingeschränkt**.

Ein Gewinn für den Datenschutz liegt auch darin, dass eine entsprechende **Kennzeichnung** derjenigen Daten verlangt wird, die aus Eingriffen in das Fernmeldegeheimnis stammen. Und die Rechte der betroffenen Personen sind zumindest im Hinblick auf die **Kenntnis** von einem Eingriff in ihr Fernmeldegeheimnis gestärkt. Die Regelung, dass im Falle der Vernichtung der Daten binnen dreier Monate eine Mitteilung an die Betroffenen unterbleiben könnte, hat das Gericht - wie einige andere Bestimmungen auch - für **unvereinbar** mit dem Grundgesetz erklärt. Dem Bundes- und den Landesgesetzgebern ist bis Mitte 2001 aufgegeben, einen verfassungsgemäßen Zustand herzustellen. Konkrete Forderungen dafür enthält die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 "Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND" (Abdruck im Anhang, Nr. 17).

5.6 Immer mehr Telefonüberwachungen

Konnte der 14. Datenschutzbericht 1999 unter 3.5.1 noch lediglich die für das gesamte Bundesgebiet bekannte Zahl angeordneter Telefonüberwachungen nennen, so teilt inzwischen das Justizministerium erfreulicherweise die nordrhein-westfälischen Zahlen von sich aus mit. Die Zahlen selbst sind aus grundrechtlicher Perspektive allerdings weniger erfreulich. Die nach den §§ 100a und 100b der Strafprozessordnung (StPO) angeordneten Grundrechtseingriffe stiegen erneut nicht unbeträchtlich, so dass sich die schon im letzten Datenschutzbericht geäußerte Besorgnis, die Telefonüberwachung könne sich einen Platz im Standardrepertoire der Ermittlungsmaßnahmen erobern, weiter verfestigt und vergrößert hat. Gegenüber den im Jahre 1998 getroffenen 316 Anordnungen mit 829 Betroffenen stieg 1999 die **Zahl der Anordnungen um circa 34 %** auf 428 und die **Zahl der Betroffenen um circa 45 %** auf 1208. Unter Betroffenen werden dabei jedoch **nicht alle** diejenigen Personen verstanden, die an einem überwachten Kommunikationsprozess beteiligt waren, sondern nur diejenigen Personen, gegen die sich die Überwachungsanordnungen gezielt richteten, also die Beschuldigten, die als Nachrichtenmittlerinnen und Nachrichtenmittler bezeichneten Personen und die Inhaberinnen und Inhaber der von Beschuldigten genutzten Anschlüsse.

Auf einem solchen Verständnis vom betroffenen Personenkreis beruht auch die bestehende **Benachrichtigungspraxis**. Wird ein Telefonanschluss überwacht, so müssen nach § 101 Abs. 1 StPO die Beteiligten benachrichtigt werden, sobald bestimmte Voraussetzungen vorliegen, etwa der Untersuchungszweck nicht mehr gefährdet wird. Nun werden aber nicht alle Personen, die von einer Telekommunikationsüberwachungsmaßnahme erfasst wurden, auch davon benachrichtigt. Denn das Justizministerium stellt sich - entgegen der in der Literatur vertretenen Auffassung - auf den Standpunkt, dass nur diejenigen Personen zu benachrichtigen seien, gegen die die Maßnahme **gezielt gerichtet** gewesen sei. Zur Begründung dieser Position werden ausgerechnet Datenschutzbelange angeführt. So zutreffend es zwar ist, dass das Interesse der gezielt abgehörten Personen daran, dass Dritte nichts von der gegen sie gerichteten Überwachung erfahren, von großem Gewicht ist, so muss es doch Möglichkeiten geben, die **Benachrichtigung** der Dritten so zu gestalten, dass die **Datenschutzbelange** - beispielsweise der Beschuldigten - gewahrt bleiben. Grundsätzlich sollten alle Personen, in deren Grundrechte mit Überwachungsmaßnahmen eingegriffen wird, von diesen Eingriffen unter Wahrung der Datenschutzrechte anderer Personen unterrichtet werden. Sind die zufällig mit abgehörten Personen allerdings nicht bekannt, dürfte es nicht mehr verhältnismäßig sein, Nachforschungen zu ih-

rer Ermittlung zu verlangen, zumal dadurch neue Datenschutzprobleme entstehen könnten.

Selbst wenn sicherlich mit zu bedenken ist, dass es immer mehr Mobiltelefone gibt, kann dieser Umstand allein den dramatischen Anstieg der Überwachungszahlen vermutlich nicht hinreichend erklären. So ist es sehr zu begrüßen - und entspricht einer seit langem erhobenen Forderung der Datenschutzbeauftragten -, dass das Bundesministerium für Justiz "Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b Strafprozessordnung (StPO)" erforschen lässt. Mit dem in Auftrag gegebenen **Forschungsvorhaben** sollen Erkenntnisse gewonnen werden, mit denen die **Notwendigkeit und Erfolgseignung von Überwachungsmaßnahmen** beurteilt werden können. Von Bedeutung sollte dabei auch die Frage sein, in welchem Umfang unbeteiligte Dritte von der Überwachung betroffen werden. Nicht zuletzt ist es erforderlich, die staatlichen Befugnisse auf ihre Effektivität im Verhältnis zur Intensität des Grundrechtseingriffs zu überprüfen. Etwas umgangssprachlicher ausgedrückt wäre zu fragen, ob die Erfolge der Überwachung bedeutsam genug sind, um den grundrechtlichen Preis rechtfertigen zu können, der dafür gezahlt wird oder ob dieser Preis zu hoch ist.

6. Strafverfahren, Strafvollzug, Maßregelvollzug

6.1 Datenschutz im Strafverfahren

Das Strafverfahrensänderungsgesetz '99 (StVÄG) trat im Herbst 2000 in Kraft. Im Zentrum des Gesetzes steht eine Novellierung der Strafprozessordnung (StPO), die bereits seit dem Volkszählungsurteil vom 15.12.1983 überfällig war. Mit der Novellierung wurden Maßnahmen wie die längerfristige Observation, die Fahndung - auch nach Zeuginnen und Zeugen - in der Öffentlichkeit sowie die Verarbeitung und Nutzung personenbezogener Daten in Dateien der Strafverfolgungsbehörden auf eine gesetzliche Grundlage gestellt.

Außerdem erlaubt die Neuregelung der StPO den Strafverfolgungsbehörden bestimmte personenbezogene Daten, die in einem Strafverfahren erhoben wurden, für **Zwecke künftiger Strafverfahren** zu verarbeiten. Daneben können Daten, die die Polizei zu Zwecken der Prävention erhoben hat, von der Staatsanwaltschaft für die Strafverfolgung genutzt werden. Allerdings gibt es für Informationen aus einem präventiv-polizeilichen "Großen Lauschangriff" gewisse Einschränkungen. Umgekehrt ist es den Polizeibehörden grundsätzlich möglich, personenbezogene Informationen aus Strafverfahren zu verwenden.

Leider wurde dabei dem Grundsatz der Datensparsamkeit kein großes Gewicht beigemessen. Die Strafverfolgungsbehörden wurden ermächtigt - zusätzlich zum Zentralen Staatsanwaltlichen Verfahrensregister, das bereits 1994 durch das Verbrechensbekämpfungsgesetz eingeführt worden ist - eigene Dateien zu benutzen und zu betreiben. Der Gesetzgeber stellt dabei lediglich darauf ab, dass die Datei "für Zwecke des Strafverfahrens" erforderlich ist, er hat aber davon abgesehen, den Datenumfang und den von der Datenverarbeitung betroffenen Personenkreis festzulegen. Diese Regelungen soll die datenverarbeitende Stelle selbst in einer Errichtungsanordnung bestimmen. Nach dem Grundsatz des Gesetzesvorbehaltes hätte der Gesetzgeber hier selbst präzisere Vorgaben für diese Dateien formulieren müssen.

Die **längerfristige Observation** ist auch ohne richterliche Anordnung möglich und kann bei Gefahr im Verzug sogar durch die Polizei angeordnet werden. Es ist bedenklich, dass eine solche einschneidende Maßnahme ohne die Überprüfung durch unabhängige Richterinnen oder Richter durchgeführt werden darf. Bedenklich ist auch, dass eine Benachrichtigung der betroffenen Personen bei dieser Maßnahme nicht vorgesehen ist, so dass die betroffenen Personen nicht einmal die Möglichkeit haben, die Rechtmäßigkeit dieser Maßnahme gerichtlich überprüfen zu lassen.

Die Öffentlichkeitsfahndung stellt ebenfalls einen tiefen Eingriff in das Persönlichkeitsrecht der betroffenen Personen dar. Gefahndet werden kann nach Tatverdächtigen und nach Zeuginnen und Zeugen. Dabei besteht die Gefahr, dass in der Öffentlichkeit im Zusammenhang mit einer Straftat Personen gesucht werden, die sich als unschuldig erweisen oder Zeuginnen und Zeugen von der Öffentlichkeit nicht als solche wahrgenommen, sondern als Tatverdächtige betrachtet werden.

Die **Sammlung** personenbezogener Daten durch die Strafverfolgungsbehörden **für Zwecke künftiger Strafverfahren** ist nicht erforderlich. Denn die Datenerhebung aus Präventionsgründen fällt in den Aufgabenbereich der Polizei, die auch über entsprechende Dateien verfügt.

Das StVÄG regelt auch Auskunfts- und Akteneinsichtsrechte. Bei der Auskunftserteilung an öffentliche Stellen ist lediglich zu prüfen, ob die Daten für bestimmte Zwecke erforderlich sind, eine Abwägung mit den Interessen der betroffenen Person ist dagegen leider nicht vorgesehen. Zu begrüßen ist aber, dass das StVÄG auf die besonderen Nutzungsbeschränkungen abstellt, die sich aus den polizeirechtlichen bzw. strafprozessualen Vorschriften über den Einsatz nachrichtendienstlicher Mittel ergeben.

Zusammenfassend bleibt festzustellen, dass auch die geänderte Strafprozessordnung beim Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgung die Persönlichkeitsrechte der betroffenen Personen nicht immer angemessen berücksichtigt.

6.2 Strafvollzug

6.2.1 Kontrolle der Gefangenenpost

Streit um die Zulässigkeit der flächendeckenden Kontrolle von Gefangenenpost

Die **Überwachung des Schriftverkehrs** von Gefangenen bildete bereits in der Vergangenheit wiederholt den Grund für Beschwerden von Betroffenen. Auch im Berichtszeitraum gab es damit wieder Probleme. In einigen Justizvollzugsanstalten ist aus Gründen der Sicherheit der Anstalt die Kontrolle des **gesamten** Schriftverkehrs aller Gefangenen angeordnet worden. Diese Praxis widerspricht § 29 Strafvollzugsgesetz (StVollzG), der im Grundsatz vorsieht, dass die Post von Gefangenen nicht kontrolliert wird. Die Kontrolle kann **ausnahmsweise** dann erfolgen, wenn dies aus Gründen der

- etwa medizinischen - Behandlung oder der Sicherheit oder Ordnung der Anstalt erforderlich ist.

Die **Überwachung des Briefverkehrs** der Gefangenen schränkt ihre Kommunikation mit der Außenwelt ein. Sie stellt einen Eingriff in das Grundrecht aus Art. 10 GG dar und muss sich deshalb am Verhältnismäßigkeitsmaßstab messen lassen. Die Gründe, die für eine Überwachung sprechen, müssen objektivierbar und konkretisierbar sein. Nach § 81 Abs. 2 StVollzG sind die Pflichten und Beschränkungen, die den Gefangenen zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt auferlegt werden, so zu wählen, dass sie in einem angemessenen Verhältnis zu ihrem Zweck stehen und die Gefangenen nicht mehr und nicht länger als notwendig beeinträchtigen. Es ist daher im Einzelfall, also für jede einzelne Gefangene und für jeden einzelnen Gefangenen zu prüfen, ob die Voraussetzungen einer zulässigen Postkontrolle vorliegen. Da die Anordnung einer alle umfassenden Postkontrolle auch in die Rechte derjenigen Gefangenen eingreift, die die Sicherheit oder Ordnung der Anstalt überhaupt nicht gefährden, ist sie unverhältnismäßig. Das Justizministerium ist der Empfehlung, die bestehende Praxis zu ändern und die Kontrolle der Gefangenenpost einzelfallbezogen zu regeln, bedauerlicherweise nicht gefolgt.

Unter Beibehaltung der eben dargestellten Rechtsauffassung wurde das Justizministerium gebeten zu prüfen, ob alternativ mildere Maßnahmen zur umfassenden Kontrolle des Briefverkehrs ergriffen werden können. Ausgehend von dem Grad des Sicherheitsbedürfnisses der jeweiligen Anstalt könnte beispielsweise eine **Sichtkontrolle** (statt der Textkontrolle) der eingehenden oder ausgehenden Post ausreichen. Auch wäre denkbar, die eingehende Post **im Beisein** der Empfängerinnen und Empfänger zu öffnen. Darüber hinaus sollte festgelegt werden, dass jeweils **nur eine oder einer der Bediensteten** die Briefkontrolle vornimmt. Im Übrigen käme auch in Betracht, die Gefangenen je nach Grad der Sicherheitsgefährdung in verschiedenen Anstalten unterzubringen. In einigen Justizvollzugsanstalten könnte dann eventuell ganz auf eine Briefkontrolle verzichtet werden.

6.2.2 Namensgleichheit und Postzustellung

Wenn zwei Personen denselben Namen tragen, hat das nicht immer nur harmlose Konsequenzen.

Aus den Fällen, in denen die Aushändigung von Postsendungen an falsche Adressatinnen oder Adressaten zu Nachteilen für Inhaftierte geführt haben, sei nur ein besonders eklatantes Beispiel herausgegriffen. Hier wurde der

Brief einer Staatsanwaltschaft fälschlicherweise an einen Mitgefangenen mit gleichem Vor- und Familiennamen ausgehändigt. In diesem Schreiben ging es um die Aberkennung des Sorgerechts im Zusammenhang mit einem sexuellen Missbrauch. Der Inhalt des Briefes wurde unter den Mitgefangenen in der Justizvollzugsanstalt schnell bekannt. Weil der eigentliche Adressat des Schreibens daraufhin massiv bedroht wurde, musste er in eine andere Justizvollzugsanstalt verlegt werden. Eine geplante Resozialisierungsmaßnahme konnte dann nicht mehr durchgeführt werden.

Die Justizvollzugsanstalt hat für die Zukunft eine besonders sorgfältige Überprüfung bei der Aushändigung von Post zugesagt.

6.2.3 Eine Weihnachtsfeier im Knast – und kein Geld

Auch aus Anlass einer Weihnachtsfeier ist es nicht zulässig, Daten über die Zahlungsfähigkeit eines Gefangenen an Mitgefangene zu übermitteln.

In einer Justizvollzugsanstalt wurde von Inhaftierten eine Weihnachtsfeier für die Mitgefangenen organisiert. Die Teilnahme an dieser Feier setzte voraus, dass die Inhaftierten sich an den Kosten dieser Veranstaltung beteiligten. Ein Gefangener konnte an der Feier nicht teilnehmen, da ihm keine Geldmittel zur Verfügung standen. Dies wurde den Organisatoren durch einen Bediensteten der Justizvollzugsanstalt mitgeteilt.

Auf meine Empfehlung hin hat das Justizministerium sichergestellt, dass Auskünfte über die wirtschaftlichen Verhältnisse von Gefangenen grundsätzlich nicht mehr an Mitgefangene weitergegeben werden.

6.2.4 Installation einer Wächterschutz- und Kontrollanlage

Datenschutz gilt auch für die Bediensteten in den Justizvollzugsanstalten.

Dass nicht nur der Umgang mit den personenbezogenen Daten der Inhaftierten Probleme bereitet, zeigt ein Fall, in dem sich der Personalrat einer Justizvollzugsanstalt an meine Dienststelle gewandt hat. Dort waren im Rahmen von Rationalisierungsmaßnahmen verschiedene computergesteuerte Systeme - unter anderem eine so genannte Wächterschutz- und Kontrollanlage sowie eine Kameraüberwachungsanlage - installiert worden. Dabei stellte sich die Anstaltsleitung auf den Standpunkt, durch das System wür-

den keine personenbezogenen Daten verarbeitet, obwohl damit unter anderem das Verhalten der Bediensteten ausgewertet werden kann.

Die Dienstanweisung zum Umgang mit dem System wies erhebliche Mängel auf. So war es zum Beispiel unzulässigerweise möglich, die Daten zur Leistungskontrolle der Bediensteten auszuwerten. Ferner war der Verwaltungsleiter, dem auch die Systemadministration oblag, (quasi als sich selbst kontrollierender) Beauftragter für den Datenschutz vorgesehen. Welchen Stellenwert die Datenschutzproblematik dabei für die betroffene Justizvollzugsanstalt einnimmt, zeigt der Umstand, das sie zwischenzeitlich zwar zugesagt hatte, statt des Verwaltungsleiters einen anderen Mitarbeiter, der nicht als Administrator in der Datenverarbeitung tätig ist und auch sonst keine dienstrechtliche Leitungsfunktion wahrnimmt, mit der Aufgabe des Datenschutzbeauftragten zu betrauen. In der aktuellen Dienstanweisung ist jedoch wiederum der Verwaltungsleiter als Beauftragter für den Datenschutz festgelegt worden.

6.3 Maßregelvollzugsgesetz

Auch Straftäterinnen und Straftäter, die wegen psychischer Erkrankungen in psychiatrischen Krankenhäusern und Entziehungsanstalten untergebracht sind (Maßregelvollzug), besitzen das Recht auf informationelle Selbstbestimmung.

Seit dem 16. Juli 1999 gilt in Nordrhein-Westfalen das neue Maßregelvollzugsgesetz, durch das die Zuständigkeiten neu geregelt wurde. War es früher Aufgabe der Landschaftsverbände den Maßregelvollzug durchzuführen, hat jetzt das Land die umfassende Zuständigkeit für den Maßregelvollzug. Neu geschaffen wurde auch die Einrichtung eines Maßregelvollzugsbeauftragten, der bisherige Aufgaben und Zuständigkeiten der Zentralverwaltung der Landschaftsverbände, der Bezirksregierung und des Ministeriums zusammenfasst und umfassend Aufsicht über die Einhaltung aller Vorschriften führt.

Im Maßregelvollzug leben Täterinnen und Täter, die wegen psychischer Erkrankungen schuldunfähig oder vermindert schuldfähig sind und bei denen das Begehen weiterer Straftaten zu erwarten ist. Auch wenn sich der Maßregelvollzug vom Strafvollzug in einigen Punkten unterscheidet - im Gegensatz zur Freiheitsstrafe ist beispielsweise die Unterbringung im Maßregelvollzug nicht von vorneherein zeitlich befristet - besteht aus datenschutzrechtlicher Sicht kein Grund für eine Schlechterstellung der untergebrachten Personen gegenüber den Strafgefangenen.

Vor diesem Hintergrund hat sich meine Dienststelle im Rahmen der Novellierung des Maßregelvollzugsgesetzes NRW für die Stärkung der Datenschutzrechte der Betroffenen eingesetzt. Den Anregungen ist in Teilen Rechnung getragen worden.

So ist beispielsweise in Angleichung an die entsprechende Bestimmung des Strafvollzugsgesetzes auch im Maßregelvollzugsgesetz der ungehinderte Schriftwechsel mit den Datenschutzbeauftragten des Bundes und der Länder aufgenommen worden. Der Gesetzesentwurf sah unter anderem vor, dass eine Überwachung von Außenkontakten (Besuche, Post, Telekommunikation) sowie die Durchsuchung der Räume der Betroffenen, ihrer Sachen und der Betroffenen selbst auch ohne konkrete Verdachtsgründe zu Kontrollzwecken erlaubt sein sollte. Angesichts der Tatsache, dass es sich hierbei um Bereiche mit hoher Eingriffsintensität handelt, war aus datenschutzrechtlicher Sicht zu fordern, dass Eingriffe nur "bei zwingenden Anhaltspunkten für eine erhebliche Gefährdung der Therapie oder des geordneten Zusammenlebens" zulässig sind. Diese Forderung ist - wenn auch in abgeschwächter Form - insoweit übernommen worden, als nach dem neuen Maßregelvollzugsgesetz "zwingende Gründe" für einen entsprechenden Eingriff in die oben genannten Bereiche vorliegen müssen.

7. Verfassungsschutz

Das Tagebuch einer Person, die sich am bewaffneten Kampf der PKK in Kurdistan beteiligt hatte, fand sich im Internet auf der Homepage des nordrhein-westfälischen Verfassungsschutzes. Das Tagebuch umfasste einen Zeitraum von einem Jahr, in dem die betreffende Person über ihr Leben und den Kampf in Kurdistan berichtete. Dabei wurde zwar nicht der Klarname preisgegeben, aber auch die Veröffentlichung der Informationen unter dem Decknamen, den die Person benutzt hatte, ist ein Eingriff in das Recht auf informationelle Selbstbestimmung, der keine gesetzliche Grundlage hat.

§ 15 Abs. 2 Verfassungsschutzgesetz (VSG) erlaubt der Verfassungsschutzbehörde die Veröffentlichung von Informationen zum Zwecke der Aufklärung der Öffentlichkeit über Bestrebungen und Tätigkeiten nach § 3 Abs. 1 VSG. Die Veröffentlichung personenbezogener Daten ist jedoch nur dann zulässig, wenn die Bekanntgabe für das Verständnis des Zusammenhangs oder der Darstellung von Organisationen erforderlich ist und die Interessen der Allgemeinheit das schutzwürdige Interesse der betroffenen Person überwiegen. Die Veröffentlichung des Tagebuchs war aber weder zum Verständnis des Zusammenhangs noch zur Darstellung der Organisation PKK erforderlich. Die Beschreibung der Strukturen der PKK kann in mindestens ebenso verständlicher Form durch einen Bericht der Verfassungsschutzbehörde ohne Verwendung personenbezogener Daten erfolgen.

Nachdem die betroffene Person sich an den Verfassungsschutz gewandt hatte, wurden die entsprechenden Seiten gelöscht. Hinsichtlich der Rechtmäßigkeit der Veröffentlichung des Tagebuchs bestehen zwischen dem Verfassungsschutz und meiner Dienststelle zur Zeit noch erhebliche Differenzen. Eine endgültige Stellungnahme steht aber noch aus.

Dem 14. Datenschutzbericht 1999 gingen umfangreiche Kontrollbesuche beim Verfassungsschutz voran. Die dort unter 3.6 thematisierten unterschiedlichen Standpunkte und Rechtsauffassungen sollten ursprünglich nochmals in einem Abschlussgespräch mit dem Verfassungsschutz diskutiert werden. Dazu konnte es unter anderem auf Grund personeller Engpässe bei extremer Arbeitsbelastung in diesem Berichtszeitraum noch nicht kommen. Das Thema bleibt weiterhin auf der Tagesordnung.

8. Ausländerinnen und Ausländer

8.1 "Ehe-TÜV" für binationale Paare

Binationale Partnerschaften, die eine Eheschließung beabsichtigen, werden häufig von den Standesämtern daraufhin überprüft, ob sie wirklich den Willen haben, eine eheliche Lebensgemeinschaft zu führen. Am 01.07.1998 wurde mit Verabschiedung des Eheschließungsrechtsgesetzes sowohl das Personenstandsgesetz (PStG) als auch das Bürgerliche Gesetzbuch (BGB) geändert. Dadurch wurden die Rechte und Pflichten der Standesämter klar geregelt. Außerdem wurde festgelegt, dass eine Ehe aufzuheben ist, wenn beide Ehegatten sich bei der Eheschließung darüber einig waren, dass sie sich nicht zur Führung einer ehelichen Lebensgemeinschaft verpflichten wollten. Dies gilt für alle Ehepaare unabhängig von der Nationalität der Partner. In der Praxis werden diese Vorschriften jedoch fast ausschließlich auf deutsch-ausländische Ehen angewendet.

Bestehen konkrete Anhaltspunkte dafür, dass die zu schließende Ehe nach den Vorschriften des Bürgerlichen Gesetzbuches aufhebbar wäre, können die Standesbeamtinnen und Standesbeamten die Verlobten in dem hierzu erforderlichen Umfang einzeln oder gemeinsam befragen und ihnen die Beibringung geeigneter Nachweise aufgeben; notfalls kann auch eine eidesstattliche Versicherung über Tatsachen verlangt werden, die für das Vorliegen oder Nichtvorliegen von Aufhebungsgründen von Bedeutung sind.

