Vorlage 12/2633

Datenschutzbericht 1999



Die Landesbeauftragte
für den Datenschutz
Nordrhein Westfalen

Vierzehnter Datenschutzbericht

der

Landesbeauftragten für den Datenschutz

Nordrhein-Westfalen

Bettina Sokol

LANDTAG
NORDRHEIN-WESTFALEN
12. WAHLPERIODE

VORLAGE
12/2633

Alle Abg.

für die Zeit vom 1. Januar 1997
bis zum 31. Dezember 1998

Herausgeberin:

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

40217 Düsseldorf

Tel.: 0211/38424-0
Fax: 0211/3842410
E-mail: datenschutz@mail.lfd.nrw.de
mailbox@mail.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 1999

Gedruckt auf chlorfrei gebleichtem Recyclingpapier

14. Datenschutzbericht

Inhaltsverzeichnis

		Seite
	Vorbemerkung	1
1.	**Zur Situation im Datenschutz: Gestalten statt verwalten**	2
2.	**Technische und rechtliche Aspekte der Medienentwicklung**	8
2.1	Datenschutzfreundliche Technologien	8
2.2	Kryptographie - Schlüsseltechnologie für Informationssicherheit und vertrauenswürdige Kommunikation	11
2.2.1	Einführung	11
2.2.2	Verschlüsselungsverfahren	12
2.2.3	Digitale Signaturverfahren	17
2.2.4	Fazit	21
2.3	Internetnutzung in der Verwaltung	21
2.3.1	Kopplung interner Netze über Firewallsysteme	22
2.3.2	Direktanschluß über separate Geräte	27
2.4	Konventionelle und unkonventionelle rechtliche Regelungen für die Medien	28
2.4.1	Grundlinien	28
2.4.2	Telekommunikation	29
2.4.3	Medien- und Teledienste	34

3.	**Polizei und Verfassungsschutz**	49
3.1	Sicherheit auf Kosten der Grundrechte?	49
3.2	Der große Lauschangriff	51
3.3	DNA-Analysedatei	52
3.4	Schleierfahndung	54
3.5	Ermittlungsinstrument Telefon	54
3.5.1	Wachsende Zahl von Telefonüberwachungen	54
3.5.2	Verbindungsdaten bleiben nicht immer geheim	55
3.5.3	Unzureichende Benachrichtigungen von Abhörmaßnahmen	56
3.5.4	Transparenz für die Betroffenen und die Nichtbetroffenen	56
3.6	Verfassungsschutz und polizeilicher Staatsschutz	57
3.6.1	Bereich Verfassungsschutz	57
3.6.2	Bereich Sicherheitsüberprüfung	59
3.6.3	NADIS - Personenzentraldatei (PZD)	61
3.6.4	Erfassung einfacher Mitglieder von Organisationen	61
3.6.5	Staatsschutz, Verfassungsschutz und die Versammlungsfreiheit	62
3.7	Polizeiliche Datenverarbeitung - Spiel ohne Grenzen?	66
3.7.1	Schengener Informationssystem (SIS)	66
3.7.2	Europol - Strafrechtliche Immunität der Europol-Angehörigen	71
3.7.3	INPOL - Neukonzeption	72
3.7.4	Datenübermittlung durch die Polizei	75
3.8	Überwachung auf Schritt und Tritt?	76
3.8.1	Videoüberwachung	76
3.8.2	Identifizierung mit Hilfe von Fotos	80
4.	**Die Bürgerinnen und Bürger und die Justiz**	83
4.1	Justizmitteilungsgesetz, MiStra, MiZi	83

4.2	Zutritt zu den Gerichten	83
4.3	Akteneinsicht	84
4.4	Angaben auf Briefumschlägen	84
4.5	Formulare bei Familiengerichten	85
4.6	Terminsaushänge	85
5.	**Bürgerämter**	87
5.1	Bürgerämter - Service nur mit Datenschutz	87
5.1.1	Das neue Melderecht	87
5.1.2	Datenschutz im Bürgeramt	90
5.2	Neue Steuerungsmodelle	92
6.	**Ausländerinnen und Ausländer**	93
6.1	Ausländerzentralregister	93
6.2	Der Echtheitsgrad von Ehen	93
6.3	Gläserne Gastgeberinnen und Gastgeber	94
6.4	Familienzusammenführung mit unzulänglichem Datenschutz	95
6.5	EURODAC	96
7.	**Sozialbereich**	98
7.1	Sozialämter schießen über das Ziel hinaus	99
7.2	Prüfung von Pflegeleistungen	100
7.3	Datenabrufe erfordern Übermittlungsbefugnisse	101
7.4	Datenschutz bei den Krankenkassen	102

7.5	Dürfen Krankenkassen Arztberichte anfordern?	104
7.6	Mehr Bürgernähe bei den Rentenversicherungsträgern	105
8.	**Gesundheit**	107
8.1	Trotz guter Zusammenarbeit noch ungelöste Probleme	107
8.2	Gesundheitsnetze - höchste Anforderungen an Datenschutz und Datensicherheit	109
8.2.1	Ziele von Gesundheitsnetzen	109
8.2.2	Rechtsgrundlagen	110
8.2.3	Sicherheitspolitik	110
8.2.4	Sicherheitskonzept	112
8.2.5	Zusammenfassung	116
9.	**Statistik - Kommt wieder eine Volkszählung?**	118
10.	**Bildung und Wissenschaft**	121
10.1	Die Schulen und das Internet	121
10.1.1	Basisinformation der Schülerinnen und Schüler	121
10.1.2	Nutzungsordnungen	123
10.2	Keine Wahl beim Studierendenausweis mit Chip?	124
10.3	Forschung	125
11.	**Öffentlicher Dienst**	128
11.1	"Ihre Personalakte konnte trotz umfangreicher und wiederholter Bemühungen nicht wieder aufgefunden werden ..."	128
11.2	Bewerbungsverfahren	129
11.3	Befragungen von Mitarbeiterinnen und Mitarbeitern - zuverlässige Ergebnisse sind gefragt	129

11.4	Tele-Heimarbeit - Hinweise für eine datenschutzgerechte Einführung	130
11.4.1	Allgemeines	131
11.4.2	Grundsätzliche Anforderungen/Hinweise	131
11.4.3	Anforderungen an technische und organisatorische Maßnahmen	133
12.	**Verkehr, Wirtschaft und öffentliche Unternehmen**	137
12.1	Führerschein im neuen Gewand - was verbirgt sich dahinter?	137
12.2	Bekämpfung von mißbräuchlicher Betätigung in Verwaltung und Wirtschaft	138
12.2.1	Korruptionsregister	138
12.2.2	Bekanntgabe von Wettbewerbsverstößen	138
12.2.3	Geldwäsche	140
12.2.4	Warndateien der Versicherungen	140
12.3	Direktmarketing von Sparkassen und öffentlichen Versicherungen	141
12.4	Datenspuren, Datenschatten im elektronischen Zahlungsverkehr	142
12.4.1	Elektronisches Lastschriftverfahren	143
12.4.2	Elektronische Geldbörse - GeldKarte	143
12.4.3	Homebanking mit dem HBCI-Verfahren	147
12.4.4	Elektronisches Geld - Netzgeld	148

Anhang 149

Arbeitsergebnisse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 149

Entschließungen der Datenschutzbeauftragten des Bundes und der Länder 149

Nr. 1 vom 17./18. April 1997 - 53. Konferenz
Achtung der Menschenrechte in der Europäischen Union 149

Nr. 2 vom 17./18. April 1997 - 53. Konferenz
Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen 149

Nr. 3 vom 20.10.1997
zu den Vorschlägen der Arbeitsgruppe der ASMK "Verbesserter Datenaustausch bei Sozialleistungen" 151

Nr. 4 vom 23./24. Oktober 1997 – 54. Konferenz
Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts 154

Nr. 5 vom 23./24. Oktober 1997 – 54. Konferenz
Erforderlichkeit datenschutzfreundlicher Technologien 156

Nr. 6 vom 19./20. März 1998 – 55. Konferenz
Datenschutz beim digitalen Fernsehen 158

Nr. 7 vom 19./20. März 1998 – 55. Konferenz
Datenschutzprobleme der Geldkarte 159

Nr. 8 vom 5./6. Oktober 1998 – 56. Konferenz
Dringlichkeit der Datenschutzmodernisierung 160

Nr. 9 vom 5./6. Oktober 1998 – 56. Konferenz
Entwicklungen im Sicherheitsbereich 161

Nr. 10 vom 5./6. Oktober 1998 – 56. Konferenz
Weitergabe von Meldedaten an Adreßbuchverlage und Parteien 161

Nr. 11 vom 5./6. Oktober 1998 – 56. Konferenz
Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge 162

Thesenpapier zum Allgemeinen Informationszugangsrecht und zum Recht auf informationelle Selbstbestimmung 162

Stichwortverzeichnis 171

Bestellformular Informationsmaterial

Vorbemerkung

Im Berichtszeitraum ist eine Fülle neuartiger - und oft genug vermehrter altbekannter - Anforderungen auf meine Mitarbeiterinnen und Mitarbeiter zugekommen, die sie engagiert gemeistert haben. Dafür sei ihnen allen an dieser Stelle auch einmal öffentlich recht herzlich gedankt. Die Dienststelle besitzt inzwischen beispielsweise ein modernes Intranet, mit dem der Umgang erst einmal gelernt sein will. Auch unsere seit Ende 1998 unter **"www.lfd.nrw.de"** oder **"www.nordrhein-westfalen.datenschutz.de"** abrufbare Homepage hätte ohne den außerordentlichen Einsatz aller Kräfte nicht erstellt werden können. Die herausgegebenen Informationsblätter und -broschüren erfreuen sich einer ebenso regen Nachfrage wie die Dokumentation der im November 1997 gemeinsam mit dem Institut für Informations-, Telekommunikations- und Medienrecht sowie der Deutschen Vereinigung für Datenschutz veranstalteten Tagung "20 Jahre Datenschutz - Individualismus oder Gemeinschaftssinn?". Positive Rückmeldungen aus der Beratungstätigkeit und der Interessenvertretung für die Durchsetzung des Rechts auf informationelle Selbstbestimmung sind weitere wichtige Steine im Mosaik der für die Dienststelle zu ziehenden Bilanz.

Der Datenschutzbericht 1999 versucht, Konzeption und Akzente des letzten Berichts weiterzuentwickeln. Obwohl die Zahl der Einzelfälle, die aus Beschwerden von Bürgerinnen und Bürgern oder aus Anfragen öffentlicher Stellen entstehen, weiter angestiegen ist, wurde die Beschreibung der einzelnen Fälle nochmals reduziert zugunsten von Fragestellungen mit größerer Allgemeingültigkeit und von neueren Entwicklungstendenzen. Die sich wandelnden Verhältnisse zwingen dazu. Neben dem Schwerpunkt zu Polizei und Verfassungsschutz liegt daher - wie schon im letzten Bericht - auch dieses Mal wieder ein Schwerpunkt auf den technischen Problemen des Datenschutzes. Dies wird voraussichtlich auch so bleiben müssen. Dabei soll allerdings Schritt für Schritt versucht werden, technische und rechtliche Aspekte stärker miteinander zu verzahnen. So finden sich etwa die technischen Datenschutzanforderungen an Gesundheitsnetze im Gesundheitskapitel und die Tele-Heimarbeit wird im Kapitel über den öffentlichen Dienst behandelt. Auch dieser Bericht - und folgenden wird es nicht anders ergehen - ist daher wieder ein Experiment. Voilà!

1. Zur Situation im Datenschutz: Gestalten statt verwalten

"Kommunikation total"- so titelte Mitte Dezember 1998 ein großes bundesdeutsches Printmedium und erfaßte damit gleichwohl nur die halbe Wahrheit. Zutreffend beschrieben wurde dort das **Zusammenwachsen** der einzelnen kabel- und funkgestützten Kommunikationsmedien wie etwa Telefon, Computer, Internet und Fernsehen. Nicht erwähnt wurden jedoch die damit verbundenen **Risiken** für die informationelle Selbstbestimmung: Die - objektiv - leichte Überwachbarkeit der Kommunizierenden. Der Thriller, in dem ein lernfähiges Computersystem sämtliche für die Menschen lebensnotwendigen oder auch nur praktischen Gebäudefunktionen selbsttätig steuert, könnte bald von der Realität eingeholt werden, wenn alle automatisierbaren Haushaltsfunktionen mittels neuer Technologien aus der Ferne gesteuert, aber auch **überwacht** werden können. Von kontrollfreien Räumen für Jugendliche etwa könnte keine Rede mehr sein, wenn die Eltern - oder auch andere Personen - von jedem Ort aus zu jeder Zeit problemlos von der Haushaltselektronik abrufen könnten, in welchen Zimmern welche elektronischen Geräte mit wieviel Stromverbrauch eingeschaltet sind und was sich eigentlich noch im Kühlschrank befindet oder per Internet schon automatisch nachbestellt worden ist. Und das ist noch das harmloseste Beispiel für die Nutzung der vielen neuen technischen Möglichkeiten.

So faszinierend und reizvoll es ist, sich beispielsweise mit dem Notebook übers Handy ins **Internet** einzuwählen, so wenig dürfen bei aller Begeisterung über den technischen Fortschritt dessen **Mißbrauchspotentiale** vergessen werden. Das Netz liegt zweifellos im Trend, sowohl bei den öffentlichen Stellen als auch bei den privaten Nutzerinnen und Nutzern. Der Reiz weltweiter Kommunikation und der Entgrenzung von Zeit und Raum läßt allerdings manche vergessen, welche qualitativ neuen Risiken für die informationelle Selbstbestimmung mit der Netznutzung verbunden sind. Mit verhältnismäßig geringem Aufwand ist es möglich, nachzuvollziehen, wer sich wie oft und wie lange wo aufgehalten und mit wem kommuniziert hat. Die **Kommunikationstätigkeit** ist überwachbar, ihre **Vertraulichkeit** ist ohne den Einsatz von sicheren Verschlüsselungstechniken ebensowenig gewährleistet wie ihre **Authentizität** ohne den Einsatz einer digitalen Signatur. Eine unverschlüsselte und unsignierte E-Mail ist einer maschinengeschriebenen Postkarte vergleichbar, die von allen gelesen und sogar verändert werden kann, ohne daß überhaupt Absenderin oder Absender stimmen muß. Zudem sind ins Netz eingestellte Daten oder Informationen nicht mehr rückholbar. Ist eine Information einmal im Netz, ist sie möglicherweise immer im Netz, und ob in der ursprünglichen Form oder verfälscht, ist außerdem **ungewiß**.

Wer surft, chattet, E-Mails versendet, im Netz einkauft oder Bankgeschäfte abwickelt, hinterläßt elektronische **Spuren**, die zum Teil jahrelang nicht verwehen. Die Preisgabe der personenbezogenen Daten geschieht mehr oder weniger **beiläufig**. Jeder Mausklick, jeder Tastendruck verbreitert die Datenspur. Der elektronische Informationsaustausch ist alltäglich geworden und durch seine Normalität jeder Warnfunktion beraubt. Dem steht gegenüber, daß viele die Datenspur zu lesen und gewinnbringend zu vermarkten verstehen. Noch niemals zuvor wurden so viele personenbezogene Daten so systematisch gesammelt, verarbeitet und verwertet. Der aus der Netznutzung zu ziehende Umfang personenbezogener Daten und die nach ihrer Zusammenführung aus ihnen gewinnbare Informationsqualität haben eine **neue Dimension** erreicht. Die damit verbundene Gefährdung der informationellen Selbstbestimmung springt ins Auge, nicht zuletzt liegt sie auch darin, daß die wachsenden Datenbestände in privater Hand ebenfalls Begehrlichkeiten bei staatlichen Stellen wecken könnten. Ob rechtlich erlaubt oder nicht, könnten Kommunikationsüberwachung und daraus entstandene Bewegungs-, Nutzungs- und letztlich Persönlichkeitsprofile eventuell den Alltag begleiten, wenn keine gesellschaftliche **Diskussion** geführt wird über Funktion und Stellenwert der kommunikativen **Selbstbestimmung** in der entstehenden Medien-, Informations- und Wissensgesellschaft.

Nicht nur Internet und Medienkonvergenz prägen die derzeitigen **technischen Veränderungen** der Datenverarbeitung. Schritt für Schritt werden die Großrechneranlagen aus den 70er Jahren ersetzt durch Verwaltungsnetze, die von jedem Arbeitsplatz aus zugänglich sind. Diese vernetzte **Dezentralisierung** und die sich abzeichnende **Internationalisierung** der Datenflüsse - nicht nur im Bereich von Strafverfolgung und Gefahrenabwehr - lassen es für die einzelnen nahezu unüberschaubar werden, wer was wann und bei welcher Gelegenheit über die eigene Person weiß.

Die Veränderungen der **tatsächlichen Ausgangssituation**, aber auch eine **kritische Bestandsaufnahme** der bisherigen datenschutzrechtlichen Regelungen zwingen dazu, über konzeptionelle Veränderungen des Datenschutzes nachzudenken. Im Berichtszeitraum hat es eine Fülle von Publikationen, Foren und Veranstaltungen zu Fragen der Notwendigkeit und der Richtung eines **neuen Datenschutzes** gegeben. Zur Beteiligung meiner Dienststelle an dieser Diskussion seien hier lediglich zwei Beispiele genannt, nämlich die Tagung **"20 Jahre Datenschutz - Individualismus oder Gemeinschaftssinn?"** sowie das Symposium **"Neue Instrumente im Datenschutz"**, das im November 1998 ebenfalls in Kooperation mit dem Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster durchgeführt wurde. Der Dokumentationsband der Tagung kann sowohl in meiner Dienststelle angefordert als auch unter **"www.lfd.nrw.de"**

oder **"www.nordrhein-westfalen.datenschutz.de"** abgerufen werden. Gleiches gilt demnächst für die Dokumentation des Symposiums.

In der Analyse der Situation des Datenschutzes herrscht weitgehend Einigkeit: Das Datenschutzrecht ist kompliziert, unübersichtlich und kaum noch verständlich. Das Verhältnis von allgemeiner Datenschutzgesetzgebung und bereichsspezifischen Regelungen steht - soweit diese Lücken lassen - in der Praxis häufig im Streit. Langatmige, bis ins kleinste Detail gehende Vorschriften haben in der Sache oft lediglich die bereits stattfindende Verwaltungstätigkeit gesetzlich legitimiert und in vielen Fällen darüber hinaus die Datenverarbeitungsbefugnisse vorsorglich noch erheblich ausgeweitet. Von einer Stärkung der informationellen Selbstbestimmung, die gleichermaßen Voraussetzung und Ergebnis einer **selbstbestimmten Kommunikationsteilhabe** ist, kann insoweit ebensowenig die Rede sein wie von einer **Begrenzung von Informationsmacht**. Die Anforderungen des Bundesverfassungsgerichts, daß Bürgerinnen und Bürger wissen können müssen, wer was wann und bei welcher Gelegenheit über sie weiß, sind auf diese Weise kaum erfüllbar. Eingestellt hat sich vielmehr eine Undurchschaubarkeit, die bei den **Betroffenen** zu einem tiefen **Mißtrauen** geführt hat - flankiert von einer Mischung aus **Ohnmacht** und **Verärgerung**. Dies ist jedenfalls das Ergebnis einer im Jahre 1998 von einem Forschungsinstitut durchgeführten **Repräsentativbefragung** von 3000 Personen. Danach genießt der Datenschutz selbst allerdings eine recht große Unterstützung in der Bevölkerung. Daß der Datenschutz **mehr Bedeutung** bekommen sollte, befürworteten immerhin mehr als die Hälfte (55%) der befragten Personen.

Ein wirklich wirksamer Schutz des Rechts auf informationelle Selbstbestimmung kann im Ergebnis aber auch in tatsächlicher Hinsicht kaum festgestellt werden, und das hat seine Ursachen nicht nur in Vollzugsdefiziten, sondern auch in dem höchst unterschiedlichen Schutzniveau gegenüber staatlicher und privater Datenmacht sowie nicht zuletzt in der technischen Entwicklung, die bewirkt, daß das Recht an die Grenzen seiner Steuerungsfähigkeit stößt. Ein **moderner Datenschutz** hat demgegenüber einen **ganzheitlichen** Ansatz zu verfolgen und muß stärker **präventiv** ansetzen. Er muß Recht und Technik gemeinsam in den Blick nehmen. Das Datenschutzrecht kann beispielsweise den Einsatz datenschutzfreundlicher Technik fordern und fördern. Es kann - im Bewußtsein seiner begrenzten ordnungsrechtlichen Steuerungsfähigkeit - die notwendige **Verbindung** von **Datenschutz** und **Technik** herstellen, indem es unter anderem Anreizsysteme schafft für die Entwicklung datenvermeidender oder auch datensparsamer Technologien und Verfahren sowie für den Einsatz innovativer Datenschutz- und Datensicherheitskonzepte.

Ein modernes Datenschutzrecht wird zudem verstärkt gefordert sein, die **informationelle Gewaltenteilung** und die Bindung personenbezogener Datenverarbeitung an den festgelegten **Verarbeitungszweck** zu sichern. Es muß für die Betroffenen mehr subjektive **Rechte** enthalten, die ihnen **Transparenz**, **Entscheidungsfreiheit** und **Handlungsoptionen** eröffnen, um ihre informationelle Selbstbestimmung effektiv wahrnehmen, aber auch selber schützen zu können. Dazu zählen Informations- und Benachrichtigungsrechte ebenso wie Einwilligungserfordernisse, Widerspruchsrechte und Wahlmöglichkeiten. Werden personenbezogene Daten zudem etwa verschlüsselt gespeichert oder übermittelt - sei es von öffentlichen Stellen oder von den Betroffenen selbst -, so erhöht dies nicht nur den Vertraulichkeitsschutz, sondern könnte einen Beitrag zur **Selbstverständlichkeit** des Gebrauchs **datenschutzfreundlicher Technik** im **Alltag** leisten. Konkrete Vorschläge für neue Akzente habe ich im Rahmen der Diskussion um die anstehende Novelle des nordrhein-westfälischen Datenschutzgesetzes gemacht. Der gesetzliche Änderungsbedarf, der sich aus der Notwendigkeit ergibt, die europäische Datenschutzrichtlinie auch in Landesrecht umzusetzen, könnte und sollte für einen umfassenden Modernisierungsschub genutzt werden.

Die Erfordernisse, die sich aus der europäischen Integration und der technischen Entwicklung für den Datenschutz ergeben, waren 1998 auch Thema des **62. Deutschen Juristentages**. In den dort gefaßten Beschlüssen kommt deutlich zum Ausdruck, daß eine Neuorientierung des Datenschutzes geboten ist. Zwar wird die Fachdiskussion um die generelle Möglichkeit und die einzelne Ausgestaltung einer perspektivisch zu schaffenden, umfassenden Informationsordnung noch einige Zeit in Anspruch nehmen müssen, doch hat der Juristentag auch zu Problemen Stellung genommen, die unmittelbar auf der Tagesordnung stehen. So hat er sich beispielsweise nicht nur für die Beibehaltung unreglementierter Verschlüsselungsmöglichkeiten ausgesprochen, sondern **Verschlüsselung** bei besonderen Gefährdungslagen sogar für **geboten** erachtet. Als **Leitlinien** des künftigen Informationsrechts wurden benannt: Datenvermeidung und Datensparsamkeit, Zweckbindung der Daten, Systemdatenschutz, klare Verantwortlichkeiten im Datenumgang, Anonymisierung und Pseudonymisierung personenbezogener Daten, Datensicherheit durch technische und organisatorische Vorkehrungen, Folgenausgleich. Außerdem wurde empfohlen, ein grundsätzlich **einheitliches materielles Datenschutzrecht** für den **öffentlichen** und den **privaten Bereich** zu schaffen, dessen innere Differenzierungen sich nach den Unterschieden in der Schutzbedürftigkeit unter Beachtung der Selbstbestimmung (Freiwilligkeit) und des Gefahrenpotentials zu richten haben. Gefordert wurde ebenfalls und nicht zuletzt die **Verselbständigung** und **Weisungsfreiheit** der öffentlichen Stellen, die für die **Datenschutzkontrolle** zuständig sind.

Es wäre schön, wenn die Diskussionsergebnisse der letzten Jahre in die Überlegungen für die Änderungen des Landes- wie auch des Bundesdatenschutzgesetzes einfließen würden. Insbesondere für das **Bundesdatenschutzgesetz** gilt es allerdings noch Lösungen zu finden, mit denen der zunehmenden Kommerzialisierung personenbezogener Daten wirkungsvoll begegnet werden kann. Die Kurzformel "privacy or property" kennzeichnet eine Entwicklung, die den Betroffenen geldwerte Vorteile für die Nutzung ihrer Daten zu anderen Zwecken oder durch andere Personen zukommen läßt. Wer etwa im Internet Ware bei manchen Firmen mit Sitz außerhalb Deutschlands bestellt, braucht sich über das Angebot eines Preisnachlasses für den Fall der Einwilligung in die anderweitige Verarbeitung der eigenen Daten durch die Firma nicht zu wundern. Ob bei einer entsprechenden Einwilligung die Einhaltung der Vereinbarung auch verläßlich kontrolliert werden kann, bleibt allerdings zweifelhaft. Es kommt hinzu, daß vor dem Hintergrund der ohnehin bestehenden Netzrisiken damit möglicherweise Türen geöffnet werden, die sich kaum wieder schließen lassen.