Damit ist die **Aufnahme von Ermittlungen** an eine bestimmte Schwelle geknüpft. Das Erfordernis des Vorhandenseins "konkreter Anhaltspunkte" schließt jedenfalls Ermittlungen durch die Standesbeamten in den Fällen aus, in denen lediglich bloße Vermutungen über das Vorliegen einer so genannten Scheinehe angestellt werden. Die Standesbeamten haben kein beliebiges Nachforschungsrecht. Die geforderten Anhaltspunkte dürfen sich außerdem nicht mehr allein auf das Merkmal "ausländische Staatsangehörigkeit" beziehen, da das Gesetz das Aufenthaltsmotiv nicht mehr enthält. Deshalb reicht auch ein genereller Pauschalverdacht in den Fällen, in denen einer der Verlobten eine ausländische Staatsangehörigkeit besitzt, nicht aus.

Wie sich aus der Formulierung des Gesetzes ergibt, ist es erforderlich, dass mindestens zwei konkrete Anhaltspunkte vorliegen müssen, damit die Eingriffsschwelle überschritten wird. Um dem Verhältnismäßigkeitsgrundsatz zu genügen, bedarf es darüber hinaus aber vor der Aufnahme von Ermittlungen auch einer Gesamtwürdigung aller - bereits vor der Aufnahme von Ermittlungen bekannten - Umstände des jeweiligen Einzelfalls, bei der auch

solche Lebenssachverhalte berücksichtigt werden, die gegen die Annahme einer beabsichtigten so genannten Scheinehe sprechen.

Der Rat der Europäischen Union hat am 04.12.1997 in einer Entschließung dargelegt, welche Kriterien für die Annahme einer so genannten Scheinehe sprechen. Als Indizien gelten danach: die fehlende Aufrechterhaltung der Lebensgemeinschaft, das Fehlen eines angemessenen Beitrags zu den Verpflichtungen aus der Ehe, die Ehegatten sind sich vor ihrer Ehe nie begegnet, die Ehegatten machen widersprüchliche Angaben hinsichtlich ihrer jeweiligen Personalien (Name, Adresse, Staatsangehörigkeit, Beruf), der Umstände ihres Kennenlernens oder sonstiger sie betreffender wichtiger persönlicher Informationen, die Ehegatten sprechen nicht eine für beide verständliche Sprache, für das Eingehen der Ehe wird ein Geldbetrag übergeben (abgesehen von den im Rahmen einer Mitgift übergebenen Beträgen bei Angehörigen von Drittländern, in denen das Einbringen einer Mitgift in die Ehe gängige Praxis ist), es gibt Anhaltspunkte dafür, dass ein oder beide Ehegatten schon früher Scheinehen eingegangen sind oder sich unbefugt in einem Mitgliedstaat aufgehalten haben. Diese Entschließung ist für die Mitgliedstaaten der Europäischen Union zwar nicht verbindlich, sie ist jedoch eine Arbeitsgrundlage für die zuständigen Behörden. Die in der Entschließung genannten Gründe beziehen sich auf die Situation, in der bereits eine Ehe geschlossen worden ist und sind insoweit Orientierungshilfen für die Ausländerbehörden, die ebenfalls bei Vorliegen von Anhaltspunkten für eine so genannte Scheinehe ermitteln. Allerdings richten sich die Standesämter auch nach diesen oder ähnlichen Kriterien.

Einige der genannten Umstände können allerdings nicht ohne weiteres als konkrete Anhaltspunkte für die Aufnahme von Ermittlungen dienen. Beispielsweise können auch Paare mit einem großen Altersunterschied lebenslange eheliche Partnerschaften führen; der Wille zur Führung einer ehelichen Gemeinschaft setzt ersichtlich auch keinen gemeinsamen Wohnsitz voraus. Auch die fehlende Aufenthaltsgenehmigung des ausländischen Teils des Paares spricht noch nicht gegen das Bestehen einer ehelichen Lebensgemeinschaft. Kann sich das Paar allerdings nicht in einer gemeinsamen Sprache verständigen, spielen Geldzahlungen eine Rolle oder kennen sich Partnerin und Partner überhaupt nicht, so kann dies zusammen mit anderen Indizien durchaus Anlass zu weiteren Ermittlungen geben.

Die möglichen **Ermittlungstätigkeiten** der Standesbeamtinnen und Standesbeamten sind in § 5 Abs. 4 PStG abschließend geregelt. Danach ist eine gemeinsame oder getrennte Befragung der Verlobten in dem erforderlichen Umfang zulässig sowie die Anforderung geeigneter Nachweise und **notfalls**

auch eine eidesstattliche Versicherung über Tatsachen, die für das Vorliegen oder Nichtvorliegen von Aufhebungsgründen von Bedeutung sind.

Die Bestimmung überlässt den Standesbeamtinnen und -beamten lediglich die Auswahl der Mittel, die sie nach Maßgabe des Grundsatzes der Verhältnismäßigkeit zu treffen haben. Die Ermittlungen haben sich auf Tatsachen zu beschränken, die für das Vorliegen oder Nichtvorliegen von Aufhebungsgründen von Bedeutung sind. Dabei ist das allgemeine Persönlichkeitsrecht der betroffenen Personen zu beachten. Fragen, die sich auf die Intimsphäre der betroffenen Personen beziehen, insbesondere Fragen nach ihrem Gefühlsleben, sind zu unterlassen. Auch Fragen nach der Aufteilung der Hausarbeit, die in Fragekatalogen enthalten sind, die von deutschen Auslandsvertretungen erstellt wurden und einigen Ausländerbehörden vorlagen, sind nicht zulässig. Auch das von einigen Standesämtern praktizierte Verfahren, die gesamte Ausländerakte anzufordern, ist wegen der Masse der Überschussinformationen, die für die Aufgabe der Standesämter nicht erforderlich sind, datenschutzrechtlich unzulässig.

Auch die Ausländerbehörden haben bei ihren Ermittlungen den Verhältnismäßigkeitsgrundsatz zu beachten und zum Beispiel zunächst die Betroffenen zu befragen, bevor weitere Personen befragt oder Hausbesuche durchgeführt werden. Sowohl bei Befragungen als auch bei der Durchführung von Hausbesuchen darf die Intimsphäre der betroffenen Personen nicht angetastet werden.

Vor dem Hintergrund der gesetzlichen Änderungen und einiger Beschwerden wurden im Jahr 2000 etliche Ausländer- und Standesämter nach deren Umgang bei den Ermittlungen im Zusammenhang mit so genannten Scheinehen befragt. Dabei ging es sowohl um die Frage, welche Umstände Anlass zu Ermittlungen geben als auch um die Art der durchgeführten Ermittlungen und um die Verarbeitung der erhobenen Daten.

Nach dem Ergebnis der **Befragung** führen die Standesämter bei deutsch-ausländischen Paaren in ca. 6%, bei deutschen Paaren in 0,1% der Fälle Ermittlungen durch. In ca. 9% der Fälle, in denen Ermittlungen durchgeführt wurden, verweigerten die Standesämter anschließend ihre Mitwirkung an der Eheschließung.

Einige **Standesämter** sehen unzulässigerweise bereits dann Anlass zu weiteren Ermittlungen, wenn ein Teil des Paares Ausländer oder Ausländerin ist oder wenn die Ehewilligen nicht unter derselben Adresse gemeldet sind, wenn die Ehewilligen unterschiedliche Sprachen sprechen, auch wenn sie sich miteinander verständigen können. Wenn Ermittlungen durchgeführt

werden, werden die Ehewilligen in der Regel gemeinsam oder getrennt befragt, wobei ein Standesamt angab, auch nach dem Intimleben der Ehewilligen zu fragen, was nicht erlaubt ist. Außerdem ziehen zahlreiche Standesämter die gesamte Ausländerakte bei, was unverhältnismäßig ist. Selten werden auch Hausbesuche durchgeführt, was allerdings die vom Gesetzgeber festgesetzten Grenzen überschreitet. Zum Teil werden auch Dritte befragt, wobei diese nicht immer auf die Freiwilligkeit der Mitwirkung hingewiesen werden. Einige Standesämter scheinen auch regelmäßig eine eidesstattliche Versicherung zu verlangen, in der die Ehewilligen erklären müssen, dass sie sich zur Führung einer ehelichen Lebensgemeinschaft verpflichten wollen. Ob dabei immer berücksichtigt wird, dass dieses Mittel nach dem Wortlaut des Gesetzes nur "notfalls" zur Anwendung kommen soll, konnte nicht eindeutig geklärt werden.

Die **Ausländerämter** führen in der Regel dann Ermittlungen durch, wenn ihnen durch andere Behörden oder Privatpersonen Umstände bekannt werden, die ein Indiz für das Vorliegen einer so genannten Scheinehe sein könnten. Dabei gehen sie auch anonymen Hinweisen nach. Routinemäßige Überprüfungen bestehender Ehen werden eher selten vorgenommen. Auch die Ausländerämter führen bei Anhaltspunkten für das Nichtbestehen einer ehelichen Lebensgemeinschaft Befragungen der Ehepartner durch und beauftragen auch sehr häufig den Außendienst mit der Durchführung von Hausbesuchen, die in der Regel unangekündigt stattfinden. Dabei werden die Wohnverhältnisse besichtigt, und oftmals werden auch Dritte, wie Nachbarinnen und Nachbarn, Vermieterinnen oder Vermietern befragt. Die Befragung der Eheleute bewegt sich dabei manchmal an der Grenze zum Intimleben, das grundsätzlich vor staatliche Eingriffen geschützt ist.

Ermittlungen werden fast immer aufgenommen, wenn die Ehepartner unter verschiedenen Adressen gemeldet sind. In einigen Fällen erscheint es zweifelhaft, ob der Grundsatz, dass die Datenerhebung vorrangig bei der betroffenen Person zu erfolgen hat, immer berücksichtig wird. Auch werden die betroffenen Personen nicht immer nach der Durchführung von Ermittlungen benachrichtigt.

8.2 Ausschreibungen im Schengener Informationssystem (SIS) durch Ausländerbehörden

Der 14. Datenschutzbericht 1999 enthält unter 3.7.1 einen ausführlichen Abschnitt zum Schengener Informationssystem (SIS), auf den hier nur verwiesen wird.

8.2.1 Ausschreibungen im SIS häufig ohne Rechtsgrundlage

Der größte Teil der Ausschreibungen von Ausländerinnen und Ausländern im Schengener Informationssystem erfolgt nach Art. 96 Abs. 3 Schengener Durchführungsübereinkommen (SDÜ). Dabei handelt es sich um eine Ausschreibung zum Zweck der Einreiseverweigerung. Die Ausschreibung erfolgt durch einen Antrag der Ausländerbehörde, der über das Landeskriminalamt weitergeleitet wird. Häufig wird dabei als Rechtsgrundlage Art. 96 Abs. 3 SDÜ herangezogen, obwohl die entsprechenden Voraussetzungen nicht erfüllt sind: Eine Ausschreibung nach Art. 96 Abs. 3 SDÜ setzt voraus, dass eine Ausweisung, Zurückweisung oder Abschiebung mit Einreiseverbot stattgefunden hat, weil die Ausländerin oder der Ausländer ausländerrechtliche Einreise- oder Aufenthaltsvorschriften nicht beachtet hatte. **Art. 96 Abs. 3 SDÜ kann somit keine Rechtsgrundlage für Ausschreibungen zum Zweck der Aufenthaltsermittlung darstellen.** Wenn eine Person, deren Asylantrag abgelehnt worden ist, untertaucht, kann eine Ausschreibung im polizeilichen Informationssystem (INPOL) oder im Ausländerzentralregister (AZR) erfolgen. Eine Ausschreibung zur Einreiseverweigerung im SIS ist in diesen Fällen jedoch unzulässig.

In mehreren Fällen waren Personen, deren Asylanträge negativ beschieden worden waren, vor der Abschiebung untergetaucht. Die Ausländerbehörden nahmen dies zum Anlass, neben der nationalen Ausschreibung in INPOL auch eine Ausschreibung zur Einreiseverweigerung im SIS zu veranlassen. Im Gegensatz zu der Ausschreibung zur Fahndung in INPOL war dies unzulässig. Die "schengenwidrige" Ausschreibung abgelehnter Asylbewerberinnen und Asylbewerber wurde bereits mehrfach von französischen Gerichten festgestellt.

Das Innenministerium des Landes Nordrhein-Westfalen hat sich meiner Rechtsauffassung angeschlossen und seinen nachgeordneten Bereich entsprechend unterrichtet.

8.2.2 Löschungsfristen nach Art. 112 SDÜ werden häufig missachtet

Die zur Personenfahndung im Schengener Informationssystem aufgenommenen personenbezogenen Daten dürfen nur so lange gespeichert werden wie dies erforderlich ist. Nach Art. 112 Abs. 1 SDÜ ist die Erforderlichkeit der weiteren Speicherung nach spätestens 3 Jahren zu prüfen. Damit ergibt sich aus Art. 112 SDÜ eine **regelmäßige Löschungsfrist von drei Jahren**, sofern nicht die zuständige (hier: Ausländer-) Behörde aufgrund eigener

Prüfung im Einzelfall eine Verlängerung beschließt. Das Innenministerium des Landes Nordrhein-Westfalen ist dieser Rechtsauffassung inzwischen beigetreten. Eine Reihe von Ausländerämtern hat daraufhin einen Teil ihrer Ausschreibungen im SIS löschen lassen. In einigen Fällen weigern sich Ausländerbehörden, die Ausschreibungen von Ausländern vor mehr als drei Jahren veranlasst haben, diese zu löschen, obwohl keine Gründe erkennbar sind, die eine Verlängerung der Ausschreibung im Einzelfall rechtfertigen würden, und die Datenspeicherung im SIS damit ohne Rechtsgrundlage erfolgt.

Das Innenministerium bleibt aufgerufen, insoweit für eine einheitliche landesweite datenschutzkonforme Ausschreibungspraxis Sorge zu tragen.

9. Kommunales

In den Berichtszeitraum fielen die Landtagswahl und die Kommunalwahlen. Das Thema "Wahlwerbung" löst in solchen Zeiten immer wieder eine Lawine von Anfragen und Beschwerden über die Datenflüsse zwischen den Einwohnermeldeämtern und den zur Wahl stehenden Parteien aus. Dies zeigt einmal mehr, dass es schön gewesen wäre, wenn bei der letzten Änderung des Melderechts für Nordrhein-Westfalen (siehe dazu unter 5.1.1 im 14. Datenschutzbericht 1999) nicht nur die Übermittlung von Einwohnerdaten an Adressbuchverlage, sondern auch an politische Parteien an die Einwilligung der betroffenen Personen geknüpft worden wäre.

9.1 Öffentliche Auslegung von Wählerverzeichnissen

Auch die öffentliche Auslegung von Wählerverzeichnissen muss Datenschutzbelange berücksichtigen.

Die Transparenz von Wählerverzeichnissen ist wünschenswert und notwendig. Wer aus Gründen einer konkreten Gefahr für Leben, Gesundheit oder andere gewichtige Belange eine melderechtliche Auskunftssperre für die Daten zur eigenen Person erwirken konnte, besitzt jedoch ein schutzwürdiges Interesse daran, dass die Daten nicht öffentlich ausgelegt werden. Das Problem ist altbekannt und steht seit langem im Streit mit dem Innenministerium (siehe dazu schon im 12. Datenschutzbericht 1993/94 unter 5.2.2.)

Das Innenministerium bleibt aufgefordert, nunmehr endlich für eine datenschutzgerechte Änderung der Vorschriften über Wahlen initiativ zu werden.

9.2 Anschrift als Hinweis auf mangelnde Bonität?

Eine Stadt bat um Auskunft, ob es rechtens sei, einer Privatfirma die Anschriften aller Sammelunterkünfte von Asylbewerberinnen und Asylbewerbern zu übermitteln.

Hintergrund der Firmenbitte um Datenübermittlung war, Telekommunikationsunternehmen bereits im Vorfeld eines Vertragsabschlusses Hinweise hinsichtlich der möglichen Bonität der jeweiligen Antragstellerinnen und Antragsteller geben zu können. Bei den von der Privatfirma gewünschten Adressdaten aller Sammelunterkünfte von asylbegehrenden Ausländerinnen und Ausländer handelt es sich um personenbezogene Daten im Sinne des § 3 DSG NRW, da es zumindest mit Hilfe von Zusatzwissen ohne weiteres

möglich ist, die Bezugspersonen zu bestimmen. Eine zulässige Datenübermittlung setzt das Vorliegen einer entsprechenden Rechtsgrundlage voraus. Nach § 16 Abs. 1 Buchstabe d) DSG NRW ist die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs zulässig, wenn sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und die betroffene Person der Datenübermittlung nicht widersprochen hat. Es kommt hinzu, dass die betroffene Person zuvor über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise zu unterrichten ist und der beabsichtigten Übermittlung nicht widerspricht. Eine solche Unterrichtung scheidet vorliegend jedoch aus. Denn es geht ja gerade darum, im Vorfeld einer konkreten Kontaktaufnahme bestimmte personenbezogene Hinweise ohne Wissen der Betroffenen zu erlangen, um hieraus entsprechende Rückschlüsse auf die finanzielle Leistungsfähigkeit ziehen zu können. Somit ist die Datenübermittlung nicht zulässig.

Das Innenministerium hat sich meiner Rechtsauffassung angeschlossen und die Bezirksregierungen gebeten diesbezügliche Anfragen aus dem kommunalen Raum entsprechend zu beantworten.

10. Sozialbereich

Die im Fünften Buch des Sozialgesetzbuchs (SGB V) geregelte gesetzliche Krankenversicherung wurde im Berichtszeitraum in datenschutzrechtlich wichtigen Bereichen abermals geändert. Zu einem ersten Entwurf eines **Gesetzes zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000**, der datenschutzrechtliche Mängel aufwies, haben sich die Datenschutzbeauftragten in ihrer **Entschließung vom 25.08.1999 "Gesundheitsreform 2000"** (Abdruck im Anhang, Nr. 6) kritisch geäußert. Zahlreiche Regelungen dieses Gesetzentwurfes waren geeignet, das Recht auf informationelle Selbstbestimmung der Versicherten zu beeinträchtigen, ohne dass dies durch die mit dem Gesetz beabsichtigten Ziele gerechtfertigt gewesen wäre. Gegenüber dem Ministerium für Frauen, Jugend, Familie und Gesundheit habe ich mich dafür eingesetzt, dass die gemeinsamen Forderungen der Datenschutzbeauftragten in ihrer oben genannten Entschließung im Gesetzgebungsverfahren berücksichtigt werden.

Auch ein weiterer, in einer Pressemitteilung vom 24.11.1999 veröffentlichter Appell der Datenschutzbeauftragten verhallte nicht ungehört: Das am 04.11.1999 vom Bundestag beschlossene Gesundheitsreformgesetz 2000 berücksichtigte zunächst datenschutzfreundlichere Regelungen zum Umgang mit Versichertendaten in der gesetzlichen Krankenversicherung, etwa durch die Beschränkung der Datenzugriffsrechte innerhalb der Krankenkassen. Da jedoch der "versichertenfreundliche" Gesetzesteil infolge der Zustimmungspflicht durch den Bundesrat so nicht Gesetz wurde, sind noch mehrere datenschutzrechtlich bedeutsame Fragen (unter anderem Klarstellung der Verarbeitung von Sozialdaten Versicherter zu Werbezwecken der Krankenkassen, Mitteilung von Krankheitsursachen und drittverursachten Gesundheitsschäden durch Ärztinnen und Ärzte an die Krankenkassen) offen, die einer gesetzlichen Regelung bedürfen. Hierzu liegen dem Bundesministerium für Gesundheit Vorschläge der Datenschutzbeauftragten vor.

Die erforderlichen Regelungen lassen auf sich warten. Insbesondere werden damit bis auf weiteres auch die **langjährigen Bemühungen der Datenschutzbeauftragten** um einen datenschutzgerechten Umgang mit den Daten der Versicherten **nicht realisiert.** In einer Presseerklärung vom 19.04.2000 - abrufbar unter www.lfd.nrw.de - wurde die Haltung der Krankenkassen kritisiert, **unverändert kassenweite Zugriffsmöglichkeiten auf automatisiert gespeicherte sensible Versichertendaten** zu ermöglichen. Das Recht der Versicherten auf informationelle Selbstbestimmung wird von den betreffenden Krankenkassen nicht zur Kenntnis genommen. Dies, obwohl durchaus Möglichkeiten bestehen, eingeschränkte Zugriffsbefugnisse auf die

EDV-gespeicherten Daten durch programmsteuernde Maßnahmen zu vergeben.

Auch im Bereich der **Pflegeversicherung** gibt es neue Entwicklungen: So soll mit dem Entwurf eines Gesetzes zur Qualitätssicherung und zur Stärkung des Verbraucherschutzes in der Pflege das Pflegeversicherungsgesetz (SGB XI) geändert werden, um Mängel in der Pflegequalität abzubauen und die Rechte der Betroffenen zu erweitern. In diesem Zusammenhang und mit vergleichbarer Zielsetzung im Bereich der vollstationären Pflege steht auch der Entwurf eines Gesetzes zur Verbesserung der Rechtsstellung und des Schutzes der Bewohnerinnen und Bewohner von Heimen, mit dem das Heimgesetz neugefasst werden soll. Beide Gesetzentwürfe tangieren die Zusammenarbeit und das Verhältnis von Pflegeselbstverwaltung, staatlicher Heimaufsicht, Pflegekassen, Medizinischem Dienst der Krankenversicherung und den Trägern der Sozialhilfe.

Ob die zahlreichen hierin vorgesehenen Übermittlungen personenbezogener Daten tatsächlich in diesem Umfang erforderlich sind, ist allerdings **zweifelhaft.** Gleiches gilt für den großen Kreis der Empfänger dieser Daten. Auch mit milderen, das Recht auf informationelle Selbstbestimmung der Betroffenen weniger tangierenden Mitteln - etwa durch Verwendung anonymisierter Daten - ließen sich in vielen Bereichen die gesetzgeberischen Ziele verwirklichen. Besonders **kritisch** zu betrachten sind Neuregelungen, durch die beispielsweise für Beschäftigte in Sozialämtern die Möglichkeit entstehen kann, Einblick in Pflegedokumentationen zu nehmen, ohne dass dies für die Zweckerfüllung der jeweiligen Norm erforderlich ist.

Die Datenschutzbeauftragten haben dementsprechende Vorschläge unterbreitet, die vom Bundesbeauftragten für den Datenschutz dem Bundesministerium für Gesundheit und dem Bundesministerium für Familie, Senioren, Frauen und Jugend übermittelt wurden.

10.1 Veraltete Formulare in den Sozialämtern

Die verschiedenen Tätigkeitsfelder eines Sozialamtes bringen es mit sich, dass aus den verschiedensten Gründen von den betroffenen Personen Daten erhoben und weiter verarbeitet werden. Hierzu werden zahlreiche Formulare verwendet, die nach dem jeweiligen Sachgebiet unterschiedlich ausgestaltet sind.

Beschwerden von Bürgerinnen und Bürgern sowie im Berichtszeitraum durchgeführte Kontrollbesuche haben gezeigt, dass diese Formulare dem

Recht auf informationelle Selbstbestimmung der Betroffenen durchweg nur unzureichend Rechnung tragen.

Als Mängel waren beispielsweise auszumachen, dass

- die Rechtsgrundlagen für den Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen **generell** nicht genannt werden,
- bei Erhebung von Daten mittels eines Formulars hinsichtlich der weiteren Phasen der Verarbeitung dieser Daten die Betroffenen hierüber weder belehrt noch unterrichtet werden,
- immer wieder unzulässigerweise **Aufgabenzuweisungsnormen** als Rechtsgrundlagen für eine Datenerhebung und weitere Datenverarbeitung genannt und benutzt werden,
- unzulässigerweise Normen, die eine Verpflichtung der Betroffenen enthalten, an der Datenerhebung und weiteren Datenverarbeitung mitzuwirken, als **Befugnisnormen** der öffentlichen Stelle angesehen werden, Daten zu erheben und weiter zu verarbeiten,
- mit einem Formular unzulässigerweise **gemeinsam** Daten der betroffenen Antragstellerin und des betroffenen Antragstellers sowie dritter **Personen** erhoben werden, ohne dass eine gesetzliche Verpflichtung für die dritten Personen besteht, ihre Daten den Antragstellerinnen und Antragstellern gegenüber zu offenbaren,
- gleichzeitig von den Antragstellerinnen und Antragstellern selbst verlangt wird, die **Vollständigkeit** und **Richtigkeit** ("Wahrheit") dieser Drittdaten mit ihrer Unterschrift zu bestätigen, obwohl sie insoweit auf die Angaben der Dritten allein angewiesen sind,
- in vielen Fällen der **Grundsatz der Datenvermeidung und der Datensparsamkeit** auch im Ansatz nicht gesehen wird,
- in zahlreichen Fällen nicht zwischen den Daten, die zur Aufgabenerfüllung **erforderlich** sind, und denen, die der Aufgabenerfüllung lediglich dienen und nützlich sind, unterschieden wird,
- immer wieder eine **unwirksame Zustimmung auf Vorrat** für Anfragen gegenüber einer nicht eingegrenzten Zahl von - zumindest bestimmbaren - dritten Personen oder Stellen verlangt wird,
- in gleicher Weise eine **nicht eingegrenzte Erklärung zur Entbindung von der Schweigepflicht** gegenüber beliebigen Ärztinnen und Ärzten verlangt wird,

- Daten, die der ärztlichen Schweigepflicht unterliegen, zur Speicherung in den Verwaltungsakten angefordert werden, obwohl sie der ausschließlichen Bewertung durch das **Gesundheitsamt** unterliegen.

Schon diese wenigen Beispiele machen bereits hinreichend deutlich, wie gering das Bewusstsein für den Datenschutz in vielen Sozialämtern ist. Die Betroffenen haben Eingriffe in ihr Grundrecht auf informationelle Selbstbestimmung nur hinzunehmen, wenn solche gesetzlich geregelt sind oder wenn aufgrund einer wirksamen Einwilligung der Betroffenen der Eingriffscharakter der Maßnahme entfällt. Insoweit ist ein **grundsätzliches Umdenken** in diesem Verwaltungsbereich notwendig.

Ein solches Umdenken setzt unter anderem voraus, dass

- diese Formulare möglichst im jährlichen Abstand auf ihre **Berechtigung** hin überprüft werden,
- ein Formular umgehend **überarbeitet** wird, wenn die Rechtsvorschriften, auf denen es basiert, geändert werden,
- auch bei Vorgabe entsprechender Formulare durch Organisationen, Verbände und übergeordnete Stellen eine entsprechende Überprüfungs- und Überarbeitungsverpflichtung aufgrund der **eigenen Verantwortung** als speichernde Stelle stets auch **bei der anwendenden Stelle** verbleibt und von dieser entsprechend wahrzunehmen ist und
- der Inhalt und Umfang der auf diese Formulare gestützten oder der in diesem Zusammenhang geführten **EDV-Dateien** ständig überprüft und den Erfordernissen des Datenschutzes und der Datensicherung angepasst werden.

Detaillierte Ausführungen sind unter www.lfd.nrw.de im Internet abrufbar.

Die Sozialämter bleiben insoweit aufgerufen, die bei ihnen verwendeten Formulare datenschutzkonform zu überarbeiten.

10.2 Verarbeitung von Sozialdaten im Auftrag

Kostendruck und Personaleinsparungen führen auch bei den Leistungsträgern nach dem Sozialgesetzbuch zu Überlegungen, auf verschiedene Weise die Sachbearbeitung auf dritte Stellen zu verlagern.

So bestand beispielsweise die Absicht eines Sozialamtes, die Gewährung der Sozialhilfe in bestimmten Stadtteilen gegen Erstattung einer Kostenpau-

schale auf Träger der freien Wohlfahrtspflege zu übertragen. Ebenso versuchen private Firmen, verschiedene Sozialämter davon zu überzeugen, die Gewährung von **Krankenhilfeleistungen** für Sozialhilfeempfängerinnen und Sozialhilfeempfänger auf diese Firmen gegen eine vertraglich vereinbarte Kostenerstattung zu übertragen. Diese Fälle sind unterschiedlich zu bewerten.

Das Sozialgesetzbuch sieht für Sozialleistungsträger nicht die Möglichkeit vor, einzelne eigene Aufgaben **privaten** Stellen zu übertragen. Die gesetzlichen Regelungen sind in dieser Hinsicht bereichspezifisch abschließend. Deshalb ist die Übertragung der Aufgabe der Gewährung von Sozialhilfeleistungen und der damit verbundenen Verarbeitung personenbezogener Daten, die dem Sozialgeheimnis unterliegen, auf private Stellen unzulässig. Möglich wäre insoweit eine Verlagerung lediglich unter engen Voraussetzungen als **Datenverarbeitung im Auftrag.**

Welche Punkte bei einer solchen Vereinbarung der Datenverarbeitung im Auftrag im Einzelnen zu beachten sind, ist der Orientierungshilfe "Datenverarbeitung im Auftrag (hier: Übertragung von Sachbearbeitung)" zu entnehmen. Die Orientierungshilfe ist unter www.lfd.nrw.de im Internet abrufbar.

10.3 Neues Steuerungsmodell bei der Jugendhilfe

Ein allein erziehender Familienvater, dem Jugendhilfeleistungen gewährt wurden, hat darüber geklagt, dass der Datenschutz durch eine Zusammenfassung von Arbeitsbereichen innerhalb des Jugendamtes einer Kommune nicht gewährleistet ist.

In seiner Stellungnahme hat das Jugendamt betont, bereits im Vorfeld der Entscheidungen über die Jugendhilfeleistungen müssten auch wirtschaftliche Überlegungen mit einbezogen werden. Die jugendhilferechtlichen Aufgaben sind in der Kommune so organisiert, dass das (ausgabenverantwortende) Sachgebiet "Wirtschaftliche Jugendhilfe" und das (aufgabenverantwortende) Sachgebiet "Sozialpädagogische Jugendhilfe" durch eine Person geleitet werden.

Im Rahmen des **Neuen Steuerungsmodells** sind Organisationsformen datenschutzrechtlich problematisch, die bei Beschäftigten zu Interessenkonflikten führen. Dies kann zum Beispiel bei der Aufgaben- und Ausgabenverantwortung "in einer Hand" der Fall sein.

Dies ist problematisch. Dem Sachgebiet "Wirtschaftliche Jugendhilfe" können so bei Teambesprechungen über die im Einzelfall gebotene Hilfeart Daten zur Kenntnis gelangen, die notwendigerweise tief in die Persönlichkeitssphäre der betroffenen Kinder und ihrer Eltern hineinreichen. Besonders brisant wird diese Aufgabenzusammenfassung, wenn dem Sachgebiet "Wirtschaftliche Jugendhilfe" ärztliche oder psychologische Begutachtungen zur Kenntnis gelangen, die in die Hilfeplanung für seelisch behinderte Kinder und Jugendliche miteinzubeziehen sind (§§ 36 Abs. 3, 35a SGB VIII). Den Persönlichkeitsrechten der Betroffenen und den sozialdatenschutzrechtlichen Erfordernissen kann nur dadurch Rechnung getragen werden, dass Aufgaben- und Finanzverantwortung nicht in einer Person liegen, sondern diese Arbeitsbereiche organisatorisch getrennt bleiben. Die **Anforderungen des Neuen Steuerungsmodells** werden dabei **nicht in Frage gestellt.**

Hierzu empfiehlt sich, dem Bereich "Wirtschaftliche Jugendhilfe" grundsätzlich nur die Ergebnisse der Antragsbearbeitung durch das für die Aufgaben verantwortliche Sachgebiet mitzuteilen. Dabei könnte im Einzelfall, etwa auf Grund konkreter Einwände, über weitere, für die Kostentragungsentscheidung gegebenenfalls erforderliche Einzelheiten informiert werden. Zu vergleichbaren Interessenkonfliktsituationen von Sozialarbeiterinnen und Sozialarbeitern im Kommunalbereich wurde bereits früher gefordert, von Aufgabenwahrnehmungen durch eine Person abzusehen, damit unzulässige Datennutzungen vermieden werden (siehe unter 5.8.7 im 12. Datenschutzbericht 1993/94, mit zustimmender Stellungnahme der Landesregierung, LT-Vorlage 12/291).

Der Kommune wurde vorgeschlagen, diese Erfordernisse durch eine entsprechende organisatorische Regelung zu berücksichtigen und in einer **Dienstanweisung** unter anderem festzulegen, dass der Bereich "Wirtschaftliche Jugendhilfe" grundsätzlich keinen Zugriff auf die Unterlagen des die Aufgaben verantwortenden Sachgebiets hat.

10.4 Gewährung von Akteneinsicht in Sozial- und Jugendämtern

Verschiedene Beschwerden von Bürgerinnen und Bürgern zeigten, dass bei den betroffenen Sozial- oder Jugendämtern Unsicherheiten bestanden, wie Anträge auf Akteneinsicht der Personen, um deren eigene Daten es sich in erster Linie handelte, zu erledigen sind.

Rechtsgrundlage für die Akteneinsicht von Beteiligten während eines entsprechenden Verwaltungsverfahrens ist § 25 Abs. 1 SGB X. Wie die Absätze 2 und 3 in der Vorschrift zeigen, ist dieser Anspruch unter bestimmten Voraussetzungen eingeschränkt. Bei Vorliegen eines rechtlichen Interesses in der Zeit vor und nach einem Verwaltungsverfahren steht es im pflichtgemäßen Ermessen der jeweiligen Behörde, den Beteiligten Akteneinsicht zu gewähren.

Demgegenüber knüpft der Auskunftsanspruch nach § 83 Abs. 1 Satz 1 SGB X allein an die Tatsache an, dass eine Person **Betroffene** ist (§ 67 Abs. 1 Satz 1 SGB X). Insbesondere bei einer Datenspeicherung in Akten ist Voraussetzung für eine Auskunftserteilung, dass die Betroffenen Angaben machen, die das Auffinden der Daten ermöglichen. Außerdem darf der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse stehen (§ 83 Abs. 1 Satz 3 SGB X).

Da nach § 83 Abs. 1 Satz 4 SGB X die verantwortliche Stelle das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen bestimmt, kann insoweit auch eine Auskunft in der Form der Akteneinsicht gewährt werden. Zwar besteht somit kein direkter Anspruch der Betroffenen auf Akteneinsicht, doch hat die Stelle bei ihrer Ermessenausübung auch solche Wünsche zu berücksichtigen.

Zusätzliche Datenschutzprobleme entstehen, wenn zum Beispiel mehrere unterhaltspflichtige Personen vorhanden sind, von denen aber nur eine Person in Anspruch genommen wird. Möchte diese Person Einsicht in die Akten der anderen Unterhaltspflichtigen nehmen, wird ihr dies regelmäßig verwehrt. Realisieren kann sie ihr Anliegen unter Umständen mit gerichtlicher Hilfe.

Um den Aufwand, der mit der Durchführung von Gerichtsverfahren verbunden ist, eventuell zu vermeiden, könnte die Verwaltung auch wie folgt verfahren:

Bei Vorliegen der Voraussetzungen könnten die jeweils anderen Unterhaltsverpflichteten nach § 12 Abs. 1 Nr. 4 SGB X zu dem jeweiligen Verfahren hinzugezogen werden oder zumindest nach § 12 Abs. 2 Satz 2 SGB X von der Einleitung der anderen Verfahren benachrichtigt werden, um so eine entsprechende Antragstellung auf Hinzuziehung als Beteiligte zu ermöglichen. In beiden Fällen wäre eine Akteneinsicht nach § 25 SGB X grundsätzlich zulässig.

10.5 Politisches Flugblatt in einer Sozialhilfeakte

Eine Sozialhilfeempfängerin engagierte sich im Bereich der Arbeitslosenhilfe. Zu Arbeitslosenaktionstagen verfasste sie ein Flugblatt. Dieses fand sie später in ihrer Sozialhilfeakte wieder. Es war mit Textmarkierungen versehen und teilweise kommentiert.

Die Mitarbeiterin des betroffenen Sozialamtes vertrat hierzu zunächst die Auffassung, dass das Flugblatt, das an jedermann verteilt wurde, als Information aus "allgemein zugänglicher" Quelle gelte und dass deshalb eine beliebige Nutzung, wie etwa ein Abheften in der Fallakte, erlaubt sei. Dabei wurde jedoch übersehen, dass öffentliche Stellen personenbezogene Daten nur insoweit zu den Akten nehmen dürfen, als die Erkenntnis aus dem Dokument für die Bearbeitung des konkreten Leistungsfalles Voraussetzung ist.

Da kein "Leistungszusammenhang" bestand, war das Flugblatt aus der Akte zu entfernen, was dann auch geschah.

10.6 Versorgungsverwaltung bietet "InfoLine für Gewaltopfer" an

Zur besseren Betreuung der Opfer von Gewalttaten hat die Versorgungsverwaltung im Frühjahr 1999 ein "Opfer-Info-Telefon" eingerichtet, über das sich Betroffene zu Fragen des Opferentschädigungsgesetzes beraten lassen können. Daneben war vorgesehen, dass Rat suchende Betroffene Fragen oder Informationen zu ihren Anliegen auch auf Anrufbeantwortern hinterlassen konnten.

Sofern Betroffene anonym bleiben wollen und ihre Anonymität auch während der telefonischen Beratungsgespräche gewahrt bleibt, ergeben sich keine datenschutzrechtlichen Probleme. Anders liegt es bei telefonischen Beratungen etwa im Zusammenhang mit bereits anhängigen Opferentschädigungsverfahren. Hier müssen die Beratungskräfte in aller Regel auf im Versorgungsamt bereits vorliegende Daten der Betroffenen zurückgreifen. Diese Angaben unterliegen dem Sozialgeheimnis (§ 35 Abs. 1 SGB I). Es liegt auf der Hand, dass bei einer solchen Beratung die **Gefahr einer unbefugten Übermittlung von Sozialdaten an Dritte** besteht, weil die Anrufenden am Telefonhörer grundsätzlich nicht als die wirklich Betroffenen identifizierbar sind. Die telefonische Beratung im Einzelfall muss daher jedenfalls im Regelfall ausscheiden. Den Ratsuchenden sollte vielmehr angeboten werden,

ihr Anliegen entweder persönlich vorzubringen oder sie zu Hause zu besuchen.

Problematisch ist auch das Angebot, Informationen etwa zu bestimmten Gewalttaten auf einen Anrufbeantworter sprechen zu lassen. Von dieser Möglichkeit sollte allein wegen der **Gefahr denunziatorischer Anrufe**, die zu fehlerhaften Datenspeicherungen führen, dringend Abstand genommen werden.

In diesen datenschutzkritischen Fragen zeigte sich das Landesversorgungsamt kooperativ, so dass die aufgezeigten datenschutzrechtlichen Erfordernisse künftig beachtet werden.

11. Gesundheit

Zu verschiedenen Gesetzesvorhaben, unter anderem den Entwürfen eines **Dritten Gesetzes zur Änderung des Betäubungsmittelgesetzes**, eines **Landeshebammengesetzes** und eines **Gesetzes zur Ausführung des Transplantationsgesetzes,** waren Stellungnahmen gegenüber dem Ministerium für Frauen, Jugend, Familie und Gesundheit erforderlich.

Während der parlamentarischen Beratungen des Entwurfs für ein **Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG)** konnte ich Anregungen zum Datenschutz geben. Folgende Regelungen sind meinen Vorschlägen entsprechend gestaltet: Der gesetzlich gebotenen Rücksichtnahme auf den Willen und die Bedürfnisse der Betroffenen wird durch eine **ausreichende Dokumentation** nachprüfbar Geltung verschafft. Bei Anhaltspunkten für eine psychische Erkrankung, die ein behördliches Eingreifen erfordern, ist den Betroffenen die **Möglichkeit** zu eröffnen, **entweder zu einer Untersuchung** in der Sprechstunde des sozialpsychiatrischen Dienstes zu erscheinen **oder** sich **unverzüglich in ärztliche Behandlung nach eigener Wahl** zu begeben. Gesetzlich ist nunmehr klargestellt, dass eine Behandlung ohne oder gegen den Willen Betroffener, ihrer gesetzlichen Vertretung oder ihrer Bevollmächtigten **nur** in den Fällen von Lebensgefahr, von erheblicher Gefahr für die eigene oder für die Gesundheit anderer Personen zulässig ist. Auch die Forderung, dass **Schriftverkehr** der Betroffenen mit den in § 21 Abs. 2 PsychKG genannten Stellen **weder unterbunden noch überwacht** werden darf, wurde berücksichtigt. Schließlich sind notwendige Regelungen zur Verarbeitung personenbezogener Daten durch die **Besuchskommissionen** getroffen worden. Damit ist das Recht der Betroffenen auf informationelle Selbstbestimmung insgesamt gestärkt und der Umgang mit ihren Daten für sie transparenter gestaltet. Gleichwohl ist darauf hinzuweisen, dass das Recht auf informationelle Selbstbestimmung der Betroffenen auf der Strecke bleibt, wenn das Untersuchungsergebnis allein der gesetzlichen Vertreterin oder dem gesetzlichen Vertreter bekannt gegeben wird (§ 9 Abs. 6 PsychKG). Bei der nächsten Novellierung wird deshalb erneut zu diskutieren sein, dass die Betroffenen stets über das Ergebnis ihrer ärztlichen Untersuchung zu informieren sind.

Wichtige berufsrechtliche, in einigen Punkten aus datenschutzrechtlicher Sicht jedoch noch änderungsbedürftige Vorschriften enthalten die neu gefassten, im wesentlichen inhaltsgleichen **Berufsordnungen der Ärztekammern Nordrhein und Westfalen-Lippe (BO).** Zur Verbesserung der Patientendatenschutzrechte wurden dem Ministerium für Frauen, Jugend, Familie und Gesundheit mehrere Änderungsvorschläge zu diesen Bestimmungen unterbreitet. Sie wurden vom Ministerium leider nur nachträglich

aufgegriffen und den Ärztekammern zunächst zur eingehenden Stellungnahme übersandt.

Die wichtigsten Vorschläge:

- Klarstellende Regelung, dass der Ärztekammer zu erteilende ärztliche Auskünfte über eingeführte Maßnahmen zur Qualitätssicherung keine patientenbezogenen Daten beinhalten dürfen (§ 5 BO);
- Verzicht auf den Zusatz in dem die Einsichtnahme in Krankenunterlagen regelnden § 10 Abs. 2 BO (*"...; ausgenommen sind diejenigen Teile, welche subjektive ärztliche Eindrücke oder Wahrnehmungen enthalten"*), der subjektive Eindrücke entgegen der Rechtsprechung **stets** vom Recht der Patientinnen und Patienten auf Einsicht in ihre Krankenunterlagen ausnimmt;
- Anpassung des § 10 Abs. 5 der Berufsordnung der Ärztekammer Westfalen-Lippe an die (Muster-) Berufsordnung für die deutschen Ärztinnen und Ärzte - MBO-Ä 1997 - mit dem Ziel, im Einzelfall erforderliche Datenschutz- und Datensicherungsmaßnahmen in der ärztlichen Praxis durch Empfehlungen der Ärztekammer zu erwirken;
- Normenklare Regelung, unter welchen Voraussetzungen der Schweigepflicht unterliegende Tatsachen und Befunde zum Zwecke der wissenschaftlichen Forschung und Lehre offenbart werden dürfen (§ 15 Abs. 3 BO);
- Regelung, dass nur solche Angaben in ärztliche Gutachten und Zeugnisse aufgenommen werden dürfen, die für die zu treffende Entscheidung der auftraggebenden Stelle erforderlich sind (§ 25 BO).

Es wäre schön, wenn für Patientinnen und Patienten datenschutzfreundlichere Regelungen in diesem Sinne getroffen würden.

Dringender Bedarf besteht nicht zuletzt für eine Novellierung des **Gesundheitsdatenschutzgesetzes.** Nicht geregelt ist zum Beispiel die Frage, von welcher Stelle Krankenunterlagen weiter aufzubewahren sind, wenn Krankenhäuser geschlossen werden sollen. Archive können diese Aufgabe während der arztrechtlich festgelegten Aufbewahrungsfristen nicht übernehmen. Des weiteren sollte dieses Gesetz bereichspezifische Vorschriften für die im nicht-öffentlichen Bereich in ärztlicher Praxis tätigen Ärztinnen und Ärzte vorsehen. Wichtig sind etwa Regelungen, die Probleme und Unsicherheiten bei der Aufgabe ärztlicher Praxen oder bei Praxisübernahmeverträgen künftig vermeiden.

Schwierige arzt- und datenschutzrechtliche, aber auch ethische und gesellschaftspolitische Fragen und Probleme wirft die **Entschlüsselung des menschlichen Genoms** auf, bei der in den letzten Monaten wohl entscheidende Durchbrüche gelungen sind. Hierzu hat die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 12./13. Oktober 2000 zahlreiche Forderungen** formuliert, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine **genetische Diskriminierung** bei der Gewinnung oder Verwendung genetischer Informationen zu verhindern (Abdruck im Anhang, Nr. 25).

11.1 Unverändert: Datenschutzgerechte Kostenerstattung bei Schwangerschaftsabbrüchen in besonderen Fällen nicht gewährleistet

Die Bemühungen um eine datenschutzgerechte Ausgestaltung der Kostenerstattungsverfahren bei Schwangerschaftsabbrüchen in besonderen Fällen sind nicht entscheidend vorangekommen: Das Gesetz zur **Hilfe für Frauen bei Schwangerschaftsabbrüchen** verlangt, das Persönlichkeitsrecht der Frau unter Berücksichtigung der besonderen Situation der Schwangerschaft im gesamten Verfahren, also auch bei Erstattungen ärztlicher Rechnungen, zu achten. Dieses Recht wird in den Kostenerstattungsverfahren jedoch immer noch nicht hinreichend geschützt, worauf **bereits** im **14. Datenschutzbericht 1999** unter 8.1 hingewiesen wurde.

Im Rahmen dieser Verfahren werden dem zuständigen Versorgungsamt von den Krankenkassen und den Kassenärztlichen Vereinigungen unter Beifügung der Einzelrechnungen der jeweiligen Ärztinnen und Ärzte auch Namen und Anschriften der betroffenen Frauen übermittelt. Dies ist **nicht erforderlich.** Wie die Praxis in mehreren anderen Bundesländern zeigt, lässt sich das Verfahren auch unter Verzicht auf die Offenlegung der personenbezogenen Daten durchführen. Hierzu sollten die **Abrechnungsunterlagen lediglich fallbezogen gekennzeichnet** werden, was bisher vom Ministerium für Frauen, Jugend, Familie und Gesundheit leider noch nicht veranlasst wurde. Es bleibt zu hoffen, dass die immer noch andauernde Prüfung des Ministeriums bald zu einem datenschutzgerechten Abschluss führt.

Für Nordrhein-Westfalen bietet sich etwa eine Verfahrensregelung wie in Brandenburg an: Dort wurde zur "Vereinfachung der Verwaltungsaufgaben und einer datenschutzgerechten Ausgestaltung des Kostenerstattungsverfahrens" im Mai 2000 eine Zusatzvereinbarung zur bestehenden Verwaltungsvereinbarung zwischen der AOK für das Land Brandenburg und dem Land geschlossen, die die Datenschutzerfordernisse berücksichtigt.

11.2 Erstattung der Krankenhausrechnung nur gegen Vorlage des ärztlichen Entlassungsberichts?

Im Berichtszeitraum ließen zahlreiche Anfragen von Krankenhäusern erkennen, dass Krankenkassen die gesetzlichen Vorschriften bei der Abrechnung von Krankenhausbehandlungskosten nicht genügend beachten.

Leider war die Haltung einiger Krankenkassen so zu verstehen, dass erbrachte Leistungen ohne Vorlage ärztlicher Krankenhausentlassungsberichte nicht erstattet werden. Dabei regeln die gesetzlichen Bestimmungen der §§ 275 bis 277, 284 und 301 SGB V klar, wie das Abrechnungsverfahren zu erfolgen hat: § 301 SGB V enthält einen abschließenden Katalog der von den Krankenhäusern an die Krankenkassen zu übermittelnden Daten. Ein Krankenhaus wäre etwa bei Überschreitung der üblichen stationären Behandlungsdauer weder befugt noch verpflichtet, anstelle oder als Ersatz einer medizinischen Begründung hierfür den Krankenkassen die Krankenakte - oder auch nur Auszüge hieraus - zu übersenden. Das Gesetz sieht insoweit lediglich vor, dass "auf Verlangen der Krankenkasse die medizinische Begründung" zu übermitteln ist (§ 301 Abs. 1 Nr. 3 SGB V). Eine solche Begründung verlangt eine ärztliche Stellungnahme, die zur Ausräumung aufgetretener Zweifel an der Kostenrechnung geeignet ist. Die Krankenkassen dürfen demnach also keine Operationsberichte, sonstige Krankenunterlagen oder Entlassungsberichte - sämtliche Unterlagen, die dem Arzt-Patienten-Geheimnis unterliegen - für sich anfordern.