Ein Beispiel für eine Datenkommerzialisierung ganz **anderer Art** soll gleichwohl nicht unerwähnt bleiben, um ein Schlaglicht auf mögliche Entwicklungen in diesem Bereich zu werfen: In Island ist im Dezember 1998 trotz nationaler und internationaler Proteste ein Gesetz verabschiedet worden, das einer isländischen Firma den Aufbau einer speziellen Datenbank ermöglicht und ihr das Monopol für deren langjährige Nutzung gibt. In der Datenbank sollen Erkenntnisse über die individuelle Zusammensetzung des genetischen Materials der gesamten, etwa 273.000 Personen umfassenden isländischen Bevölkerung mit weiteren Informationen aus dem zentralen Gesundheitsregister zusammengeführt werden. Der schweizer Arzneimittelkonzern, der mit der isländischen Firma zusammenarbeitet, wird die eventuell aus der Kooperation entstehenden Arzneimittel der isländischen Bevölkerung kostenlos zur Verfügung stellen. Die Erfassung und Vermarktung der genetischen Informationen eines ganzen Volkes durch eine private Firma ist in Island beschlossen worden. Sie hat aber auch eine noch nicht beendete Debatte ausgelöst um die **ethische Problematik** dieses Projektes, um die Gefahren eines eventuellen Mißbrauchs der Erkenntnisse und - gerade angesichts der geringen Bevölkerungszahl - um vielleicht vorhandene Identifizierungsmöglichkeiten.

Im Rahmen der Diskussionen über einen neuen Datenschutz haben die Datenschutzbeauftragten auch ihre eigene Tätigkeit kritisch reflektiert. Es gilt, das eigentliche **Anliegen** des Datenschutzes wieder verstärkt **bewußt** zu machen. Datenschutz ist kein Selbstzweck. Nicht irgendwelche Daten sollen etwa um ihrer selbst willen geschützt werden, sondern geschützt werden sollen **Menschen** in ihren **grundrechtlich garantierten Kommunika-**

tionsmöglichkeiten. Sie sollen grundsätzlich selbst darüber entscheiden können und informiert sein, wer was wann wie lange und bei welcher Gelegenheit über sie weiß. Um dazu beizutragen, die Voraussetzungen für eine effektive Wahrnehmung des Rechts auf informationelle Selbstbestimmung im alltäglichen Leben zu schaffen, lautet die Handlungsleitlinie eines neuen Datenschutzes: **"Gestalten statt verwalten"**. Dabei kommt es darauf an, nicht nur auf Außenanforderungen zu reagieren, sondern eigene Zielsetzungen sowie Ideenreichtum für lebensnahe Problemlösungskonzepte zu entwickeln, Bürgerinnen und Bürger wie auch öffentliche Stellen innovativ zu beraten und dies mit der Kontrolle der Einhaltung datenschutzrechtlicher Bestimmungen zu verbinden.

2. Technische und rechtliche Aspekte der Medienentwicklung

2.1 Datenschutzfreundliche Technologien

Der immer größer werdende Einfluß von Informations- und Telekommunikationstechnik auf unser Leben bringt es mit sich, daß wir an vielen Stellen elektronische Spuren hinterlassen, ohne zu wissen, welche unserer Daten an welchem Ort, für welche Dauer und für welchen Zweck gespeichert werden. Mit den Datenspuren wächst die Gefahr des Mißbrauchs und der Zusammenführung von Einzelinformationen zu komplexen Persönlichkeitsprofilen. Datenschutzfreundliche Techniken und Verfahren, die Prinzipien der anonymen Nutzung, Datenvermeidung und Datenreduzierung beinhalten, können diesem Trend entgegenwirken.

IT-Systeme wurden bisher ausschließlich unter Verfügbarkeits-, Performance-, Integritäts- und Vertraulichkeitsaspekten der Betreibenden konzipiert. Werden sie aus der Sicht der Nutzenden und Betroffenen betrachtet, sind diese Gestaltungsaspekte jedoch nicht mehr allein ausreichend, da sie die Erfordernisse des Datenschutzes nur soweit berücksichtigen, als der Schutz der Privatheit der einzelnen auf die Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert wird. Gestaltungsmerkmal sollte vielmehr sein, daß bereits vor der Erhebung und Verarbeitung die zu speichernde **Datenmenge** auf das nicht zu vermeidende **Maß reduziert** wird. Dieser Aspekt ist aus Sicht der Nutzenden von zentraler Bedeutung, um die Akzeptanz neuer Dienste zu erhöhen. Datenschutzfreundliche Technik läßt sich daran messen, daß das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IT-Systemen ebenso stark beeinflußt wie die Forderung nach Datensicherheit.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 23./24. Oktober 1997 eine Entschließung zur Erforderlichkeit datenschutzfreundlicher Technologien verabschiedet (Abdruck im Anhang, Nr. 5). Hierin fordert sie, zukünftig bereits beim **Design** und bei der **Entwicklung** technischer Systeme den Schutz der Privatsphäre in den Vordergrund zu stellen. Systeme sollten so konzipiert sein, daß möglichst erst gar keine personenbezogenen Daten erhoben und gespeichert werden. Oberster Grundsatz sollte die **Datenvermeidung** sein und, wenn dies nicht möglich ist, die weitgehende Datensparsamkeit.

In der Praxis bedeutet dies, daß eine in der nicht automatisierten Welt oder auch beim Einsatz analoger Techniken mögliche anonyme Nutzungsmög-

lichkeit von Dienstleistungen ebenfalls bei der Automatisierung oder Digitalisierung dieser Bereiche umgesetzt oder zumindest als Wahlmöglichkeit angeboten werden sollte. So sollte das Internet durch technische Mittel so verbessert werden, daß beispielsweise anonymes Browsing, E-Mail und Anbieten von Informationen möglich ist. Elektronische Zahlungsverfahren wie die Geldkarte sollten auch die Möglichkeit eröffnen, ohne die Angabe und Verarbeitung von personenbezogenen Daten auszukommen. Ebenso sollte die mit der Digitalisierung der Fernseh- und Hörfunkübertragung entstehende Infrastruktur nicht dazu genutzt werden, beispielsweise das individuelle Fernsehverhalten zu registrieren. Gerade der in diesem Zusammenhang zum Einsatz vorgesehene Decodertyp ist möglicherweise nicht so gut geeignet, Datenschutzanforderungen zu gewährleisten. Er ist weiter ein Beispiel dafür, daß eine Diskussion über den Einsatz datenschutzfreundlicher Technologien immer dann wenig zielführend ist, wenn - wie in diesem Fall - bereits fertige Geräte präsentiert werden; siehe die Entschließung vom 19./20. März 1998 zum Datenschutz beim digitalen Fernsehen (Abdruck im Anhang, Nr. 6).

Der stetig zunehmende Einfluß der Telekommunikation auf unser tägliches Leben macht den Einsatz datenschutzfreundlicher Technologien besonders dringend. Die Datenschutzbeauftragten haben deshalb hier einen besonderen Schwerpunkt gesetzt. In einer Arbeitsgruppe des Arbeitskreises Technik wurde unter Federführung meiner Dienststelle der Stand der Forschung und Entwicklung zusammengestellt und in einem **Workshop** mit Vertreterinnen und Vertretern aus den Bereichen Politik, Verwaltung, Herstellerindustrie, Netzbetreiber und Wissenschaft diskutiert, welche Techniken und Verfahren zur **anonymen Nutzung, Datenvermeidung** und **Datenreduzierung** in die Netz- und Geräteplanungen einbezogen werden könnten. Als Ergebnis des Workshops kann festgestellt werden, daß die erforderlichen Techniken weitgehend zur Verfügung stehen - Prepaid Chipkarten, Kryptographie, Mixe - jedoch in der Öffentlichkeit noch nicht hinreichend bekannt sind. Auf Seiten der Nutzerinnen und Nutzer gibt es noch Informations- und Aufklärungsbedarf, auf Seiten der Herstellerinnen und Hersteller sowie Betreiberinnen und Betreiber überwiegt zur Zeit eine zu zögerliche Haltung. Hier ist noch Überzeugungsarbeit zu leisten. Ziel ist, daß die Industrie Datenschutzfreundlichkeit als **Qualitätsmerkmal** ihrer Produkte versteht.

Im **Endgerätebereich** sind die Voraussetzungen für eine breite Einführung von wiederaufladbaren Prepaid Chipkarten sicherlich am leichtesten umzusetzen. Diese Technik ist geeignet, Dienste anzubieten, mit denen die Erhebung und Speicherung von Verbindungs-, Bestands- und Entgeltdaten weitgehend zu vermeiden oder zumindest zu reduzieren ist. Geeignete Telekommunikationsendgeräte mit Chipkartenleser sind kein technisches Problem mehr. Sie existieren, werden zur Zeit allerdings nicht zur anonymen

Entgeltabrechnung benutzt. Allen Nutzerinnen und Nutzern von TK-Diensten sollte zumindest diese Möglichkeit der Entgeltzahlung wahlweise angeboten werden.

Soll die gesamte Kommunikation zwischen Sender und Empfänger geschützt werden, so wären die derzeitigen **Netzstrukturen** mehr oder weniger stark zu modifizieren. Im Dialog mit den Herstellerinnen und Herstellern und Betreiberinnen und Betreibern von TK-Netzen sowie den wissenschaftlichen Forschungsgemeinschaften und -instituten sollte die Einbringung datenvermeidender und anonymisierender Technologien in zukünftige Netze weiter erörtert werden. Unter Berücksichtigung des Ziels, die unbeobachtbare, gesicherte Kommunikation zu erreichen, erscheint auch der technische Aufwand und die teilweise noch notwendige Entwicklungsarbeit hierzu gerechtfertigt. Ein Beispiel für derartige Schutzmaßnahmen ist der **Einbau von Mixen** in die Netzstruktur. Mixe sind Netzknoten, die dem Schutz der Kommunikationsbeziehung dienen, indem sie die Verkettbarkeit zwischen Sender und Empfänger einer Nachricht verhindern. Dies wird durch das folgende, erstmals von David Chaum in den achtziger Jahren entwickelte und mittlerweile in der Wissenschaft weiter verfeinerte Verfahren erreicht:

- Sammlung eingehender Nachrichten
- Umkodierung der Nachrichten
- Ausgabe der Nachrichten in veränderter Reihenfolge an den nächsten (Mix-)Netzknoten bis zum Empfänger und zur Empfängerin.

Mit der Mix-Technik lassen sich die Anonymität oder Pseudonymität der sendenden und/oder empfangenden Person gegenüber Dritten und der Schutz weiterer Verbindungsdaten umsetzen, wie etwa Beginn, Dauer oder Dienstart der Kommunikation insgesamt und Aufenthaltsinformationen bei Mobilkommunikation.

Ein konsequenter Datenschutz zählt zu den zentralen Akzeptanzvoraussetzungen einer Informationsgesellschaft. Für die Einlösung dieser Forderung reichen die bisherigen Ansätze nicht aus. Der ausschließliche Schutz der Systeme und damit der Herstellenden und Betreibenden von Informations- und Kommunikationstechnik beleuchtet nur die eine Seite der Kommunikation. Zukünftig ist der Schutz der persönlichen Daten der einzelnen und damit der Schutz der informationellen Selbstbestimmung in den Vordergrund zu stellen. Hierbei sind Herstellende und Diensteanbietende aufgefordert, anonyme oder datensparsame Lösungen zu entwickeln und bereitzustellen.

2.2 Kryptographie - Schlüsseltechnologie für Informationssicherheit und vertrauenswürdige Kommunikation

2.2.1 Einführung

Nicht zuletzt bedingt durch die rasante Entwicklung der Informationstechnologie vollzieht sich ein Paradigmenwechsel im Datenschutz. Während der Datenschutz über viele Jahre geprägt war von der Vorstellung einer monolithischen Großrechnerwelt, sieht er sich heute konfrontiert mit dezentralisierten und verteilten Strukturen **vernetzter Systeme**, die nach dem Client/ Server-Prinzip miteinander kommunizieren. Früher war der Datenschutz primär verbunden mit dem Schutz der Rechner, die in hermetisch abgeschlossenen Rechenzentren betrieben wurden. Der Zugang zum Rechner und damit zu den Daten konnte nur über die angeschlossenen Terminals erfolgen. Heute schwirren die Daten über Datenautobahnen und es existieren vielfältige Möglichkeiten, auf diese Datenautobahnen zu gelangen, um an der globalen elektronischen Kommunikation teilzunehmen. Damit erhält der Datenschutz eine neue Qualität. Datenschutz ist nicht mehr an den Rechenanlagen, sondern - im eigentlichen Sinne des Wortes - an den **Daten selbst** festzumachen. Attribute wie vertraulich, integer und authentisch sind als Eigenschaften der Daten anzusehen, die unabhängig vom aktuellen Aufenthaltsort der Daten sowie der Art und dem Stadium ihrer Verarbeitung gesichert werden müssen.

Die Kryptographie stellt Methoden zur Verfügung, um diesen "datenbezogenen" Datenschutz zu realisieren. Datenschutz ohne Kryptographie ist bei den Möglichkeiten der heutigen Informationstechnologie nicht mehr denkbar. Außerdem versetzen die Mechanismen der Kryptographie die Bürgerinnen und Bürger in die Lage, ihre Daten eigenverantwortlich und sicher schützen zu können, ohne wissen zu müssen, welche Wege die Daten im weltweiten Netz nehmen, welche Systeme sie passieren und welchen Bedrohungen sie dabei ausgesetzt sind. Die folgenden Ausführungen sollen - ohne zu sehr auf technische Details einzugehen - einen Eindruck vermitteln, welche Schutzziele sich alleine schon durch Verschlüsselungsverfahren und Verfahren zur digitalen Signatur verwirklichen lassen.

2.2.2 Verschlüsselungsverfahren

2.2.2.1 Symmetrische Verschlüsselungsverfahren

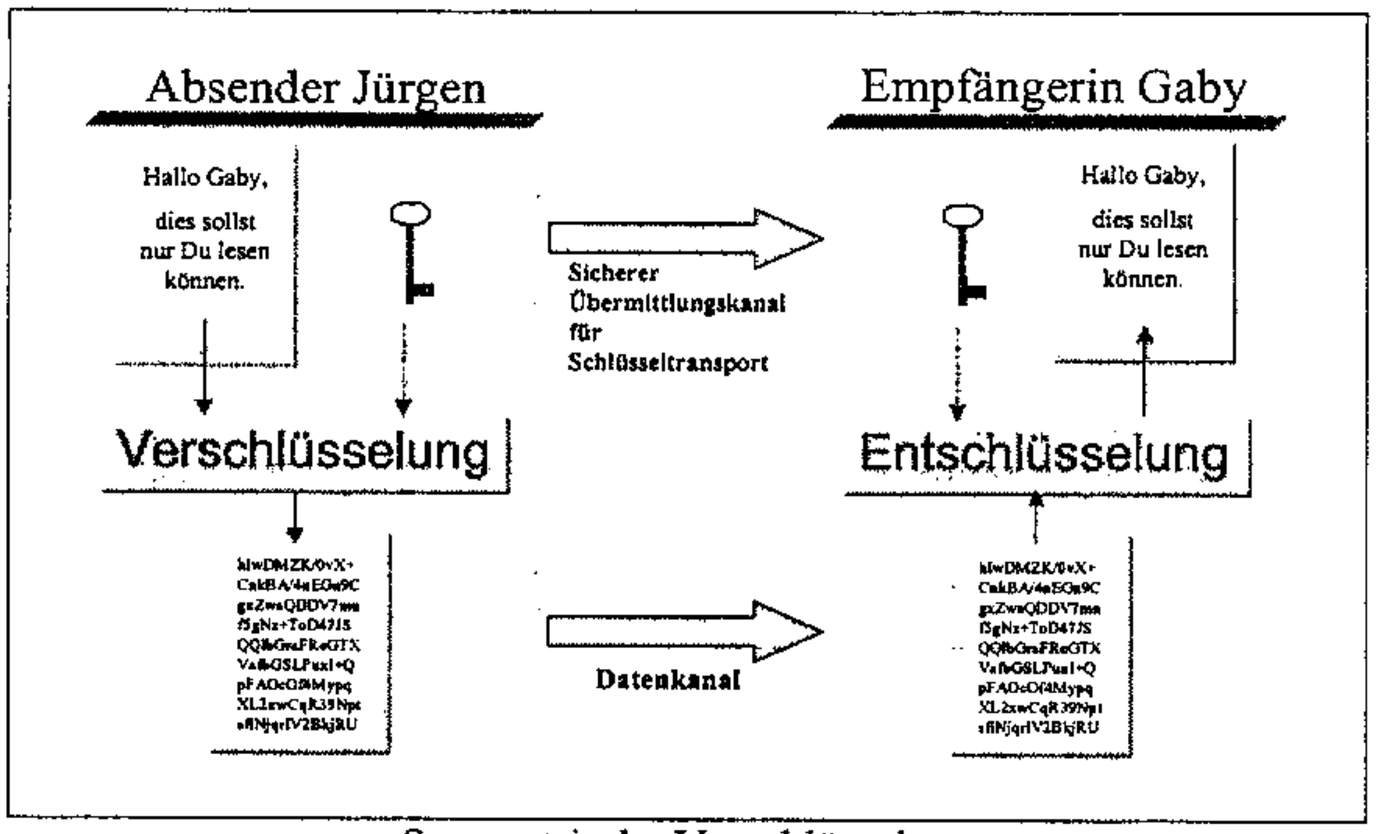
Bei **symmetrischen** Verschlüsselungsverfahren erfolgt sowohl die Verschlüsselung eines Klartextes als auch die Entschlüsselung des entstandenen Schlüsseltextes nach dem gleichen Verfahren mit **jeweils identischen** Schlüsseln. Dies setzt voraus, daß die Absenderin oder der Absender einer verschlüsselten Nachricht, der Empfängerin oder dem Empfänger dieser Nachricht zusätzlich zum Schlüsseltext auch den verwendeten Schlüssel zukommen lassen muß. Da eine verschlüsselte Nachricht und der zugehörige Schlüssel **nie gemeinsam** übermittelt werden dürfen, ist neben dem Datenkanal zur Übermittlung des Schlüsseltextes ein davon getrennter "sicherer Übermittlungskanal" für den Transport des Schlüssels von der absendenden zur empfangenden Person erforderlich.

Beispiel: Angenommen, Jürgen möchte seiner Freundin Gaby eine mit einem symmetrischen Verfahren verschlüsselte Nachricht übermitteln. Was ist zu tun?

- Zunächst muß Jürgen mit Gaby über einen "sicheren Kanal" den Schlüssel vereinbaren, mit dem er die Nachricht zu verschlüsseln beabsichtigt. Dies kann Jürgen beispielsweise tun, indem er Gaby den Schlüssel in einem versiegelten Brief schickt oder über eine Vertrauensperson übermitteln läßt. Er könnte die Schlüsselabsprache mit Gaby aber auch mit einem persönlichen Treffen verbinden.

- Erst nach erfolgreich durchgeführtem Schlüsselaustausch kann Jürgen die Nachricht mit dem vereinbarten Schlüssel verschlüsseln und an Gaby übermitteln.

- Gaby, die Empfängerin der Nachricht, nimmt ihrerseits den mit Jürgen vereinbarten Schlüssel und entschlüsselt mit diesem die erhaltene Nachricht. Haben Gaby und Jürgen sichergestellt, daß außer ihnen niemand den verabredeten Schlüssel kennt, können sie sich darauf verlassen, daß bei einer hinreichenden Länge des Schlüssels mit hoher Wahrscheinlichkeit ausschließlich Gaby die Nachricht entschlüsseln kann.



Symmetrische Verschlüsselung

Symmetrische Verschlüsselungsverfahren haben den **Vorteil**, daß sie softwaretechnisch **einfach** umzusetzen und sehr **effizient** sind. Ihr **Nachteil** liegt in der Notwendigkeit der **Schlüsselabsprache**. Da a priori meist nicht abzusehen ist, wer mit wem irgendwann einmal verschlüsselte Nachrichten austauschen möchte, müssen sich quasi auf Verdacht alle potentiell miteinander kommunizierenden Personen jeweils paarweise auf einen gemeinsamen Schlüssel verständigen, oder aber der Schlüsselaustausch wird erst vor jeder konkret anstehenden Kommunikation unter den Beteiligten durchgeführt. Die entstehende **Flut von Schlüsseln** und die damit verbundene aufwendige **Verwaltung** und **Verteilung** der Schlüssel stellen ein praktisch unüberwindbares Hindernis dar. Außerdem ist eine spontane Kommunikation mit symmetrischen Verfahren nicht möglich. Diese Mängel beseitigen asymmetrische Verschlüsselungsverfahren.

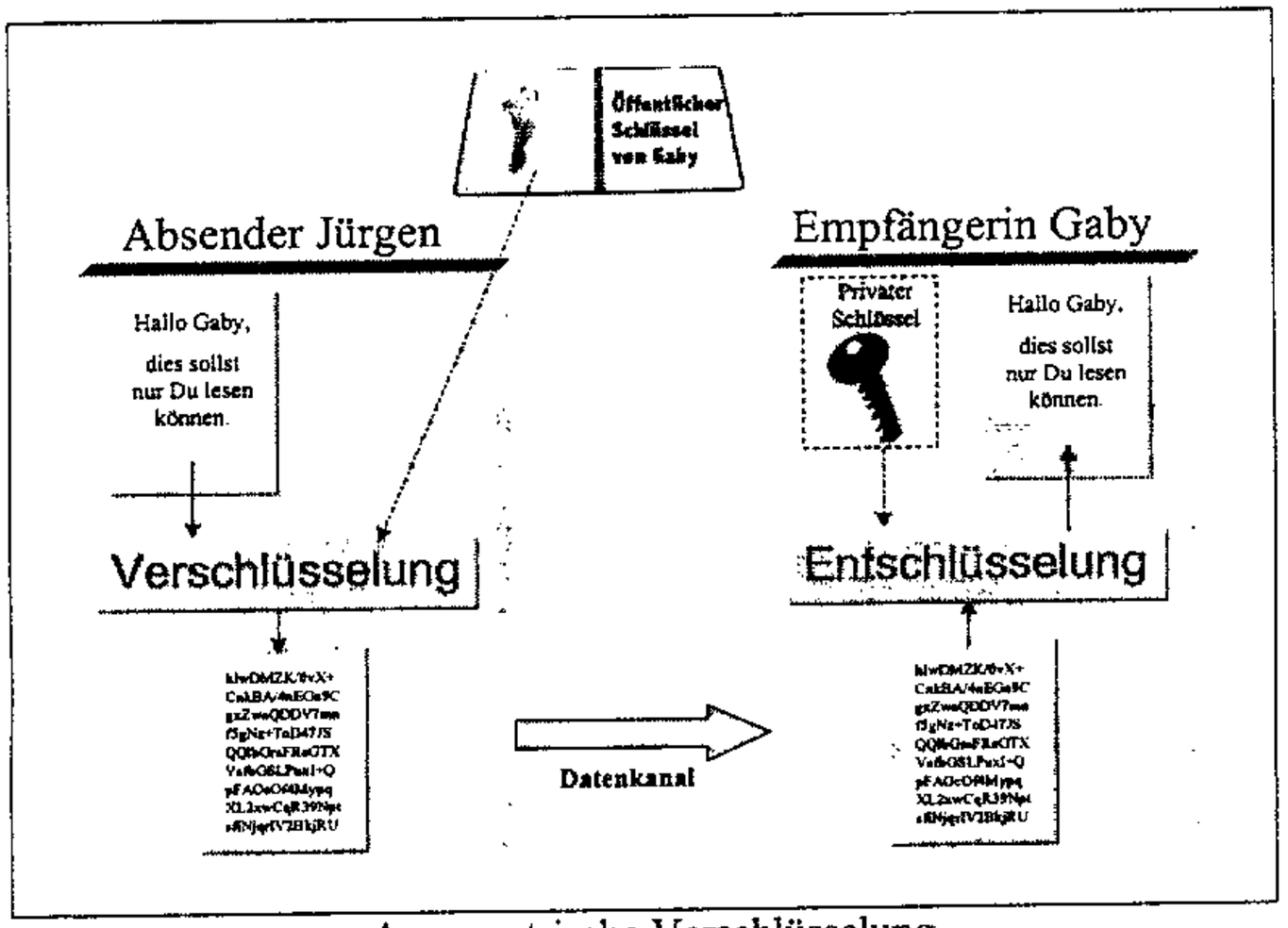
2.2.2.2 Asymmetrische Verschlüsselungsverfahren

Asymmetrische Verschlüsselungsverfahren zeichnen sich dadurch aus, daß alle potentiellen Kommunikationspartnerinnen und Kommunikationspartner im Besitz eines Schlüsselpaares sind, bestehend aus einem **öffentlichen** Schlüssel (Public Key) und einem **privaten** Schlüssel (Private Key). Der öffentliche Schlüssel dient der Verschlüsselung von Klartexten und kann allen über ein öffentliches **Verzeichnis** zugänglich gemacht werden - ähnlich einem elektronischen Telefonbuch. Nur mit dem von der Besitzerin oder vom Besitzer **geheimzuhaltenden** privaten Schlüssel können die mit dem

zugehörigen öffentlichen Schlüssel erzeugten Schlüsseltexte wieder entschlüsselt werden.