Über diese und weitere, die Einschaltung des Medizinischen Dienstes der Krankenversicherung (MDK) betreffende Fragen wurden Datenschutzbeauftragte verschiedener nordrhein-westfälischer Krankenhäuser unterrichtet. Ausführliches zu diesem Thema ist zu finden unter www.lfd.nrw.de und unter 7.5 auch schon im 14. Datenschutzbericht.

11.3 Wenn Männer sich in frauenärztliche Behandlung begeben...

....dann handelt es sich meist um Leistungen aus der Reproduktionsmedizin, etwa der Herbeiführung einer Schwangerschaft durch künstliche Befruchtung. Die Kassenärztlichen Vereinigungen, über die die Abrechnung derartiger Leistungen erfolgt, fielen im Berichtszeitraum insoweit allerdings als etwas zu datenhungrig auf.

Eine Kassenärztliche Vereinigung etwa verlangte von den Praxen **Listen** mit den Personalien der Paare, um die Zulässigkeit der Abrechnung für den Mann feststellen zu können. Ohne Vorliegen konkreter Verdachtsmomente für unkorrekte Abrechnungen im Einzelfall wurden von vornherein von den Arztpraxen derartige Auflistungen angefordert, um jeden Einzelfall überprüfen zu können. Hierfür gab es weder einen Anlass noch für die entsprechende Datenerhebung auf Vorrat eine Rechtsgrundlage. Anhand dieser Listen wäre die Kassenärztliche Vereinigung zudem in der Lage, sexuelle Partnerschaftsprofile über Versicherte und dritte Personen zu erstellen. Die Schaffung derartiger Datenverarbeitungsmöglichkeiten und das Vorhandensein derartiger Datensammlungen geht weit über den Aufgabenbereich einer Kassenärztlichen Vereinigung hinaus. Diese Vorgehensweise ist deshalb insgesamt unzulässig.

Eine andere Kassenärztliche Vereinigung verlangte zwar keine Paarliste, sondern die Angabe der Personalien der mitbehandelten Partnerin auf den Behandlungsunterlagen des Partners. Unter bestimmten Voraussetzungen ist nach § 285 Abs. 2 SGB V die Erhebung von Einzelangaben über die **persönlichen** und sachlichen **Verhältnisse der Versicherten** erlaubt. Weil Leistungen erbracht wurden, dürfen zu Abrechnungszwecken auch personenbezogene Daten verarbeitet werden. In dieses Versicherungsverhältnis ist jedoch die "Partnerin" nicht mit einbezogen. Es handelt sich insofern um eine Datenerhebung über eine dritte Person, die unzulässig ist, weil es dafür keine Rechtsgrundlage gibt.

Zu Abrechnungszwecken kann in solchen Fällen erst dann eine Auskunft über die Partnerin und die Art ihrer Beziehung zu dem behandelten Patienten verlangt werden, wenn sich diese Erhebung für den Nachweis eines rechtmäßigen Leistungsbezugs als unumgänglich erweist.

11.4 Eine Bitte um Vertraulichkeit und ihre Erfüllung

Im Zusammenhang mit einem Medikament, das vom Ausland aus auf dem Schwarzen Markt in Deutschland angeboten wurde, hatte ein aufmerksamer Apotheker das Bundesgesundheitsministerium angeschrieben und diese über den Sachverhalt in Kenntnis gesetzt. Am Schluss des Schreibens erfolgte die unmissverständliche Bitte, den Namen des Betroffenen vertraulich zu behandeln.

Trotz dieser Bitte ist das Schreiben als vollständige Kopie unter zusätzlicher Nennung des Namens des Apothekers im Versendungsschreiben an das Gesundheitsministerium eines Bundeslandes, sowie nachrichtlich an alle

obersten Landesgesundheitsbehörden, an das Bundesinstitut für Arzneimittel und Medizinprodukte, an die Zentralstelle der Länder für Gesundheitsschutz bei Arzneimitteln und Medizinprodukten sowie an das Bundeskriminalamt übersandt worden. Auch das hiesige Ministerium für Frauen, Jugend, Familie und Gesundheit hat das Schreiben seinerseits **ungeschwärzt** weiter im Lande verteilt, und zwar an alle Bezirksregierungen sowie an das Landesinstitut für den öffentlichen Gesundheitsdienst. Die so angeschriebenen Stellen haben ihrerseits ebenfalls ungeschwärzt das Schreiben an die Kreise und kreisfreien Städte verteilt, die es ihrerseits ungeschwärzt an interessierte dritte Stellen weitergereicht haben. Die Weitergabe von Name und Anschrift war auch ohne die Bitte um Vertraulichkeit rechtswidrig, denn sie war weder für die übermittelnden noch für die empfangenden Stellen zur Aufgabenerfüllung erforderlich. Die ganze Angelegenheit ist leider nur ein Beispiel für die viel zu oft herrschende Gedankenlosigkeit im Umgang mit personenbezogenen Daten.

12. Schule

12.1 Schulen ans Netz

Die Hinweise im 14. Datenschutzbericht 1999 (unter 10.1) haben längst nicht gereicht, die Fragen zur Internetnutzung im Schulbereich abschließend zu behandeln, zumal auch immer neue Ideen aufkommen, etwa Daten der Schülerinnen und Schüler (auch mit Foto) auf der Homepage zu veröffentlichen oder den Jugendlichen einen Raum zur Selbstdarstellung zur Verfügung zu stellen. Deshalb ist eine ausführlichere Ausarbeitung zu den wichtigsten datenschutzrechtlichen Fragen unter www.lfd.nrw.de zu finden.

12.2 Datenverarbeitung auf häuslichen PCs der Lehrkräfte

Bereits früher ist im Hinblick auf die Gefährdung der Datensicherheit immer empfohlen worden, den Einsatz von privaten PCs in der öffentlichen Verwaltung für dienstliche Zwecke nur ausnahmsweise zuzulassen und gegebenenfalls von einer schriftlichen Genehmigung abhängig zu machen. Diese Empfehlung ist für den Bereich der Schule in der Verordnung über die Verarbeitung von Daten der Schülerinnen, Schüler und Erziehungsberechtigten auch umgesetzt worden (§ 2 Abs. 2 VO-DV I). Danach dürfen personenbezogene **Daten der Schülerinnen und Schüler** zur Leistungsbeurteilung grundsätzlich automatisiert auch auf den privaten PCs der Lehrkräfte verarbeitet werden, sofern eine **schriftliche Genehmigung** der Schulleitung dies gestattet.

Da der Computer zunehmend Einzug in die Schulen hält und der Anschluss an das Internet auch immer mehr Lehrkräfte fasziniert, nehmen die häuslichen PCs, Laptops oder Notebooks zu. Damit verbreitet sich die automatisierte Verarbeitung von Daten der Schülerinnen und Schüler in den privaten Rechnern, leider aber nicht automatisch auch die Kenntnis der verordnungsrechtlichen Vorgaben. Eine stichprobenartig durchgeführte Umfrage zur Verfahrensweise bei Realschulen, Gymnasien und Berufsschulen ließ allgemeinen Beratungsbedarf erkennen. Unter Einbeziehung der aus der Umfrage gewonnenen Erkenntnisse wurde ein Muster erstellt, das unter www.lfd.nrw.de als Orientierungshilfe für Antrag und Genehmigung heruntergeladen werden kann.

12.3 Überprüfung der Verfassungstreue in Personalakten

Die Berufsverbote in Folge des so genannten "Radikalenerlasses" und ihre Nachwirkungen: Es gab einmal eine Zeit in Deutschland, in der Lehrerinnen und Lehrer bei außerdienstlichen Aktivitäten für kommunistische Parteien um ihre berufliche Zukunft im Schuldienst fürchten mussten. Im Fall einer niedersächsischen Lehrerin, die wegen ihres parteipolitischen Engagements zeitweise aus dem Schuldienst entlassen worden war, entschied der Europäische Gerichtshof für Menschenrechte am 26. September 1995, dass dies Artikel 10 (Meinungsfreiheit) und Artikel 11 (Vereinigungsfreiheit) der Europäischen Menschenrechtskonvention verletzt. Im Klartext: Das Berufsverbot war menschenrechtswidrig. Mussten sich manche arbeitswilligen Lehrerinnen und Lehrer damals also erst von Gerichten ihre Verfassungstreue bestätigen lassen, um in den Schuldienst gelangen zu können, verbietet es sich spätestens heute, derartige Verfahren in den Personalakten zu dokumentieren.

Umso erstaunlicher ist es, dass eine Bezirksregierung in den Personalakten noch immer Unterlagen über Arbeitsgerichtsverfahren aufbewahrt, in denen Lehrkräfte vor circa 20 Jahren erfolgreich gegen die Ablehnung ihrer Einstellung geklagt hatten. Dabei handelte es sich zum Teil allein um die Gerichtsentscheidungen, zum Teil aber auch um die kompletten Verfahrensakten. Diese Unterlagen sind nach Intervention meiner Dienststelle zunächst aus den Personalakten herausgenommen worden.

Das Innenministerium vertritt im Wesentlichen die Auffassung, die Aufnahme der Gerichtsentscheidungen entspreche dem damals geltenden Personalaktenrecht. Mit Inkrafttreten des neuen Personalaktenrechts sei die Zuordnung zur Personalakte nicht rechtswidrig geworden, so dass ihre Entfernung deshalb auch nicht von Amts wegen geboten sei. Die betroffenen Lehrkräfte hätten daher zwar **keinen Anspruch** auf Entfernung und Vernichtung der Gerichtsurteile, da jedoch nicht auszuschließen sei, dass ihnen der Gesamtvorgang auch heute noch nachteilig werden könne, solle aus Gründen der Fürsorgepflicht zugunsten der Betroffenen entschieden und **Anträgen** auf Entfernung und Vernichtung der Unterlagen **entsprochen** werden.

Die Bereitschaft, die in Rede stehenden arbeitsgerichtlichen Entscheidungen auf Antrag zu entfernen, stellt einen richtigen, allerdings **nicht ausreichenden Schritt** zur Wahrung der Belange des Datenschutzes dar. Dabei kann dahinstehen, ob die ursprüngliche Entscheidung, die Urteile in die Personalakten aufzunehmen, rechtlich bedenkenfrei war, zumal Einvernehmen zu-

mindest darin besteht, dass die vollständigen Prozessakten zu keiner Zeit in die Personalakten gehörten.

Die Entscheidungen sind **von Amts wegen** aus den Personalakten zu entfernen, da die Gerichtsentscheidungen Behauptungen und Bewertungen enthalten, die sich als unbegründet oder falsch erwiesen haben. Sie sind deshalb gemäß § 102e Abs. 1 Satz 1 Nr. 1 LBG mit **Zustimmung** und nicht auf Antrag der Beamtin oder des Beamten aus den Personalakten zu entfernen und zu vernichten. Durch diese Norm wird nunmehr dem Grundsatz der Personalaktenwahrheit Vorrang vor dem Prinzip der Aktenvollständigkeit eingeräumt. Dabei kommt es weder darauf an, ob die Aufnahme in die Personalakte rechtswidrig war, noch darauf, ob die Unterlagen zu den Personalaktendaten im Sinne des § 102 LBG gehören. Im Übrigen würde eine Entfernung nur auf Antrag zu dem unhaltbaren Zustand führen, dass die Entscheidungen unzulässigerweise immer in den Personalakten blieben, wenn die Betroffenen nichts von ihrer dortigen Aufbewahrung wissen.

Die fraglichen Unterlagen sind von Amts wegen, aber nur mit Zustimmung der betroffenen Lehrkräfte aus ihren Personalakten zu entfernen und zu vernichten. In den Personalakten dürfen auch keine sonstigen Hinweise auf die früheren Überprüfungen - schon gar nicht Hinweise auf Dritte - enthalten sein. Etwa noch gespeicherte Sachakten zu damals geführten Verfahren sind unter Berücksichtigung der archivrechtlichen Bestimmungen von Amts wegen zu vernichten.

13. Wissenschaft und Forschung

13.1 Neues Hochschulgesetz

Das neue Hochschulgesetz trifft für insbesondere zwei Problemkreise spezielle Datenschutzregelungen, die von den Hochschulen bei der Einführung der dafür notwendigen Datenverarbeitungssysteme zu beachten sein werden:

- Die Durchführung der Evaluation von Forschung und Lehre erfordert eine regelmäßige Qualitätsbewertung, an der alle Mitglieder und Angehörigen der Hochschulen mitzuwirken verpflichtet sind. Das bedeutet in datenschutzrechtlicher Hinsicht, dass in einem **Datenverarbeitungskonzept** die Durchführung eines Bewertungsverfahrens vorzubereiten und der Erarbeitung einer Evaluationsordnung zugrunde zu legen ist. Dabei wird insbesondere zu berücksichtigen sein, dass vor allem verwendete Personaldaten der Beteiligten nur im Rahmen des § 29 DSG NRW erfasst, gespeichert und veröffentlicht werden dürfen.
- Zur Einführung des elektronischen Studierendenausweises, die bereits an einigen Hochschulen geplant wird, ist eine Änderung der Einschreibeordnungen erforderlich. Grundlage der Änderung muss auch hier ein Datenverarbeitungskonzept sein, das eine datenschutzrechtliche **Vorabkontrolle** nach § 10 Abs. 3 DSG NRW einschließt. Nach den bisher bekannt gewordenen Planungen wird zum Teil übersehen, dass dieser Ausweis nur auf freiwilliger Basis eingeführt werden kann (§ 29a DSG NRW). Im Übrigen ist auf die Ausführungen im 13. und 14. Datenschutzbericht (13. DSB 1995/96 unter 15.1; 14. DSB 1999 unter 10.2) zu verweisen.

13.2 Internetnutzung durch die Hochschulen

Die interne Missbrauchskontrolle durch die Systemadministration und der Abruf von Prüfungs- oder sonstigen Leistungsergebnissen durch die Studierenden werfen immer wieder Probleme auf.

An einer Universität werden beispielsweise den Studierenden vom Rechenzentrum, das für die Administration der Internetnutzung zuständig ist, in regelmäßigen Abständen Mitteilungen über den Umfang ihrer Internetnutzung zur **Selbstkontrolle** übersandt - etwa wie lange gesurft und wie viel heruntergeladen wurde. Gegen diese Art der internen Kontrolle ist datenschutzrechtlich nichts einzuwenden, wenn eine Nutzungsordnung diese Kontrollmöglichkeit anordnet und sie ausschließlich der Systemadministration zuweist, die notwendigen Kontrolldaten innerhalb der Systemadministration

bleiben und die möglichen Konsequenzen einer missbräuchlichen Nutzung genau festgelegt sind. Alle Studierenden müssen vor Erhalt der Zugangsberechtigung die Kenntnisnahme dieser Bedingungen bestätigen.

Problematischer wird es allerdings, wenn den Studierenden die Nutzung des Internets über die Studienzwecke hinaus auch zur Versendung und zum Empfang **privater E-Mails** zur Verfügung gestellt wird. Dann ist der Hochschule auf Grund des Fernmeldegeheimnisses die Einsichtnahme in diese elektronische Post untersagt. Allenfalls könnte eine aus begründetem Anlass vorgenommene **Missbrauchskontrolle** erfolgen, die durch eine besondere Vereinbarung mit den Nutzungsberechtigten vorher genau festzulegen ist.

Die Möglichkeit, **Prüfungs- oder Leistungsergebnisse** auf der Homepage der Hochschule abrufbar zur Verfügung zu stellen, ist zwar als Serviceangebot insbesondere für externe Studierende gemeint. Es muss aber dabei bedacht werden, dass das Internet als ein offenes und deshalb unsicheres Medium die bereitgestellten personenbeziehbaren Daten weltweit lesbar macht. Insoweit ist eine ausreichende Vertraulichkeit und Identifikation sicherzustellen (siehe auch oben unter 2.1.4.1). Die Fernuniversität Hagen hat mit ihrer einschlägigen Erfahrung im "elektronischen Fernstudium" ein Verfahren erarbeitet, das diesen Erfordernissen übergangsweise Rechnung trägt, bis ein digitales Signaturverfahren auch an den Hochschulen allgemein verfügbar ist. Die Information hierüber kann abgerufen werden unter www.fernuni.hagen.de/URZ/Projekt.

13.3 Forschung in der Schule

Unter den Forschungsvorhaben im schulischen Bereich finden sich sowohl solche, die die Schule selbst zum Gegenstand ihrer Untersuchung machen, als auch solche, die sich schwerpunktmäßig mit nicht-schulischen Fragen beschäftigen und denen Schulen nur als Kontaktstellen dienen.

13.3.1 Schule als Gegenstand der Forschung

Die Organisation für wirtschaftliche Zusammenarbeit (OECD) hat ein Projekt namens PISA (Programme for International Student Assessment) ins Leben gerufen, das alle drei Jahre über Leistungstests von Schülerinnen und Schülern die Leistungsfähigkeit der Schulsysteme in 30 Mitgliedsstaaten der OECD - auf nationaler Ebene unter Federführung des Max-Planck-Instituts für Bildungsforschung in Berlin - vergleichen soll.

In Deutschland waren die Datenschutzbeauftragten der Länder leider erst in einer sehr späten Phase, teilweise erst nach der Erteilung der Genehmigung durch die Kultusministerien, an der Konzeption dieser Befragung beteiligt worden. Zu diesem Zeitpunkt war im PISA-Projekt bereits eine datenschutzrechtliche Schieflage entstanden, durch die das ganze Projekt - zumindest die deutsche Beteiligung daran - zu scheitern drohte. Dabei kamen zu den üblichen Schwierigkeiten, Datenschutz und Forschungsfreiheit auszutarieren, zwei weitere Problemebenen dazu: Einerseits waren bereits internationale Vorgaben geschaffen worden, die nicht oder nur schwer mit nationalen datenschutzrechtlichen Anforderungen in Einklang zu bringen waren; andererseits entstanden im Teilnehmerland Deutschland zusätzliche Probleme durch die föderale Struktur und die Kulturhoheit der Länder. In einem gemeinsamen Treffen der Datenschutzbeauftragten und des nationalen Projekt-Konsortiums wurden datenschutzrechtliche Verbesserungen bei der Durchführung des Projekts erarbeitet; Optimierungen konnten - maßgeblich bedingt durch die späte Beteiligung - allerdings nicht mehr in allen Punkten erreicht werden.

Beispielsweise ist nicht, wie ursprünglich vorgesehen, allein die Einwilligung der Erziehungsberechtigten einzuholen. Entscheidend kommt es auf die **Einwilligung der einsichtsfähigen** (meist 15-jährigen) **Jugendlichen** an, während die Einwilligung der Eltern nur im Hinblick auf die im Fragebogen auch über sie selbst erhobenen personenbezogenen Daten - etwa die Berufsangabe - überhaupt erforderlich ist. Deshalb mussten die Schülerinnen und Schüler dieselben Informationen erhalten wie die Eltern.

Die Notwendigkeit, Einwilligungserklärungen von einsichtsfähigen Jugendlichen selbst einzuholen, wird für künftige Forschungsvorhaben in NRW zu beachten sein.

13.3.2 Schule als Kontaktstelle für Forschung

Vermehrt wurde Beratung zu Forschungsvorhaben gewünscht, bei denen letztlich Jugendliche bestimmter Altersgruppen über die Schulen lediglich gezielt angesprochen und für die Teilnahme gewonnen werden sollten. Der eigentliche Untersuchungsgegenstand betraf dann zumindest schwerpunktmäßig außerschulische Problembereiche der Jugendlichen. Erforscht wurden beispielsweise die Lebenssituation von Kindern und Jugendlichen, die wechselseitige Wahrnehmung, Integration und Interaktion von Jugendlichen unterschiedlicher ethnischer Herkunft oder auch die Einstellung zu Kriminalität. Die Untersuchungen bezogen sich zum Teil auf äußerst sensible Daten der Teilnehmenden. Auch bei diesen Projekten ging es um die übli-

chen datenschutzrechtlichen Probleme: Anonymisierung oder Pseudonymisierung der Untersuchung, Art der Auswahl der Schul- und Schülerstichprobe, Aufklärung von Jugendlichen, Eltern und Schulleitungen, Durchführung der Befragung und Datenauswertung. Außerdem mussten für die speziellen Problemstellungen datenschutzgerechte Lösungen zum Schutz der Befragten gefunden werden. Es wurde veranlasst, die personenbezogenen Daten der Befragten, etwa in den Einwilligungserklärungen und den Listen mit den Adressen für die Nacherhebung, völlig getrennt von den Forschungsdaten und außerhalb des Forschungsbereichs aufzubewahren. Weiter wurde sichergestellt, dass Aufklärungs- und Einwilligungsschreiben in den Landessprachen der Zielgruppen verfasst, die Einwilligungen von den einsichtsfähigen Jugendlichen selbst eingeholt, aber ihre Eltern darüber ausführlich informiert wurden. Bei der kriminologischen Untersuchung wurde im Hinblick darauf, dass sich die Befragten mit ihren Angaben zum Teil möglicherweise selbst belasten konnten, ein **Codierungsverfahren** gewählt, das eine nachträgliche Zuordnung der Befragungsergebnisse zu einer bestimmten Person sicher ausschloss. Das Pseudonym wurde nur von den Befragten selbst nach einem vorgegebenen Muster gebildet, das sie bei der Nacherhebung nach zwei Jahren wieder anwenden müssen, um so eine Zuordnung beider Befragungsergebnisse zueinander zu ermöglichen.

Durch frühzeitige intensive Beratung und gute Kooperation mit den Forschenden gelang es, eine datenschutzgerechte Konzeption und Durchführung des jeweiligen Vorhabens sicherzustellen.

13.4 Forschungsdaten in Kompetenznetzen

In der medizinischen Forschung sind zunehmend Planungen erkennbar, die vorhandene bundesweit zersplitterte Kompetenz durch den Einsatz moderner Datenverarbeitungssysteme zu bündeln und so besser nutzbar zu machen. Das Bundesministerium für Bildung und Forschung unterstützt gezielt den Aufbau überregionaler so genannter Kompetenznetzwerke für spezifische Krankheiten. Die besten Einrichtungen der Forschung und Versorgung sollen ihre Kompetenz und Infrastruktur in diese Netzwerke einbringen. Ziel der Kooperation ist ein deutlicher Mehrwert im Hinblick auf Qualität und Ergebnisorientierung von Forschung, ärztlicher Aus- und Weiterbildung und Gesundheitsversorgung.

Dieses aus medizinischer Sicht begrüßenswerte Vorhaben wirft allerdings erhebliche datenschutzrechtliche Probleme auf. Die **Gesundheitsdaten**, die in solche „vernetzte" Forschungsvorhaben eingebracht werden, sind nicht mehr nur einer überschaubaren Forschungsgruppe zugänglich, sondern sol-

len durch eine zentrale Speicherung und bundesweite Vernetzung einer Vielzahl Forschender über das Internet zur Verfügung gestellt werden.