Beispiel: Zur Übermittlung einer verschlüsselten Nachricht an Gaby geht Jürgen bei einem asymmetrischen Verfahren folgendermaßen vor:

- Er entnimmt den öffentlichen Schlüssel von Gaby einem öffentlichen Schlüsselverzeichnis.
- Mit diesem Schlüssel verschlüsselt er die Nachricht und übermittelt sie an Gaby.
- Gaby kann nun mit ihrem privaten Schlüssel die Nachricht wieder entschlüsseln. Da der private Schlüssel außer Gaby niemandem bekannt ist, kann beim derzeitigen Stand der technischen Entwicklung Jürgen ziemlich sicher sein, daß die Nachricht auch nur von Gaby entschlüsselt werden kann, weil eine hinreichende Länge des Schlüssels gewählt wurde.



Asymmetrische Verschlüsselung

Der **Nachteil** asymmetrischer Verfahren besteht in ihrer **Ineffizienz**. Sie benötigen eine hohe Rechenleistung und sind daher zur Verschlüsselung lan-

ger Nachrichten schlecht geeignet. Sie haben aber den großen **Vorteil**, daß eine potentielle Kommunikationspartnerin oder ein potentieller Kommunikationspartner sich nur **einmal** einen öffentlichen und einen privaten Schlüssel besorgen muß. Von da an können mit allen anderen, die im Besitz eines Schlüsselpaares desselben asymmetrischen Verfahrens sind, verschlüsselte Nachrichten ausgetauscht werden. Damit wird eine spontane Kommunikation möglich und die Zahl der erforderlichen Schlüssel gegenüber symmetrischen Verfahren drastisch **reduziert.**

Die Erzeugung, Verteilung und Verwaltung der Schlüssel kann über sogenannte vertrauenswürdige **Dritte** (Trusted Third Party) erfolgen. Diese erzeugen die Schlüsselpaare, stellen jeweils den öffentlichen Schlüssel in ein öffentlich zugängliches Verzeichnis ein und übermitteln den privaten Schlüssel an die Besitzerin oder den Besitzer. Dabei ist zu gewährleisten, daß die oder der Dritte den privaten Schlüssel sicher zustellt, selbst von diesem Schlüssel keine Kenntnis erlangt und die Einträge im öffentlichen Verzeichnis korrekt vornimmt. Eine andere Möglichkeit besteht darin, daß die Kommunizierenden durch entsprechende technische Möglichkeiten in die Lage versetzt werden, ihre Schlüsselpaare **selbst zu erzeugen**. Damit befindet sich der private Schlüssel bereits von Beginn an bei der Person, die ihn berechtigterweise benutzt. Der zugehörige öffentliche Schlüssel ist dann noch an ein öffentliches Verzeichnis zu übermitteln und dort einzutragen.

2.2.2.3 Hybride Verschlüsselungsverfahren

In der Praxis kommen häufig Hybridverfahren zum Einsatz, die aus einer **Kombination** von symmetrischen und asymmetrischen Verfahren bestehen. Hierbei wird ein Klartext mittels eines symmetrischen Verfahrens verschlüsselt. Der dazu verwendete symmetrische Schlüssel wird ebenfalls verschlüsselt und zwar mit einem asymmetrischen Verfahren. An die empfangende Person werden der Schlüsseltext und der verschlüsselte symmetrische Schlüssel übertragen.

Beispiel: Jürgen übermittelt Gaby eine verschlüsselte Nachricht mittels eines Hybridverfahrens:

- Zuerst erzeugt er einen symmetrischen Schlüssel, den sogenannten Session Key, der nur für die aktuell zu übermittelnde Nachricht seine Gültigkeit hat.

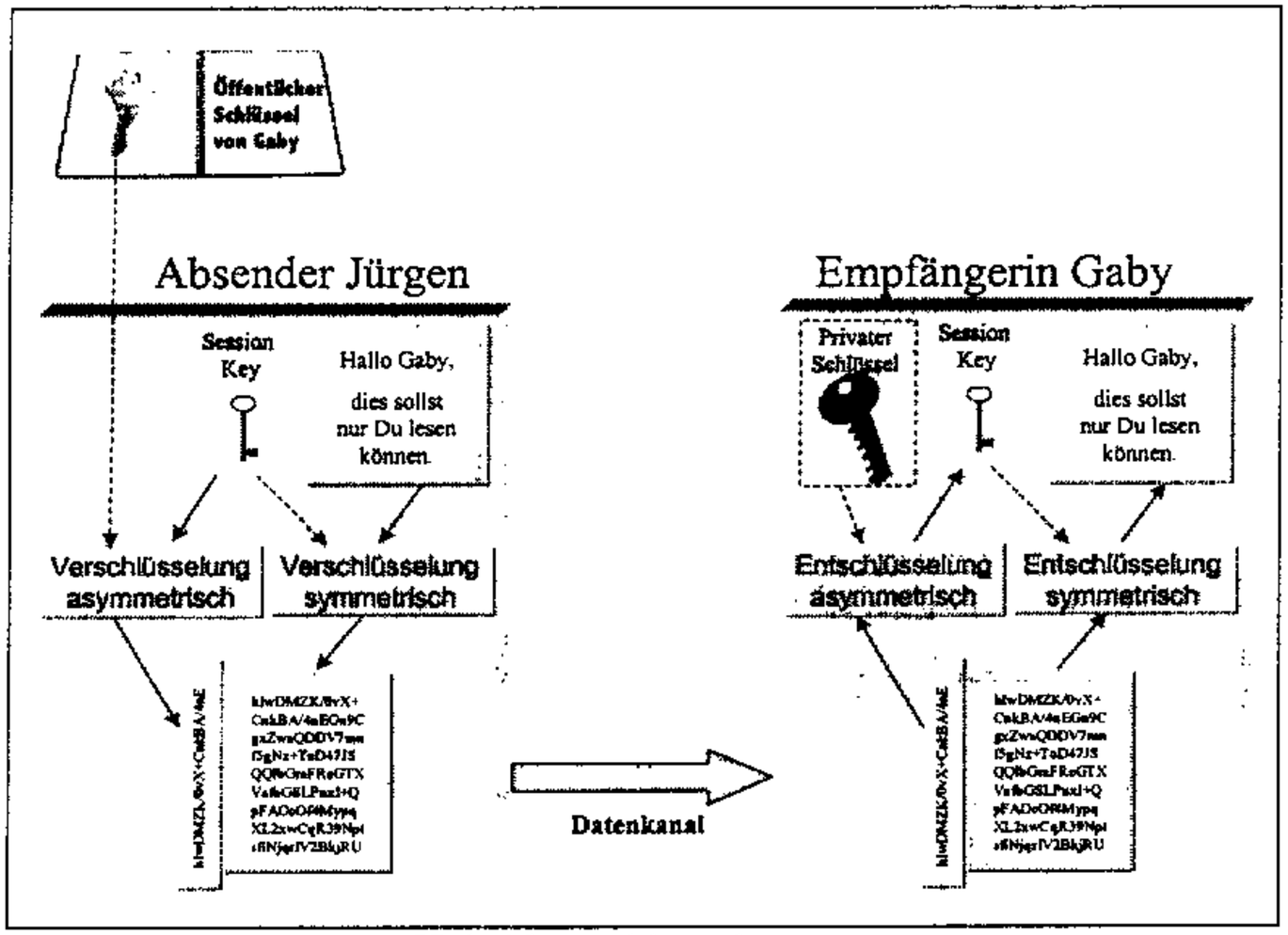
- Anschließend verschlüsselt er mit dem Session Key die Nachricht.

- Nun entnimmt er den öffentlichen asymmetrischen Schlüssel von Gaby dem öffentlichen Schlüsselverzeichnis und verschlüsselt mit diesem Schlüssel den von ihm erzeugten symmetrischen Session Key.

- Die verschlüsselte Nachricht übermittelt Jürgen zusammen mit dem verschlüsselten symmetrischen Session Key an Gaby. Da der symmetrische Session Key verschlüsselt übertragen wird, ist eine Schlüsselabsprache mit Gaby über einen getrennten "sicheren Kanal" nicht erforderlich.

- Empfängt Gaby die verschlüsselte Nachricht von Jürgen, entschlüsselt sie zunächst den mitgesandten verschlüsselten Session Key mit ihrem asymmetrischen privaten Schlüssel.

- Den entschlüsselten Session Key verwendet sie dann zur Entschlüsselung der eigentlichen Nachricht.



Hybridverschlüsselung

Hybridverfahren vereinigen die **Vorteile** von symmetrischen und asymmetrischen Verfahren unter **Kompensation ihrer Nachteile.** Diese Verfahren sind sehr **effizient**, da die Verschlüsselung der Nachricht mit einem symmetrischen Verfahren durchgeführt wird. Außerdem vermeiden sie das Erfordernis der Schlüsselabsprache und das problematische Schlüsselmana-

gement symmetrischer Verfahren, da der zur Nachrichtenverschlüsselung eingesetzte symmetrische Schlüssel mit einem asymmetrischen Verfahren selbst verschlüsselt wird und somit über den Datenkanal übertragen werden kann.

Verschlüsselungsverfahren sind nicht nur anwendbar für den Spezialfall der Ende-zu-Ende-Kommunikation (wie in den obigen Beispielen), sondern allgemein bei einer Client/Server-Kommunikation. Ebenso können gespeicherte Informationen verschlüsselt abgelegt werden und damit nur von Berechtigten wieder in eine lesbare Form überführt werden.

Eine verschlüsselte Information hat die Eigenschaft vertraulich zu sein. Nur Berechtigten - also der Inhaberin oder dem Inhaber des richtigen Schlüssels - offenbart sie ihren Inhalt. Vertraulichkeit muß damit **nicht auf der Ebene der DV-Systeme** und Kommunikationsmedien hergestellt werden, sondern ist davon unabhängig an das **zu schützende Objekt** Information selbst gebunden.

Starke Verschlüsselungsverfahren gewährleisten die Vertraulichkeit digitaler Informationen!

2.2.3 Digitale Signaturverfahren

Digitale Signaturverfahren **basieren** auf **kryptographischen Verfahren,** die auch bei der asymmetrischen Verschlüsselung Verwendung finden. Auch zur Bildung einer Signatur wird ein Schlüsselpaar benötigt. Der private Schlüssel dient dem Signieren und wird als privater Signaturschlüssel bezeichnet. Der öffentliche Schlüssel dient der Überprüfung einer Signatur und wird auch als öffentlicher Signaturschlüssel bezeichnet. Darüber hinaus verwenden digitale Signaturverfahren sogenannte kryptographische **Hash-Funktionen**. Hash-Funktionen transformieren nach mathematischen Methoden einen beliebigen Klartext in eine Zeichenkette fester Länge, das Hash-Komprimat. Eine für Signierverfahren verwendbare Hash-Funktion muß folgende Bedingungen erfüllen:

- Sie ist eine Einwegfunktion. Dies bedeutet, daß aus dem Hash-Komprimat der ursprüngliche Klartext nicht rekonstruierbar ist.

- Sie ist kollisionsfrei. Damit ist gemeint, daß es nicht möglich sein darf, zwei verschiedene Klartexte zu konstruieren, die das gleiche Hash-Komprimat haben.

Beispiel: Wie muß Jürgen nun vorgehen, wenn er Gaby eine von ihm digital signierte Nachricht übermitteln möchte?

- Zuerst erzeugt er mit der Hash-Funktion das Hash-Komprimat seiner Nachricht.

- In einem zweiten Schritt verschlüsselt er dieses Komprimat mit seinem privaten Signaturschlüssel, wobei dieser Prozeß hier der Erzeugung der digitalen Signatur dient und nicht - wie sonst - der Herstellung von Vertraulichkeit. Soll die Nachricht zusätzlich vertraulich übermittelt werden, muß sie mit einem der beschriebenen Verschlüsselungsverfahren verschlüsselt werden. Das Ergebnis dieses Prozesses ist die digitale Signatur der Nachricht.

- Nun sendet er die Nachricht zusammen mit der digitalen Signatur an Gaby.

- Hat Gaby die Nachricht erhalten, entnimmt sie den öffentlichen Signaturschlüssel von Jürgen aus einem öffentlichen Verzeichnis.

- Mit diesem Schlüssel entschlüsselt sie das zusammen mit der Nachricht übertragene verschlüsselte Hash-Komprimat, die digitale Signatur.

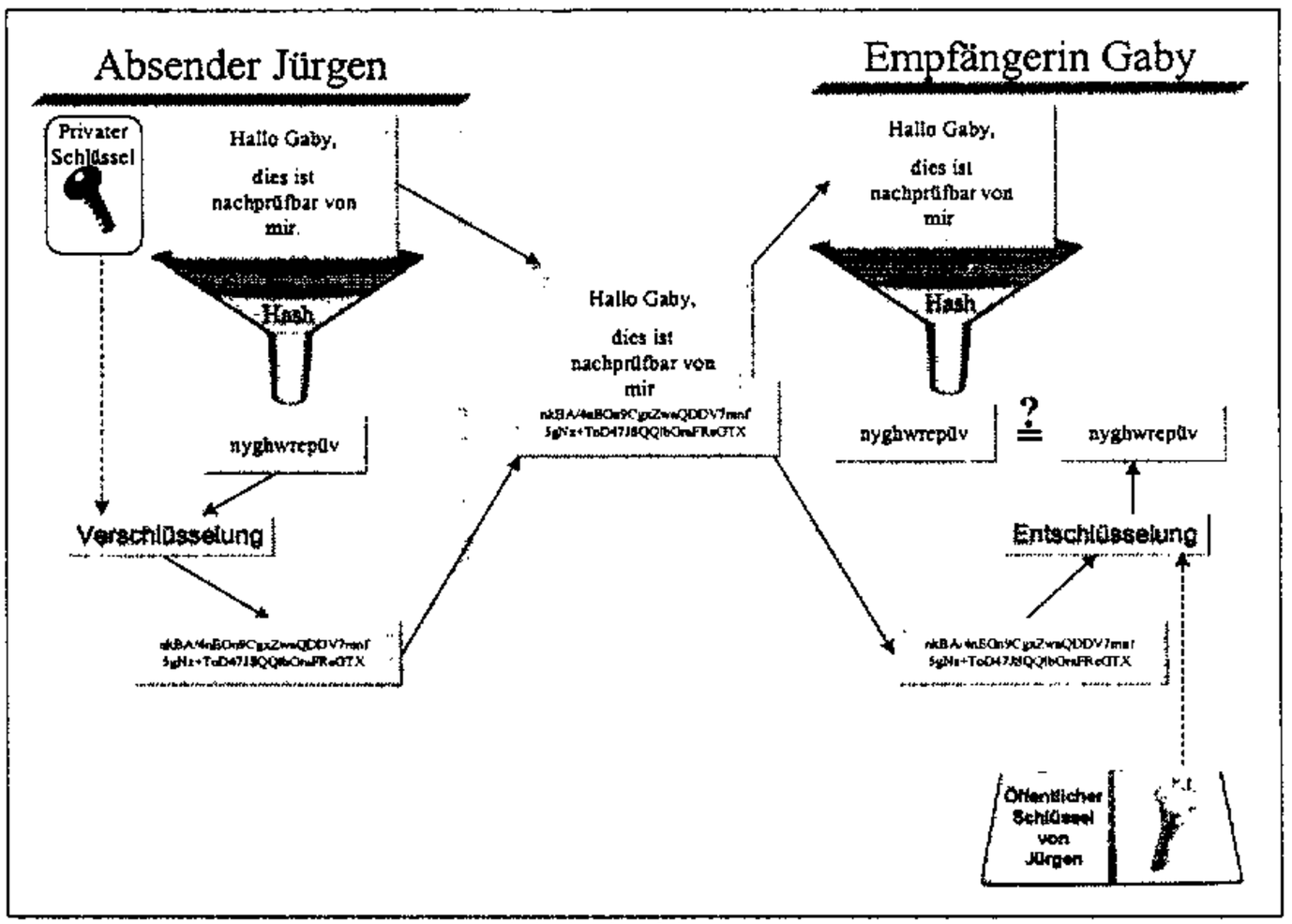
- Anschließend bildet sie selbst mit der Hash-Funktion das Hash-Komprimat der von Jürgen erhaltenen Nachricht.

- Nun überprüft Gaby, ob das von ihr selbst erzeugte Hash-Komprimat identisch mit der Zeichenkette ist, die sie durch die Entschlüsselung des von Jürgen verschlüsselten Hash-Komprimats erhalten hat.

Stellt Gaby die Identität der beiden Zeichenketten fest, kann sie nach dem heutigen Erkenntnisstand recht sicher sein, daß

1. die digitale Signatur von Jürgen und sonst niemandem erzeugt wurde, denn nur er kennt den privaten Signaturschlüssel, der dem von Gaby verwendeten öffentlichen Signaturschlüssel zugeordnet ist und

2. die digitale Signatur von Jürgen genau zu dieser Nachricht gehört, da nämlich das von Gaby selbst berechnete Hash-Komprimat mit dem ursprünglich von Jürgen berechneten Hash-Komprimat übereinstimmt, was gleichzeitig auch bedeutet, daß die Nachricht unverfälscht übermittelt wurde.



Digitale Signatur

Eine entscheidende Rolle spielen auch bei digitalen Signaturverfahren die vertrauenswürdigen **Dritten**. Nur durch die von ihnen mit Zertifikaten bestätigten Zuordnungen der öffentlichen Schlüssel zu bestimmten natürlichen Personen kann von einer digitalen Signatur auf ihre Erzeugerin oder ihren Erzeuger geschlossen werden. Die Erstellung von Signaturschlüssel-Zertifikaten ist eine Kernaufgabe der nach dem Gesetz zur digitalen Signatur (SigG) definierten Zertifizierungsstellen.

Dienstleistungen einer Zertifizierungsstelle für die Teilnehmenden an Verfahren für digitale Signaturen:

- **Identifizierung und Registrierung**: Die Teilnehmenden werden gegen Vorlage eines Ausweises identifiziert und registriert.

- **Schlüsselzertifizierung**: Für alle Teilnehmenden ist jeweils ein Zertifikat zu erzeugen, das unter anderem ein Identifizierungsmerkmal für die Teilnehmerin oder den Teilnehmer, ihren oder seinen öffentlichen Schlüssel und einen Gültigkeitszeitraum beinhaltet. Das Zertifikat wird mit der digitalen Signatur der Zertifizierungsstelle versehen.

- **Verzeichnisdienst**: Die Zertifikate der Teilnehmenden müssen in einem öffentlichen Verzeichnis abrufbar bereitgehalten werden, wenn die Teilnehmenden individuell einer solchen Veröffentlichung zustimmen.

- **Schlüsselgenerierung**: Verfügt eine teilnehmende Person nicht über ein selbst generiertes Schlüsselpaar, ist ein Schlüsselpaar für sie zu generieren.

- **Personalisierung**: Werden die Schlüssel einer teilnehmenden Person in der Zertifizierungsstelle generiert, muß der private Schlüssel auf einer geeigneten Signierkomponente gespeichert werden - beispielsweise einer Chipkarte.

- **Zeitstempeldienst**: In bestimmten Fällen kann es notwendig sein, digitale Daten authentisch mit einem bestimmten Zeitpunkt zu verknüpfen. Solche Daten werden mit einem Zeitstempel der Zertifizierungsstelle verknüpft und das Ergebnis anschließend digital signiert.

- **Sperrlistenmanagement**: Zertifikate, die vor Ablauf ihrer regulären Gültigkeit gesperrt werden, sind in entsprechenden Sperrlisten zu führen.

Da Zertifizierungsstellen selbst digitale Signaturen erzeugen, müssen auch für sie von einer Zertifizierungsstelle Zertifikate mit ihren öffentlichen Signaturschlüsseln erstellt werden. Theoretisch könnten beliebige Hierarchien von Zertifizierungsstellen entstehen. Das Signaturgesetz sieht allerdings nur eine zweistufige Zertifizierungshierarchie vor. Dabei werden alle Zertifizierungsstellen unmittelbar von der Wurzelinstanz zertifiziert, die bei der Regulierungsbehörde angesiedelt ist.

Die bei digitalen Signaturverfahren zur Anwendung kommenden Mechanismen gewährleisten nicht nur die **Authentizität** und **Integrität** von übermittelten Nachrichten, sondern sind ebenso geeignet zur **Sicherung** von Authentizität und Integrität gespeicherter Informationen und auch der Programme, die auf dem jeweiligen Computersystem zur Ausführung gebracht werden. Die mit einer Information verbundene digitale Signatur verleiht ihr die Eigenschaften, über ihren Zustand und ihre Urheberin oder ihren Urheber Auskunft zu geben. Die Merkmale der **Unversehrtheit** und der **Zurechenbarkeit** sind an die Information selbst geknüpft und müssen nicht durch technische Mechanismen der informationsverarbeitenden Systeme sichergestellt werden.

Digitale Signaturen gewährleisten die Authentizität und Integrität digitaler Informationen.

2.2.4 Fazit

Verfahren zur Verschlüsselung und zur digitalen Signatur gewährleisten die Vertraulichkeit, Authentizität und Integrität digitaler Informationen.

Darüber hinaus sind die Methoden der Kryptographie geeignet

- zur - gegenseitigen - Authentifizierung der an einer informationstechnischen Kommunikation Beteiligten, wie der Authentifizierung einer Benutzerin oder eines Benutzers gegenüber einem DV-System, der Authentifizierung der Prozesse bei einer Prozeß-Prozeß-Kommunikation innerhalb eines DV-Systems oder über DV-Systemgrenzen hinweg und der Authentifizierung der Personen einer Ende-zu-Ende-Kommunikation,

- zur Gewährleistung der Nicht-Abstreitbarkeit von Kommunikationsbeziehungen und

- zur Pseudonymisierung und (faktischen) Anonymisierung personenbezogener Daten.

Die Kryptographie ist die Schlüsseltechnologie zur Gewährleistung von Informationssicherheit und vertrauenswürdiger Kommunikation.

2.3 Internetnutzung in der Verwaltung

Sollen Internetdienste aus internen Verwaltungsnetzen heraus genutzt werden, entstehen erhebliche Gefährdungen der Datensicherheit der für die Verarbeitung personenbezogener Daten genutzten DV-Systeme und -Netze durch Ausspähung, Manipulation oder gar Zerstörung. Aus der Sicht des Datenschutzes ist ein unmittelbarer Anschluß an das Internet deshalb nur dann vertretbar, wenn er zur Erledigung der Aufgaben zwingend erforderlich ist und die Risiken durch technische und organisatorische Maßnahmen wirksam beherrscht werden. Aber auch beim Direktanschluß über separate Geräte sind einige Grundregeln zu beachten.

Internettechnik und -nutzung lassen sich aus der heutigen IT-Strategie öffentlicher Stellen nicht mehr wegdenken. Informationsangebote und -verfahren sowie Benutzeroberflächen orientieren sich an diesen Standards,

um einerseits intern Produktivitätsvorteile zu erzielen und andererseits für die Informationsgewinnung und -bereitstellung auf die Möglichkeiten des weltweiten Netzangebotes zurückgreifen zu können. Dabei ist der Anschluß an das Internet mit erheblichen **Gefährdungen des Datenschutzes** und der **Datensicherheit** verbunden. Die Rechner und Übertragungswege dieses weltweiten Computernetzes sind nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht transparent. Das Internet wurde ursprünglich nur unter Verfügbarkeitsaspekten entwickelt - auch wenn neuere Entwicklungen versuchen, weiteren Sicherheitsbedürfnissen Rechnung zu tragen. Deshalb wird den Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit vielfach nicht in der gebotenen Weise begegnet.

2.3.1 Kopplung interner Netze über Firewallsysteme

Als Regelanschluß wird zukünftig sicherlich die Ankoppelung über Firewallsysteme vorherrschen. Viele öffentliche Stellen planen derzeit ihre internen Netze über Firewallsysteme an das Internet zu koppeln, um damit die Risiken für die "internen Netze" zu begrenzen. Dabei hängt deren Stärke wesentlich von der **eingesetzten Technik** und ihrer **Administration** ab. Voraussetzung ist deshalb geeignetes Fachpersonal zur fortlaufenden Administration, zur Reaktion auf Angriffe und zur Umsetzung der notwendigen Anpassungen.

Eine Firewall kann lediglich symbolisch als Brandschutzmauer betrachtet werden. Es ist nicht so, daß sie einmal aufzubauen ist und dann wartungsfrei jahrelangen Schutz gewährleistet. Vielmehr gilt, daß der Einsatz spezieller Technik - siehe Darstellung "Screened Gateway" Seite 25 - notwendig ist, die **fortlaufend** dem aktuellem Sicherheitsstandard und den Nutzungsanforderungen **angepaßt** werden muß. Eine Firewall ist ein reaktives System, das den ständig sich ändernden Bedrohungen jeweils unmittelbar folgen muß. Eine **hundertprozentige Sicherheit** ist mit dieser Technik **nicht zu erreichen**. Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat seine **"Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet"** überarbeitet und neu veröffentlicht. Sie ist als download unter unseren Adressen **"www.lfd.nrw.de"** oder **"www.nordrhein-westfalen.datenschutz.de"** erhältlich und soll den für den Betrieb von Verwaltungssystemen und -netzen Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der internen Systeme beim Anschluß an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können.

Bei einer systematischen Planung einer Internetanbindung ist zunächst eine **Risikoanalyse** und darauf aufbauend ein **Sicherheitskonzept** zu erarbeiten, in dem schlüssig dargelegt wird, unter welchen Rahmenbedingungen ein Internetzugang auszuwählen und zu betreiben ist sowie die Sicherheitsmaßnahmen fortzuentwickeln sind. Im Sicherheitskonzept sind alle technischen und organisatorischen Maßnahmen festzulegen, die zu treffen sind, um die mit der Internetnutzung verbundenen Risiken zu minimieren und die internen Systeme und Netze sicher betreiben zu können. Dieses Regelwerk (Security Policy) sollte folgende Festlegungen enthalten (vgl. BSI - Sicherheit im Internet):

- Was soll geschützt werden?
- Welche Dienste sind erforderlich?
- Welche Benutzerinnen und Benutzer werden zugelassen?
- Welche Ereignisse werden protokolliert und wer wertet diese Daten aus?
- Welcher Datendurchsatz ist zu erwarten?

Aufgrund von **Kontrollbesuchen** ist festzustellen, daß diese dargestellten Schritte im allgemeinen nicht durchgeführt wurden. Das Vorgehen wird zwar generell als notwendig anerkannt, in der Praxis jedoch **nicht umgesetzt**. Hier besteht Nachbesserungsbedarf. Unter Datenschutzaspekten hat die öffentliche Stelle für die Internetnutzung eine allgemein transparente Vorgehensweise festzulegen, aus der ihre Vorgaben zum Rahmen der erlaubten Internetnutzung verbindlich hervorgehen. Diese ist so zu dokumentieren, daß sie nachvollziehbar ist.

Diensteauswahl

Bei den kontrollierten Stellen wurden Internetdienste ausschließlich von innen - also aus dem Verwaltungsnetz heraus - nach außen genutzt. Freigegeben waren die Dienste HTTP, HTTPS, FTP, E-Mail. Zur Kontrolle der Zulässigkeit von HTTP waren in der Firewall Gruppenprofile (Name, TCP/IP - Adresse und DNS) eingerichtet und in der Folge als Verbindungspartner lediglich Proxy-Server erlaubt. Verbindungen zu Endanwenderinnen und Endanwendern waren nicht vorgesehen. Der Dienst FTP wurde im allgemeinen restriktiver gehandhabt. Teilweise waren nur ausgewählte Nutzerinnen und Nutzer zugelassen; in jedem Fall war eine personenbezogene Ver-

waltung realisiert. Der Dienst E-Mail wurde unterschiedlich behandelt. Teilweise erfolgte eine Kontrolle aller Eingänge und deren Anlagen mit einer automatischen Prüfung auf Virenbefall, teilweise lediglich eine ungeprüfte Durchschaltung.

Zum Verfahren der Dienstenutzung ist festzustellen, daß in Bezug auf die kritischeren Dienste wie etwa telnet oder eine Nutzung von außen nach innen noch keine Freischaltung erfolgt ist. Hier wird empfohlen, nur dann einer Freischaltung zuzustimmen, wenn das zwingende **Erfordernis in jedem Einzelfall** vorliegt. Voraussetzung ist in jedem Fall, daß **funktionsfähige Proxys** für die Firewall vorliegen und auch ausgetestet sind. Weiter sollte bei allen Diensten das Prinzip der **Gruppenfreischaltungen** für ganze Bereiche **aufgegeben werden**. Vielmehr muß klar sein, daß jedes zusätzliche zur Internetnutzung freigegebene Endgerät ein neues **Sicherheitsrisiko** beinhaltet und das Erfordernis in jedem Einzelfall geprüft wird. In diesem Sinne wären bestimmte Bereiche (z.B. die Verarbeitung von Sozial- oder Personaldaten) möglichst ganz vom Internet zu trennen. Insgesamt sollte das Verfahren der Dienstefreischaltung **verbindlich festgelegt** sein.

Firewalltechnik

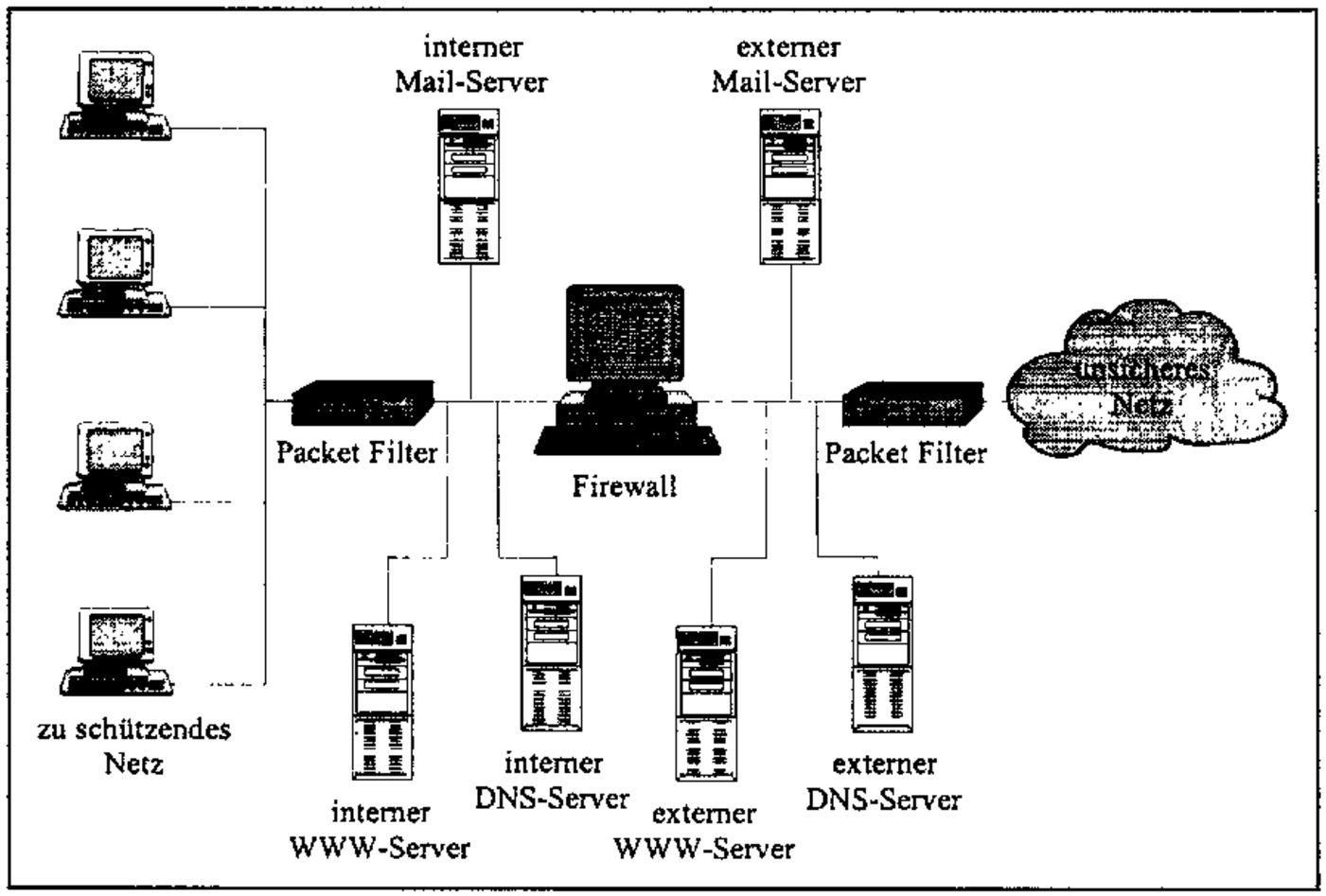
Firewall-Systeme müssen so aufgebaut sein, daß sie **so schlank wie möglich** konfiguriert sind und nur Anwendungen und Systemprogramme beinhalten, die für den Betrieb erforderlich sind. Hardwaretechnisch sollten sie aus den in der nachfolgenden Darstellung ersichtlichen Einzelkomponenten bestehen. Bedienung und Konfiguration der Firewall müssen **benutzungsfreundlich** sein, um unbeabsichtigte Fehleinstellungen zu vermeiden. Vertrauenswürdige Systeme müssen ihre Funktionsweise offenlegen, um Fachleuten Einblick in die Sicherheitsarchitektur zu geben. **Sicherheitszertifikate** für Firewalls können dazu beitragen, daß sich der Grad des Schutzes, den das jeweilige Produkt bietet, leichter einschätzen läßt und Vergleiche zwischen verschiedenen Produkten möglich werden.

Grundlage jeder Konfiguration sollte die Regel sein:

"Alles, was nicht ausdrücklich erlaubt ist, ist verboten."

Diese Regel bedeutet, daß jede Funktion ausdrücklich freigeschaltet und nicht erst im Nachhinein ausgeschaltet werden muß. Sie verhindert, daß **Sicherheitslücken** bei der Konfiguration übersehen werden und unbemerkt bestehen bleiben. Bei den besuchten Stellen waren jeweils Firewallsysteme eingesetzt oder in Planung, die diesen Grundprinzipien entsprachen. Als ge-

nereller Mangel war allerdings festzustellen, daß qualifizierte Informationen zusammengefaßt zu der jeweiligen Firewall, die mehr aussagen als eine Hochglanzbroschüre, nicht existierten.



"Screened Gateway" ist eine Kombination von Packet Filter und Application Level Firewall. Ein **Packet Filter** ist ein Netzwerkrouter, der erlaubte IP-Pakete passieren läßt und unerlaubte abweist. Ein **Application Level Firewall** ist ein speziell konfigurierbarer Rechner, der die gesamte Kommunikation zwischen dem zu schützenden und dem unsicheren Netz auf Anwendungsebene steuert. Für jeden Dienst (Telnet, FTP usw.) werden Security Proxys eingeführt, die den direkten Zugriff auf den Dienst verhindern.

Administration

Die Organisation der Administration ist bei allen öffentlichen Stellen bereits durch die personellen Möglichkeiten und erst in zweiter Linie durch die eingesetzte Technik vorgegeben. **Teilungen der Administration** des gesamten Internetgateways - etwa in die Bereiche Server-, Netz- oder Firewalladministration - sind wegen der besseren Kontrollmöglichkeit zwar wünschenswert, aber im allgemeinen bereits aufgrund der personellen Gegebenheiten nicht machbar. Ein besonderes Augenmerk sollte in jedem Fall darauf gelegt werden, eine **Kontrolle** der Administrationstätigkeiten zu ermöglichen. Die Wahrnehmung der Administrationsrechte sollte idealerweise über eine separate Konsole erfolgen. Ist der Anschluß zusätzlich über eine Verschlüsselung abgesichert, so ist ein Mißbrauch praktisch weitgehend ausgeschlossen.

Bei den überprüften Firewalls hatten die für die Administration Verantwortlichen keinen Zugriff auf die Systemebene. Zertifizierte Firewallsysteme lassen dieses bereits deshalb nicht zu, damit keine Änderungen am System vorgenommen werden. Verbleiben die Rechte über den Systemzugriff bei der **Herstellerfirma**, so stellt sich das Problem für die öffentliche Stelle, wie nach Eingriffen der Firma **geprüft** werden kann, daß das System funktional seinen Ausgangszustand nicht verändert hat oder die Veränderung nur nach den Wünschen der öffentlichen Stelle erfolgt ist. Hier müßten geeignete **Revisionstools** eingesetzt werden, mit denen dies festgestellt werden könnte. Unabhängig hiervon sind in bestimmten Abständen Integritätstests, Überprüfungen der Security-Policy, allgemeine Kontrollen und bei Änderungen sofortige Überprüfung der Funktionen auch in **eigener Verantwortung** durchzuführen. Dies beinhaltet auch das Erstellen und das Überwachen von Filterregeln und die Überprüfung nach Systemabstürzen oder schweren Angriffen. Die Sicherungskonzepte müssen so gestaltet sein, daß eine **Rekonstruktion** der Ausgangssituation möglich ist. Bei den Kontrollen wurde festgestellt, daß Regelungen in diesem Bereich eher **lückenhaft** waren. Auch Handbücher für den Bereich Firewall-Administration waren nicht vorhanden, so daß hier erheblicher **Nachbesserungsbedarf** besteht.

Protokollierung

Bei den kontrollierten Stellen wurden im allgemeinen alle über die Firewall laufenden **Verbindungsdaten mitgelesen und gesichert.** Hierdurch sollen die Erstellung von (nicht personenbezogenen) Statistiken, Kontrollen und auch Abrechnungen ermöglicht werden sowie das Störungsverhalten bei der Datenvermittlung nachvollziehbar bleiben. Zwar waren aus den Protokolldaten **Personenbezüge** häufig nicht unmittelbar erkennbar; sie waren allerdings **wiederherstellbar**. Einstellmöglichkeiten der Firewall, die erlauben, nur Daten zu protokollieren, die für die Verfolgung von Angriffen und Fehleranalysen erforderlich sind oder sich auf ausgewählte Ereignisse beziehen, wurden meist nicht genutzt. Dies ist jedoch **zu empfehlen**. Solange dies nicht geschieht, ist folgendes zu beachten: Da es sich bei den Protokolldateien im wesentlichen um die Aufzeichnung von Nutzungsprofilen der Beschäftigten handelt, sind **strenge Maßstäbe** an den Umfang, den Archivierungszeitraum und die Weiterverarbeitung zu legen. Es bestehen gegen die Protokollierung dann keine datenschutzrechtlichen Bedenken, wenn der Grundsatz der Erforderlichkeit zu Abrechnungszwecken oder zu festgelegten Sicherungs- und Nachweiszwecken beachtet wird. Der unmittelbare Personenbezug ist jedoch sobald als möglich zu entfernen und eine **frühzeitige Löschung** der Protokolldateien anzustreben. Weiter sollte der Umgang mit

den Protokollen und deren Auswertung ausschließlich für zuvor **festgelegte Zwecke** erfolgen dürfen. Insofern ist eine schriftliche Verfügung zwingend notwendig.

Kontrolle
Interne Kontrollen der IT-Umgebung sind ein wesentliches Merkmal der nach den Datenschutzgesetzen zu treffenden Maßnahmen zur IT-Sicherheit. Bei den Überprüfungen wurde - wie bei anderen Prüfungen in der Vergangenheit auch - festgestellt, daß keine Kontrollmechanismen entwickelt wurden. Hier besteht noch **Nachholbedarf**. Um zukünftig zu gewährleisten, daß angeordnete Maßnahmen auch korrekt umgesetzt werden, sollte das Instrument der **internen Kontrolle** so festgelegt sein, daß Art und Umfang der Maßnahmen sowie das Berichtswesen verbindlich vorgegeben sind.

2.3.2 Direktanschluß über separate Geräte

Im Rahmen der Kontroll- und Beratungstätigkeit war festzustellen, daß bei den öffentlichen Stellen zur Zeit noch überwiegend Direktanschlüsse für die Internetnutzung eingesetzt sind. Hierbei sind zwei Anschlußvarianten zu unterscheiden:

- Direktanschluß über separate, ausschließlich für diesen Zweck genutzte Geräte.

- Direktanschluß von alternativ im Verwaltungsnetz und im Internet genutzten Rechnern.

Zwar ist die erste Anschlußart aus der Sicht des Datenschutzes die unproblematischste, da eine direkte Kopplung mit dem Verwaltungsnetz und damit zu personenbezogenen Daten in der Regel nicht gegeben ist. Dies rechtfertigt jedoch nicht den im allgemeinen vorgefundenen Zustand, daß keine Regelungen über zu treffenden Maßnahmen zum Betrieb und zur Sicherung der Systeme existierten. Zu einem **ordnungsgemäßen Betrieb** gehören generelle **Vorgaben** über vorzunehmende Grundeinstellungen in den Rechnern und Programmen. Durch Aktivierung von Schutz- und Informationsmöglichkeiten der Browser und Anwendungsprogramme ist eine **Reduzierung** der Gefahren aus dem Internet mit einfachen Mitteln **möglich**. Zur Verhinderung der Erstellung von Nutzungsprofilen sollte eine Reduzierung temporärer Speicherungen und Historieneinträge vorgegeben sein oder ganz auf sie verzichtet werden. Für den Datenimport in die internen Systeme sind das Verfahren und selbstverständlich die **Virenscannung** festzulegen. Weiter sollten die Nutzerinnen und Nutzer dieser Geräte über Abläufe und Ge-

fahren im Zusammenhang mit der Internetnutzung informiert sein. Auch eine Verlagerung der Verantwortung auf die Ämter - wie häufig angetroffen - kann nur dann akzeptiert werden, wenn sichergestellt ist, daß von diesen die Risiken eingeschätzt und geeignete Maßnahmen ergriffen werden können.

Grundsätzlich **inakzeptabel** ist die zweite, ebenfalls häufig vorzufindende Anschlußart mit der **Doppelnutzung** von Geräten sowohl im Internet als auch im Verwaltungsnetz. Technisch werden hierbei PCs mit wahlweise unterschiedlicher "Boot-Einstellung" betrieben. Verständlich ist zwar der Wunsch, durch die Doppelnutzung von Geräten Kosten zu sparen. Aufgrund der vielfältigen **Gefährdungen**, die hierbei insbesondere für die System- und Datenintegrität der Verwaltungsverfahren und der in ihnen verarbeiteten personenbezogenen Daten entstehen, ist von der parallelen Nutzung von Geräten mit Direktanschluß zum Internet und zu internen Netzen generell abzuraten. Es wird empfohlen, diese Einsatzart insbesondere dann nicht zu gestatten, wenn auf den Geräten auch personenbezogene Daten verarbeitet werden.

2.4 Konventionelle und unkonventionelle rechtliche Regelungen für die Medien

2.4.1 Grundlinien

Die im 13. Datenschutzbericht (Seite 46 f.) dargestellte Entwicklung der Medienwelt ist weiter fortgeschritten. Die dort genannten Vorgaben für einen wirkungsvollen Datenschutz haben nach wie vor Gültigkeit: Datenvermeidung, Anonymität, Zweckbindung und Transparenz der Datenverarbeitung. Die auf der Grundlage der ersten Medienversuchsverordnung (siehe 13. Datenschutzbericht, Seite 52 f.) gestarteten **Modellversuche** sind noch nicht abgeschlossen. Im Rahmen der **Begleitforschung** zum Projekt "Info-City NRW" hat die Landesanstalt für Rundfunk Nordrhein-Westfalen 1998 eine von ihr beim Hans-Bredow-Institut in Auftrag gegebene und von Wolfgang Schulz erstellte Untersuchung der Rechtsfragen des Datenschutzes bei Online-Kommunikation publiziert. Die **Expertise** kommt zu den Ergebnissen, daß die hergebrachten Maßnahmen für den Datenschutz unzureichend seien und die **informationelle** Selbstbestimmung der Nutzerinnen und Nutzer auf eine **neue Weise gesichert** werden müßte. In den Bereichen, die wie die Online-Kommunikation für Nutzerinnen und Nutzer schwer durchschaubar seien, erhalte der Grundsatz der Datenvermeidung besondere Bedeutung. Es seien Systeme zu fördern und zu fordern, die eine anonyme oder pseudonyme Nutzung von Online-Diensten ermöglichten. Trotz mancher Differenzen im Detail können die Ergebnisse der Studie insgesamt die Her-

zen von Datenschützerinnen und Datenschützern nur höherschlagen lassen, erweisen sich unsere schon seit längerer Zeit erhobenen Forderungen nun auch aus wissenschaftlicher Perspektive als zutreffend.

Das - noch - zögerliche Zusammenwachsen der Medien für die Individual- und die Massenkommunikation wird begleitet von der Änderung und Neuschaffung der für sie geltenden rechtlichen Bestimmungen, die die **datenschutzrechtlichen Grundsätze weitgehend übereinstimmend regeln.** Der Mediendienstestaatsvertrag, das Teledienstedatenschutzgesetz, das Rundfunkgesetz für das Land Nordrhein-Westfalen, das Gesetz über den "Westdeutschen Rundfunk Köln" und der Diskussionsentwurf zum Vierten Rundfunkänderungsstaatsvertrag enthalten den Grundsatz der **Datenvermeidung** bei der Gestaltung und Auswahl **technischer Einrichtungen,** die - unter dem Vorbehalt der technischen Möglichkeit und Zumutbarkeit - stehende Pflicht zur Gewährung **anonymer** oder **pseudonymer Nutzung** der jeweiligen Medien oder Dienste, **Zweckbindungsregelungen** beim Umgang mit personenbezogenen Daten sowie umfassende **Informations- und Auskunftsrechte** der Nutzerinnen und Nutzer. Dies ist erfreulich. Wie sich die Normen in der Praxis bewähren, zeigt sich in ersten Erfahrungen, die beispielhaft im Abschnitt über die Medien- und Teledienste dargestellt werden. Zunächst jedoch zur "Medienbasis" - der Telekommunikation, die eben nicht mehr allein auf die Sprachtelefonie beschränkt ist.

2.4.2 Telekommunikation

2.4.2.1 Europäische Richtlinie zum Telekommunikationsdatenschutz

Das Europäische Parlament und der Rat haben 1997 als erste bereichsspezifische europäische Datenschutzregelung die europäische Telekommunikationsdatenschutzrichtlinie verabschiedet - Richtlinie 97/66 vom 15.12.1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (ABl. EG Nr. L 24/1). Die Richtlinie hätte bis zum 24.10.1998 in nationales Recht umgesetzt werden müssen. Der Grundsatz der **Vertraulichkeit** der Kommunikation ist in Artikel 5 Abs. 2 der Richtlinie leider **nur unzureichend verankert** worden. Denn die Richtlinie sieht das Aufzeichnen von Kommunikation im Rahmen einer rechtmäßigen Geschäftspraxis zum Nachweis kommerzieller Transaktionen oder einer sonstigen geschäftlichen Kommunikation als rechtlich zulässige Ausnahme davon an. Dies steht im Gegensatz zum deutschen Recht, wonach das Mitschneiden von Gesprächen - etwa im Rahmen des Telefonbanking - der ausdrücklichen Einwilligung aller Beteiligten bedarf.

Im Dezember 1997 legte die Kommission außerdem ein Grünbuch vor zur **Konvergenz** der Branchen Telekommunikation, Medien und Informationstechnologie und ihren ordnungspolitischen Auswirkungen - ein Schritt in die Richtung der Informationsgesellschaft (KOM (97) 623 end.; Ratsdok. 13289/97; BR-Drs. 1064/97). Die Initiative der Kommission zielt darauf, einen **europaweiten Diskussionsprozeß** zu einem künftigen Regelungsrahmen für das Zusammenwachsen der Telekommunikation, der Medien und des Rundfunks zu eröffnen. Mit dem Grünbuch beabsichtigt die Kommission, die derzeitigen Regelungen im Medien- und Telekommunikationsbereich einer kritischen Betrachtung zu unterziehen, um etwaige Wachstums- und Entwicklungshemmnisse zu beseitigen und - so deutet es sich an - ein neues integriertes Regelungsmodell zu entwerfen.

2.4.2.2 Verstärkte Überwachungstendenzen auf Kosten des Datenschutzes

Seit dem 01.01.1998 gehört das Monopol der Deutschen Telekom AG für den Sprachtelefondienst der Vergangenheit an. Praktisch können die Kundinnen und Kunden jetzt zwischen verschiedenen technischen Verfahren sowie verschiedenen Anbieterinnen und Anbietern wählen. Diese haben sich alle an das **Fernmeldegeheimnis** zu halten, das den Inhalt und die näheren Umstände der Telekommunikation schützt - einschließlich der Beteiligung an einem Telekommunikationsvorgang und erfolgloser Verbindungsversuche. Wer wann mit wem wie lange telefoniert hat, unterfällt dem Fernmeldegeheimnis ebenso wie Telefaxverkehr und E-Mail.

Zur Wahrung des Fernmeldegeheimnisses ist nach § 85 Abs. 2 Telekommunikationsgesetz (TKG) verpflichtet, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. Über die Legaldefinition des "geschäftsmäßigen Erbringens von Telekommunikationsdiensten", die unabhängig von einer Gewinnerzielungsabsicht das nachhaltige Anbieten von Telekommunikation erfaßt, unterliegen dem Fernmeldegeheimnis auch private **Netze** in Firmen (Corporate Networks) sowie **Nebenstellenanlagen** beispielsweise in Krankenhäusern und Hotels. Dies gilt im übrigen auch für Privatgespräche von Beschäftigten.

Jedoch ist nicht nur die Wahrung des Fernmeldegeheimnisses, sondern es sind auch die Eingriffsbefugnisse der Sicherheits- und Strafverfolgungsbehörden, mit denen das Fernmeldegeheimnis gerade eingeschränkt wird, daran geknüpft, daß Telekommunikationsdienste geschäftsmäßig erbracht werden. Die **weite Begriffsdefinition** ist damit **janusköpfig**. Sie schützt die Kommunizierenden um den Preis einer umfassenden Durchbrechungsmög-

lichkeit ihres Fernmeldegeheimnisses. Gerichte, Staatsanwaltschaften, Polizeien, Nachrichtendienste und andere Stellen dürfen nämlich - wenn auch unter unterschiedlichen Voraussetzungen - die Inhalte der Kommunikation überwachen, Verbindungs- und Bestandsdaten erfragen und den Zugriff auf Verzeichnisse von Kundinnen und Kunden realisieren. Gesteigert hat sich damit die schon im 13. Datenschutzbericht angesprochene Tendenz (Seiten 9 und 48), daß das Telekommunikationsnetz in der Gefahr steht, verstärkt als **Fahndungsnetz** eingesetzt zu werden.