Um den damit verbundenen Risiken Rechnung zu tragen, erarbeiten die Datenschutzbeauftragten des Bundes und der Länder zurzeit datenschutzrechtliche (Mindest-) Anforderungen an den Aufbau von Kompetenznetzen. Am Beispiel des Kompetenznetzes Parkinson ist bisher festgestellt worden, dass es zum Beispiel einer besonderen Aufklärung und Einwilligung der teilnehmenden Patientinnen und Patienten und parallel dazu einer schriftlichen Vereinbarung zwischen Ärztin oder Arzt und Kompetenznetzverantwortlichen über die weitere Verwendung der Daten bedarf. Es muss sichergestellt sein, dass in den Kompetenznetzen mindestens **pseudonymisierte** Daten, deren Reidentifizierung durch die Forschenden nicht möglich ist, verarbeitet werden. Personenbezogene Daten dürfen durch die behandelnde Ärztin oder den behandelnden Arzt nur zu dem Zweck übermittelt werden, die Ergebnisse der Forschung für die Weiterbehandlung der teilnehmenden Patientinnen oder Patienten nutzbar zu machen; die Übermittlung dieser personenbezogenen Daten soll allerdings nicht direkt an die Forschenden, sondern an eine **Treuhänderin** oder einen **Treuhänder** - also eine außenstehende Person oder eine rechtlich selbständige Stelle - erfolgen, bei der oder dem die Daten durch Schweigepflicht und Beschlagnahmeverbot gegen eine Kenntnisnahme durch Dritte gesetzlich geschützt sind - etwa bei einer Notarin oder einem Notar. Der Einsatz eines Pseudonymisierungsverfahrens setzt spezielle Sicherungsmaßnahmen voraus, um insbesondere **Reidentifizierungsrisiken** für die betroffenen Patientinnen und Patienten auszuschließen. Aus diesem Grund darf auch keine einheitliche Identifizierungsnummer für eine betroffene Person in verschiedenen Kompetenznetzen verwendet werden. Schließlich ist noch nicht geklärt, ob entnommene Gewebeproben mit dem Pseudonym anderen Forschenden zur Verfügung gestellt werden können, da mit Hilfe neuer Techniken - etwa der Genomanalyse - eine Reidentifikation durch Vergleich mit in anderen Kompetenznetzen analysiertem Gewebematerial möglich ist. Mit der Einigung auf bestimmte Mindestanforderungen zur Wahrung des Datenschutzes in Kompetenznetzen ist indes nur eine gemeinsame Ausgangsbasis für die weitere Beratungstätigkeit geschaffen worden; die zukünftige Entwicklung wird kritisch begleitet.

Bis jetzt wurde von meiner Dienststelle beratend Stellung genommen zu einem dieser Kompetenznetze, dem BrainNet-Zentrum Bonn und seinem Projekt "Depression und andere psychische Erkrankungen". Dieses Projekt weist - im Vergleich zu dem oben genannten Forschungsnetz Parkinson - allerdings zwei erhebliche Unterschiede auf: zum Einen werden ausschließlich Todesursachendaten verarbeitet und Organteile Verstorbener untersucht, zum Anderen wird das Projekt, das ursprünglich als Teil eines bun-

desweiten Forschungsnetzwerks geplant war, wegen der bisher ungelösten datenschutzrechtlichen Schwierigkeiten als in sich geschlossenes Forschungsvorhaben durchgeführt, also findet keine Vernetzung des BrainNet-Zentrums Bonn mit anderen Forschungszentren statt. Nach eingehender Beratung bestanden gegen die Durchführung dieses Projekts keine durchgreifenden datenschutzrechtlichen Bedenken.

14. Statistik

"Kommt wieder eine Volkszählung?" fragte die Überschrift zu Kapitel 9 des 14. Datenschutzberichts 1999. Die Frage konnte schon nach dem damaligen Diskussionsstand verneint werden. Der vorgesehene "Paradigmenwechsel von der primärstatistischen Totalerhebung zu einem registergestützten System" führt dazu, dass in erster Linie Daten aus vorhandenen amtlichen Registern genutzt und ausgewertet werden sollen mit der Maßgabe, dass die bei der statistischen Bearbeitung der Register gewonnenen Erkenntnisse **nicht** in den Verwaltungsbereich zurückfließen dürfen. Mit einem weitgehend registergestützten Zensus gäbe die Bundesrepublik ihre bisherige Tradition primärstatistischer Vollerhebungen auf und vollzöge einen tiefgreifenden Methodenwechsel. Es bedarf sowohl administrativer als auch legislativer Maßnahmen, um die Register auf eine solche Nutzung auszurichten. Die neuen Verfahren zur Datengewinnung für eine Volkszählung müssen eingehend getestet werden. Dafür müssen spezielle Rechtsgrundlagen geschaffen werden.

Der Entwurf eines **Gesetzes zur Vorbereitung eines registergestützten Zensus (Testgesetz)** liegt nunmehr vor. Meine Stellungnahme gegenüber dem Innenministerium NRW hat zum Ziel, dass insbesondere folgende grundlegenden Erfordernisse des Datenschutzes bei statistischen Erhebungen Beachtung finden:

- Verbindliche Festlegung im Gesetz, dass sämtliche erhobenen Daten ausschließlich in den Statistischen Ämtern des Bundes und der Länder verarbeitet werden, der strikten statistischen Geheimhaltung unterliegen und in keiner Form für Zwecke des Verwaltungsvollzugs genutzt werden dürfen.
- Klare Definition des Gesetzeszwecks, der allein in der Erprobung neuer statistischer Methoden besteht und nicht, auch nicht mittelbar, auf die Gewinnung aktueller statistischer Erkenntnisse für eine Bundesstatistik abzielt.
- Auch im Testgesetz selbst sollte eine dem § 22 des Bundesstatistikgesetzes entsprechende Strafvorschrift vorgesehen werden.
- Verbindliche gesetzliche Festlegungen, dass Personenkennzeichen oder personenkennzeichenähnliche Merkmale vermieden werden.

Die weitere Entwicklung bleibt insoweit abzuwarten.

Im Rahmen der **Bevölkerungsstatistik** haben Datenschutzbeauftragte in der Vergangenheit wiederholt darauf hingewiesen, dass die zur Übermittlung

von Daten zu Geburt, Sterbefall und Eheschließung von den Standesämtern an das Statistische Landesamt verwendeten Zählkarten Erhebungen enthalten, die durch das Bevölkerungsstatistikgesetz nicht gedeckt sind. Eine Anpassung an den im Volkszählungsurteil geforderten Standard ist weiterhin notwendig.

Zu Zwecken der **Sozialhilfestatistik** werden immer wieder weitere, für die eigentliche Antragsbearbeitung nicht erforderliche Sozialdaten **auf freiwilliger Grundlage** bei den Antragstellerinnen und Antragsstellern erhoben. Die Sozialhilfestatistik ist bereichspezifisch abschließend in den §§ 127 ff. Bundessozialhilfegesetz (BSHG) geregelt. In diese Erhebung als Sekundärstatistik dürfen nur solche Daten fließen, die im Rahmen des Verwaltungsvollzugs für den jeweiligen Einzelfall als erforderlich erhoben worden sind. Dementsprechend ist nach § 131 Abs. 2 BSHG allein der Sozialhilfeträger auskunftspflichtig. Eine Erhebung weiterer, zur Erfüllung der Sozialhilfeaufgaben nicht erforderlicher Angaben allein zum Zweck der Sozialhilfestatistik ist - auch auf freiwilliger Grundlage - ausgeschlossen (siehe dazu unter 5.11.2 im 12. Datenschutzbericht 1993/94).

14.1 Wie gelangen statistische Erhebungsdaten in ein Verwaltungsgerichtsverfahren?

Eine Stadtverwaltung hielt sich in einem Verwaltungsgerichtsprozess für besonders gut vorbereitet und verletzte damit den Datenschutz.

In einem Verwaltungsgerichtsverfahren, in dem die Betriebsgröße eines landwirtschaftlichen Betriebes entscheidungserheblich war, legte die beteiligte Stadtverwaltung Angaben zu einer über zehn Jahre zurückliegenden Agrarstatistik vor. Sie hatte Duplikate der Erhebungsbögen für diese vom Landesamt für Datenverarbeitung und Statistik (LDS NRW) durchgeführte Statistik aufbewahrt.

In seinem „Volkszählungsurteil" (BVerfGE 65, 1 ff.) hat das Bundesverfassungsgericht die herausragende und konstitutive Bedeutung des Statistikgeheimnisses für die Funktionsfähigkeit der amtlichen Statistik hervorgehoben. Für den Schutz des Rechts auf informationelle Selbstbestimmung ist das Statistikgeheimnis unverzichtbar. Die Speicherung von Angaben aus einer (Agrar-)Statistik und deren Übermittlung an eine andere als die gesetzlich dafür zuständige Stelle, das LDS NRW, ist unzulässig. Ebenso unzulässig ist der Zugriff auf diese Angaben durch Stellen, die sich außerhalb der Erhebungsstelle - die räumlich, organisatorisch und personell von der übrigen Gemeindeverwaltung getrennt sein muss - befinden (§ 16 BStatG und

§§ 3 und 5 der Verordnung über die Durchführung des Agrarstatistikgesetzes NW). Sowohl die Anfertigung von Duplikaten der Erhebungsbögen, deren Aufbewahrung als auch deren Weitergabe an das Gericht stellten Datenschutzverstöße dar.

Die Stadtverwaltung hat sämtliche Duplikate von Erhebungsbögen mittlerweile vernichtet und zugesichert, die Vorschriften über die statistische Geheimhaltung künftig zu beachten. Auch sind sämtliche Schriftsätze, in denen die Statistikangaben datenschutzwidrig verwendet wurden, durch datenschutzkonforme Schriftsätze ersetzt oder die entsprechenden Angaben geschwärzt worden.

14.2 Abschottung eines Statistikbereichs datenschutzgerecht organisieren

Eine kleinere Kommune beabsichtigte die Neustrukturierung ihres Einwohnermeldeamtes in einem Großraumbüro.

Dabei war vorgesehen, einen der neuen Arbeitsplätze für einen Mitarbeiter einzurichten, der mit Aufgaben der agrarstatistischen Erhebungsstelle im Umfang von ca. 10 bis 15 % der Arbeitszeit betraut werden sollte. Fraglich ist, ob hierbei dem gesetzlichen Erfordernis einer Abschottung dieses Aufgabenbereichs von Aufgaben des Verwaltungsvollzugs genügt wird. Die Kommune hat dies selbst bezweifelt und um Stellungnahme gebeten.

Das Agrarstatistikgesetz sieht in § 3 seiner Durchführungsverordnung vom 23. Oktober 1990 (GV. NW. S. 584) vor, dass die Erhebungsstelle räumlich, organisatorisch und personell von anderen mit Aufgaben des Verwaltungsvollzugs befassten Stellen zu trennen ist. Sichergestellt werden muss weiter, dass die Erhebungsunterlagen anderen als den in der Erhebungsstelle tätigen Personen nicht zugänglich gemacht und für andere Aufgaben nicht verwendet werden.

Auch in Verwaltungen kleinerer Kommunen, in denen Beschäftigte zwangsläufig mit mehreren Aufgaben betraut sind, darf **keine dem Abschottungsgebot zuwiderlaufende Aufgabenkumulierung** vorliegen. Ein Beschäftigter, der Aufgaben im Bereich der Statistik mit einem Zeitanteil von nur 10 bis 15 % seiner Arbeitszeit zu erledigen hat, wird diese nur dann "getrennt" von ihm im übrigen übertragenen Aufgaben des Verwaltungsvollzugs verrichten können, wenn ein gebotener zeitlich versetzter Einsatz erfolgt. Erst hierbei kann von einer Trennung der Statistik von anderen kommunalen

Aufgabenbereichen im Sinne des Volkszählungsurteils gesprochen werden (BVerfGE 65, 1/ 69).

In solchen Fällen muß demnach sichergestellt werden, dass für den Bereich der Statistik eine mindestens tageweise Aufgabenzuordnung vorgesehen wird. Dies sollte in einer **Dienstanweisung** geregelt werden, in der auch die sonstigen organisatorischen und technischen Maßnahmen, die bei Einrichtung eines Großraumbüros zu treffen sind, festgelegt werden.

15. Beschäftigte und Arbeitsorganisation

Im Rahmen des **Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften** hat der Gesetzgeber eine gesetzliche Grundlage für den Zugang der Innenrevision zu Personalakten geschaffen. Die gesetzliche Neuregelung berücksichtigt leider nicht den dem Innenministerium unterbreiteten Vorschlag, das Personalakteneinsichtsrecht der Innenrevision von der Erforderlichkeit im Einzelfall abhängig zu machen.

Auch die Beteiligungsrechte der Gleichstellungsbeauftragten sind inzwischen gesetzlich geregelt. Nach dem **Landesgleichstellungsgesetz** (LGG) kann die Gleichstellungsbeauftragte oder ihre Stellvertreterin im Rahmen ihrer Mitwirkungsbefugnisse beispielsweise an Auswahlverfahren und Vorstellungsgesprächen teilnehmen. Zudem steht ihr in allen Angelegenheiten, die Maßnahmen betreffen, an denen sie zu beteiligen ist, ein Akteneinsichtsrecht zu.

Das seit langem und von vielen Seiten eingeforderte **Arbeitnehmerdatenschutzgesetz** hat das Stadium eines Gesetzentwurfs immer noch nicht erreicht. Ein solches Gesetz ist nicht nur im Rahmen der Umsetzung der EG-Datenschutzrichtlinie von 1995 notwendig. Es ist insbesondere auch deshalb erforderlich, weil die geltenden Regelungen des Bundesdatenschutzgesetzes keine zureichenden Bestimmungen zum Arbeitnehmerdatenschutz enthalten. Die vorhandenen Lücken können auch nicht durch tarifvertragliche Regelungen oder Betriebsvereinbarungen geschlossen werden. Der Arbeitnehmerdatenschutz muss dringend gesetzlich geregelt werden, um für die Arbeitnehmerinnen und Arbeitnehmer **Rechtsklarheit** und **Transparenz** zu schaffen, was mit ihren Daten zu welchen Zwecken im Arbeitsverhältnis geschieht.

Nur eine Bemerkung noch am Rande: Es bleibt zu bedauern, dass bei einer **Mitarbeiterbefragung im Innenministerium** Hinweise und Anregungen zur Durchführung eines datenschutzkonformen Verfahrens nicht berücksichtigt wurden. Bemerkenswert ist in diesem Zusammenhang allerdings, dass bei einer gleichgelagerten, durch eine andere Abteilung desselben Ministeriums initiierten Befragung dieselben datenschutzrechtlichen Mängel behoben werden konnten.

15.1 Telearbeit: Datensicherheit auch hier an erster Stelle

Öffentliche Stellen ermöglichen ihren Beschäftigten verstärkt, die beruflichen Aufgaben in Telearbeit im häuslichen Bereich zu verrichten. Verschiedene Modellprojekte dieser Arbeitsform wurden im Berichtszeitraum weiter begleitet.

Soweit Schwachstellen erkennbar wurden, die einer endgültigen Einführung entgegenstanden, wurden Möglichkeiten aufgezeigt, wie die Datensicherheit gewährleistet werden kann. Den im **14. Datenschutzbericht** unter 11.4 beschriebenen Anforderungen an die Telearbeit muss Rechnung getragen werden. Diese Arbeitsform wird sich nur dann durchsetzen können, wenn die erforderlichen Datensicherheitsmaßnahmen zuverlässig getroffen und in geeigneter Weise überwacht werden (§ 10 DSG NRW).

Es empfiehlt sich, vor einer dauerhaften Einrichtung von Telearbeitsplätzen eine **Dienstvereinbarung mit dem Personalrat** abzuschließen (§ 70 LPVG). Durch Kontrollbesuche und verschiedene Beratungsgespräche hat sich bestätigt, dass eine solche Regelung besonders geeignet ist, die datenschutz-, dienst- und arbeitsrechtlichen sowie die organisatorisch-technischen Voraussetzungen als Bedingungen für eine Telearbeit verbindlich festzuschreiben. Dabei sollten besonders folgende Gesichtspunkte berücksichtigt werden:

- Soweit im Rahmen der Telearbeit auch personenbezogene Daten außerhalb der öffentlichen Stelle verarbeitet werden, hängt der Umgang mit diesen entscheidend von der **Verlässlichkeit der auszuwählenden Beschäftigten** ab.
- In **Vereinbarungen mit den Beschäftigten**, die die Telearbeit zum Gegenstand haben, sollte auf die in der Dienstvereinbarung geregelten Rechte und Pflichten der Beteiligten Bezug genommen werden.
- Bei **Abrechnung dienstlich veranlasster Telekommunikationskosten** dürfen die Betroffenen nicht im Unklaren gelassen werden, dass sie nur Abrechnungsdaten über die dienstlich veranlassten Telekommunikationskosten bekannt zu geben haben und Daten über privat geführte Telefonate nicht vorzulegen brauchen.

Spezielle Datensicherheitsanforderungen: Die Einrichtung von Telearbeitsplätzen bedarf grundsätzlich eines **Sicherheitskonzepts**, in dem die organisatorischen und technischen Maßnahmen zu ermitteln und zu dokumentieren

sind (§ 10 DSG NRW). Die folgenden Beispiele verdeutlichen einige festgestellte Defizite, die sich durch ein solches Konzept vermeiden lassen:

- In einer Kommune wurden **Sozialdaten** in Telearbeit verarbeitet. Der Telearbeitsplatz war über ISDN an das städtische Verwaltungsnetz angebunden. Die zwischen dem Telearbeitsplatz und dem städtischen Netz übermittelten Daten wurden nicht mittels eines anerkannten und sicheren kryptographischen Verfahrens verschlüsselt übertragen. Insofern wurde der hohen Sensibilität der übermittelten Daten nicht durch entsprechende Datensicherheitsmaßnahmen Rechnung getragen.

- Auch die **eingesetzte Software** erwies sich in dieser Kommune als nicht geeignet. Das eingesetzte Verfahren zur Verarbeitung der Sozialdaten befand sich auf dem Arbeitsplatzrechner der Beschäftigten in ihrem Büro bei der Stadtverwaltung und wurde von ihrem Telearbeitsplatz aus unter Verwendung einer für Zwecke der **Fernwartung** entwickelten Software ferngesteuert. Dadurch ergaben sich Risiken, die bei der Verarbeitung von Sozialdaten nicht hingenommen werden können. Daher musste dieser Kommune empfohlen werden, die Telearbeit vorläufig einzustellen.

- In einem anderen Telearbeitsprojekt war vorgesehen, zur Sicherung des Zugangs durch Online-Verbindung zum Datennetz einer öffentlichen Stelle einen so genannten **elektronischen Fingerabdruck** auf dem Server der öffentlichen Stelle zu hinterlegen. Aus Sicht des Datenschutzes ist dies nicht akzeptabel. Biometrische Authentifikationsverfahren sind zur sicheren Identifikation der Nutzerinnen und Nutzer zwar geeignet, zu bedenken ist jedoch, dass von dem elektronischen Fingerabdruck, einem biometrischen Merkmal, unmittelbar auf die Person rückgeschlossen werden kann. Außerdem ist die Bindung zwischen biometrischen Referenzdaten und Personen häufig auf natürliche Weise gegeben und hält dauerhaft an. Die zentrale Speicherung dieser Daten auf einem Serversystem birgt grundsätzlich eine nicht zu vernachlässigende Gefahr für das informationelle Selbstbestimmungsrecht der Betroffenen. Deshalb dürfen gegebenenfalls nur solche biometrischen Authentifikationsverfahren eingesetzt werden, die eine Speicherung der erforderlichen biometrischen Referenzdaten ausschließlich auf einem im Besitz der Nutzerin oder des Nutzers verbleibenden Speichermedium - zum Beispiel einer Chipkarte - vorsehen.

Der Einsatz ungeeigneter Hard- oder Software und Defizite bei sonstigen organisatorischen oder technischen Maßnahmen bergen **vermeidbare Risiken** für die zu verarbeitenden Daten. Diesen lässt sich durch Erstellung eines Sicherheitskonzepts wirksam begegnen. Erst hierdurch wird dem besonderen gesetzlichen Sicherstellungsauftrag genügt.

15.2 Zuviel Transparenz in einem Beurteilungsverfahren

Um das Beurteilungsverfahren durchschaubarer zu machen, hat die Leitung einer Polizeibehörde in einer Verfahrensanweisung Informationsgrundlagen für alle Erstbeurteilenden schaffen wollen.

Die Personalstelle hatte zu diesem Zweck allen Erstbeurteilenden, durch die Beamtinnen und Beamte einer Vergleichsgruppe zu beurteilen waren, Namenslisten mit Personalaktendaten (Angaben über den Eintritt in den Polizeidienst bis zur 2. Fachprüfung) aller in der Vergleichsgruppe zu Beurteilenden überlassen. Auf Grund dieser Daten waren über die zu Beurteilenden so genannte "Kompetenzprofile" zu erstellen, die von den Erstbeurteilenden in verschiedenen "Maßstabsbesprechungen" erläutert werden sollten. Hierdurch sollten sie in die Lage versetzt werden, die erbrachten Leistungen der zu Beurteilenden in den Gesamtkontext der jeweiligen Laufbahn und Besoldungsgruppe einzuordnen.

Die Beurteilung von Beschäftigten ist eine wenig beliebte Angelegenheit. Umso wichtiger ist es, dass die für die Erstellung von Beurteilungen Verantwortlichen auf die richtigen Informationsgrundlagen achten und die Verfahrensschritte in den für die Polizeibehörden verbindlichen Beurteilungsrichtlinien berücksichtigen. Dies wurde von der Polizeibehörde übersehen. Es war bereits datenschutzrechtlich unzulässig, den Erstbeurteilerinnen und Erstbeurteilern die genannten Listen auszuhändigen. In den Beurteilungsrichtlinien ist dies nicht vorgesehen. Sie konkretisieren die Aufgaben und Pflichten der Erstbeurteilenden dahin, dass sie in der Lage sein müssen, sich aus eigener Anschauung und nach ihren Kenntnissen und Erfahrungen ein Urteil über die von ihnen zu Beurteilenden zu bilden. In die Erstbeurteilung dürfen demnach keine Erkenntnisse über von den jeweiligen Erstbeurteilerinnen oder Erstbeurteilern **nicht** zu beurteilende Beamtinnen und Beamte einfließen.

Die beabsichtigte Schaffung der Informationsgrundlagen stand darüber hinaus nicht mit dem Grundsatz im Einklang, dass der Kreis der mit Personalakten und Personalaktendaten befassten Beschäftigten möglichst eng zu halten ist.

Erfreulicherweise hat sich die Polizeibehörde davon überzeugen lassen, dass dem Folgenbeseitigungsanspruch der Betroffenen genügt werden musste. Die Unterlagen wurden wieder eingesammelt. Nach einer Sperrfrist werden sie gelöscht oder Betroffenen auf Wunsch ausgehändigt.

15.3 Ab in den Reißwolf – oder in die "Vorstehernebenakte"?

Bemerkenswerte Kreativität entwickeln Behörden bei der Aufbewahrung von Vorgängen, die nicht zugeordnet oder - aus welchen Gründen auch immer - nicht erledigt werden können, die man sich aber auch nicht zu vernichten traut.

So machte der Personalrat eines Finanzamtes auf die Existenz von "**Vorstehernebenakten**" aufmerksam, in denen solche Vorgänge, aber auch Vermerke über "geringfügige Verfehlungen" von Beschäftigten, die keiner dienst- oder arbeitsrechtlichen Behandlung bedurften, gesammelt und unbegrenzt aufgehoben wurden. Nach Intervention des Personalrates wurden diese Bestände allerdings bereits aus der "Vorstehernebenakte" entfernt und vernichtet. Personalaktenrelevante Vorgänge werden dort somit nicht mehr in Sachakten aufbewahrt, sondern gemäß den personalakten- oder tarifrechtlichen Vorschriften behandelt. Vergleichbare Sammelakten haben unter dieser oder anderer Bezeichnung nicht nur in Finanzämtern Tradition und werden nicht selten von einem Amtsinhaber zum anderen gereicht.

Es empfiehlt sich dringend, solche Sammlungen sehr kritisch durchzusehen.

16. Wirtschaft

Mit dem neuen Landesdatenschutzgesetz wurden Mitte 2000 die Datenschutzkontrolle in der öffentlichen Verwaltung und in der privaten Wirtschaft unter dem Dach der Landesbeauftragten für den Datenschutz zusammengefasst. Damit ist eine bürgerfreundliche Lösung gefunden worden, die Datenschutzaufsicht aus einer Hand gewährleistet und die schwer vermittelbare Zuständigkeitsaufsplitterung beendet.

Seit der gesetzlichen Zuweisung des neuen Aufgabenfeldes sind schon vielfältige Kontakte zu Organisationen der Wirtschaft und der Verbraucherverbände, aber auch zu einzelnen Unternehmen entstanden. Auch mit berufsständischen Organisationen wie Handelskammern und Handwerkskammern werden Gespräche geführt. Vor allem ist mit dem Deutschen Industrie- und Handelstag (DIHT) intensiv erörtert worden, welche Möglichkeiten der Einrichtung einer bundesweiten Online-Datenbank über seine Mitgliedsfirmen bestehen. Die hierzu notwendige Gesetzesänderung des IHK-Gesetzes ist in Vorbereitung.

16.1 Umgang mit Schuldnerdaten in der Wirtschaft

16.1.1 Handel mit Schuldnerdaten

Unter der Bezeichnung "**Vertrauliche Mitteilungen**" veröffentlicht ein Verlag gegen Entgelt "im Auftrag und mit Genehmigung der Industrie- und Handelskammern zu Berlin, Bochum, Dortmund, Land Hessen, Münster und Land Schleswig-Holstein" die kompletten Schuldnerdaten aus den Schuldnerverzeichnissen der genannten Gebiete in Papierform und in elektronischer Form. Die Schuldnerlisten enthalten alle eidesstattlichen Versicherungen zu Vermögensverhältnissen (früher: Offenbarungseid), Haftbefehle zur Erzwingung solcher Erklärungen und die mangels Masse abgewiesenen Konkursanträge aus den amtlichen Registern der Vollstreckungsgerichte bei den Amtsgerichten. Das Angebot richtet sich an Unternehmen, die Mitglied einer Handelskammer oder Handwerkskammer sind. Der Verlag wirbt damit, dass die "Vertraulichen Mitteilungen" im besonderem Maße geeignet sind, sich vor Firmen und Personen zu schützen, die zahlungsunfähig oder zahlungsunwillig sind.

Grundsätzlich kann gegen solche Datenverkäufe nicht vorgegangen werden. Nach § 915 ZPO dürfen personenbezogene Schuldnerdaten für Zwecke verwendet werden, die mit der Feststellung der wirtschaftlichen Zuverlässigkeit zu tun haben, um unter anderem wirtschaftliche Nachteile abzuwen-

den, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Zu diesem Zweck ist es den Kammern erlaubt, unter bestimmten Voraussetzungen von den Gerichten Abdrucke der Schuldnerverzeichnisse zum laufenden Bezug zu erhalten und diese in Listenform an ihre Mitglieder weiter zu geben. Mit dem Versand der Schuldnerlisten können auch Dritte beauftragt werden (§ 915e ZPO).

Die Bewilligung der Anträge auf laufenden Bezug der Schuldnerlisten erfolgt durch die Kammer selbst und nicht etwa durch den Verlag. Allerdings stellte sich heraus, dass die Kammer lediglich prüfte, ob die Bestellerin oder der Besteller Kammermitglied ist. Dies aber ist unzureichend, weil zusätzlich bei einer Bestellung glaubhaft zu machen ist, dass die Schuldnerdaten zur Beurteilung der wirtschaftlichen Zuverlässigkeit benötigt werden **und** dies nicht bereits durch Einzelauskünfte erfolgen kann.

Ein spezielles Problem stellt die Einhaltung der **Löschungsverpflichtung** bei den Bezieherinnen und Beziehern der Listen dar. Sie sind wie die Amtsgerichte verpflichtet, die in den Schuldnerverzeichnissen enthaltenen Eintragungen grundsätzlich nach Ablauf von drei Jahren zu löschen. Eine vorzeitige Löschung hat beispielsweise zu erfolgen, wenn die Schulden beglichen sind.

Der Abonnementvertrag enthält einen umfangreichen Verpflichtungstext zum datenschutzgerechten Umgang mit den Schuldnerdaten. Darin wird darauf hingewiesen, dass die personenbezogenen Schuldnerinformationen nur zur Prüfung der wirtschaftlichen Zuverlässigkeit genutzt werden dürfen. In der Verpflichtungserklärung wird insbesondere die vertrauliche Behandlung auch innerhalb des Unternehmens verlangt und auf die Beachtung der Löschungsregelungen hingewiesen. Der Verpflichtungstext ist aber verbesserungsbedürftig.

Die Verpflichtungserklärung sollte um den Passus ergänzt werden, dass bei einem Verstoß gegen diese Pflichten das Abonnement gekündigt werden und insbesondere bei einer unzulässigen Nutzung der Schuldnerdaten von den Betroffenen Schadensersatz verlangt werden kann.

16.1.2 Schuldnerdaten zur Bonitätsprüfung

Zur Bonitätsprüfung bedienen sich Kreditinstitute in der Regel der Datenbestände der Wirtschaftsauskunfteien, insbesondere der der Schutzgemeinschaft für allgemeine Kreditsicherung, kurz **Schufa** genannt. Sie gehört zu jenen Einrichtungen, denen regelmäßig Abdrucke aus den Schuldnerver-

zeichnissen überlassen werden dürfen. Damit ist ihnen erlaubt, zentrale bundesweite oder regionale Schuldnerverzeichnisse zu führen.

Bei der Schufa verbleiben Angaben über Haftbefehle und eidesstattliche Versicherungen für drei Jahre im Datenbestand. Wird eine vorzeitige Löschung gewünscht, ist eine Löschungsbescheinigung des zuständigen Amtsgerichtes einzureichen. Ein Kreditinstitut erfährt von diesen Eintragungen nur auf Anfrage und nur im Zusammenhang mit der Eröffnung eines Girokontos, der Aufnahme eines Kredites, der Eingehung einer Bürgschaftsverpflichtung oder dem Abschluss eines Kreditkartenvertrages. Die Kundin oder der Kunde ist hierbei regelmäßig vor Unterzeichnung der Schufa-Klausel über das Schufa-Verfahren zu informieren. Nach erteilter Auskunft kann es zu Nachmeldungen der Schufa an das Kreditinstitut kommen, wenn eine Eintragung im Schuldnerverzeichnis gelöscht wurde.

Der Umgang mit den Daten der Kundinnen und Kunden wurde bei mehreren Sparkassen geprüft: In einem Fall speicherte eine Sparkasse über einen Betroffenen noch Angaben über die Abgabe seiner eidesstattlichen Versicherung, obwohl diese Eintragung nach Ablauf der Dreijahresfrist bereits in dem Schuldnerverzeichnis gelöscht war. Überdies konnten auch fremde Personen an seinem früheren Finanzproblem teilhaben, weil bei jedem Aufruf seines Kontos am Bildschirm des Kassenschalters der Hinweis "Eidesstattliche Versicherung" in Schriftgröße 30 erschien.

Diese Sparkasse hat zugesagt, dass derartige Merkmale nach Eingang der entsprechenden Servicemeldung der Schufa sofort gelöscht werden. Die großformatige Bildschirmanzeige wurde abgestellt. Darüber hinaus sollen generell nur noch die Merkmale und Informationen über Kundinnen und Kunden per Anforderung auf dem Bildschirm erscheinen, die zur Abwicklung des jeweiligen Geschäftsvorganges erforderlich sind.

Von einer **"ewigen" Speicherung von Schuldnerdaten** kann im Zusammenhang mit einer anderen Sparkasse gesprochen werden. Dem Dateiauszug der Sparkasse war zu entnehmen, dass zu der Eintragung im Schuldnerverzeichnis zusätzlich ein Vermerk über die Löschung gespeichert war, statt die Eintragung tatsächlich zu löschen. Mit einer weiteren Dateneingabe wurde verfügt, dass diese Angaben in einhundert Jahren gelöscht werden sollten. Darauf hingewiesen löschte diese Sparkasse die Daten sofort. Bei näherer Prüfung stellte sich zudem heraus, dass die Datenspeicherung auf einem "elektronischen Schmierzettel" erfolgte. Das automatisierte Sparkassenverfahren sieht die Anwendung einer solchen so genannten Notizfunktion vor, die es den Sparkassenbeschäftigten ermöglicht, Aktenvermerke über ihre Kundinnen und Kunden, wie in dem Beschwerdefall über frühere

Zwangsvollstreckungsmaßnahmen anzufertigen. Insbesondere sollten solche Daten nicht darin gespeichert werden dürfen, die besonders sensibel sind und bei denen gesetzliche Verwendungsregelungen beachtet werden müssen. Im übrigen sieht das ADV-Verfahren bereits in einem Schlüsselverzeichnis die Speicherung und automatische Löschung derartiger Warnvermerke vor.

Zur Anwendung von "elektronischen Schmierzetteln" sollte in den internen Geschäftsanweisungen festgelegt werden, welche Daten in der Notizfunktion festgehalten werden dürfen. Dabei sind Hinweise auf Aufbewahrungs- und Löschungsfristen zu geben.

16.1.3 Schuldnerdaten im Internet

Ein markantes Beispiel für den datenschutzrechtlich unzulässigen Umgang mit Schuldnerdaten in der Wirtschaft ist folgendes: Eine Handelsagentur hatte auf ihrer Homepage im Internet die Daten ihrer säumigen Schuldnerinnen und Schuldner eingestellt. Aufgeführt waren der Name und Wohnort, die Rechnungsnummer, der Betrag und, besonders bemerkenswert, der derzeitige Stand des Verfahrens. Unter dieser Rubrik war nachzulesen, ob ein Gerichtsvollzieher eingeschaltet, eine eidesstattliche Versicherung abgegeben, ein Inkassounternehmen beauftragt oder ein Mahn- oder Vollstreckungsbescheid beantragt worden war.

Die Einstellung von Daten in das Internet ist eine Übermittlung an Dritte im Sinne des BDSG und bedarf deshalb einer gesetzlichen Grundlage. Eine solche existiert jedoch nicht. Selbst wenn ein berechtigtes Interesse des Unternehmens im Sinne des einschlägigen § 28 BDSG angenommen würde, dürften jedenfalls die schutzwürdigen Interessen der betroffenen Personen am Ausschluss der Übermittlung dies überwiegen. Die Veröffentlichung der Daten im Internet macht sie weltweit allen Interessierten zugänglich. Derart sensible Daten gehören aber nicht in die Öffentlichkeit, weil eine Kenntnisnahme durch Dritte für die betroffenen Personen in jedem Fall diskriminierend wirkt. Demgegenüber muss das Interesse des speichernden Unternehmens an der Einziehung seiner Außenstände, das selbstverständlich auch anzuerkennen ist, zurückstehen, zumal es legale Möglichkeiten gibt, um Schulden einzufordern. Überdies kann eine unbezahlte Rechnung verschiedene Ursachen haben, die nichts mit einer Zahlungsunfähigkeit oder Zahlungsunwilligkeit der Kundinnen und Kunden zu tun haben müssen. Damit überwiegt hier eindeutig das schutzwürdige Interesse der betroffenen Personen am Ausschluss der Übermittlung. Das Vorgehen des Unternehmens ist rechtswidrig und stellt einen groben Verstoß gegen datenschutzrechtliche

Vorschriften dar. Gleichwohl stehen nach dem derzeit geltenden Bundesdatenschutzgesetz keine wirksamen aufsichtsbehördlichen Mittel zur Verfügung, um ein solches Verhalten zu unterbinden.

16.2 Führung von Guthabenkonten

Nach wie vor sind Defizite bei der Bearbeitung von Anträgen auf Eröffnung von **Guthabenkonten** festzustellen. Im 13. Datenschutzbericht 1995/96 wurde unter 19.4 zur Einrichtung von Girokonten für Sozialhilfeberechtigte bereits dargelegt, dass bei ausnahmslos auf Guthabenbasis geführten Girokonten die Einholung einer Schufa-Auskunft nicht notwendig ist, weil ein wirtschaftliches Risiko für das Kreditinstitut nicht besteht. Nur dann, wenn beispielsweise die Teilnahme am Lastschriftverfahren gewünscht wird, mit dem dann auch die Möglichkeit der Kontoüberziehung eingeräumt ist, bestehen gegen die Einholung einer Schufa-Erklärung keine Bedenken. Bei mehreren Überprüfungen von Sparkassen musste allerdings festgestellt werden, dass die Kundinnen und Kunden erst gar nicht auf die Möglichkeit der Einrichtung eines "schufalosen" Kontos hingewiesen werden.

Die Kreditinstitute sollten ihre Geschäftsanweisungen zur Eröffnung von Girokonten so abfassen, dass in der Kundenberatung von vornherein auch auf die Möglichkeit der Führung eines "schufalosen" Kontos hingewiesen wird.

16.3 Moderne Technik mangelhaft

Für die banktypischen Alltagsgeschäfte verweisen die Kreditinstitute ihre Kundinnen und Kunden gerne auf ihre technischen Selbstbedienungsgeräte. Die Vorteile dieses Technikeinsatzes scheinen für die Kundinnen und Kunden zu überwiegen: Geld kann rund um die Uhr abgehoben, der Kontoauszug Tag und Nacht abgerufen werden. Jedoch sind datenschutzrechtlich problematische Nebeneffekte nicht ausgeschlossen.

So beschwerte sich ein Kunde einer Sparkasse, weil er sich beim Geldabheben an einem Bankautomaten unerwünschten Schulterblicken ausgesetzt fühlte. Er berichtete, dass gleich nachdem er seine Geheimnummer eingetippt hatte, automatisch sein Kontostand rechts oben auf dem Bildschirm erschien und von der hinter ihm wartenden Person gleich mit gelesen werden konnte. Die Sparkasse reagierte schnell: Es wurden nicht nur kurzfristig alle derart problematischen Geräte ausgetauscht, sondern auch die Software da-

hingehend geändert, dass der angeforderte Betrag nur noch per Knopfdruck eingeblendet wird.

16.4 Elektronischer Zahlungsverkehr

Die datenschutzrechtliche Bewertung der elektronischen Geldbörse durch die Aufsichtsbehörden und deren Vorschläge zur Verbesserung des Datenschutzes sind inzwischen mit der Kreditwirtschaft erörtert worden. Abschließend hat sie auch der "Düsseldorfer Kreis" zustimmend zur Kenntnis genommen. Im Wesentlichen sind damit die im 14. Datenschutzbericht 1999 unter 12.4.2 als noch offen behandelten Fragen geklärt.

- Ausgangspunkt für eine abschließende datenschutzrechtliche Bewertung ist die unter den Aufsichtsbehörden übereinstimmend getroffene Feststellung, dass die bei der Evidenzzentrale geführten Schattensalden grundsätzlich ungeeignet sind, Nutzungsprofile zu erstellen. Die Schattensalden werden getrennt von den Umsatzdaten - das sind die zu jeder Geldkarte gespeicherten Kauf-Transaktionsdaten - gespeichert. Es besteht ein erhöhtes Risiko durch die Kumulierung kartenbezogener Daten in der Evidenzzentrale, die aus den unterschiedlichen Funktionen zusammenkommen können, wenn sie miteinander verknüpft werden.

- Deshalb müssen die Kartendaten - soweit sie in den Funktionen der Kunden-, Händler- und Ladezentralen benötigt werden - in technisch und organisatorisch voneinander abgeschotteten Bereichen verarbeitet werden. Dies gilt vor allem, soweit die Evidenzzentrale zugleich als Rechenzentrum für die angeschlossenen Kreditinstitute die Kontoführung für alle geldkartenbezogenen Konten durchführt. Die meiner Kontrolle unterliegende Evidenzzentrale wird nachweisen müssen, dass sie die zur Abschottung notwendigen Sicherheitsmaßnahmen in ausreichendem Umfang getroffen hat.

- Die "Vereinbarung über das institutsübergreifende System Geldkarte" zu diesem Datentransfer ist insoweit noch unzureichend. Den Kreditinstituten und ihren Verbänden wird empfohlen, in der Vereinbarung ein Verbot kartenbezogener Auswertung in ihrer Evidenzzentrale sicherzustellen. Außerdem muss das Zusammenwirken der verschiedenen Funktionen innerhalb der Evidenzzentrale wie auch das Zusammenwirken der Evidenzzentralen untereinander geregelt werden. Insbesondere sind dazu Anlass und Entscheidungsebene für ein Zusammenwirken festzulegen sowie die Dokumentation dieses Vorganges vorzusehen.

- Die Kreditinstitute können als Auftraggeberinnen oder Auftraggeber nur insoweit befugt sein, der Evidenzzentrale Aufträge zu erteilen, die zu einer Verknüpfung von dort gespeicherten Kartendaten mit der kontobezogenen Geldkarte führen können, als dies zur Klärung eines von einer Karteninhaberin oder einem Karteninhaber vorgetragenen Reklamationsfalles erforderlich ist. Andernfalls würde eine unbegrenzte Zugriffsmöglichkeit der kontoführenden Kreditinstitute die innerhalb der Evidenzzentrale geschaffene faktische Anonymisierung durchbrechen.
- Der kritisierte Umstand, dass die Kartendaten aus den Zahlungsvorgängen in der Evidenzzentrale zu lange aufbewahrt werden, ist nicht den Kreditinstituten anzulasten. Daher soll versucht werden, die bankaufsichtlich veranlasste langjährige Dokumentation der kartenbezogenen Zahlungsvorgänge auf die unbedingt notwendige Aufbewahrungsdauer - etwa die Reklamationsspanne - zu verkürzen.
- Die Kreditinstitute müssen ihre Kundinnen und Kunden hinreichend deutlich und in allgemein verständlicher Form darüber aufklären, auf welchen Wegen die Daten aus den Transaktionen mit der Geldkarte transportiert, an welchen Stellen sie gespeichert und wie lange sie aufbewahrt werden. Nur so kann die notwendige Transparenz der Datenverarbeitung hergestellt werden, wie sie insbesondere bei der Ausgabe von Chipkarten zu fordern ist. Außerdem muss klar bestimmt sein und darüber informiert werden, wo und in welchem Umfang Auskunftsansprüche der Kundinnen und Kunden erfüllt werden. Der Auskunftsanspruch muss folgerichtig entsprechend dem begrenzten Auskunftsanspruch der Kreditinstitute gegenüber der Evidenzzentrale auf Reklamationsfälle begrenzt sein. Leider fehlt es immer noch an dementsprechenden Informationen für die Kundinnen und Kunden.
- Schließlich muss sichergestellt sein, dass Ausgabe und Rückvergütung - etwa im Falle eines Defektes - einer **kontoungebundenen** Geldkarte ohne Bekanntgabe von Namen und Bankverbindung erfolgt. Nur so ist gewährleistet, dass die Nutzung der nur mit Bargeld aufladbaren Geldkarte ohne Bindung an ein Konto **anonym** erfolgt.

Die Entwicklung auch der Geldkarte bleibt nicht stehen. So wird daran gearbeitet, die Geldkarte für den **E-Commerce** fit zu machen. Dazu ist ein Terminal für Kundinnen und Kunden mit separater Tastatur und Display vorgesehen, das an den PC angeschlossen einen in den digitalen Einkauf integrierten Zahlvorgang ermöglicht. Die Separierung der Eingabe des Geldbetrages von der Tastatur des PC stellt sicher, dass die online-Händlerin oder der online-Händler keinen Einfluss auf die Abbuchung des Geldbetrages von der Geldkarte nehmen kann. Die Übertragung der Kartendaten er-

folgt verschlüsselt. Weiterhin soll die Geldkarte mit der Zusatzanwendung "digitale Signatur" ausgebaut werden. Dazu ist ein Chip mit großer Speicherkapazität erforderlich. Eine Implantierung dieses Chips wird wahrscheinlich wegen der höheren Kosten nicht in allen Geldkarten, sondern nur in begrenzter Stückzahl für einen bestimmten Personenkreis erfolgen.

Nach wie vor ist die Verwendung der kontoungebundenen Geldkarten (white cards) zur Bezahlung an Automaten, von Kleinbeträgen und im E-Commerce zu empfehlen. Nur so werden keine Datenspuren hinterlassen.

16.5 Das intelligente Verkehrsticket

Wie oben bereits erwähnt, ist auf dem Chip der Geldkarte noch Speicherkapazität für Zusatzanwendungen vorhanden. Sie könnte unter anderem auch von Verkehrsunternehmen für "elektronische Fahrscheine" genutzt werden. Im Gegensatz zum herkömmlichen birgt allerdings der "elektronische Fahrschein" weitaus mehr technische Möglichkeiten der Datenerfassung und -speicherung und wirft somit auch einige Risiken auf, die mit entsprechenden Maßnahmen abgefangen werden müssen.

In Nordrhein-Westfalen sind die Verkehrsverbünde bisher mit dem Pilotprojekt "i-Ticket" des Verkehrsverbundes Rhein-Sieg (VRS) und dem geplanten Einsatz eines elektronischen Fahrscheins als Zusatzanwendung auf der Geldkarte durch den Verkehrsverbund Rhein-Ruhr (VRR) in Erscheinung getreten. Das Pilotprojekt ist von der damals noch zuständigen Aufsichtsbehörde, der Bezirksregierung Köln, geprüft worden; dieses Projekt ist abgeschlossen und wird im Hinblick auf einen späteren Einsatz evaluiert.

Rein optisch unterscheidet sich die für das Pilotprojekt entwickelte Chipkarte von einer bloßen Zusatzanwendung der Geldkarte dadurch, dass das "i-Ticket" mit einem eigenen Chip, also auch mit größerer Speicherkapazität versehen, die Rückseite der Geldkarte ausfüllt. Die Geldkarte selbst ist als Guthaben-Karte ausgelegt und wird ausschließlich mit Bargeld aufgeladen. Ihr fehlt damit die von den Kreditinstituten üblicherweise installierte Anbindung an ein Konto der Karteninhaberin oder des Karteninhabers, so dass hier eine **anonyme Zahlweise** gewährleistet ist. Diese Geldkarte lässt sich nicht nur in Fahrscheinautomaten, sondern selbstverständlich auch in allen anderen Automaten und allen Einkaufskassen mit dem Geldkartenlogo einsetzen. Somit kann die Verwendung einer Guthaben-Karte aus datenschutzrechtlicher Sicht auf jeden Fall positiv bewertet werden.

Bei der Ausgestaltung des auf der Rückseite aufgedruckten "i-Tickets" mit dem implantierten Chip sowie bei der Nutzung der Zusatzanwendung im Geldkartenchip (wie in der Planung des VRR) sollten im Sinne einer datenschutzgerechten Anwendung folgende Anforderungen erfüllt sein:

- **Speicherung und Nutzung im Verkehrsbetrieb und im Verbund**

  Der Verkehrsbetrieb ist speichernde Stelle und für die Einhaltung des Datenschutzes verantwortlich. Die im Zusammenhang mit der Bezahlfunktion gespeicherten Daten müssen abgeschottet von den Fahrscheindaten verarbeitet werden. Die Bezahldaten dürfen nur zur Abrechnung mit der Händlerkarte zusammengeführt und der für den Verkehrsbetrieb zuständigen Evidenzzentrale übermittelt werden. Das bedeutet insbesondere, dass die Geldkarten-Identitätsnummer nicht mit der Kartennummer der Fahrschein-Anwendung identisch sein darf. Die Zweckbindung der Fahrscheindaten muss auf die Fahrtabwicklung und den eventuellen Reklamationsfall beschränkt sein. Es darf weder eine kartenbezogene Auswertung erfolgen noch dürfen kartenbezogene Bewegungsprofile erstellt werden. Für Statistiken müssen anonymisierte Daten verwendet werden, die Kartennummer muss also durch eine andere automatisiert vergebene Zufallsnummer ersetzt werden.

  Die Speicherung von Kartennummer und Fahrscheindaten muss so kurz wie möglich sein. Sie ist allenfalls bis zum Ablauf der Gültigkeitsdauer und Reklamationsfrist notwendig. Spätestens dann sollte die fahrscheinbezogene Kartennummer im Rechner des Verkehrsunternehmens gelöscht werden. Die in den stationären und mobilen Terminals gespeicherten Daten sollten bereits nach erfolgreicher Übertragung an den Rechner gelöscht werden. Die Datenübertragung sollte automatisiert erfolgen. Die im Einreichungs-Terminal gespeicherten Bezahltransaktionsdaten aus der Geldkarte müssen, sofern sie noch nach Einreichung zur Evidenzzentrale gespeichert bleiben, unverzüglich nach Erhalt der Zahlung - spätestens nach drei Monaten - gelöscht werden. Eine Übermittlung der gespeicherten Daten an den Verkehrsverbund dürfte, soweit Fahrscheindaten zur Abrechnung unter den Verkehrsunternehmen überhaupt erforderlich sind, auch ohne die Kartennummer ausreichen, da ihre Kenntnis zur Abrechnung nicht notwendig erscheint.