So wird beispielsweise die im 13. Datenschutzbericht (Seite 9) erwähnte Pflicht, aktuelle Kundendateien für den unbemerkten Abruf durch die Regulierungsbehörde vorzuhalten, von einigen Telekommunikationsunternehmen so verstanden, daß sie sich durch § 90 TKG daran gehindert sehen, **anonyme Nutzungsmöglichkeiten** anzubieten. Diese Interpretation ist jedoch zu extensiv. Der Gesetzgeber hat mit der Verpflichtung, ein Verzeichnis der vorhandenen Kundendateien zu führen, gerade **nicht** ausdrücklich auch bestimmt, daß die entsprechenden **Daten zusätzlich zu erheben wären**, wenn sie von dem Unternehmen selbst gar nicht benötigt werden. Gerade die Entstehungsgeschichte des TKG sowie der systematische Gesamtzusammenhang der Bestimmungen seines 11. Teils legen es nahe, § 90 TKG lediglich die Verpflichtung für die Abrufmöglichkeit von **ohnehin** im eigenen Unternehmensinteresse **geführten Kundendateien** zu entnehmen.

Anläßlich der Anfrage aus einem **Krankenhaus** war zu klären, ob auch für die dortige **Nebenstellenanlage** die Pflicht zur Führung eines solchen "Kundenverzeichnisses" anzunehmen sei. Eine derartige Verpflichtung besteht jedoch nicht. Dies ergibt sich schon aus einer präzisen Bestimmung des Begriffs "Kundendatei" und wird durch die gesetzgeberische Intention gestützt. **Kundinnen und Kunden** im Sinne des Telekommunikationsgesetzes sind nämlich nur diejenigen, die **aufgrund eigener Vertragsbeziehungen** selbst die jeweilige Rufnummer zur eigenen Teilnahme am Telekommunikationsverkehr zugewiesen bekommen haben. Patientinnen und Patienten nutzen lediglich Nebenstellenanlagen in Krankenhäusern und sind damit gerade keine "Kundinnen und Kunden" in diesem Sinne. Bestätigt wird dieses Ergebnis auch durch die erklärte gesetzgeberische Zielsetzung, die mit der Vorschrift verfolgt wird. Solange die staatliche Deutsche Bundespost das Telefonmonopol besaß, konnten sich die Sicherheits- und Strafverfolgungsbehörden die von ihnen gewünschten Auskünfte vielfach im Wege der Amtshilfe einholen. Mit der **Privatisierung** und der **Marktöffnung** für weitere Unternehmen ist eine solche Praxis ausgeschlossen, wenn sie nicht mit spezifischen Rechtsgrundlagen ausdrücklich eröffnet wird. Die Vorschrift sollte **keinem weiteren Zweck** dienen als der Sicherstellung der **bis-**

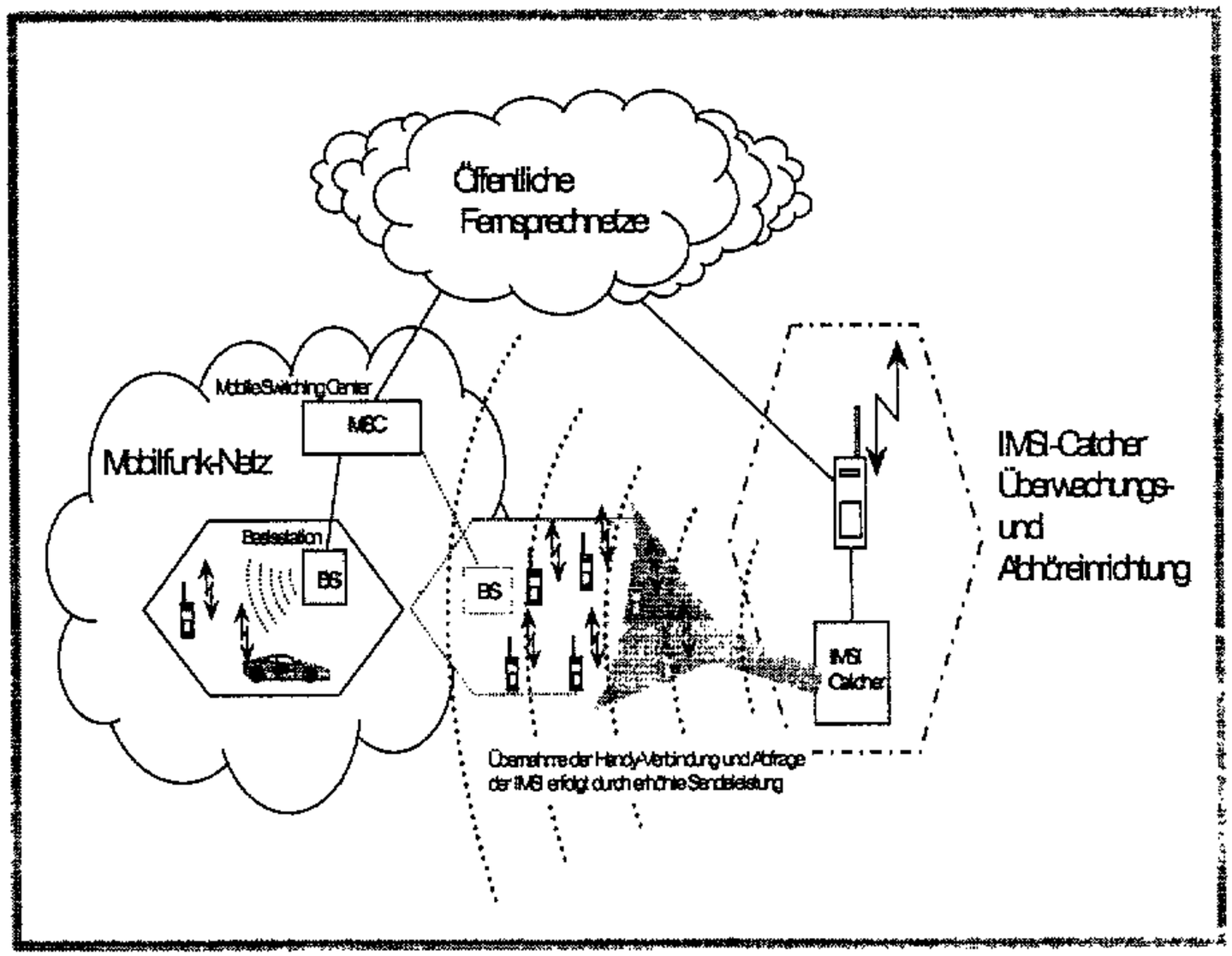
herigen Auskunftsbefugnisse auch im liberalisierten Telekommunikationsmarkt (vgl. BR-Drs. 80/96, Seite 55). Patientinnen und Patienten, aber auch Hotelgäste oder Beschäftigte in Behörden und Unternehmen fallen damit **nicht** unter die mit § 90 TKG geschaffene Regelung.

2.4.2.3 Bislang nicht realisierte Vorhaben

Im Zusammenhang der Diskussionen um die Änderungen der gesetzlichen Vorschriften im Telekommunikationsbereich ist es nicht gelungen, § 12 Fernmeldeanlagengesetz (FAG), der wegen seiner weitgehend voraussetzungslosen **Abhörbefugnisse** schon bisher heftiger Kritik ausgesetzt war, durch die Aufnahme einer Vorschrift in die Strafprozeßordnung zu ersetzen, mit der den Anforderungen des Datenschutzes eher Rechnung getragen werden könnte.

Außerdem wurde vom Innenausschuß (BR-Drs. 369/97 vom 23.08.1997) vorgeschlagen, das Gesetz zur Einschränkung des Artikel 10 GG - das sogenannte **G 10-Gesetz** - derart zu erweitern, daß die **Identifikation** der von einer Person benutzten **Anschlußnummer** durch **technische Maßnahmen** auch dann möglich sein sollte, wenn dabei das Fernmeldegeheimnis unbeteiligter Dritter technisch bedingt unvermeidbar beeinträchtigt wird. Hierzu verwies der Innenausschuß auf den **IMSI-Catcher** bzw. GA 900, der technisch in der Lage ist, vom Funktelefon abgestrahlte Funkwellen aufzufangen und so die netzinterne Rufnummer zu ermitteln.

Die Datenschutzbeauftragten des Bundes und der Länder haben den Einsatz der **IMSI-Catcher** insbesondere deshalb **abgelehnt**, weil bei der Feststellung der Rufnummer und beim Abhören der Betroffenen mit einer bisher noch nicht dagewesenen Intensität das **Recht** auf unbeobachtete Kommunikation **unbeteiligter Dritter beeinträchtigt** würde. Die Regelung zum Einsatz von IMSI-Catchern ist **nicht verabschiedet** worden. Darüber, welche Risiken gleichwohl mit der **Nutzung von Handys** verbunden sein können, informiert ein **Faltblatt** meiner Dienststelle, das in Papierform angefordert, aber auch unter **"www.lfd.nrw.de"** oder **"www.nordrhein-westfalen.datenschutz.de"** abgerufen werden kann.



IMSI-Catcher

Das Grundgerät ist nicht größer als ein PC. Der IMSI-Catcher kann in zwei Betriebsmodi (fangen, abhören) arbeiten. Er kann in verschiedenen Funknetzen eingesetzt werden und auch aus einem PKW heraus betrieben werden. Zum Fangen simulieren die Abhörgeräte eine Basisstation, die mit einer etwas stärkeren Leistung arbeitet. Geräte im Umkreis melden sich deshalb in dieser neuen Funkzelle und nicht bei der eigentlichen Basisstation an. Über diese Station laufen dann alle Verbindungsanfragen der Handys. Die Nutzerinnen und Nutzer bemerken von diesem "Fangen" nichts. Im Abhörmodus nutzen IMSI-Catcher die Möglichkeit, die Verschlüsselung auszuschalten, so daß die Gesprächsinhalte jetzt unverschlüsselt sowie mit entsprechender Software abhörbar sind und aufgezeichnet werden können.

Bislang ebenfalls **nicht erlassen** worden ist die nach § 88 Abs. 2 TKG vorgesehene Rechtsverordnung, die unter anderem die näheren Anforderungen an die Gestaltung der technischen Überwachungseinrichtungen regeln soll, die Betreiberinnen und Betreiber von Telekommunikationsanlagen auf eigene Kosten vorzuhalten haben. Schon die gesetzliche Ermächtigungsgrundlage begegnet erheblichen Bedenken, auf scharfe Ablehnung von Datenschützerinnen und Datenschützern, aber insbesondere auch von weiten Teilen der Wirtschaft stieß der darauf gestützte und im Berichtszeitraum

vorgelegte **Entwurf** einer Telekommunikationsüberwachungsverordnung (**TKÜV**). Vorgesehen waren **umfassende Überwachungsmöglichkeiten** der gesamten Telekommunikation mit nur geringen Ausnahmen. Die Überlegungen schossen derart weit über das Ziel hinaus, daß der Entwurf wieder in der Schublade verschwand.

Bedauerlich ist, daß die schon im 13. Datenschutzbericht (Seite 48) für notwendig erachtete Anpassung der Telekommunikationsdiensteunternehmen - Datenschutzverordnung (**TDSV**) immer **noch nicht** erfolgt ist.

2.4.3 Medien- und Teledienste

2.4.3.1 Das Verhältnis von Telekommunikation, Medien- und Telediensten zum allgemeinen Datenschutzrecht

Aus kompetenzrechtlichen Gründen haben die Länder im Wege einer staatsvertraglichen Vereinbarung Regelungen getroffen für diejenigen Informations- und Kommunikationsdiensteangebote, die an die **Allgemeinheit** gerichtet sind und bei denen die **redaktionelle Gestaltung** zur **Meinungsbildung** im Vordergrund steht - die **Mediendienste**. Bundesgesetzlich geregelt sind dagegen die **Teleddiensteangebote**, die für eine **individuelle Nutzung** bestimmt sind und denen der **meinungsbildende** Charakter der Mediendienste **überwiegend fehlt**. Telebanking beispielsweise ist eindeutig ein Teledienst. Die Einordnung der Dienste als Medien- oder Teledienst kann im Einzelfall Schwierigkeiten bereiten, ist für die datenschutzrechtliche Beurteilung jedoch zum Glück zumeist von untergeordneter Bedeutung, da die Bestimmungen von **Mediendienstestaatsvertrag** (MedDStV) und **Teledienstedatenschutzgesetz** (TDDSG) diesbezüglich weitgehend inhaltsgleich, überwiegend sogar wortidentisch sind. Unterschiede sind lediglich dort zu verzeichnen, wo beispielsweise journalistisch-redaktionelle Aspekte mediendiensterechtliche Besonderheiten begründen.

Abzugrenzen sind die Tele- und Mediendienste von der **Telekommunikation** als solcher, die im Telekommunikationsgesetz (TKG) normiert ist. Zwar liegt den Diensten eine Übermittlung mittels Telekommunikation zugrunde, so daß ohne Telekommunikation auch kein Tele- oder Mediendienst angeboten und in Anspruch genommen werden kann. Die unterschiedlichen Funktionen der Telekommunikation und der mit ihr erbrachten Dienste rechtfertigen jedoch **verschiedene Rechtsmaterien**. Der technische Vorgang der Telekommunikation wie auch die gewerblichen und die bloß geschäftsmäßigen Telekommunikationsangebote werden vom TKG erfaßt - vereinfacht ausgedrückt regelt es die **Transportebene der Kommunikation** oder besser

noch die Beschaffenheit und den Verlauf der Straße, auf der die Kommunikation ihren Weg zurücklegt.

Die Bestimmungen im Mediendienstestaatsvertrag und im Informations- und Kommunikationsdienstegesetz, dessen Bestandteil das Teledienstedatenschutzgesetz ist, zielen auf die Rechte und Pflichten derjenigen, die Tele- oder Mediendienste anbieten oder nutzen wollen und legen inhaltliche Anforderungen fest. Sie nehmen den eigentlichen **Transportvorgang** unter inhaltlichen Aspekten in den Blick. Gegenstand ist daher - um beim Bild von der Telekommunikationsstraße zu bleiben -, welche Voraussetzungen die Fahrzeuge erfüllen müssen, um auf der Straße fahren zu können. Der originäre **Kommunikationsinhalt** selber - etwa das Lesen einer Homepage oder die Überweisung im Wege des Homebanking - also das, was sich im Fahrzeug abspielt, richtet sich nach wie vor nach den einschlägigen **fachgesetzlichen Regelungen** und den für sie geltenden datenschutzrechtlichen Bestimmungen.

Das Verhältnis der sogenannten Multimediaregelungen zum **Bundesdatenschutzgesetz** und zu den **Landesdatenschutzgesetzen** ist das aller bereichsspezifischen Datenschutzgesetzgebung zum allgemeinen Datenschutzrecht: Die Spezialregelung hat den Vorrang. Und nur dort, wo Mediendienstestaatsvertrag und Teledienstedatenschutzgesetz keine Aussage getroffen haben, greifen die allgemeinen Datenschutzbestimmungen. Zwar nicht unkonventionell, aber datenschutzfreundlicher als derzeit noch das Bundesdatenschutzgesetz sind im Mediendienstestaatsvertrag und im Teledienstedatenschutzgesetz auch bereits **Vorgaben der Europäischen Datenschutzrichtlinie** berücksichtigt worden, so beispielsweise hinsichtlich **einheitlicher Anforderungen** an die Datenverarbeitung durch öffentliche und nicht-öffentliche Stellen und hinsichtlich dessen, daß nicht nur die Datenverarbeitung in Dateien, sondern jede Datenverarbeitung erfaßt wird. Über den derzeitigen Stand des Bundesdatenschutzgesetzes hinaus wird auch bereits die **Datenerhebung** von den Regelungen erfaßt sowie die Datenschutzkontrolle **anlaßfrei** gestellt.

2.4.3.2 Technik zum Nutzen statt zum Schaden des Datenschutzes

Im Hinblick auf die Möglichkeiten des **Datenschutzes durch Technik** enthalten der Mediendienstestaatsvertrag und das Teledienstedatenschutzgesetz sehr **positive** und durchaus **unkonventionelle Ansätze**. Datenschutz durch Technik bedeutet, in die Informations- und Kommunikationstechnologie

technische Vorkehrungen zu integrieren, die die Verarbeitung personenbezogener Daten soweit wie möglich entbehrlich machen oder auch Verfahren zu nutzen, mit denen die Unbeobachtbarkeit der Kommunikation sowie die Vertraulichkeit, Echtheit und Unversehrtheit von Daten sichergestellt werden. Es zählt nach § 12 Abs. 5 MedDStV und § 3 Abs. 4 TDDSG zu den **Grundsätzen** für die Verarbeitung personenbezogener Daten, daß sich die **Gestaltung und Auswahl technischer Einrichtungen** für die Dienste an dem Ziel auszurichten haben, **keine** oder so wenige **personenbezogene Daten** wie möglich zu erheben, zu verarbeiten und zu nutzen. Damit wird der Grundsatz der **Datenvermeidung,** der im übrigen den besten Datenschutz darstellt, bereits in die Gestaltung und Auswahl der **technischen** Komponenten einbezogen. Anders als in sonstigen datenschutzrechtlichen Vorschriften wird hier die Frage nach der **Erforderlichkeit** personenbezogener Daten schon auf der Stufe der **Entscheidung über die einzusetzende Technik** gestellt. Das heißt, bevor die Entscheidung für bestimmte technische Komponenten gefällt wird, ist immer zu prüfen, welches die am ehesten datenvermeidende und datensparsame Technik ist. Hier ist es Sache der Wirtschaft, diesen rechtlichen Anstoß aufzunehmen und sich mit datenschutzfreundlichen Innovationen zu profilieren. Datenschutzfreundliche Technologien können zu einem neuen Marktsegment werden. Die sogenannten Multimediaregelungen bringen innovativ zum Ausdruck, daß **Datenschutz** nicht mehr als Wettbewerbshemmnis, sondern als ein **Qualitätsmerkmal** angesehen werden sollte.

Ebenso **unkonventionell** und für den Datenschutz ein wirklich neues Instrument ist das **Datenschutzaudit,** das in § 17 **Mediendienstestaatsvertrag,** nicht aber in das Teledienstedatenschutzgesetz aufgenommen wurde. Zur Verbesserung von Datenschutz und Datensicherheit können Anbieterinnen und Anbieter von Mediendiensten ihr Datenschutzkonzept und ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachterinnen und Gutachter **prüfen** und **bewerten** lassen sowie das Ergebnis der Prüfung **veröffentlichen.** Damit wird erstmals der Versuch unternommen, mit Hilfe eines **Selbstregulierungsinstruments** den Datenschutz zu fördern. Übernommen wurde die Idee aus dem Umweltschutz, wo das Audit vor einigen Jahren aufgrund einer europäischen Richtlinie eingeführt worden ist. Es basiert auf der Hoffnung, daß sich die Diensteanbieterinnen und Diensteanbieter in der Erwartung von Marktvorteilen freiwillig dem Datenschutzaudit unterziehen und in eine Art **Wettbewerb um den besten Datenschutz** treten werden.

2.4.3.3 Einige Grundpflichten der Anbieterinnen und Anbieter

Anbieterinnen und Anbieter von Medien- oder Telediensten haben die Inanspruchnahme der **Dienste** sowie deren **Bezahlung** den Nutzerinnen und Nutzern **anonym** oder **unter Pseudonym** zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Zur Verwirklichung einer weitgehend **selbstbestimmten** und **unbeobachtbaren Kommunikation** wird den Diensteanbieterinnen und -anbietern darüber hinaus auferlegt, die Einhaltung von insgesamt vier datenschutzrechtlichen Pflichten durch **technische** und **organisatorische Vorkehrungen** sicherzustellen. Dabei handelt es sich im einzelnen um folgende Pflichten: Bei der Inanspruchnahme der Dienste muß die Nutzerin oder der Nutzer dagegen geschützt sein, daß **Dritte** von den eigenen Aktivitäten **Kenntnis** nehmen können. Außerdem muß es ermöglicht werden, daß die **Verbindung** mit einer Diensteanbieterin oder einem Diensteanbieter jederzeit von Seiten des Nutzers oder der Nutzerin **abgebrochen werden kann.** Weiter wird die Pflicht normiert, daß die anfallenden personenbezogenen **Daten** über den Ablauf des Abrufs oder Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung **gelöscht** werden. Diese sofortige Löschungspflicht ist allerdings mit der Einschränkung versehen, daß eine längere Speicherung nicht für Abrechnungszwecke erforderlich ist. Werden von einer Nutzerin oder von einem Nutzer **verschiedene Dienste** in Anspruch genommen, sind die dabei entstehenden personenbezogenen Daten im übrigen **getrennt** zu verarbeiten. Ausdrücklich wird eine Zusammenführung dieser Daten als unzulässig erklärt, soweit sie nicht für Abrechnungszwecke erforderlich ist.

Bei der Nutzung von Medien- oder Telediensten fallen gleichsam nebenbei Nutzungsdaten an, die von den **technischen Möglichkeiten** her leicht zur Erstellung von Nutzungs- und damit von **Persönlichkeitsprofilen** verwendet werden können. Dem begegnen § 13 Abs. 4 MedDStV und § 4 Abs. 4 TDDSG dadurch, daß die Erstellung von **Nutzungsprofilen** nur bei der Verwendung von **Pseudonymen** zulässig ist und das zu einem Pseudonym erfaßte Profil nicht mit Daten zusammengeführt werden darf, die die Trägerin oder den Träger des Pseudonyms **identifizieren** könnten. Das bedeutet zugleich, daß Nutzungsprofile unter Offenbarung der Personenidentität nicht zugelassen sind.

2.4.3.4 Notwendige konventionelle Elemente

Ebenso konventionell - wie aber auch **unverzichtbar** - greifen der Mediendienstestaatsvertrag und das Teledienstedatenschutzgesetz auf das herkömmliche und durchaus bewährte Instrumentarium des Datenschutzrechts zurück, nämlich auf die Regelung allgemeiner Grundsätze für die Verarbeitung personenbezogener Daten durch das **Verbot mit Erlaubnisvorbehalt**, auf die **Einwilligung, Zweckbindung** sowie die Regelung von **Auskunftsrechten** und passen dieses Instrumentarium an die Bedingungen der Netzwelt an. So wird für die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zur Durchführung von Diensten eine gesetzliche Erlaubnis oder die Einwilligung der Nutzerinnen und Nutzer verlangt. Die Verwendung der so gewonnen Daten wird einer engen Zweckbindung unterworfen. Für die Datenverwendung für einen anderen als den ursprünglichen Zweck bedarf es ebenfalls einer gesetzlichen Erlaubnis oder einer Einwilligung.

Zu den Grundsätzen der Verarbeitung personenbezogener Daten gehören auch umfassende **Hinweispflichten**. Ihre Einhaltung ist die Voraussetzung jeder als rechtmäßig nach dem Mediendienstestaatsvertrag oder dem Teledienstedatenschutzgesetz anzusehenden Datenverarbeitung und soll die im Netz dringend notwendige **Transparenz** schaffen. So sind die Nutzerinnen und Nutzer nach § 12 Abs. 6 MedDStV und § 3 Abs. 5 TDDSG vor jeder Datenerhebung über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. **Die Unterrichtung** ist zu **protokollieren** und muß von der Diensteanbieterin oder dem Diensteanbieter so abgelegt werden, daß Nutzerinnen und Nutzer sich jederzeit über den Inhalt der Unterrichtung informieren können. Ein Verzicht auf die Unterrichtung ist zwar möglich, darf aber nicht als Einwilligung in eine irgendgeartete Datenverarbeitung gedeutet werden. Um den spezifischen Risiken für die informationelle Selbstbestimmung im Netz Rechnung zu tragen, ist die Unterrichtungspflicht auch auf **automatisierte Verfahren** ausgedehnt worden, die eine spätere **Identifizierung** der Nutzerin oder des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten **vorbereiten**. Von derartigen Verfahren ist das Ablegen der sogenannten cookies erfaßt, so daß nunmehr vor der Ablage von cookies eine Information der Nutzerinnen und Nutzer darüber erforderlich wird. Dies zieht zwangsläufig die Notwendigkeit nach sich, für den Einsatz von **cookies** die **Einwilligung** der Nutzerin oder des Nutzers einzuholen.

Den Hinweispflichten entsprechen die in § 16 Abs. 1 MedDStV und in § 7 TDDSG geregelten **Auskunftsrechte** der Nutzerinnen und Nutzer, die weitergehend als § 34 BDSG nicht nur die zur eigenen Person, sondern auch die zum eigenen **Pseudonym** gespeicherten Daten umfassen.

2.4.3.5 Elektronische Einwilligung und Signaturgesetz

Das Datenschutzrecht fordert für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage oder die eigenhändig unterschriebene Einwilligung der betroffenen Person. Die Vorschriften zur Durchführung von Medien- und Telediensten enthalten die neue Möglichkeit, unter bestimmten Voraussetzungen eine Einwilligungserklärung auch elektronisch zu erteilen. Dafür muß die Diensteanbieterin oder der Diensteanbieter nach § 12 Abs. 8 MedDStV und § 3 Abs. 7 TDDSG **sicherstellen,** daß die Einwilligung nur durch eine eindeutige und **bewußte Handlung** der Nutzerin oder des Nutzers erfolgen kann. Damit sollen die Nutzerinnen und Nutzer vor einem unbedachten oder gar **versehentlichen Mausclick** geschützt werden, der die ungewollte Verarbeitung ihrer Daten nach sich zöge.