- **Transparente Nutzung von "i-Ticket" und Geldkarte für die Fahrgäste**

  Die Verkehrsunternehmen müssen ihre Fahrgäste umfassend über die Datenverarbeitungsvorgänge auf dem Chip des "i-Tickets" oder in der Zusatzanwendung der Geldkarte aufklären, insbesondere welcher Verarbeitungsvorgang im Einzelnen abläuft und welcher Vorgang durch sie

selbst angestoßen wird. Die Fahrgäste müssen auch darüber informiert sein, ob und welche Daten personenbezogen verarbeitet werden. Personenbezug besteht selbst dann, wenn nur die Kartennummer gespeichert ist, diese aber mit Hilfe einer Kartenausgabe-Datei einer bestimmten Person zugeordnet werden kann. Weiter sollten öffentliche, stationäre Kartenlesegeräte zum Beispiel in den Servicezentren oder an zentralen Haltestellen bereitstehen. Sie ermöglichen jederzeit das Lesen der aktuell gespeicherten unverbrauchten wie der verbrauchten Fahrscheine. Da verbrauchte Fahrscheine erst durch Überschreiben gelöscht werden, können abgelaufene Fahrscheine noch eine lange Zeit lesbar bleiben. Deswegen sollte das Kartenlesegerät außerdem mit gezieltem Zugriff auf das Fahrscheinregister und Betätigung der Löschtaste die sofortige Löschung eines verbrauchten Fahrscheines möglich machen. Über diese Einwirkungsmöglichkeit sollten die Fahrgäste selbstverständlich auch unterrichtet werden. Die notwendigen Informationen können auf einem Informationsblatt zusammengestellt und den Fahrgästen in geeigneter Form zugänglich gemacht werden.

- **Nutzung durch Kontrolleurinnen und Kontrolleure**

  Der Lesezugriff des Kontrollpersonals sollte sich grundsätzlich auf den Fahrschein beschränken, der eine Fahrberechtigung für die kontrollierte Fahrt nachweist. Bei Fahrten im Verbund erfolgt der Zugriff auf den Verbundfahrschein. Dagegen ist ein Zugriff auf alle abgespeicherten Fahrscheine, die für die kontrollierte Fahrt nicht benötigt werden nicht erforderlich.

- **Keine Nachteile für Guthabenkarten**

  Wenn der Verkehrsverbund oder der einzelne Verkehrsbetrieb die Zusatzanwendung auf der Geldkarte nutzen will, so hat er schließlich darauf zu achten, dass den Fahrgästen, die im Besitz von Guthabenkarten oder kontoungebundenen Geldkarten sind, **keine Nachteile** entstehen.

Eine rechtzeitige vorherige Beteiligung der Datenschutzaufsichtsbehörde wäre wünschenswert, damit bei Einführung der elektronischen Fahrscheine eine Beratung zur Verbesserung des Datenschutzes erfolgen kann. Gespräche mit dem Verband Deutscher Verkehrsunternehmen sind bereits ins Auge gefasst.

16.6 Call Center

Wer sich schon gefragt hat, was eigentlich hinter den so häufig anzutreffenden Vorwahlnummern 0180 oder 0800 steckt, dem wird nicht verborgen geblieben sein, dass Call Center wie Pilze aus dem Boden schießen. Die damit beabsichtigte Serviceorientierung soll eine vereinfachte Abwicklung von Geschäften oder Reklamationen ermöglichen, ist aber nicht ohne datenschutzrechtliche Probleme.

Grundsätzlich sind zwei verschiedene Arten der Call Center zu unterscheiden: die internen, die eine Fachabteilung des betreffenden Unternehmens sind, und die externen, die als rechtlich selbständige Gesellschaften als Dienstleister für andere Unternehmen arbeiten.

16.6.1 Telefonbanking

Weit verbreitet sind Call Center im Bereich des Telefonbanking. Dort werden nahezu alle Arten von einfachen Bankgeschäften abgewickelt, beispielsweise Überweisungen, Kontostandsabfragen, Einrichtung von Daueraufträgen und Wertpapiergeschäfte. Grundlage des Telefonbanking ist regelmäßig eine besondere Vereinbarung zwischen Kunde oder Kundin und Bank, die in datenschutzrechtlicher Hinsicht einigen Voraussetzungen genügen muss.

Sollen Telefongespräche zu Beweiszwecken in Reklamationsfällen aufgezeichnet werden, dann ist das nur mit ausdrücklicher Einwilligung der Kunden und Kundinnen zulässig, weil die Vertraulichkeit des Wortes geschützt ist. Die Einwilligungserklärung muss auf den Zweck der Aufzeichnung hinweisen. Wenn die Erklärung - wie üblich - im Rahmen der Telefonbankingvereinbarung abgegeben werden soll, muss sie sich zudem im äußeren Schriftbild abheben. Aufgezeichnete Telefongespräche dürfen nur solange wie erforderlich aufbewahrt werden. Dabei wird nach den Erfahrungen der Praxis eine Speicherdauer von höchstens 6 Monaten für ausreichend gehalten. Die Aufzeichnungen dürfen nur bei Beweisnot ausgewertet werden. Nebenbei bemerkt: die in Telefonbankingverträgen häufig anzutreffende Einwilligung der privaten Kunden und Kundinnen zur Telefon-Werbung ist in aller Regel wegen Verstoßes gegen das Wettbewerbsrecht und das Recht der Allgemeinen Geschäftsbedingungen unwirksam.

Wichtig ist auch, dass die zum Schutz der Daten erforderlichen technisch-organisatorischen Maßnahmen getroffen sind. Sicherzustellen ist, dass ein Einwählen in die Telefonzentralanlage des Call Centers und ein Mithören

von außen nicht möglich ist. Die Mitarbeiter und Mitarbeiterinnen der Call Center müssen gemäß § 5 BDSG auf das Datengeheimnis verpflichtet sein. Auch die sichere Authentifikation der anrufenden Person muss gewährleistet sein, etwa durch Geheimzahl, Codewörter oder Angabe bestimmter personenbezogener Daten. Gerade in diesem Bereich scheint es gelegentlich zu hapern, vor allem an der Ausbildung beziehungsweise Instruktion des Personals. So berichtete uns ein Bürger, dass er nach Angabe seines Namens, seines Geburtsdatums und des ungefähren Kontostandes einmal die erwünschte Auskunft erhalten habe, ein anderes Mal diese Daten der Mitarbeiterin des Banken Call Centers zu seiner Authentifikation nicht ausgereicht hätten, obwohl in der Woche zuvor seiner Ehefrau ohne die vorgeschriebenen Authentifikationsangaben alle gewünschten Auskünfte erteilt worden seien.

Dieser Fall zeigt deutlich, dass es mit dem Vorhandensein interner Dienstanweisungen allein nicht getan ist. Vielmehr sind alle Mitarbeiterinnen und Mitarbeiter regelmäßig und intensiv zu schulen, um sicherzustellen, dass Telefonauskünfte nur erteilt werden, wenn die Identität der Kundin oder des Kunden eindeutig feststeht.

16.6.2 Call Center als externe Dienstleister

Neben dem Telefonbanking werden Call Center in immer stärkerem Maße als externe Dienstleister im Rahmen von Kundenbefragungen, Service-Hotlines und dergleichen mehr eingesetzt. Entweder geschieht das nur punktuell, oder es werden bestimmte Dienstleistungen vollständig aus dem Unternehmen ausgelagert.

Hier stellt sich die datenschutzrechtlich bedeutsame Frage, ob in solchen Fällen **Datenverarbeitung im Auftrag** oder eine so genannte **Funktionsübertragung** vorliegt. Bei der **Auftragsdatenverarbeitung** (§ 11 BDSG) bleibt der Auftraggeber in vollem Umfang für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich; er ist "verarbeitende Stelle" im Sinne des BDSG und muss das Call Center sorgfältig auswählen. Der Auftragsdatenverarbeitungsvertrag enthält Weisungen über die Datenverarbeitung und -nutzung, die technisch-organisatorischen Maßnahmen zur Datensicherung und etwaige Unterauftragsverhältnisse. Das Call Center darf die Daten nur im Rahmen dieses Vertragsverhältnisses verarbeiten und nutzen. Adressat von Auskunftsersuchen von Betroffenen über die zu ihrer jeweiligen Person gespeicherten Daten sowie sonstiger Ansprüche nach dem BDSG bleibt der Auftraggeber. **Funktionsübertragung** bedeutet dagegen, dass ein Call Center in eigener datenschutzrechtlicher Verantwortung als

Dritter im Sinne des BDSG personenbezogene Daten für den Auftraggeber verarbeitet. Hier ist, da im Rahmen von Outsourcing regelmäßig kein gesetzlicher Erlaubnistatbestand für die Datenübermittlung vorliegt, die Einwilligungserklärung aller betroffenen Personen unabdingbar. Zur Abgrenzung zwischen Datenverarbeitung im Auftrag und Funktionsübertragung, deren Kriterien ebenso für den öffentlichen wie den nicht-öffentlichen Bereich gelten, wird auf die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder herausgegebenen "Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung" (Kapitel 8.1) verwiesen.

Im Hinblick auf den Kundendatenschutz ist zu bedenken, unter welchen Voraussetzungen im Call Center Kundengespräche von Vorgesetzten mitgehört werden dürfen, was zu Ausbildungs- und Kontrollzwecken vorkommt. Geboten ist aus Transparenzgründen mindestens eine entsprechende Unterrichtung der Kundin oder des Kunden durch eine vorgeschaltete Ansage. Im Hinblick auf den Arbeitnehmerdatenschutz hat das Bundesarbeitsgericht ein **heimliches** Mithören schon vor einiger Zeit für unzulässig erachtet.

Weitere Probleme ergeben sich, sobald ein Auslandsbezug auftritt. Denkbar, und wahrscheinlich bereits Wirklichkeit, ist folgendes Szenario: Ein Unternehmen beauftragt ein international tätiges Call Center in London mit der Beantwortung von österreichischen Anrufen durch die Niederlassung in Deutschland. Infolge der Anrufe werden personenbezogene Daten gesammelt und könnten sowohl in Deutschland als auch in den Niederlanden gespeichert werden. Auswertungen könnten in alle europäische Länder zu Niederlassungen des Unternehmens oder des Call Centers gehen.

Eine Datenübermittlung in Mitgliedstaaten der Europäischen Union ist nach vollständiger Umsetzung der EG-Datenschutzrichtlinie aus dem Jahr 1995 in nationales Recht unproblematisch, weil sie einen vergleichbaren Datenschutzstandard in allen Mitgliedstaaten gewährleistet. Für eine Übermittlung in Drittstaaten ist die Zulässigkeit im Einzelfall zu prüfen, wobei aber - wie zum Beispiel für die Schweiz und Ungarn bereits geschehen - durch Kommissionsentscheidung festgestellt werden kann, dass ein vergleichbares Schutzniveau besteht. Andernfalls muss dieses Schutzniveau vertraglich vereinbart sein.

Deutlich wird aber jedenfalls, dass die Globalisierung auch beim Datenfluss nicht Halt macht. Vermutlich werden derartige Fragen die Aufsichtsbehörden in Zukunft verstärkt beschäftigen.

Anhang

Arbeitsergebnisse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Entschließungen der Datenschutzbeauftragten des Bundes und der Länder

Nr. 1 25./26. März 1999 – 57. Konferenz

Modernisierung des Datenschutzrechts jetzt - umfassende Novellierung des BDSG nicht aufschieben

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein "Zwei-Stufen-Konzept" vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, dass das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbringung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, dass jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, dass diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nichtöffentlichen Bereich muss institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich

müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z. B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden.

Notwendig ist nach Auffassung der Konferenz, dass das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

Nr. 2 25./26. März 1999 – 57. Konferenz

Geplante erweiterte Speicherung von Verbindungsdaten in der Telekommunikation

Die Bundesregierung und der Bundesrat werden demnächst über den Erlass der seit längerem überfälligen Rechtsverordnung zum Datenschutz in der Telekommunikation auf Grund des Telekommunikationsgesetzes zu entscheiden haben.

Im Gegensatz zur früheren analogen Vermittlungstechnik erzeugt und verarbeitet das digitalisierte Telekommunikationsnetz (ISDN-Netz) in großem Umfang personenbezogene Verbindungsdaten. Dies zwingt zu begrenzenden, am Grundsatz der Datensparsamkeit orientierten Regelungen, um das Fernmeldegeheimnis und das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation zu garantieren.

Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996 sieht vor, dass die Verbindungsdaten unter Kürzung der Zielrufnummer regelmäßig bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen. Über diese Frist hinaus dürfen Verbindungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und den Kunden über die Richtigkeit der Abrechnung entsteht.

Demgegenüber gibt es Überlegungen für eine neue Telekommunikations-Datenschutzverordnung, dass alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre lang nach Ende der Verbindung gespeichert bleiben können. Da die Speicherungsfrist erst am Ende des Jahres beginnen soll, in dem die Verbin-

dung stattfand, kann dies in Einzelfällen dazu führen, dass die Daten bis zu drei Jahre lang vorgehalten werden.

Hiergegen wenden sich die Datenschutzbeauftragten des Bundes und der Länder mit Entschiedenheit. Sie sehen darin einen unverhältnismäßigen Eingriff in das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation. Auch das Telekommunikationsgesetz hebt die Grundsätze der Verhältnismäßigkeit und der Zweckbindung ausdrücklich hervor. Personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, dürfen nur solange gespeichert bleiben, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die Speicherung von Verbindungsdaten muss sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundin und der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden.

Die Dauer einer zivilrechtlichen Verjährungsfrist kann ebenfalls kein rechtfertigender Anlass für eine solche Datenspeicherung sein. Jedenfalls müssen die Daten unverzüglich gelöscht werden, wenn die Rechnung beglichen und unbestritten ist und damit der vertragliche Speicherzweck erledigt ist.

Da eine telekommunikations- oder zivilrechtlich bedingte Notwendigkeit für eine derart lange Speicherfrist der Verbindungsdaten somit nicht ersichtlich ist, würde sie eine unzulässige Datenspeicherung auf Vorrat zu unbestimmten Zwecken darstellen.

Diese Speicherung von Kommunikationsdaten wäre auch nicht mit der Überlegung zu rechtfertigen, dass diese Daten zum Zwecke eventueller künftiger Strafverfolgung benötigt werden könnten. Die mit einer solchen Speicherung verbundene vorsorgliche Überwachung unverdächtiger Bürgerinnen und Bürger wäre unzulässig.

Nr. 3 25./26. März 1999 – 57. Konferenz

Transparente Hard- und Software

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt. Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number - PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt geworde-

nen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, dass die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.

Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tageslicht, dass Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.

Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne dass sie dies bemerken, kann deren missbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten

Nr. 4 25./26. März 1999 - 57. Konferenz

Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL '98)

Gegenwärtig berät der Rat der EU über den Entwurf einer Entschließung zur grenzüberschreitenden Überwachung der Telekommunikation und der Internet-Nutzung (ENFOPOL '98).

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, dass der entsprechende Entwurf bisher geheimgehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation

und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z. B. prepaid cards) nicht konterkariert wird.

Nr. 5 17. Juni 1999 - Entschließung zwischen den Konferenzen 1999

Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern

Bei der Einführung der Befugnis zum „Großen Lauschangriff" hat der Gesetzgeber im Grundgesetz ein Verfahren zur parlamentarischen Kontrolle weitreichender Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung verankert (Artikel 13 Abs. 6 GG). Dieses Verfahren dient nach dem Willen des Gesetzgebers der parlamentarischen Kontrolle der Normeffizienz und hebt zugleich die politische Kontrollfunktion der Parlamente gegenüber der Exekutive hervor. Auch wenn es die Überprüfung von Lauschangriffen durch die Gerichte und Datenschutzbeauftragten nicht ersetzt, hat es gleichwohl eine grundrechtssichernde Bedeutung. Jetzt ist jedoch bekannt geworden, dass einige Landesjustizverwaltungen der Ansicht sind, Art. 13 Abs. 6 GG sehe eine Berichtspflicht über Lauschangriffe zu Strafverfolgungszwecken gegenüber den Landesparlamenten nicht vor.

Im Gegensatz dazu vertritt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Auffassung, dass die Verfassung eine effektive parlamentarische Kontrolle von Lauschangriffen auf Landesebene vorschreibt, die der Kontrolle auf Bundesebene gleichwertig sein muss. Bei Maßnahmen zur Strafverfolgung durch Landesbehörden besteht die parlamentarische Verantwortlichkeit gegenüber den Landesparlamenten. Die Landtage müssen die Möglichkeit haben, die ihnen in anonymisierter Form übermittelten Berichte der Landesregierungen öffentlich zu erörtern. Die Landesparlamente sollten deshalb durch Gesetz eine regelmäßige Berichtspflicht der Landesregierung für präventiv-polizeiliche und repressive Lauschangriffe vorsehen. Nur auf diese Weise ist eine wirksame parlamentarische Kontrolle der Ausübung dieser einschneidenden Überwachungsbefugnisse gewährleistet.

Wird durch eine solche Kontrolle deutlich, dass die akustische Wohnraumüberwachung für Zwecke der Strafverfolgung in der Praxis nicht die vom Gesetzgeber angestrebte Effizienz im Verhältnis zur Häufigkeit und Intensität der Grundrechtseingriffe zeigt, können Landesregierungen, die das Bundesrecht in eigener Verantwortung auszuführen haben, über den Bundesrat darauf hinwirken, die Befugnis für eine derartige Überwachung wieder aufzuheben oder zumindest zu modifizieren.

Nr. 6 25. August 1999 – Entschließung zwischen den Konferenzen 1999

Gesundheitsreform

Die Datenschutzbeauftragten von Bund und Ländern erklären zu dem Entwurf eines Gesetzes "Gesundheitsreform 2000":

Die Datenschutzbeauftragten haben großes Verständnis für die Bemühungen, die Kosten im Gesundheitswesen zu begrenzen und eine gute Versorgung der Patientinnen und Patienten sicherzustellen. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, beim Eingriff in das Recht auf informationelle Selbstbestimmung das Prinzip der Erforderlichkeit und der Verhältnismäßigkeit zu wahren.

Der Entwurf lässt jede Begründung vermissen, warum die bisherigen Kontrollmechanismen, die das Entstehen umfangreicher medizinischer Patientendatenbestände bei den Krankenkassen vermeiden, ungeeignet sein sollen, die Wirtschaftlichkeit und Qualität ärztlicher Leistungserbringung sicherzustellen.

Der Entwurf gibt das bisherige Konzept der Datenverarbeitung in der gesetzlichen Krankenversicherung auf. Insbesondere standen bisher aus dem ambulanten Bereich personenbezogene Abrechnungsdaten mit medizinischen Inhalten und Diagnosedaten den Krankenkassen nur ausnahmsweise zu Prüfzwecken zur Verfügung, künftig sollen diese Informationen den Krankenkassen dagegen generell versichertenbezogen übermittelt werden. Damit entstehen bei den gesetzlichen Krankenkassen vollständige personenbezogene medizinische Datenbestände der gesetzlich Versicherten mit der Möglichkeit, für jede einzelne Person umfassende Darstellungen ihres Gesundheitszustandes zu bilden. Bei den Kassen entstehen gläserne Patientinnen und Patienten. Das Patientengeheimnis wird ausgehöhlt.

Die Datenschutzbeauftragten richten an den Gesetzgeber die dringende Bitte, die bisher versäumte eingehende Prüfung von Erforderlichkeit und Verhältnismäßigkeit der weiterreichenden Datenverarbeitungsbestimmungen nachzuholen. Der Bundesbeauftragte für den Datenschutz, mit dem der Entwurf entgegen anders lautenden Äußerungen von Regierungsvertretern in der Sache bisher in keiner Weise abgestimmt wurde, sowie die Datenschutzbeauftragten der Länder stehen hierfür zur Diskussion zur Verfügung.

Insbesondere klärungsbedürftig sind folgende Punkte:

Der Entwurf erweitert die Aufgaben der Krankenkassen auch auf eine steuernde und durch die Patientinnen und Patienten nicht geforderte Beratung über Gesundheitserhaltungsmaßnahmen und auf eine Prüfung der u. a. durch die Ärztinnen und Ärzte erbrachten Leistungen. Er sieht dafür umfangreiche Datenerhebungs- und –verarbeitungsbefugnisse vor.

Der Wortlaut des Entwurfes beschreibt diese Aufgabe allerdings nur vage. Er lässt nicht erkennen, was auf die Patientinnen und Patienten zukommt. Weder ist klar geregelt, wie weit die Beratung reichen darf, noch mit welchen Rechtsfolgen die oder der Einzelne rechnen muss. Es ist zu befürchten, dass diese Beratung dazu dienen wird, die Patientinnen und Patienten, Ärztinnen und Ärzte und die sonstigen Leistungserbringer zu kontrollieren und zu beeinflussen und dass hierdurch das Arzt-Patienten-Vertrauensverhältnis belastet wird.

Wegen der vagen Aufgabenbeschreibung sind auch die damit verbundenen Datenverarbeitungs- und -zusammenführungsbefugnisse in gleicher Weise unklar und verschwommen. Eine Präzisierung und Eingrenzung ist dringend erforderlich.

Der Entwurf sieht im Gegensatz zum bisherigen System vor, dass Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die Diagnosen nach dem international gültigen ICD-10-Schlüssel zu codieren, sind diese medizinischen Informationen z. B. im Bereich der Psychotherapie auch hochdifferenziert.

Die zur Begründung besonders angeführten Punkte "Unterrichtung der Versicherten über die in Anspruch genommenen Leistungen, Kontrolle der Einhaltung der zweijährigen Gewährleistungspflicht bei den Zahnärzten, Unterstützung der Versicherten bei Behandlungsfehlern" vermögen insoweit nicht zu überzeugen. Bereits jetzt können die Versicherten über die beanspruchten Leistungen und deren Kosten informiert werden und von ihrer Krankenkasse auch im Übrigen Unterstützung erbitten, so dass keine Notwendigkeit für die Anlegung derart sensibler, umfangreicher und zentraler Datenbestände ersichtlich ist.

Der Eingriff in die Rechte der Patientinnen und Patienten steht damit in keinem Verhältnis zu den angegebenen Zwecken.

Die beabsichtigte Einführung von zentralen Datenannahme- und –verteilstellen, bei denen nicht einmal klar ist, in welcher Rechtsform (öffentlich oder privat) sie betrieben werden sollen, hat eine weitere, diesmal Krankenkassen übergreifende zentrale Sammlung medizinischer personenbezogener Patientendaten zur Folge. Wegen des hohen weiteren Gefährdungspotentials von derart umfassenden Datenbeständen müsste der Entwurf im Einzelnen begründen, warum eine konsequente Umsetzung der schon bisher möglichen Kontrollmechanismen nicht ausreicht.

Die angesprochenen Punkte stellen besonders gewichtige, aber keineswegs die einzigen Probleme dar. Zu nennen sind hier nur beispielsweise die Verlängerung der Speicherdau-

er von Patientendaten beim Medizinischen Dienst der Krankenversicherung (MDK) von 5 auf 10 Jahre, unzureichende Regelungen bei den Speicherfristen, bei Umfang, Zweckbindung und Freiwilligkeit der Datenerhebung beim Hausarztmodell, der integrierten Versorgung und den Bonus-Modellen sowie unzureichende Pseudonymisierung bei den Arbeitsgemeinschaften. Abzulehnen ist auch die völlig mangelhafte Zweckbindung der Daten bei den Krankenkassen.

Nr. 7 7./8. Oktober 1999 – 58. Konferenz

Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 09./10.03.1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16.08.1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss von 17.09.1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

Nr. 8 7./8. Oktober 1999 – 58. Konferenz

Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat

einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weitreichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten lässt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31.12.1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern statt dessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100 a StPO neu geregelt werden.

Nr. 9 vom 7./8. Oktober 1999 – 58. Konferenz

DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

In der Strafprozessordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u. a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis - also ohne richterliche Anordnung - erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z. B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflusst, ist dennoch davon auszugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen - abweichend von den gesetzlich vorgesehenen Verfahren - systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Reglung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßig-

keit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

Nr. 10 vom 7./8. Oktober 1999 – 58. Konferenz

Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: „Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern".

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs. 1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i.V. m. Art. 1 Abs. 1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

Nr. 11 vom 7./8. Oktober 1999 – 58. Konferenz

Patientenschutz durch Pseudonymisierung

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine

zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des „gläsernen Patienten" verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

Nr. 12 7./8. Oktober 1999 – 58 Konferenz

Eckpunkte der deutschen Kryptopolitik – ein Schritt in die richtige Richtung

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, so dass zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte (z. B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre lässt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang musste befürchtet werden, dass auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptographie als „eine entscheidende Voraussetzung für den Datenschutz der Bürger" besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,
- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,
- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),
- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,
- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,
- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offengelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

Nr. 13 vom 7./8. Oktober 1999 – 58. Konferenz

"Täter-Opfer-Ausgleich und Datenschutz"

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28.05.1999) sieht in § 155 a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut des „Täter-Opfer-Ausgleichs" nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als „objektive Dritte mit dem Gebot der Unterstützung jeder Partei" könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die „fachlich geleitete Auseinandersetzung" der „am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden".