Weiter ist sicherzustellen, daß die Einwilligung nicht unerkennbar **verändert** werden kann und es möglich ist, ihre Urheberin oder ihren Urheber eindeutig zu **erkennen**. Um diese Voraussetzungen wirklich sicher erfüllen zu können, bedarf es im Prinzip des Einsatzes von digitalen Signierverfahren. Technisch sind sie zwar bereits ausgereift, doch ist ihre Anwendung noch so kompliziert, daß es dafür mehr als einer durchschnittlichen Medienkompetenz bedarf. Sicherzustellen ist außerdem die **Protokollierung** von Inhalt und Abgabezeitpunkt der Einwilligungserklärung und die Möglichkeit für die Nutzerinnen und Nutzer, **jederzeit** den **Inhalt** ihrer Einwilligung **abrufen** zu können. Das soll die notwendige Transparenz gewährleisten. Denn wer nicht mehr weiß, in welche Datenverarbeitung er oder sie genau eingewilligt hat, ist in den rechtlich vorgesehenen **Widerrufsmöglichkeiten** zumindest beeinträchtigt.

Das schon unter 2.2 ausführlich dargestellte digitale Signierverfahren gewährleistet die Integrität von Informationen und die eindeutige Urheberschaftszuordnung. Die Verwendung digitaler Signaturen ist zwar nicht verbindlich vorgeschrieben, doch privilegiert das im Berichtszeitraum verabschiedete Signaturgesetz (SigG) sie nach Maßgabe von § 1 Abs. 2 SigG. Das Signaturgesetz und die Signaturverordnung (SigV) regeln weniger - wie vielfach angenommen - die Einsatzbedingungen der Signatur oder stellen die Signatur mit der Schriftform gleich, sondern beschäftigen sich vorrangig mit der Normierung einer **Sicherungsinfrastruktur**. Das Gesetz regelt zunächst die Voraussetzungen für die Genehmigung von Zertifizierungsstellen

für die Schlüsselzuordnung, die Pflichtleistungen der Zertifizierungsstellen hinsichtlich des Inhalts und der Vergabe von Zertifikaten und normiert weiter sonstige, mit dem Betrieb einer Zertifizierungsstelle zusammenhängende Fragen - etwa die Einstellung der Tätigkeit, den Datenschutz sowie die Kontrolle und Durchsetzung von Verpflichtungen. Kritisch zu würdigen ist der zweistufige Aufbau, der die Sicherungsinfrastruktur verletzlich und damit leichter angreifbar macht.

2.4.3.6 Homepages öffentlicher Stellen

Zunehmend mehr öffentliche Stellen präsentieren sich mit einer eigenen **Homepage** im Netz. Zu wenig bekannt sind allerdings oft die datenschutzrechtlichen **Anforderungen** daran, die sich aus den sogenannten Multimediaregelungen, aber auch aus sonstigen bereichsspezifischen Vorschriften und dem allgemeinen Datenschutzrecht ergeben. Anfragen sowie Informations- und Kontrollbesuche hatten häufig folgende Probleme zum Gegenstand:

- Können **Daten von Beschäftigten** in die Homepage aufgenommen werden?

- Unter welchen Voraussetzungen können öffentliche Stellen **Daten von Bürgerinnen und Bürgern** ins Netz einstellen?

- Ist eine ausreichende **Transparenz bei der Anbieterkennzeichnung und Weitervermittlung** gewahrt?

2.4.3.6.1 Beschäftigtendaten

Mit ihren Homepages wollen sich die öffentlichen Stellen in aller Regel umfassend präsentieren. Dazu gehört auch, über **direkte Kontaktaufnahmemöglichkeiten** zu informieren und zugleich die richtige Ansprechpartnerin oder den richtigen Ansprechpartner für bestimmte **Zuständigkeiten** zu benennen. Das spart Zeit und vor allem Nerven derjenigen Personen, die sich gleich an die Verantwortliche oder den Verantwortlichen für ihr Anliegen wenden können. **Allein** diese Art von **Bürgerfreundlichkeit** sollte allerdings auch die Leitlinie für die Aufnahme von Beschäftigtendaten sein. Anlaß zu berechtigtem Ärger - mangels Zulässigkeit - ist es dagegen, wenn pauschal einfach ein komplettes Verzeichnis aller Mitarbeiterinnen und Mitarbeiter ins Netz eingestellt würde.

Das Medium Internet ist neu und birgt - wie schon mehrfach erwähnt - durchaus gewisse **Risiken** für die Persönlichkeitsrechte der Menschen, die sich in ihm präsentieren oder bewegen. Darüber sollten die Beschäftigten **informiert sein**. Die Akzeptanz einer Präsentation im Netz ist zudem höher, wenn die Beschäftigten **selbst** darüber **entscheiden** können, ob und wie sie auf der Homepage genannt werden. Ein Vorgehen auf **freiwilliger Basis** ist damit immer zu bevorzugen.

Sollten öffentliche Stellen nicht auf freiwilliger Basis vorgehen wollen oder können, ist zunächst festzulegen, **welche** personenbezogenen **Daten** aufzunehmen sind. Ob der Nachname um den Vornamen oder um die Anrede in der weiblichen oder männlichen Form ergänzt wird, ob eine Funktionsbezeichnung zugeordnet wird, wie genau der Zuständigkeitsbereich der zu erfüllenden Aufgaben bezeichnet wird und welche Daten der dienstlichen Erreichbarkeit - insbesondere Telefonnummern - genannt werden müssen, kann in verschiedenen Dienststellen durchaus unterschiedlich sein und richtet sich nach den **Arbeitserfordernissen "vor Ort"**. Die Angabe der Daten muß zur Aufgabenerfüllung einer modernen Verwaltung wirklich **notwendig** sein.

In einem weiteren Schritt ist im **Einzelfall** zu prüfen, **welche Beschäftigten** in der Homepage genannt werden sollen. Maßgebliche Prüfungselemente sind dabei die Stichworte "**Außenkontakte**" und "**Entscheidungsverantwortung**". Wer bei der Sachbearbeitung viel Beratungstätigkeit zu erledigen hat, muß zwangsläufig von außen ansprechbar sein. Weitere Anhaltspunkte für "Außenkontakte" liegen insbesondere vor, wenn in Bescheiden oder Schreiben an Bürgerinnen und Bürger personenbezogene Bearbeitungszuständigkeiten oder Auskunftserteilungen genannt werden. Gleiches gilt nicht zuletzt für die Zeichnungsbefugnis. Ebenfalls ist die Stellung in der Hierarchie im Hinblick auf den **Zusammenhang** von **Verantwortlichkeit** und **Außenkontakten** zu berücksichtigen. Faustregel ist dabei: Je höher die Funktion, um so mehr **Transparenz** bezüglich der Entscheidungsverantwortung.

Das Stichwort "Einzelfallprüfung" kann in diesem Zusammenhang allerdings nicht bedeuten, daß es einer Dienststelle mit beispielsweise tausend Beschäftigten etwa verwehrt sei, nach **nachvollziehbaren Kriterien Beschäftigtengruppen** zu bilden, für die generell die dienstliche Erforderlichkeit einer Netzpräsenz bejaht wird - etwa alle Referatsleitungen oder bestimmte Referate in ihrer Gesamtheit. Sichergestellt werden muß nur, daß die **Beschäftigten** über die beabsichtigte Maßnahme vorher **informiert** werden und die Möglichkeit besitzen, **ausnahmsweise** vorliegende **besondere Umstände**

geltend zu machen, die in ihrem individuellen Fall gegen eine Netzpräsenz sprechen könnten. Dann wäre die Entscheidung nochmals zu **überprüfen** und gegebenenfalls abzuändern.

Zusammenfassend kann also gesagt werden, daß öffentliche Stellen nicht unbedacht beispielsweise ihr komplettes Telefonverzeichnis ins Netz einstellen dürfen, sondern nach rational begründeten Erfordernissen diejenigen Personen auszuwählen haben, deren Netzpräsenz sie wünschen. Sie haben diese Personen vorher darüber zu informieren und ihnen die Möglichkeit zu geben, gegebenenfalls entgegenstehende Umstände darzulegen.

2.4.3.6.2 Daten von Bürgerinnen und Bürgern

Homepages erfüllen nicht nur einen Informationszweck, sondern bieten sich auch für eine **direkte Kommunikation** an. So gibt es etwa **"Gästebücher"**, in die Besucherinnen und Besucher einer Seite sich selbst und ihre Meinung zu bestimmten Fragen eintragen können. Oder Personen, die an spezifischen Fragestellungen interessiert sind, soll über das Netz Gelegenheit gegeben werden, mit anderen Interessierten Kontakt aufzunehmen, wofür entsprechende **Listen** veröffentlicht werden sollen.

Gästebücher auf der Homepage oder andere elektronische Meinungsäußerungsforen erfüllen dieselbe Funktion wie etwa ein **"schwarzes Brett"**, das bei einer öffentlichen Stelle im Eingangsbereich aushängt. Wer möchte, kann unter vollem Namen, aber auch anonym oder pseudonym Kommentare abgeben - zu welchem Thema auch immer. Ob jedoch solche Kommentare tatsächlich von der **bezeichneten Person** stammen, und ob auch der dokumentierte **Inhalt** so von ihr gewollt ist, läßt sich sowohl bei realen als auch bei virtuellen schwarzen Brettern zur Zeit nur mit einem Aufwand überprüfen und sicherstellen, der die Idee der spontanen **Meinungsäußerung** - erst recht, wenn sie auch anonym möglich sein soll - in ihr Gegenteil verkehrt. Den öffentlichen Stellen kann daher nur empfohlen werden, den Bürgerinnen und Bürgern diese Umstände mit einer ausführlichen **Information** ins Bewußtsein zu rufen, die sich nicht nur auf die Darstellung der **Netzrisiken** beschränkt. Eine Art **Warnhinweis** sollte deutlich machen, daß keine Gewähr für die **Richtigkeit** der zu findenden Angaben übernommen werden kann. Weiter sollte darüber informiert werden, daß die betreffende öffentliche Stelle strafrechtlich relevante Meinungsäußerungsinhalte nicht zuläßt. Dies wird sie in eigener Verantwortung sicherzustellen haben. In der Konsequenz bedeutet dies, jeden neuen Eintrag unverzüglich unter **strafrechtlichen** Aspekten zu prüfen.

Davon zu unterscheiden sind die Fälle, in denen es darum geht, Bürgerinnen und Bürgern durch das Bereithalten von **Institutionen und Personenlisten** zu bestimmten inhaltlichen Fragestellungen eine direkte Kontaktaufnahme untereinander zu ermöglichen. Das Anliegen ist sicherlich hilfreich, ausgeschlossen sein muß jedoch, daß Personen **ungewollt** oder sogar **ohne ihr Wissen** von Dritten in solche Listen eingetragen werden. Das Vorhalten derartiger Listen mit personenbezogenen Daten ist zunächst einmal eine ganz reguläre elektronische **Datenverarbeitung.** Sie betrifft nicht die Durchführung der Dienste im Sinne des Mediendienstestaatsvertrages und des Teledienstedatenschutzgesetzes, sondern inhaltliche Fragen. Da es für sie in aller Regel keine bereichsspezifische Rechtsgrundlage gibt, bedarf es nach § 4 DSG NW zwingend einer **Einwilligung** der Betroffenen. Die Einwilligung kann erst nach einer Information und Aufklärung der Betroffenen erteilt werden und ist grundsätzlich schriftlich abzugeben. Von der Schriftform sind allerdings dann **Ausnahmen** zugelassen, wenn wegen **besonderer Umstände** eine andere Form angemessen ist. Die Betroffenen wünschen hier von sich aus und im eigenen Interesse die Aufnahme in die elektronische Liste. Dies sollte ihnen auch auf **elektronischem Wege** ermöglicht werden, allerdings gibt es zum Schutz der Betroffenen vor einer übereilten Einwilligung oder etwa einem möglichen **Eintrag** ihrer Person **durch Dritte** folgende **Voraussetzungen** durch die **öffentliche Stelle zu beachten**:

- Die Betroffenen sollten zunächst über die Risiken einer ungeschützten und offenen Übertragung ihrer personenbezogenen Daten im Netz informiert werden.

- Zum Schutz bei der Übertragung der Daten auf elektronischem Wege sollte ein Verschlüsselungsverfahren - beispielsweise PGP - angeboten und sein Gebrauch erklärt werden.

- Die Betroffenen sollten die Wahl zwischen einer Einwilligung auf schriftlichem und auf elektronischem Wege haben und auf diese Wahlmöglichkeit hingewiesen werden.

- Um eine mißbräuchliche Eintragung von Personen durch Dritte erkennen zu können, sollten die Betroffenen über ihre Eintragung sozusagen "rückinformiert" werden und damit Gelegenheit zu möglichen Korrekturen erhalten. Auch über diese Vorgehensweise sollten die Betroffenen vorab informiert werden.

2.4.3.6.3 Transparenz der Anbieterkennzeichnung und Weitervermittlung

Besucherinnen und Besucher einer Homepage müssen klar erkennen können, bei welcher öffentlichen Stelle sie sich gerade befinden, wer für den **Inhalt verantwortlich** ist und ob beispielsweise ein "link" innerhalb derselben Homepage weiterführt oder zu anderen Diensteanbieterinnen und -anbietern weitervermittelt. Nach § 6 MedDStV und § 6 Teledienstegesetz (TDG) gehören dazu Name und Anschrift der Anbietenden sowie bei Vereinigungen und Gruppen Name und Anschrift vertretungsberechtigter Personen. Daher ist nicht nur ein **Impressum** geboten, aus dem diese Angaben hervorgehen, sondern möglichst auch auf jeder Seite mit einem **Symbol** oder einer **charakteristischen Kurzbezeichnung** die Erkennbarkeit der jeweiligen öffentlichen Stelle zu gewährleisten.

Die Pflicht, den Besucherinnen und Besuchern die **Weitervermittlung** zu einer anderen Anbieterin oder zu einem anderen Anbieter **anzuzeigen,** ist in § 13 Abs. 3 MedDStV und in § 4 Abs. 3 TDDSG normiert. Leider haben viele öffentliche Stellen dies **noch nicht realisiert.** Eine der Möglichkeiten, die Weitervermittlung anzuzeigen, besteht darin, **Zwischenseiten** zu schalten - etwa mit dem Hinweis: "Sie verlassen jetzt die Homepage der Stelle xy ...". Eine zügige Umsetzung der **Anzeigepflicht** ist zudem nicht nur für die gebotene **Transparenz** wichtig, sondern kann auch im Zusammenhang mit der Frage nach der **Verantwortlichkeit** für den hinter einem "link" stehenden Inhalt Bedeutung erlangen.

Öffentliche Stellen müssen die Verantwortlichkeit für die von ihnen angebotenen Inhalte transparent gestalten und deutlich erkennbar machen, wann die eigene Homepage verlassen wird.

2.4.3.7 Antragstellung per Mausclick?

Der Einsatz elektronischer Medien in der Verwaltung ist nicht neu. Neu und mit der Entwicklung des Internet aufgekommen ist der Gedanke, **Verwaltungsverfahren** auch über das **Netz** abzuwickeln. Die Antragstellung per Mausclick soll die Dienstleistungen der Verwaltung rund um die Uhr leicht zugänglich machen und einen Modernisierungsschub in Gang setzen. Insbesondere Probleme der **Datensicherheit,** der **Authentifizierung** der kommunizierenden Beteiligten und der **Integrität** sowie der **Authentizität** der **Daten selber** sind zur Zeit aber **noch nicht** zufriedenstellend **gelöst** und stehen daher einer Online-Verwaltung per Internet noch entgegen. Die öffentliche

Verwaltung sollte auch vorbildlich hinsichtlich der Einhaltung der Datenschutzbestimmungen bei der Einführung einer "Televerwaltung" sein. Nicht Schnelligkeit darf hier allein der Maßstab sein, sondern **Service** unter Gewährleistung optimalen **Datenschutzes** und optimaler **Datensicherheit**. Es liegt weder im Interesse der Bürgerinnen und Bürger noch der Verwaltung selbst, wenn sie angesichts der Netzrisiken auf der **Grundlage eines Datensalats** handelt - und zwar eines Datensalats aus richtigen und unter Umständen manipulierten Daten, bei denen nicht einmal sicher davon ausgegangen werden kann, daß wirklich Bürgerin A die Antragstellerin ist - Stichwort: Maskerade oder schlechter Scherz.

Derzeit noch in der Entwicklung und Planung sind öffentliche Online-Angebote mit **Dialog- oder Transaktionsmöglichkeiten**. Grundlage dieser Verfahren ist allgemeinen der "**Teleantrag**". Hierbei handelt es sich im einfachsten Fall um ein Formular, das aus dem Web-Angebot bezogen, ausgefüllt und wieder zurückgesandt werden kann. Das **elektronisch versandte Formular** wird dann im folgenden bei der öffentlichen Stelle wie eingehende Post weiterbearbeitet. In weiteren Schritten kann ein derartiges Grundprinzip ablauftechnisch verbessert werden. So können für das Ausfüllen des Formulars beispielsweise Hilfen angeboten werden. Die Abwicklung kann **weitere Verarbeitungsschritte** umfassen - wie etwa Überprüfungen der Anträge, Ausstellen von Bescheiden, Rückmeldungen an die Bürgerinnen und Bürger. Bei der Gestaltung der Verfahrensabläufe ist ein Vergleich mit dem korrespondierenden Offline-Verfahren und den dort umgesetzten Grundsätzen und Zielen hilfreich. Als Prinzip sollte gelten: **"was offline nicht sein darf, darf online nicht möglich werden"**. Mit anderen Worten muß das, was für das Offline-Verfahren zu fordern ist, auch im Online-Verfahren umgesetzt werden.

Die Initiative KOM-ON! (Kommunen Online) beispielsweise ist ein Zusammenschluß 17 nordrhein-westfälischer Großstädte und Kommunen unter Einbezug von mediaNRW sowie der informell beratenden Beteiligung meiner Dienststelle. Hauptziel ist die Fortentwicklung **öffentlicher Online-Angebote** mit Transaktionsmöglichkeiten. Ein Projektvorschlag ist, die Möglichkeiten von Online-Verwaltungsabwicklungen zwischen Bürgerinnen und Bürgern und Behörden am Beispiel des **Meldewesens** zu untersuchen. Ein weiteres Entwicklungsbeispiel ist die Online-Unterstützung der **Kraftfahrzeugzulassung**. Ziel dieses Verfahrens ist es, mittels elektronischer Antragstellung und Datenvorverarbeitung das Zulassungsverfahren soweit zu unterstützen, daß online Kennzeichen reserviert und Fahrzeugscheine vorbereitet werden können. Beim immer noch erforderlichen Behördengang können die Dokumente, Stempelungen und Prüfplaketten somit schneller erteilt werden.

Technische und organisatorische Maßnahmen zur Gewährleistung von **Datenschutz** und **Datensicherheit** in Televerwaltungsverfahren sind in erster Linie daran auszurichten, daß die an der Kommunikation beteiligten Systeme, Applikationen und Übertragungswege **größtenteils nicht in der Verfügungsgewalt** der öffentlichen Stelle liegen und damit **nicht kontrollierbar** sind. So kann beispielsweise nicht gesteuert werden, **welche Wege** Nachrichten zu nehmen haben oder in **welchen Vermittlungsrechnern** sie zu bearbeiten sind. Beinhaltet das Online-Verfahren zusätzlich ein "Herunterladen" von Software-Komponenten (zum Beispiel Java-Applets) von der Homepage, mit denen dann der Verwaltungsvorgang durchzuführen ist, so ist außerdem ein **Sicherheitszertifikat** erforderlich, das die Verbindlichkeit dieser Software und deren ordnungsgemäße Verarbeitungsfunktionen bescheinigt. Ein Sicherheitsrahmen für Televerwaltungsverfahren könnte wie folgt skizziert werden:

Gewährleistung der Vertraulichkeit

Die Gewährleistung der Vertraulichkeit ist ein Dienst, der sicherstellt, daß gesendete oder gespeicherte Informationen nur von denjenigen gelesen werden können, die dazu autorisiert sind. Im erweiterten Sinne gehören dazu auch die **Vermittlungsinformationen**, da aus ihnen hervorgeht, wann Nachrichten ausgetauscht und Verbindungen aufgebaut wurden sowie, wie groß die ausgetauschte Nachrichtenmenge war und welche Leistungsmerkmale benutzt wurden. Ein geeigneter Mechanismus zur Gewährleistung der Vertraulichkeit der Informationen ist die **Verschlüsselung**. Abhängig von der konkreten Bedrohungslage und der Kommunikationsart ist festzulegen, für welche Teile von Nachrichten - alle Daten, bestimmte Dateneinheiten, bestimmte Felder - die Vertraulichkeit zu sichern ist oder gesichert werden kann.

Erkennung von Integritätsverletzungen

Das Verändern, Löschen und Einfügen von Daten - darunter fallen auch das Einpflanzen von Viren, trojanischen Pferden und sonstige Softwaremanipulationen - verletzen die **Datenintegrität** und können die Empfängerin oder den Empfänger zu **Fehlreaktionen** veranlassen. Die Überprüfung der Integrität muß gewährleisten, daß über den gesamten Verarbeitungs- und Kommunikationsweg **Manipulationen** an Dateneinheiten **erkannt** und **behoben** werden können und damit alle Daten unversehrt, vollständig und widerspruchsfrei bleiben. Mechanismen zur Erkennung von Integritätsverletzungen sind beispielsweise **Prüfsummen** und **Hashcodes**, die Daten oder Nachrichten angehängt werden. Hierbei muß sichergestellt sein, daß es Angreifenden nicht gelingen kann, die Daten und die zugehörige Prüfsumme zu

ändern oder sie gegen eine andere Nachricht **auszutauschen**, für die sich dieselbe Prüfsumme ergibt.

Authentifikation der Kommunizierenden und der Daten

Die Authentifikation der Kommunizierenden ist ein Sicherheitsdienst, der vor **unbefugtem Zugang** und **unrechtmäßiger Nutzung** von Ressourcen schützt - etwa von Programmen, Daten, Peripheriegeräten und Netzwerkzugängen. So kann es auch befugten Dienstenutzerinnen und Dienstenutzern, die Zugang zum Kommunikationssystem haben, gelingen, sich als eine **andere** Dienstenutzerin oder ein **anderer** Dienstenutzer auszugeben ("Maskerade") und damit fremde Rechte oder Dienstleistungen in Anspruch zu nehmen. Umgekehrt können Dienste unter **Vortäuschung** einer **falschen Identität angeboten** werden. Die Authentifikation der Kommunizierenden verhindert solche Angriffe durch den Nachweis der Identität. Zu unterscheiden ist hierbei zwischen einseitiger und gegenseitiger Authentifikation. Eine beiderseitige Sicherheit bietet nur eine **gegenseitige** Authentifikation. Authentifikationsmechanismen reichen von der - nur eingeschränkt anwendbaren - Passwortmethode über biometrische Verfahren bis hin zur unter 2.2 näher erläuterten **digitalen Signatur**.

Eine vom Datenaustausch losgelöste Authentifikation der Kommunizierenden stellt aber noch nicht sicher, daß die in der Folgephase ausgetauschten Daten auch tatsächlich von der authentifizierten Person stammen. **"Trittbrettfahrer"** könnten nach einer erfolgreich durchgeführten Authentifikation unter falscher Identität die Kommunikation fortsetzen. Zwingendes Erfordernis ist daher eine **Verknüpfung der Authentifikation von Daten und Personen**, um den Nachweis zu erbringen, daß die empfangenen Daten auch von den angenommenen Kommunikationspartnerinnen und Kommunikationspartnern stammen. Ein Mechanismus zur Authentifikation der Daten und Personen ist ebenfalls die **digitale Signatur**.

Urheber- und Empfängernachweis

Der Urhebernachweis geht über die Authentifizierung der Daten **hinaus**. Er ermöglicht der Empfängerin oder dem Empfänger einer Nachricht einen objektiven und für Dritte nachvollziehbaren Nachweis, daß die Daten von einer **bestimmten Urheberin** oder von einem **bestimmten Urheber** erzeugt wurden. Der Empfängernachweis ermöglicht umgekehrt der **absendenden Person** den Nachweis, daß die Empfängerin oder der Empfänger die gesendete **Nachricht** mit genau dem **übermittelten Inhalt empfangen** hat. Sowohl der Urhebernachweis als auch der Empfängernachweis sind Voraussetzungen für eine rechtsgültige, vor Gericht beweisbare Kommunikation.

Sie sind mittels eines **Quittungsverfahrens** auf der Basis der digitalen Signatur umsetzbar.

Verhinderung von Nutzungsanalysen
Die Analyse des Nutzungsverhalten ist ein Angriff, der darauf abzielt, den Zeitpunkt, den Umfang und die Struktur einer stattgefundenen **Kommunikation zu ermitteln**. Auf der Grundlage solcher Informationen sind bei manchen Verfahren **Rückschlüsse** auf die **Inhalte** ausgetauschter Nachrichten möglich. Der Sicherheitsdienst zur Verhinderung einer Verkehrsflußanalyse soll es für Lauschende unmöglich machen, aus Informationen über Verkehrsflüsse auf Nachrichteninhalte schließen zu können. Möglichkeiten der Realisierung dieses Sicherheitsdienstes geben die unter 2.1 beschriebenen **datenschutzfreundlichen Technologien.**

Zentrale Bestandteile von Online-Verfahren zur Televerwaltung sind digitale Signaturen und Verschlüsselungsverfahren. Nur sie und die nach dem Signaturgesetz hierfür erforderliche Infrastruktur zur Ausgabe und Verwaltung der Schlüssel (Trustcenter) ermöglichen ein Fortschreiten der geplanten Entwicklungen.

3. Polizei und Verfassungsschutz

3.1 Sicherheit auf Kosten der Grundrechte?

Die Sicherheits- und Kriminalpolitik der vergangenen Jahre - fast Jahrzehnte - ist überwiegend von der Tendenz geprägt, auf tatsächliche oder vermeintliche Bedrohungslagen mit der eilig erhobenen Forderung nach neuen oder verschärften Eingriffsinstrumenten zu reagieren. Grundrechte wie das Fernmeldegeheimnis, die Unverletzlichkeit der Wohnung und nicht zuletzt die informationelle Selbstbestimmung haben Einschränkungen erfahren durch immer neue Erweiterungen der staatlichen Eingriffsbefugnisse. Ohne Anspruch auf Vollständigkeit soll der folgende Abriß ein wenig plastisch machen, welchen Umfang und welches Ausmaß die Befugnisse der Sicherheitsbehörden bislang erreicht haben.

Im Jahre 1968 wurde den Nachrichtendiensten - Verfassungsschutzämtern, Bundesnachrichtendienst, militärischer Abschirmdienst - durch das **Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses** (auch als Gesetz zu Artikel 10 Grundgesetz oder kurz als G10-Gesetz bezeichnet) unter anderem die Befugnis zum Abhören und Aufzeichnen von Telefongesprächen eingeräumt. Gleichzeitig wurde die **Telefonüberwachung als zulässiges Mittel der Aufklärung schwerer Straftaten eingeführt** (§§ 100 a, 100 b Strafprozeßordnung - StPO). § 100 a StPO ist seither mindestens achtzehnmal geändert worden. Änderung bedeutete stets Verschärfung durch Erweiterung des Katalogs der Straftaten, bei denen die Telefonüberwachung zulässig ist. Anfangs reichten neben gravierenden Staatsschutzdelikten nur besonders schwere Straftaten aus. Inzwischen finden sich im Katalog auch Delikte, die hinsichtlich ihrer Gefährlichkeit mit Taten wie Mord und Totschlag, Menschenraub, erpresserischer Kindesentführung oder Menschenhandel nicht vergleichbar sind. **Seit 1968 sind mehr als 20 Tatbestände hinzugekommen**, unter anderem einfacher und schwerer Bandendiebstahl, gewerbsmäßige oder bandenmäßige Hehlerei, Geldwäsche, Brandstiftung sowie verschiedene Verstöße gegen das Waffengesetz, das Außenwirtschaftsgesetz, das Kriegswaffenkontrollgesetz, das Betäubungsmittelgesetz, das Ausländergesetz und das Asylverfahrensgesetz.

1986 wurde durch Änderungen der Paß- und Personalausweisgesetze der **automatisierte Abgleich** mit dem Bestand an Fahndungsdaten erlaubt. Im gleichen Jahr wurde durch Änderung der StPO die **Schleppnetzfahndung** eingeführt (§ 163 d StPO). Es handelt sich um eine computergestützte Fahndungsmaßnahme, bei der personenbezogene Daten, die bei Grenz- und sonstigen Kontrollen anfallen - auch solche von völlig unbescholtenen Bürgerinnen und Bürgern - gespeichert und ausgewertet werden.

Das im Jahre 1992 verabschiedete Gesetz zur Bekämpfung der organisierten Kriminalität brachte eine Reihe von Strafrechtsverschärfungen und neue, bis dahin verbotene Ermittlungsmethoden. Hervorzuheben sind:

- Straftatbestand der **Geldwäsche** (§ 261 StGB).

- Einführung der **Vermögensstrafe** (§ 43 a StGB), deren Verfassungsmäßigkeit bis heute umstritten ist und die wegen rechtlicher und tatsächlicher Schwierigkeiten selten verhängt wird.

- Einführung der **Rasterfahndung** (§§ 98 a bis 98 c StPO). Es handelt sich um einen maschinell-automatisierten Datenabgleich, bei dem Prüfungsmerkmale, die vermutlich auf die tatverdächtige Person zutreffen, mit Daten verglichen werden, die an anderen Stellen aus anderen Gründen und zu anderen Zwecken gespeichert sind.

- **Einsatz technischer Mittel** (§ 100 c StPO). Erlaubt sind damit die **heimliche Herstellung von Fotos und Videos, der Einsatz anderer technischer Observationssysteme** (z. B. Peilsender) sowie das **Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen ("kleiner Lauschangriff")**. Die Maßnahmen dürfen sich unter bestimmten Voraussetzungen nicht nur gegen Beschuldigte, sondern auch gegen andere Personen richten, insbesondere gegen mutmaßliche Kontaktpersonen.

- **Einsatz verdeckter Ermittler** (§§ 110 a bis 110 e StPO).

- **Ausschreibung zur polizeilichen Beobachtung** (§ 163 e StPO). Zweck einer solchen Maßnahme ist es, **durch planmäßiges, heimliches Erfassen, Speichern und Auswerten von Daten ein möglichst vollständiges Bewegungsbild** einer Person oder eines Fahrzeugs zu gewinnen. Die Maßnahme ist schon zulässig, "wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, daß eine Straftat von erheblicher Bedeutung begangen wurde". Sie darf sich nicht nur gegen Beschuldigte, sondern **auch gegen mutmaßliche Kontaktpersonen** richten. Personenbezogene Daten etwa einer Begleitperson der beschuldigten Person oder derjenigen, die ein ausgeschriebenes Fahrzeug führen, dürfen erfaßt, an die Strafverfolgungsbehörden übermittelt und dort verarbeitet werden, so daß im Rahmen der polizeilichen Beobachtung auch **Menschen im Visier der Ermittlungsbehörden** sind, **gegen die nichts vorliegt und die in keinerlei Zusammenhang mit irgendeiner begangenen oder befürchteten Straftat stehen**.

1993 kam das **Geldwäschegesetz mit Identifizierungs-, Aufzeichnungs- und Anzeigepflichten für die Geldinstitute**. Mit dem Verbrechensbekämpfungsgesetz von 1994 wurde das länderübergreifende staatsanwaltschaftliche Verfahrensregister (§ 474 StPO) eingeführt. **Außerdem kann der Bundesnachrichtendienst den per Funk übertragenen internationalen Fernsprech- und Faxverkehr lückenlos überwachen**; dabei werden die Gespräche automatisiert nach bestimmten Schlüsselworten durchsucht. Gegen die weitreichenden Datenerhebungs-, Verarbeitungs- und Übermittlungsbefugnisse sind ebenso wie gegen die unzureichenden Kontrollmöglichkeiten mit guten Argumenten verfassungsrechtliche Bedenken erhoben worden. Das Bundesverfassungsgericht wird darüber aller Voraussicht nach demnächst entscheiden. Nicht zuletzt ermöglicht das im Jahre 1996 erlassene **Telekommunikationsgesetz den Strafverfolgungsbehörden den automatisierten Zugriff auf Kundendaten der Telekommunikationsdiensteanbieter**.

Vor diesem Hintergrund gewinnen die im Berichtszeitraum liegenden Entwicklungen nochmals zusätzliches Gewicht. Zu nennen sind hier beispielhaft der stark umstrittene große Lauschangriff, die DNA-Analysedatei, die sogenannte Schleierfahndung und der Anstieg der Telefonüberwachungsmaßnahmen.

3.2 Der große Lauschangriff

Artikel 13 Grundgesetz garantierte die Unverletzlichkeit der Wohnung, die deshalb als letztes privates Refugium von den immer umfassender gewordenen Überwachungs- und Abhörbefugnissen ausgenommen war. Nachdem Bundestag und Bundesrat das Grundgesetz geändert hatten, war der Weg frei, durch ein einfaches Gesetz auch das Abhören und Aufzeichnen des in einer Wohnung nichtöffentlich gesprochenen Wortes zu Strafverfolgungszwecken zu erlauben. Dies geschah durch das Gesetz vom 04.05.1998 (Gesetz zur Verbesserung der Bekämpfung der organisierten Kriminalität) mit der Einführung von § 100 c Abs. 1 Nr. 3 StPO.

Der große Lauschangriff dringt noch tiefer als die bislang bestehenden Instrumente in die Privatsphäre ein, ohne daß eine überzeugende Begründung für die unabweisbare Notwendigkeit eines derart gravierenden Einschnitts gegeben worden wäre. Es gehört nicht viel Phantasie dazu, sich auszumalen, daß gerade die Mitglieder gut durchstrukturierter Verbrecherbanden diejenigen sein werden, die sich mit ihren finanziellen und organisatorischen Möglichkeiten am ehesten vor dem Abhören in Wohnungen schützen können und auch schützen werden. Trifft die Grundrechtseinschränkung aber dann vielleicht in etlichen Fällen nicht das organisierte Schwerverbre-

chen, sondern völlig unbeteiligte Personen, dann ist **der Preis zu hoch, der für die Chance der zusätzlichen Aufklärung der einen oder anderen Straftat gezahlt wird**. Die Gewißheit, daß in den eigenen vier Wänden Gespräche mit Familienmitgliedern, Freundinnen und Freunden oder beruflichen Beiständen vertraulich und außerhalb des staatlichen Zugriffs bleiben, entspricht einem grundlegenden Bedürfnis der Bürgerinnen und Bürger, das grundrechtlich geschützt ist. Der Grundsatz, daß es Aufklärung um jeden Preis nicht gibt, gehört zu den wichtigsten Errungenschaften einer modernen, freiheitlichen Sozial- und Rechtsordnung. Die häusliche Privatheit muß deshalb auch gegenüber den Strafverfolgungsbehörden als letzte Rückzugsmöglichkeit für die Verwirklichung der Persönlichkeit unangetastet bleiben.

3.3 DNA-Analysedatei

Am 08.09.1998 ist das **DNA-Identitätsfeststellungsgesetz** in Kraft getreten. Bis dahin bestand keine gesetzliche Grundlage für das Verarbeiten von Erbmerkmalen zum Zwecke der Aufklärung künftiger, also zum Zeitpunkt der Probenentnahme, der Untersuchung und der Speicherung des Ergebnisses noch gar nicht begangener Straftaten. Die im Jahre 1997 in die StPO eingefügten §§ 81 e, 81 f erlauben zwar die DNA-Analyse, aber nur im Einzelfall im Rahmen eines bereits laufenden Ermittlungsverfahrens.

Das neue Gesetz ermöglicht den Aufbau einer weiteren zentralen Datei beim Bundeskriminalamt (BKA). Künftig werden jedem Menschen, der einer Straftat von erheblicher Bedeutung, insbesondere eines Verbrechens, eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls im besonders schweren Fall oder einer Erpressung verdächtig ist, zwecks Feststellung des DNA-Identifizierungsmusters Körperzellen entnommen, wenn "Grund zu der Annahme besteht, daß gegen ihn künftig erneut Strafverfahren wegen einer der vorgenannten Straftaten zu führen sind". Das Ergebnis der molekularbiologischen Untersuchung der Proben, das DNA-Profil, wird in der Zentraldatei gespeichert. Unter den genannten Voraussetzungen müssen ab sofort auch rechtskräftig Verurteilte, deren Strafen im Bundeszentralregister noch nicht getilgt sind, mit einer nachträglichen Probenentnahme und der Speicherung des Analyseergebnisses rechnen.

Die Einrichtung einer zentralen DNA-Analysedatei ist aus datenschutzrechtlicher Sicht nicht unbedenklich. Zwar ermöglichen die zur Speicherung vorgesehenen DNA-Merkmale, die sich auf sogenannte nicht-codierende Abschnitte der DNA beziehen, nach dem gegenwärtigen Stand der Wissenschaft keine Rückschlüsse auf Erbanlagen und körperliche oder psychische Eigenschaften. Es gibt aber Anhaltspunkte dafür, daß diese Merkmale jeden-

falls in Einzelfällen mit codierenden Merkmalen, also solchen, die nicht persönlichkeitsneutral sind, korrespondieren könnten. Außerdem weisen die nicht-codierenden DNA-Abschnitte, die ja ebenfalls zum Erbgut gehören, bei Verwandten Ähnlichkeiten auf. Diese Tatsache wird bereits vielfach genutzt, indem die Gen-Analyse für die Bestimmung von Verwandtschaftsverhältnissen eingesetzt wird (Beispiele: Vaterschaftsfeststellung oder Klärung der Familienzugehörigkeit bei Kindern von Asylbewerbern). Schon heute läßt sich mithin nicht sagen, das Ergebnis der DNA-Analyse habe - wie der Fingerabdruck - über seine Eignung als Grundlage eines Identitätsvergleichs hinaus keine Aussagekraft.

Noch gravierender fällt folgender Gesichtspunkt ins Gewicht: In Anbetracht der weltweiten, mit erheblichem Aufwand betriebenen Forschung zur Entschlüsselung des menschlichen Genoms ist es nicht auszuschließen, daß in Zukunft auch auf der Basis der Untersuchung von bislang als nichtcodierend angesehenen Merkmalen inhaltliche Informationen über genetische Dispositionen gewonnen werden können, daß also die gespeicherten Analyseergebnisse die Erstellung von Persönlichkeitsprofilen ermöglichen. Diesem Gesichtspunkt ist im Gesetz nicht ausreichend Rechnung getragen worden. Zwar werden Untersuchungen verboten, die auf überschießende Informationen gerichtet sind. Es wird aber nicht der zweite Schritt getan: Es müßte zum Schutz des Persönlichkeitsrechts der Betroffenen schon im Gesetz sichergestellt werden, daß bei bereits in der DNA-Analysedatei gespeicherten Informationen im Falle eines wissenschaftlichen Fortschritts ein Nutzungsverbot hinsichtlich persönlichkeitsrelevanter Erkenntnisse greift.

Um es klarzustellen: Trotz der generellen Bedenken gegen die Nutzung der aus dem menschlichen Erbgut gewonnenen Erkenntnisse in einer zentralen Datei möchte ich mich nicht auf eine gänzlich ablehnende Position zurückziehen. Vielmehr halte ich es unter bestimmten strengen Vorgaben und Restriktionen für denkbar, die Vorbehalte hintanzustellen zugunsten des mit der Analysedatei verfolgten Ziels, nämlich der Aufklärung und eventuell auch Verhinderung (Wiederholungstäter) allerschwerster Straftaten etwa gegen Leib und Leben. Die notwendigen Einschränkungen enthält das Gesetz indessen nicht im erforderlichen Umfang. Zunächst ist der Straftatenkatalog zu weit gefaßt. Ferner ist ein ausdrückliches Verbot der Speicherung von Analyseergebnissen zu fordern, die auf freiwilliger Probenabgabe beruhen. Schließlich wären angesichts der besonderen Sensibilität der Daten aus DNA-Analysen klare gesetzliche Vorgaben für die Verarbeitungs- und Nutzungsbefugnisse am Platze gewesen. Der statt dessen in das Gesetz aufgenommene pauschale Verweis auf das BKA-Gesetz führt zu Rechtsunklarheiten und zu der Gefahr einer untragbar ausgeweiteten Nutzungspraxis.

3.4 Schleierfahndung

Verdachtsunabhängige Kontrollen durch die Polizei haben einige Bundesländer in den letzten Jahren eingeführt. Seit dem 1. September 1989 darf auch der Bundesgrenzschutz dann zur Verhinderung unerlaubter Einreisen Personen etwa auf Bahnhöfen und in Zügen anlaßfrei überprüfen, wenn auf Grund von Lageerkenntnissen oder grenzpolizeilicher Erfahrung anzunehmen ist, daß diese Orte zur unerlaubten Einreise genutzt werden. Die bezeichneten Orte liegen damit unter einer Art Schleier der jederzeitigen Kontrollmöglichkeit.

Nach der in Nordrhein-Westfalen geltenden Rechtslage darf die Polizei Personenkontrollen nur bei konkreten Anhaltspunkten für eine Zuwiderhandlung gegen Rechtsnormen vornehmen. Zwar reicht es dabei aus, daß im Einzelfall eine Gefahr vorliegt oder eine Person sich an gefährlichen oder gefährdeten Orten aufhält oder Tatsachen für die Begehung bestimmter Straftaten sprechen, doch wird damit nach wie vor dem Grundsatz Rechnung getragen, daß der Staat einen sich aus seinen Aufgaben ergebenden Grund haben muß, um mit polizeilichen Mitteln gegen seine Bürgerinnen und Bürger vorgehen zu können. Eine Schleierfahndung in Form anlaß- und verdachtsunabhängiger Personenkontrollen würde dieses Prinzip geradezu umkehren. Im übrigen müssen auch die sonstigen Auswirkungen anlaßfreier Personenüberprüfungen gesehen werden. Sie führten zu der bisher nicht bestehenden Pflicht, sich jederzeit gegenüber der Polizei ausweisen zu müssen, statt - wenn kein Anlaß zur Kontrolle vorliegt - das Recht auf Anonymität zu haben. Die Identitätsfeststellung würde auch zwangsläufig zum Abgleich mit den polizeilichen Dateien führen, weil sie anders keinen Sinn hätte.

Dem Landtag liegt ein Gesetzentwurf zur Einführung verdachtsunabhängiger Kontrollen vor. Nach dem bisherigen Verlauf der parlamentarischen Beratungen zeichnet sich jedoch ab, daß die Landtagsmehrheit verdachtsunabhängige Polizeikontrollen nicht befürworten wird. Dies wäre ein sehr erfreuliches Ergebnis.

3.5 Ermittlungsinstrument Telefon

3.5.1 Wachsende Zahl von Telefonüberwachungen

Ein oft gehörter Satz: "Deutschland ist Weltmeister beim Abhören". Die Formulierung mag polemisch überspitzt sein. Sie läßt sich aber mit Zahlen stützen: **Wie stets in den Vorjahren ist die Anzahl der Überwachungsanordnungen auch im Jahr 1997 weiter angestiegen, und zwar um mehr als 20% auf insgesamt 7776 gegenüber 6428 im Jahr 1996**. Hierbei ist zu

berücksichtigen, daß von vielen Anordnungen mehrere Telefonanschlüsse betroffen sind. Schätzungen, nach denen die Anzahl der Menschen, die - überwiegend rein zufällig - pro Jahr in eine Abhöraktion geraten, eine sechs- oder gar siebenstellige Größenordnung erreicht, sind wohl nicht übertrieben.

Die wachsende Zahl der Telefonüberwachungsmaßnahmen sollte Anlaß zur Sorge um die Wahrung der Grundrechte sein. Ursprünglich als Ausnahme und allerletztes Mittel bei Ermittlungen gedacht, scheint die Telefonüberwachung inzwischen einen Platz im Standardrepertoire der Ermittlungsmaßnahmen gefunden zu haben. Werden sich auch der große Lauschangriff oder die Sammlung der DNA-Analysen nach einer Schamfrist in diese Richtung entwickeln? Oder wird es bald nicht nur das heimliche Lauschen, sondern auch das heimliche Filmen - also den Spähangriff - auf Wohnungen geben? Einer ausufernden Entwicklung muß Einhalt geboten werden. Zunächst einmal gehören die Telefonüberwachungsmaßnahmen und auch die anderen, in den letzten Jahren erweiterten und neu geschaffenen Ermittlungsbefugnisse auf den Prüfstand. Dies fordern die Datenschutzbeauftragten des Bundes und der Länder auch in ihrer Entschließung vom 5./6. Oktober 1998 (Abdruck im Anhang, Nr. 8). Es muß wissenschaftlich ausgewertet und untersucht werden, wie oft die Befugnisse eingesetzt werden, mit welchem Erfolg und zu welchen Kosten - zu welchem finanziellen und zu welchem grundrechtlichen Preis. Erst diese Erkenntnisse können eine seriöse Beurteilungsgrundlage dafür liefern, ob diese Befugnisse wirklich benötigt oder schleunigst wieder abgeschafft werden sollten.

3.5.2 Verbindungsdaten bleiben nicht immer geheim

Die flächendeckende Einführung des digitalen Festnetzes hat eine neue, für die Strafverfolgungsbehörden attraktive **Rasterfahndung** möglich gemacht. Die Telefongesellschaften halten die Verbindungsdaten zu Abrechnungszwecken mindestens ein bis zwei Tage fest. Dadurch ist es möglich festzustellen, mit welchem Anschluß telefoniert wurde. Will nun die Staatsanwaltschaft wissen, ob irgendwer in Deutschland eine bestimmte Rufnummer gewählt und mit diesem Anschluß ein Gespräch geführt hat, beauftragt sie die Telekom mit der systematischen Suche. **Die Großrechner der Telefongesellschaft rastern sämtliche Verbindungsdaten durch und liefern, falls vorhanden, den Anschluß, von dem aus angerufen wurde, nebst Zeitpunkt und Dauer des Gesprächs**. Als Rechtsgrundlage wird § 12 Fernmeldeanlagengesetz herangezogen, der ein Auskunftsrecht "über den Fernmeldeverkehr" einräumt, falls "die Auskunft für die Untersuchung Bedeutung hat". Einschränkungen hinsichtlich der Schwere der Tat, die es aufzu-

klären gilt, macht die Vorschrift nicht. Nicht nur aus diesem Grund begegnet sie verfassungsrechtlichen Bedenken.

3.5.3 Unzureichende Benachrichtigungen von Abhörmaßnahmen

Die Strafverfolgungsbehörden sind verpflichtet, die Beteiligten zu benachrichtigen, sobald hierdurch die Ermittlungen nicht mehr gefährdet werden können (§ 101 StPO). Beteiligte sind nicht nur diejenigen, gegen die sich eine Überwachungsanordnung richtete, sondern alle Personen, deren Telefongespräche abgehört wurden. **In der Praxis erfahren zahlreiche Menschen** dennoch **nie, daß staatliche Stellen ihre Gespräche belauscht haben**; denn wer mit der mutmaßlichen Straftat, die aufgeklärt werden soll, nichts zu tun hat und zufällig mit dem überwachten Anschluß oder von dort aus telefoniert, ist den Behörden vielfach nicht bekannt - es kann sich beispielsweise um Verwandte, Bekannte, Geschäftspartnerinnen oder Geschäftspartner handeln. Daß die Benachrichtigung stets zum frühestmöglichen Zeitpunkt erfolgt, ist nicht gewiß. So ist durch eine Beschwerde etwa ein Fall bekannt geworden, in dem die Staatsanwaltschaft den betroffenen Anschlußinhaber, der selbst nicht einmal Beschuldigter war, aufgrund einer "Panne" erst mit einer Verzögerung von mehr als einem Jahr benachrichtigt hat.

3.5.4 Transparenz für die Betroffenen und die Nichtbetroffenen

Im Berichtszeitraum wollte eine Reihe von Bürgerinnen und Bürgern wissen, ob sie selbst von einer Abhörmaßnahme betroffen waren oder sind. Bei den Nachforschungen tauchte ein Problem auf, das schon vor Jahren als von meinem Vorgänger gelöst galt (vgl. den 9. Tätigkeitsbericht, Seiten 49 bis 51 für den Bereich der Staatsanwaltschaft und den 10. Tätigkeitsbericht, Seiten 69/70). Das Landeskriminalamt brachte Bedenken gegen die Erteilung einer Negativauskunft vor: Es bestehe die Gefahr, daß der Auskunftsantrag ausschließlich dazu diene, polizeiliches Wissen auszuforschen; wegen dieser Gefahr könne regelmäßig in den Fällen, in denen das Telefon nicht überwacht werde und nicht überwacht worden sei, eine den Tatsachen entsprechende Auskunft nicht gegeben werden. Diese Auffassung mußte erneut korrigiert werden. Bürgerinnen und Bürgern sollte nicht ohne weiteres unterstellt werden, sie wollten in unlauterer Absicht die Sicherheitsbehörden ausforschen. Der in § 18 DSG NW normierte Auskunftsanspruch ist eine Ausprägung des in der Verfassung garantierten Rechts auf informationelle Selbstbestimmung. Das Auskunftsrecht würde in wichtigen Bereichen unterlaufen, wenn schon seine Inanspruchnahme als solche zur

Verweigerung der Auskunft führen könnte. Die Problematik ist inzwischen mit dem Ministerium für Inneres und Justiz erörtert worden. Dabei konnte sich meine Auffassung durchsetzen.

Es kann davon ausgegangen werden, daß in Zukunft in den Regelfällen die im Gesetz vorgeschriebene Auskunft erteilt wird.