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z. B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, dass an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, dass die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am „Täter-Opfer-Ausgleich" Beteiligten muss gesetzlich geschützt werden.

Nr. 14 vom 14./15. März 2000 – 59. Konferenz

Risiken und Grenzen der Videoüberwachung

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht darin die Gefahr, dass diese Entwicklung zur einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen

- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen
- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten
- sowie die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozessrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch video-technisch gewonnener - insbesondere biometrischer - Daten und deren Abgleiche.

Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch öffentliche Stellen dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.

   - Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. Dafür kommen - **soweit nicht überwiegende schutzwürdige Belange von Betroffenen entgegenstehen** - unter Anderem in Betracht[1]:
     - die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden.
     - für die Verkehrslenkung nur Übersichtsaufnahmen,
     - der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.
   - Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.
   - Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.

[1] Die fett gedruckte Passage wurde bei Stimmenthaltung der Datenschutzbeauftragten der Länder Brandenburg, Bremen, Mecklenburg-Vorpommern und Nordrhein-Westfalen angenommen.

- Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.
- Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.
- Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.

Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung durch Private Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

Nr. 15 vom 14./15. März 2000 – 59. Konferenz

Für eine freie Telekommunikation in der freien Gesellschaft

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

- **Erhebliche Zunahme der Telekommunikationsvorgänge**

  Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, e-mail und mail-boxen sowie das Internet genutzt.

- **Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten**
  - Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.
  - Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch e-mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.
  - Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.
  - Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.
  - Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.

- **Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten**
  Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.

- **Entwicklung des Internets zum Massenkommunikationsmittel**
  Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.

- **Schwer durchschaubare Rechtslage**
  Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

- Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: 1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802
- Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen – der Katalog wurde seit Einführung 11 mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.
- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.
- Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen „ENFOPOL", befasst sich u. a. mit der Frage, welchen Anforderungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weitergehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

- Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.
- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.

- Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.
- Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.
- Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.
- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.
- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstelenanlagen in Hotels, Krankenhäuser oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.
- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselung von elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.

- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.
- Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

Nr. 16 vom 14./15. März 2000 – 59. Konferenz

Data Warehouse

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an. Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im „Data Warehouse" werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. „Data Mining" bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

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

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem „Daten-Lagerhaus" gesammelt werden.
- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden ist. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.
- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verar-

beiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.

- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.
- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern" rechtswidrig.
- Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). „Data Mining" ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von „Data Warehouse"- und „Data Mining"-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

Nr. 17 vom 14./15. März 2000 – 59. Konferenz

Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zu den Abhörmaßnahmen des BND

Das Bundesverfassungsgericht hat für die Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen wurden, deutliche Schranken gezogen, die weit über den Gegenstand des Verfahrens hinaus bedeutsam sind.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses zur Aufrechterhaltung einer freien Telekommunikation, die eine Grundvoraussetzung der Informationsgesellschaft darstellt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichtes zu den verdachtslosen Abhörmaßnahmen des BND auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird (Telefon, E-Mail, Telefax, Internet-Abrufe o.ä.).

Die Anforderungen des Urteils müssen auch Konsequenzen für Fallgestaltungen haben, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem Einsatz technischer Mittel.

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

- Zur Sicherung der Zweckbindung der erlangten Daten und für die Kontrolle ihrer Verwendung muss ihre Herkunft aus Eingriffen in das Fernmeldegeheimnis oder vergleichbaren Eingriffen durch eine entsprechende Kennzeichnung nach der Erfassung auch bei den Übermittlungsempfängern erkennbar bleiben.
- Die erlangten Daten müssen bei allen speichernden Stellen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind - es sei denn, der Rechtsschutz der Betroffenen würde dadurch verkürzt. Die Praxis von Verfassungsschutzämtern, nicht (mehr) erforderliche Daten, wenn sie sich in Unterlagen befinden, nicht zu schwärzen, kann - zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden - nicht mehr aufrechterhalten werden. Um die Notwendigkeit einer späteren Schwärzung zu vermeiden, sollten bereichsspezifischen Vernichtungsregelungen bereits bei der Aktenführung Rechnung getragen werden.
- Die Vernichtungspflicht ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln. Eine Löschung oder Vernichtung ist nach einem Auskunftsantrag bei allen personenbezogenen Daten unzulässig. Zudem sind personenbezogene Daten, die durch die o.g. Maßnahmen erlangt wurden, nach einer Unterrichtung der Betroffenen für einen angemessenen Zeitraum - ausschließlich zum Zweck der Sicherung des Rechtsschutzes - aufzubewahren.
- Überwachte Personen müssen von Eingriffen unterrichtet werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet wird; dies gilt auch für weitere Betroffene, es sei denn, überwiegende schutzwürdige Belange der überwachten Person stehen dem entgegen (Schutz vor unnötiger Bloßstellung).
- Wie bei Eingriffen in das Fernmeldegeheimnis ist dies auch bei anderen verdeckten Maßnahmen Voraussetzung dafür, dass die Betroffenen von den ihnen zustehenden Rechten Gebrauch machen können, und daher von Art. 19 Abs. 4 GG geboten. Speicherfristen können die Unterrichtungspflicht nicht beseitigen, irrelevante Daten sind umgehend zu löschen.
- Damit sind Regelungen z.B. in Landesverfassungsschutz- und Polizeigesetzen nicht zu vereinbaren, wonach eine Unterrichtung der Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmeldegeheimnis gleichkommen, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Eingriffes ausgeschlossen werden kann.
- Zusätzlich zur unbefristeten Benachrichtigungspflicht ist eine Mitteilung an die Datenschutzkontrollstelle für den Fall vorzusehen, dass die Unterrichtung der Betroffenen länger als fünf Jahre zurückgestellt wird.
- Der Umgang des Verfassungsschutzes mit personenbezogenen Daten, die in Durchbrechung des Fernmeldegeheimnisses erhoben worden sind, ist durch eine unabhängige Datenschutzkontrollstelle lückenlos zu überprüfen.

- Eine Kontrolllücke bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden, wäre verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet.
- Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten einschließlich der Benachrichtigung - bei Datenübermittlungen auch bei den Datenempfängern - erstrecken.
- Der Gesetzgeber sollte festlegen, dass die Übermittlung der Daten, die Prüfung der Erforderlichkeit weiterer Speicherung sowie die Durchführung der Vernichtung und Löschung der Daten aus G 10-Maßnahmen zu protokollieren sind.
- Für eine effektive Kontrolle sind die zuständigen Stellen personell und sachlich angemessen auszustatten.
- Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weitergehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist.

Nr. 18 vom 14./15. März 2000 – 59. Konferenz

Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluss des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,
- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z. B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, so dass sie uneingeschränkt zur Strafverfolgung genutzt werden können,
- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,
- nicht am Verfahren beteiligte Dritte schon bei „berechtigtem Interesse" Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

Nr. 19 vom 14./15. März 2000 – 59. Konferenz

Unzulässiger Speicherungsumfang in "INPOL-neu" geplant

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung „INPOL-neu" eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur soweit eingegriffen wird, wie dies im Rahmen der Erforderlichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes-Kriminalaktennachweis (KAN) die „gesamte kriminelle Karriere" jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereit gehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventiven als auch im repressiven Bereich auf „Straftaten mit länderübergreifender, internationaler oder erheblichen Bedeutung". Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-

relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die „Straftaten", nicht die einzelne Person und auch nicht das „Gesamtbild einer Person". Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten einzelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

Nr. 20 vom 10. Oktober 2000

Auftragsdatenverarbeitung durch das Bundeskriminalamt

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollen auf Grund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden.

§ 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen, zu. Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises und der Innenministerkonferenz gefasst worden.

Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.

Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im Wesentlichen mit Kosten- und Zeitargumenten begründet. Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen.

Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz statuierte Schwelle, dass nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.

Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren an die Innenminister/-senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

Die Datenschutzbeauftragten warnen vor einer solchen Entwicklung und fordern dazu auf, die für die Datenverarbeitung beim BKA gesetzlich gezogenen Grenzen strikt zu beachten.

Nr. 21 vom 12./13. Oktober 2000 – 60. Konferenz

Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 3 GG zur Strafverfolgung eingesetzten "Großen Lauschangriffe" zu unterrichten. § 100e StPO konkretisiert die Berichtspflicht dahingehend, dass die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.

Diese Berichte sollen eine laufende parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen. Der Bundestag soll aufgrund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahmen zu überprüfen.

Diesen Anforderungen wird der erste von der Bundesregierung vorgelegte Bericht nicht in vollem Umfang gerecht. So wurde nur die Gesamtzahl der von der Anordnung Betrof-

fenen erfasst, wobei zwischen Beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird.

Nach § 100e Abs. 1 StPO muss über den Umfang der Maßnahme berichtet werden. Hierzu zählt die Angabe über die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der gerichtlichen Anordnung genannten. Von dem "Großen Lauschangriff" ist jeder betroffen, dessen gesprochenes Wort in der Wohnung abgehört wird. Er greift auch in die grundrechtlich geschützten Rechte der am Verfahren Unbeteiligten, wie z.B. unverdächtige Familienangehörige, Bekannte, Besucherinnen und Besucher sowie sonstige Personen, die nicht selbst Wohnungsinhaber sind, ein. Dem wollte der Gesetzgeber mit der Einführung der Berichtspflicht Rechnung tragen.

Die Beschränkung der Berichtspflicht auf Wohnungsinhaber und Beschuldigte gibt nicht den wirklichen Umfang der von der Maßnahme betroffenen Personen wieder. Somit erfüllt sie den Zweck der im Grundgesetz vorgesehenen Berichtspflicht nicht.

Darüber hinaus wäre es wünschenswert, wenn - wie in den "Wire-tap-Reports" der USA - die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Die oben genannten Forderungen gelten deshalb gleichermaßen bzw. in entsprechender Weise für die den Landesparlamenten vorzulegenden jährlichen Berichte über die nach § 100c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen bzw. über die von der Polizei zur Gefahrenabwehr veranlassten "Großen Lauschangriffe".

Nr. 22 vom 12./13. Oktober 2000 – 60. Konferenz

Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung

Bei der Modernisierung der öffentlichen Verwaltung soll insbesondere die Dienstleistungs- und Serviceorientierung verbessert werden. Dazu sollen unter anderem Dienstleistungen in multifunktionalen Servicecentern (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) gebündelt und die Möglichkeiten der modernen Informations- und Kommunikations-Technik intensiver genutzt werden (Information, Kommunikation und Transaktion über das Internet, Einrichtung von Call-Centern).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauftragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personenbezogener Daten gewährleistet wird. Nur Serviceangebote, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen letztlich sowohl Bürgerinnen und Bürgern als auch der Verwaltung selbst.

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

Nr. 23 vom 12./13. Oktober 2000 – 60. Konferenz

Novellierung des BDSG

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz - § 3a E-BDSG) und die Einführung des Datenschutzaudit (§ 9a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in die bewährten Strukturen des betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltensweisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.

Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudit in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe

der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

Nr. 24 vom 12./13. Oktober 2000- 60. Konferenz

Datensparsamkeit bei der Rundfunkfinanzierung

Die Finanzierung des öffentlich-rechtlichen Rundfunks ist derzeit Gegenstand öffentlicher Diskussion in der Politik und unter den Rundfunkanstalten selbst. Erörtert wird hierbei auch, ob die Erhebung von Rundfunkgebühren, die an das "Bereithalten eines Rundfunkempfangsgerätes" anknüpfen, im Hinblick auf veränderte Gerätetechniken und bestehende Mängel im Verfahren modifiziert oder durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte.

Künftig wird kaum noch überschaubar sein, welche Geräte zum Rundfunkempfang geeignet sind. Über die eigentlichen Fernseh- und Rundfunkgeräte hinaus ist dies bereits heute beispielsweise mit Personalcomputern, die über einen Internetzugang verfügen, oder mit bestimmten Mobiltelefonen möglich. In naher Zukunft werden neue Technologien wie UMTS weitere Empfangsmöglichkeiten eröffnen. Sofern der Besitz derartiger multifunktionaler Geräte zum Kriterium für die Rundfunkgebührenpflicht gemacht wird, würde das zu einer erheblichen Ausweitung von Datenabgleichen führen. Schon das gegenwärtig praktizierte Gebühreneinzugsverfahren erfordert in großem Umfang die Verarbeitung personenbezogener Daten. Nach den Angaben der Rundfunkanstalten meldet ein signifikanter Teil der Rundfunkteilnehmerinnen und -teilnehmer trotz der Verpflichtung hierzu seine Geräte nicht an. Um möglichst alle Gebührenpflichtigen zu erfassen, nutzen die Rundfunkanstalten Daten aus dem Melderegister, vom privaten Adresshandel und setzen vor Ort Rundfunkgebührenbeauftragte ein, die einzelne Haushalte aufsuchen. Damit wird in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung vieler gesetzestreuer Bürgerinnen und Bürger eingegriffen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesländer auf, einer Neuordnung ein Modell zu Grunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Nach ihrer Überzeugung lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen, das Recht auf informationelle Selbstbestimmung weniger stark einschränkenden Finanzierungsmodellen als dem derzeit praktizierten gewährleisten.

Nr. 25 vom 12./13. Oktober 2000 – 60. Konferenz

Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.

Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine "genetische Diskriminierung" bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen zu verhindern. Auf der Grundlage dieser und in der "Entschließung über Genomanalysen und informationelle Selbstbestimmung" vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.

2. Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnnen Informationen zu löschen oder an den Betroffenen herauszugeben.

3. Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten.

4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.

5. Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u.a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.

6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe.

Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden. Demnächst werden nicht nur - wie bisher - Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

Stichwortverzeichnis

A

Abrechungsdaten	24 f., 127, 149 f.
Abschottung	124, 136
Accessproviding	21
ActiveX	31 f.
Agrarstatistik	123 f.
Akteneinsicht	84, 103 f., 126
- in Jugend- und Sozialämtern	103
- in Personalakten	126
Anbieterkennzeichnung	12 f., 23
Arbeitnehmerdatenschutz	126, 143
Arbeitnehmerdatenschutzgesetz	126
Attachments	19, 33, 35
Aufzeichnung	60 ff., 65, 67, 69 ff., 79, 141, 158, 160
Auskunftsanspruch	12, 79, 104, 137
Ausländerinnen und Ausländer	90, 94, 96

B

Bankautomaten	135
Behandlungskosten	110
- Krankenhausbehandlung	110
- Reproduktionsmedizin	110
- Schwangerschaftsabbruch	109, 175
Behördliche Datenschutzbeauftragte	4
Benachrichtigung	62 f., 65, 81, 83, 166 f.
Benachrichtigungspraxis	81
Berufsordnung der Ärztekammern	107 f.
Bestandsdaten	22 f., 161, 162
Besuchskommission	107
Betäubungsmittelgesetz	107
Beurteilungsverfahren	129
Bevölkerungsstatistik	122 f.
Bewegungsprofil	79, 139
Biometrische Authentifikationsverfahren	128
Browser	29 ff., 34 f.
Bundesdatenschutzgesetz	5, 64 f., 126, 135, 145, 172

C

Call Center	141 ff.
Chipkarte	3 f., 47, 128, 137 f., 144
Codierungsverfahren	119
Common Criteria	43
Cookies	13 ff., 23

D

Data Mining	37 ff., 164 f.
Data Warehouse	37 ff., 164 f.
Datei Gewalttäter Sport	72 f.
Datenschutzaudit	5, 51, 144, 172
Datenschutzaufsicht	4, 131, 140
datenschutzfreundliche Technologien	2, 155
Datenschutzkontrolle	131, 144, 155
Datenschutzpolicies	15
Datenverarbeitung im Auftrag	52, 57 f-, 102, 142 f.
Datenvermeidung	2, 14, 22, 24, 77, 100, 144, 160, 162, 172 f.
Dienstrechtliche Vorschriften	126
Duplikate	123 f.

E

ECHELON	17, 75
E-Commerce	19 f., 137 f., 161
Elektronische Einwilligung	13
Elektronische Signatur	9
Elektronischer Fahrschein	138 ff.
Elektronischer Studierendenausweis	116
Elektronischer Zahlungsverkehr	136
E-Mails	16 ff., 76, 117
Enfopol	75, 147, 162
Entlassungsbericht	110
ePost-Language-Format	58
Erhebungsbögen	123 f.
Evaluation	25, 43, 116

F

Fernmeldeanlagengesetz	78 f., 152, 163
Fernmeldegeheimnis	19 ff., 80, 117, 145, 148, 155, 160, 162 ff.
Fernmeldeverkehr	80, 152
Fingerabdruck	128
Firewallsysteme	30
Formulare	26, 99, 101
Forschung	3, 108, 116 ff.
FTP-Dienst	34 f.

G

Geldkarte	136 ff.
Genomanalyse	120, 174 f.
Gesundheitsdaten	5, 58, 108, 119
Gesundheitsdatenschutzgesetz	58, 108
Gesundheitsreform	98, 149, 154
Gewaltopfer	105
Girokonto	133
Großraumbüro	124 f.

H

Heimgesetz	99
High-Level-Formatierung	54
HTML	30 ff., 35, 37
HTTP	30, 34 f., 37

I

Informationspflichten	11, 13, 15
Info-Telefon	105
Innenrevision	126
INPOL	73 f., 94, 168 ff.
Interaktive Verwaltung	26
Internetnutzung	5, 15, 21, 113, 116

J

Java	32 ff.
JavaScript	14, 32 f.
Jugendhilfe	102 f.

K

Kennzeichnung	12 f., 23
Kommerzialisierung	6
Kommunikation	9, 11, 18 ff., 26, 29, 37, 40, 43 f., 48, 76, 79 ff., 85, 145 f., 152, 161 ff., 171 f.,
Kommunikationsfreiheit	79
Kompetenznetzwerke	119
Krankenhilfeleistungen	102
Krankenversicherung	98 f., 110, 149, 151

L

Landesdatenschutzgesetz	1 ff., 131
Landesgleichstellungsgesetz	126
Landeshebammengesetz	107
Löschung	40, 47, 52 ff., 66, 94, 132 ff. 140
Low-Level-Formatierung	54

M

Maßregelvollzug	83, 87 f.
Mediendienstestaatsvertrag	9, 11
Medizinischer Dienst	99, 110, 151
Miniaturisierung	5
Missbrauchskontrolle	116 f.
Mitarbeiterbefragung	126
Modernisierung	2, 5, 144, 171

N

Neues Steuerungsmodell 102
Nichtabstreitbarkeit 44
Nutzungsdaten 22 ff., 75, 161

O

Outsourcing 58, 143

P

Patientendaten 30, 34, 36, 107, 149 ff., 154 f.
Patientendatenverarbeitungssysteme 30, 34, 36
Personalakten 114 f., 126, 129 f.
Pflegedokumentation 99
Pflegekasse 99
Pflegeversicherung 99
Pflegeversicherungsgesetz (SGB XI) 99
Polizei 4, 63 f., 66, 72 f., 76, 83 f., 94, 129, 148, 159, 166 ff.
Postdienstunternehmendatenschutzverordnung 58
Postkontrolle 85
Prävention 5, 83 f.
Privatheit 1, 5 ff., 147, 164
Protection Profile 43 f.

R

Rechtsverbindlichkeit 9
Reidentifizierungsrisiken 120

S

Schengener Informationssystem 93 f.
Schufa 132 f., 135
Schuldnerdaten im Internet 134

Schuldnerverzeichnis 131 ff.
Schule 113, 116 ff.
- häuslicher PC 113
- Personalakte 115
Security Target 43 f.
Selbstbestimmung 2 f., 7, 11, 15, 51, 60, 63, 65, 80, 87, 89, 98 ff., 107, 109, 123, 128, 149, 157 f., 164, 168, 172 ff.
Sicherheitskonzept 29, 46, 48 ff., 52, 74, 127 f.
Sicherheitsziele 48 f.
Signaturgesetz 9 ff.
Sozialamt 99, 101, 105
Sozialdaten 57, 98, 101, 103, 105, 123, 128
- Verarbeitung im Auftrag 102
Sozialgeheimnis 102, 105
Sozialhilfestatistik 123
Sozialleistungsträger 102
Sparkasse 5, 66 f., 133, 135
Statistik 122 ff., 139
Strafvollzug 83 f., 87 f.
StVÄG 83 f., 167
Systembetreuung 52 f.

T

Telearbeit 127 f.
Teledienste 20 ff., 26, 144
Teledienstedatenschutzgesetz 6, 9, 11, 14, 20, 22, 24 ff., 162
Teledienstegesetz 19, 20 f., 25
Telefonbanking 141 f.
Telefonüberwachung 80 f.
Tele-Heimarbeit (siehe Telearbeit)
Telekommunikation 1, 10, 20 ff., 46, 75 ff., 88, 127, 145 ff., 151 f., 156, 160 ff.
Telekommunikationsdaten 77 f., 80
Telekommunikationsdatenschutzverordnung 77
Telekommunikationsgesetz 20 f., 76 f., 145 f.

Telekommunikationsüberwachungsverordnung 78
Transparenz 4, 11 ff., 15, 23, 42, 49, 96, 126, 129, 137, 143, 147
Transplantationsgesetz 107
Treuhänderschaft 120

U

Übermittlung 48, 58, 75, 79, 96 f., 99, 105, 120, 122 ff., 139, 143, 167
Überwachung 5, 8, 17, 60 ff-, 75 f., 78 ff., 84 f., 88, 146 ff., 152, 158 f., 162
Unterlagenvernichtung 55 ff., 59

V

Verarbeitungsprozess 80
Verbindungsdaten 78 f., 145 f., 151 ff., 161, 163
Verfassungsschutz 89, 166
Verhaltensanpassung 79
Verkehrsbetriebe 139 f.
Verkehrsdaten 75
Vernetzung 5, 46, 120 f.
Verschlüsselung 8 f., 18, 26, 77, 155 ff. 163
Versichertendaten 98
- kassenweiter Zugriff 98
- Angaben zu persönlichen Verhältnissen 111
Vertraulichkeit 8 f., 17, 26, 29, 31, 33, 43, 49, 111 f., 117, 141
Verzeichnisdienste 40 ff.
Videoüberwachung 4, 6, 60 ff., 69, 144, 158 ff.
- öffentliche Stelle 60, 62
- Polizei 63, 66
- durch Private 65 f., 69
- öffentliche Verkehrsmittel 69 f.

Virtual Network Computing 36
Volkszählung 80, 83, 122 f., 125, 151
Vorabkontrolle 3, 4, 51 f., 116, 159

W

Wählerverzeichnisse 96
Web-Cam 60, 70 f.
Webportale 8, 11 f.
Weitergabe 6, 53 f., 80, 112, 124, 159
Weitervermittlung 13
WWW-Dienst 30, 35

X

X.500 Dienst 40 f.

Z

Zensus 122
Zertifizierungsdienste 9 f., 29
Zielwahl-Suche 78

Datum: .....

Absender/in:

.....
(Vorname, Name)

.....
(Behörde)

Landesbeauftragte
für den Datenschutz
Reichsstraße 43

.....
(Straße, Hausnummer/Postfach)

40217 Düsseldorf

.....
(PLZ, Ort)

Betr.: Informationsmaterial

Hiermit bitte ich um Übersendung folgender Broschüren:

_____ Aufkleber zum Adressenhandel

_____ Datenschutzfreundliche Technologien

_____ Datenschutzrecht des Landes NRW

_____ Datenschutz und Anonymität

_____ den neuesten Datenschutzbericht

_____ den ..... Datenschutzbericht

_____ 20 Jahre Datenschutz - Individualismus oder Gemeinschaftssinn?

_____ Datenscheckheft

_____ Die Bedeutung der EG-Datenschutzrichtlinie für öffentliche Stellen

_____ E-Mails ... aber sicher (ohne CD-ROM)

_____ Faltblatt Datenschutz ... ist Ihnen egal?

_____ Handys - Komfort nicht ohne Risiko

_____ Orientierungshilfe Datenschutz bei der Nutzung von Internet und Intranet

_____ Orientierungshilfe Archivierung von Krankenunterlagen/Outsourcing

_____ Orientierungshilfe Datenschutz und Datensicherheit beim Betrieb von IT-Systemen

_____ Orientierungshilfe Datenverarbeitung im Auftrag

_____ Orientierungshilfe Telefax

_____ Orientierungshilfe Unterlagenvernichtung

_____ Serviceorientierte Verwaltung "Vom Bürgerbüro zum Internet"

_____ Tips zum Adressenhandel

Mit freundlichen Grüßen

NRW.

http://www.lfd.nrw.de