3.6 Verfassungsschutz und polizeilicher Staatsschutz

Beschwerden und Anfragen führen meine Mitarbeiterinnen und Mitarbeiter mit einer gewissen Regelmäßigkeit zur Klärung von Einzelfällen zum Verfassungsschutz. Darüber hinaus sind im Berichtszeitraum zwei Kontrollbesuche beim Verfassungsschutz durchgeführt worden. Der erste Besuch diente einer allgemeinen Bestandsaufnahme der Datenschutzsituation beim Verfassungsschutz nach Inkrafttreten des neuen Verfassungsschutzgesetzes Nordrhein-Westfalen (VSG NW) vom 20.12.1994. Der zweite Besuch betraf die Datenverarbeitung im Zusammenhang mit Demonstrationen und die Anlieferung personenbezogener Daten von Teilnehmenden an solchen Veranstaltungen durch den Staatsschutz. Im Rahmen dieses Berichts beschränkt sich die Darstellung auf eine Auflistung der wesentlichen Ergebnisse der Kontrollen.

3.6.1 Bereich Verfassungsschutz

- **Ohne jede Regelung** zu Inhalt, Umfang, Löschung und anderes mehr werden beim Verfassungsschutz **word-perfect-Dateien** auf den einzelnen Sachbearbeitungsplätzen geführt. Diese Dateien befinden sich von Inhalt und Gestaltung her im beliebigen Zugriff der eingesetzten Dienstkräfte. Eine **Kontrolle**, ob die Datenverarbeitung in diesen und mit Hilfe dieser Dateien den gesetzlichen Vorgaben des Verfassungsschutzgesetzes entspricht, ist faktisch **nicht möglich**. Der Verfassungsschutz hat bereits zugesagt, dieses Problem im Rahmen der Neuorganisation der automatisierten Datenverarbeitung bei der Verfassungsschutzbehörde zu lösen.

- Nach § 16 Abs. 3 VSG NW darf der Verfassungsschutz unter bestimmten Voraussetzungen amtliche Register, zum Beispiel Melderegister, Personalausweisregister, Paßregister, Führerscheinkartei, Waffenscheinkartei einsehen. Seit Inkrafttreten des Gesetzes im Jahre 1994 brauchte eine solche Einsichtnahme nicht zu erfolgen. Dies legt die Frage danach nahe, ob die Ermächtigungsbestimmung nicht überflüssig ist. Ob es einen tatsächlichen Bedarf für Datenverarbeitungsbefugnisse gibt, sollte auch nach Inkrafttreten eines Gesetzes kontinuierlich kritisch

überprüft werden. Erweist sich eine solche Befugnis als nicht notwendig, sollte sie auch wieder aufgehoben werden.

- Nach § 17 Abs. 4 Satz 2 VSG NW führt der Verfassungsschutz über Auskünfte an Stellen außerhalb des öffentlichen Bereichs, die nach dem Willen des Gesetzgebers nur unter engen Voraussetzungen **ausnahmsweise** erteilt werden dürfen, einen schriftlichen Nachweis, dessen Inhalt und dessen Aufbewahrungsdauer im Gesetz geregelt sind. Hinsichtlich der Voraussetzungen für die Auskunftserteilung entspricht die Bestimmung inhaltlich dem früheren § 6 Abs. 3 VSG NW. Im Rahmen des Kontrollbesuchs wurde festgestellt, daß unter Geltung des alten Verfassungsschutzgesetzes eine hohe Zahl von Fällen in der vorgeschriebenen Weise dokumentiert wurden. Obwohl durch die Übernahme der alten Vorschrift in das neue Verfassungsschutzgesetz keine Änderung der Aufzeichnungspraxis zu erwarten war, wird inzwischen kein einziger Datenverarbeitungsvorgang mehr aufgezeichnet.

  Das Fehlen solcher Aufzeichnungen verhindert, daß derartige Datenübermittlungen auf ihre Rechtmäßigkeit hin kontrolliert werden können.

- Eine zumindest zweifelhafte Praxis ergab sich auch im Zusammenhang mit der Beteiligung der Verfassungsschutzbehörde am zentralen nachrichtendienstlichen Informationssystem des Verfassungsschutzes (NADIS). So verpflichtet § 10 Abs. 3 Satz 2 VSG NW die Verfassungsschutzbehörde bei Vorliegen der Voraussetzungen einen Datensatz "spätestens 10 Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen". Während bei der Verfassungsschutzbehörde der Vorgang über die erfolgte Löschung im Wege der Datensicherung nur eine Woche vorgehalten wird, werden die Protokollbänder für das NADIS-System **noch 10 Jahre** aufbewahrt. Dies bedeutet faktisch eine Verlängerung der Speicherung des Datensatzes um weitere 10 Jahre und damit ein Unterlaufen der gesetzlich vorgesehenen Löschungsfrist.

- Auch im übrigen ist das gesetzliche Gebot der **Löschung** personenbezogener Datensätze ein **zentrales Problem** der Datenverarbeitung der Verfassungsschutzbehörde. Der Grundsatz der Erforderlichkeit verlangt von einer öffentlichen Stelle, daß personenbezogene Daten stets dann zu löschen sind, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind. Abgesehen von den Bereichen, in denen Personenakten geführt werden, löscht die Verfassungsschutzbehörde jedoch lediglich in den elektronischen Dateien die Datensätze und bewahrt die zugrundeliegenden Papierunterlagen weiterhin auf. Von Zeit zu Zeit werden zwar alte

Aktenjahrgänge vernichtet, doch bis dahin ist die Rekonstruktion jedes in den elektronischen Dateien gelöschten Datensatzes aus den Papierunterlagen möglich.

Wie sich aus § 11 Abs. 3 VSG NW ergibt, hat die Verfassungsschutzbehörde "zur Person geführte Akten zu vernichten, wenn diese zu ihrer Aufgabenerfüllung nicht mehr erforderlich sind". Dies bedeutet zunächst einmal, daß zumindest auch die nach § 3 Abs. 3 Satz 3 VSG NW über die Verhaltensweisen von Einzelpersonen angelegten Akten zum gleichen Zeitpunkt zu vernichten sind, in dem der entsprechende Datensatz im EDV-System gelöscht wird. Soweit die Verfassungsschutzbehörde ihre Organisationsakten - also die zu den beobachteten Organisationen geführten Unterlagen - von der zeitgleichen Löschungspflicht freigestellt wissen will, vermag dies nicht zu überzeugen. Selbst die Organisationsakten enthalten Daten über die in den Organisationen tätigen Menschen und sind damit letztlich ebenfalls Akten, die zu Personen geführt werden. Auch in diesen Akten sind die personenbezogenen Datensätze fristgemäß zu löschen. Einfacher könnte die Einhaltung des Gesetzes für die Verfassungsschutzbehörde sein, wenn sie ihre Aktenführung in einer Weise umorganisieren würde, die ihr die Trennung einzelner personenbezogener Datensätze von den übrigen Aktenbestandteilen erleichtern könnte.

Die gesetzlichen Löschungsfristen hat jedenfalls auch die Verfassungsschutzbehörde einzuhalten. Dafür Sorge zu tragen, bleibt das Ministerium für Inneres und Justiz aufgerufen.

3.6.2 Bereich Sicherheitsüberprüfung

Im Bereich der Personenüberprüfung werden Daten etwa von Bediensteten öffentlicher Stellen verarbeitet, die bisher schon als vertrauenswürdig galten und denen nach einer Sicherheitsüberprüfung besonders verantwortungsvolle Aufgaben im Hinblick auf ihre besondere Zuverlässigkeit und Vertrauenswürdigkeit übertragen werden. Die Verarbeitung personenbezogener Daten dieses Personenkreises durch den Verfassungsschutz als mitwirkende Behörde läßt eher den Eindruck zu, als handele es sich im Sinne der Aufgabenstellung des Verfassungsschutzes **um besonders verdächtige Personen**. So werden etwa die Datensätze **aller** sicherheitsüberprüften Personen in dem bundesweit abrufbaren Informationssystem der Verfassungsschutzbehörden NADIS gespeichert. Grund genug, den Kreis derjenigen, die sich einer Sicherheitsüberprüfung zu unterziehen haben, möglichst klein zu halten und die erhobenen Daten in einer separaten Datei zu speichern.

- Die Datenschutzrechte der in das Verfahren möglicherweise einzubeziehenden Partnerinnen und Partner - Ehegatten, Ehegattinnen, Personen in eheähnlicher Lebensgemeinschaft - werden nur **unzureichend** gewahrt. Auch wenn nach § 7 Abs. 2 SÜG NW insoweit als Voraussetzung für eine Datenverarbeitung von einer Einwilligung ausgegangen werden muß, werden auch bei Verweigerung der Einwilligung der Partnerinnen und Partner deren Daten einer Abfrage im Informationssystem des Verfassungsschutzes unterzogen.

  Dem ist entgegenzuhalten, daß jede weitergehende Verarbeitung von Daten der Partnerinnen und Partner bei Fehlen einer Einwilligung nicht mehr möglich ist. Die Daten dieses Personenkreises sind vielmehr unverzüglich zu löschen.

- Wenig überzeugend ist auch, daß **jede** festgestellte Straftat und **jedes** Ermittlungsverfahren unter dem Gesichtspunkt der Zuverlässigkeit als **sicherheitserheblich** eingestuft und an die zuständige Behörde übermittelt werden. Straftaten im Straßenverkehr und andere Straftaten, die auch fahrlässig begangen werden können, sind vom Grundsatz her - soweit nicht besondere Umstände des Sachverhalts andere Schlüsse nahelegen - nicht als sicherheitserheblich einzustufen. Gleiches gilt für nicht abgeschlossene Ermittlungsverfahren, da diese schwebenden Verfahren stets ungesicherte Daten enthalten. Möglich ist in diesem Zusammenhang jeweils nur eine Entscheidung über die Verwertung der Erkenntnisse im konkreten Einzelfall.

  Durch ein schematisches Vorgehen beteiligt sich die Verfassungsschutzbehörde an der Verbreitung ungesicherter Erkenntnisse über die Betroffenen.

- Die Sicherheitsüberprüfung **ehrenamtlich tätiger Personen** im Bereich des Strafvollzuges erfolgt derzeit insgesamt **ohne Rechtsgrundlage**.

Bei der Kontrolle des Verfahrens der Sicherheitsüberprüfung hat sich gezeigt, daß das Gesetz im Hinblick auf die Datenschutzrechte der Betroffenen eine Reihe von Mängeln aufweist, die eine **Novellierung des Sicherheitsüberprüfungsgesetzes** nahelegen. Insbesondere im Hinblick auf eine **Trennung der Datenverarbeitung** zwischen Verfassungsschutzbehörde und der an einer Sicherheitsüberprüfung mitwirkenden Behörde sollte auch überlegt werden, die entsprechenden Datenverarbeitungsaufgaben aus dem Bereich des Verfassungsschutzes auszulagern. Eine solche Funktionentrennung dürfte dem Recht auf informationelle Selbstbestimmung der betroffenen Bürgerinnen und Bürger deutlich besser Geltung verschaffen.

3.6.3 NADIS - Personenzentraldatei (PZD)

In der Personenzentraldatei von NADIS werden nach § 6 Abs. 2 Bundesverfassungsschutzgesetz (BVerfSchG) nur die Daten gespeichert, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Es darf danach nicht jedes beliebige, der Identifizierung einer Person dienende Datum gespeichert werden, sondern nur solche Identifizierungsdaten, ohne die ein Auffinden der zu dieser Person angelegten Akten nicht möglich ist. Im Informationssystem der Polizei INPOL, das auch als Aktennachweissystem konzipiert ist, reichen zum Auffinden des Datensatzes stets die Angaben Namen, Vornamen, Geburtsdatum und Geburtsort aus.

Demgegenüber ist es **Praxis** bei der Verfassungsschutzbehörde, zahlreiche zusätzliche Informationen in der Datei NADIS zu speichern. Eine Rechtsgrundlage für eine Speicherung eines erweiterten Datenspektrums ist nicht vorhanden. Trotz meiner entsprechenden Hinweise auf diese Rechtslage ist die Verfassungsschutzbehörde nicht bereit, ihre Speicherpraxis zu ändern. Die Datenverarbeitung des Verfassungsschutzes mußte **förmlich beanstandet** werden. Dem ist die Verfassungsschutzbehörde **nicht gefolgt**.

3.6.4 Erfassung einfacher Mitglieder von Organisationen

Aufgrund einer Umfrage eines anderen Bundeslandes zur Frage der Zulässigkeit der Erfassung einfacher Mitglieder von extremistischen Personenzusammenschlüssen durch die zuständige Verfassungsschutzbehörde, ist die in diesem Zusammenhang bestehende Datenverarbeitungspraxis der Verfassungsschutzbehörde Nordrhein-Westfalen erörtert worden. Danach werden die Daten einfacher Mitglieder solcher Organisationen zwar in den Akten der Organisation erfaßt, die Speicherung des Datensatzes in elektronischen Dateien erfolgt jedoch nur dann, wenn das Mitglied die Organisation durch Aktivitäten nachdrücklich unterstützt.

Diese Vorgehensweise ist nur in geringem Umfang eine bessere Gewährleistung des Rechts auf informationelle Selbstbestimmung der betroffenen Bürgerinnen und Bürger gegenüber der Praxis der Verfassungsschutzbehörden in anderen Bundesländern, die Betroffenen zusätzlich auch elektronisch zu erfassen. Zwar fehlt es an einer automatisierten Recherchemöglichkeit, doch es hängt lediglich von der Größe der Organisation ab, mit welchem Suchaufwand die Datensätze einzelner Mitglieder aus den Organisationsakten herausgefunden und durch die Verfassungsschutzbehörde weiterverarbeitet werden können. Hinzu kommt, daß die Datensätze - wie oben bereits erwähnt - nicht dann aus einer Organisationsakte gelöscht werden, wenn sie

zur Aufgabenerfüllung des Verfassungsschutzes nicht mehr erforderlich sind, sondern erst dann, wenn die Organisationsakte selbst vernichtet wird.

Die Erfassung und Verarbeitung personenbezogener Daten einfacher Mitglieder von Organisationen ist ein weiteres Beispiel für die Notwendigkeit der datenschutzkonformen Neugestaltung der Verarbeitung personenbezogener Daten in Organisationsakten.

3.6.5 Staatsschutz, Verfassungsschutz und die Versammlungsfreiheit

"Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird, und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Artikel 8, 9 GG) verzichten" (BVerfGE 65, 1/43).

Die Folgen eines solchen Verzichts hat das Bundesverfassungsgericht darin gesehen, daß dies nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen würde, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist (BVerfGE 65, 1/43).

Nach dem Ergebnis des Kontrollbesuchs beim Staatsschutz werden ca. 85% der **Anmelderinnen und Anmelder einer Versammlung** unter freiem Himmel, die im Bereich Verwaltung der (allgemeinen) Polizei um eine Bestätigung ihrer Veranstaltung nachsuchen, an den polizeilichen Staatsschutz gemeldet. Dort werden deren Daten personenbezogen gespeichert. Der polizeiliche Staatsschutz unterrichtet seinerseits das Bundesamt für Verfassungsschutz, die Verfassungsschutzbehörde des Landes Nordrhein-Westfalen, das Bundeskriminalamt und das Landeskriminalamt. Die Übermittlung der personenbezogenen Daten führt regelmäßig dazu, daß die Anmelderinnen und Anmelder in diesen Behörden **suchfähig gespeichert sind** und auch in die entsprechenden **überregionalen Informationssysteme des Verfassungsschutzes und der Polizei eingegeben werden**. Auch wenn die Versammlung, die angemeldet wurde, "friedlich", das heißt ohne zusätzliche polizeiliche oder verfassungsschutzrelevante Erkenntnisse, verlaufen ist, besteht das Risiko für die Anmelderinnen und Anmelder, aus Anlaß der Wahrnehmung ihres Grundrechts auf Versammlungsfreiheit 10 Jahre lang bei Polizei und Verfassungsschutz gespeichert zu sein.

Ähnliche Probleme ergeben sich für **Teilnehmerinnen** und **Teilnehmer von** derartigen **Versammlungen**, denen es passieren kann, daß ihre schlichte Anwesenheit, das heißt ohne staats- oder verfassungsschutzrelevante Vorfälle, vom Staatsschutz registriert und an den Verfassungsschutz übermittelt wird. Der Umfang der Unterrichtung und die weitgehende Gleichheit des Erkenntnisstandes von Staatsschutz und Verfassungsschutz wirft die zusätzliche Frage auf, ob bei dieser Art und Weise der Datenverarbeitung der polizeiliche Staatsschutz faktisch eine Außenstelle des Verfassungsschutzes ist.

Aus der Sicht des Datenschutzes sind deshalb eine Reihe von Feststellungen und Forderungen zur Verarbeitung personenbezogener Daten von Anmelderinnen und Anmeldern sowie Teilnehmerinnen und Teilnehmern von und an Versammlungen unter freiem Himmel zu stellen:

- Die **Weitergabe** der Anmeldung einer derartigen Versammlung **an** den polizeilichen **Staatsschutz hat zu unterbleiben**, soweit nicht im Einzelfall konkrete Anhaltspunkte für Staatsschutzdelikte oder sonstige politisch motivierte Straftaten vorliegen. Eine Datenübermittlung "aus Vorsicht" wäre zudem eine unzulässige Datenübermittlung auf Vorrat.

- Die beim **Staatsschutz** im Zusammenhang mit einer Versammlung gespeicherten personenbezogenen Daten über Anmelderinnen und Anmelder sowie Teilnehmerinnen und Teilnehmer sind **unverzüglich zu löschen und** die dazugehörigen Unterlagen **zu vernichten**, wenn sich spätestens nach Durchführung der Versammlung eine konkrete Staatsschutzrelevanz nicht ergeben hat. Eine Speicherung dieser personenbezogenen Daten in den Akten über die Organisation, der die Anmelderinnen und Anmelder sowie Teilnehmerinnen und Teilnehmer zugerechnet werden, hat zu unterbleiben.

- Die **regelmäßige** Unterrichtung des Verfassungsschutzes, des Bundeskriminalamts sowie des Landeskriminalamts über die Anmelderinnen und Anmelder sowie die Teilnehmerinnen und Teilnehmer **hat zu unterbleiben**, da eine Rechtsgrundlage hierfür fehlt (§ 9 Abs. 8 DSG NW). Lediglich nach Prüfung im konkreten Einzelfall wäre eine gezielte Unterrichtung einzelner Behörden zulässig.

- Ist die Unterrichtung einer Behörde erfolgt, so besteht die Notwendigkeit eines **Nachberichts, wenn** sich die personenbezogenen Daten durch weitere Erkenntnisse als **unrichtig** herausgestellt haben. Als unrichtig sind die Daten auch dann anzusehen, wenn sich die Einschätzung als staatsschutz- oder verfassungsschutzrelevant nicht mehr aufrechter-

halten läßt. Dies gilt insbesondere dann, wenn eine entsprechende gerichtliche oder staatsanwaltschaftliche Entscheidung vorliegt.

- Die Übermittlung von Listen über Teilnehmerinnen und Teilnehmer, die während einer Versammlung in polizeilicher Hinsicht auffällig geworden sind, an Staatsschutz und Verfassungsschutz setzt voraus, daß **jeder einzelne Datensatz auf dieser Liste** Staatsschutz- bzw. Verfassungsschutzrelevanz besitzt. Datensätze mit negativem Prüfergebnis sind auf der Liste vor einer Übermittlung zu **schwärzen**. Wird diese Feststellung erst nachträglich getroffen, ist nachzuberichten und die Schwärzung von der die Liste empfangenden Stelle vorzunehmen.

Eine Überprüfung der weiteren Datenverarbeitung der Meldungen der polizeilichen Staatsschutzstellen bei der **Verfassungsschutzbehörde des Landes Nordrhein-Westfalen** hat ergeben, daß dort in den einzelnen Sachbereichen unterschiedlich verfahren und die Zulässigkeit der Datenverarbeitung in diesem Zusammenhang unterschiedlich bewertet wird: Während in dem **einen Bereich** davon ausgegangen wird, daß ca. 80% der Staatsschutzmeldungen für den Verfassungsschutz nicht verwertbar sind, wird in einem **anderen Bereich** regional differenziert mit der Folge, daß ein vollständiges Informationsinteresse nur für Anmelderinnen und Anmelder sowie Teilnehmerinnen und Teilnehmer aus bestimmten Regionen besteht. Schließlich wird in einem **dritten Bereich** Wert darauf gelegt, **alle** beim Staatsschutz vorhandenen Datensätze in diesem Zusammenhang übermittelt zu erhalten. Nur der Verfassungsschutz könne über die Verfassungsschutzrelevanz eines gemeldeten Datensatzes entscheiden, lautet hier die Auffassung.

Insbesondere die letzte Verfahrensweise macht das Bestreben danach deutlich, daß der Umfang der Erkenntnisse über Anmelderinnen und Anmelder sowie Teilnehmerinnen und Teilnehmer von Versammlungen zwischen Verfassungsschutz und Staatsschutz **identisch** sein sollen. Dem stehen allerdings die unterschiedlichen Aufgabenstellungen von Verfassungsschutz und Staatsschutz sowie die fehlenden Rechtsgrundlagen für eine parallele Datenspeicherung entgegen. **Der Staatsschutz ist keine Außenstelle des Verfassungsschutzes.** Hinzu kommt, daß sich die Verpflichtung zur Datenübermittlung nach § 16 Abs. 1 Satz 2 VSG NW lediglich auf Datenübermittlungen im Einzelfall, nicht jedoch auf die **regelmäßige** Übermittlung **aller** Datensätze des Staatsschutzes in diesem Zusammenhang bezieht. Im übrigen dürfen nach § 16 Abs. 1 VSG NW nur bekannte Tatsachen über Bestrebungen und Tätigkeiten im Sinne von § 3 Abs. 1 VSG NW übermittelt werden. Gerade bei Erst- und Einzeltätern liegen diese Voraussetzungen häufig **nicht** vor. Aufgrund der bei den Kontrollbesuchen gewonnenen Eindrücke drängt es sich auf, daß beim polizeilichen Staatsschutz der unge-

schriebene Grundsatz zu gelten scheint: **Staatsschutzrelevanz = Verfassungsschutzrelevanz.** Dies wäre jedoch nicht gesetzeskonform. Vielmehr ist nach den allgemeinen Regeln der Datenübermittlung die Polizei verpflichtet (§ 26 Abs. 3 Satz 2 PolG NW), die **Zulässigkeit** der Datenübermittlung zu **prüfen**. Sie trägt die **Verantwortung** für die Übermittlung. Dies schließt die **Verlagerung** der **Prüfung** der Zulässigkeit der Übermittlung **auf** die **Verfassungsschutzbehörde** aus, da in diesen Fällen ein **Ersuchen** der Verfassungsschutzbehörde als Empfängerin der Daten in der Regel **nicht** vorliegt.

Auffällig ist im übrigen, daß ein **sehr hoher Teil der an den Verfassungsschutz übermittelten personenbezogenen Datensätze** von Anmelderinnen und Anmeldern - sowie Teilnehmerinnen und Teilnehmern - zur Aufgabenerfüllung des Verfassungsschutzes **objektiv nicht erforderlich** ist. Es ist deshalb zusätzlich notwendig, daß die Melderichtlinien im Bereich Staatsschutz im Hinblick auf diese negativen Fälle klarstellend überarbeitet werden mit dem Ziel, **überflüssige Datenübermittlungen an den Verfassungsschutz zu verhindern**. Dies könnte in der Praxis auch in der Weise geschehen, daß die zur Aufgabenerfüllung des Verfassungsschutzes nicht erforderlichen Mitteilungen an die jeweilige Staatsschutzdienststelle wieder zurückgesandt werden.

Die Aufarbeitung der bei den Kontrollbesuchen festgestellten Datenschutzprobleme ist noch nicht abgeschlossen. Die Stellungnahmen des Ministeriums für Inneres und Justiz, der Verfassungsschutzbehörde, des Landeskriminalamts und der örtlichen Staatsschutzdienststellen stehen noch aus. Es bleibt zunächst also abzuwarten, ob auf dem Wege der gemeinsamen Diskussion datenschutzkonforme Problemlösungen gefunden werden können.

Ein **besonderes Beispiel** für die zu umfangreiche Datenverarbeitungspraxis einer Staatsschutzbehörde war die Akte eines Bürgers, der im politischen Raum sehr aktiv war. Obwohl in seiner Kriminalakte kein staatsschutzrelevanter Sachverhalt gespeichert war, waren über 40 Merkblätter abgeheftet, die die Teilnahme dieses Bürgers an politischen Versammlungen und Demonstrationen in vielfacher Weise dokumentierten. Wie der Betroffene aus einer Gerichtsverhandlung berichtete, hätten die als Zeugen vernommenen Beamten des Staatsschutzes bekundet, ihnen würde vor den Einsätzen immer wieder das Bild des Betroffenen gezeigt. Entsprechend seien dann bei Antreffen des Betroffenen Berichte über seine Anwesenheit für die Kriminalakte zu fertigen gewesen. Dies kann nur als die gezielte Erstellung eines politischen Betätigungs- und letztlich Persönlichkeitsprofils bezeichnet werden, gewonnen in erster Linie aus der Wahrnehmung eines Grundrechts des Betroffenen, nämlich seines Grundrechts auf Versammlungsfreiheit aus

Artikel 8 Grundgesetz. Es ist erfreulich, daß der Betroffene nicht die eingangs zitierten, vom Bundesverfassungsgericht befürchteten Konsequenzen gezogen hat, sondern sich dadurch gewehrt hat, daß er meine Dienststelle eingeschaltet hat. Ich habe die Datenverarbeitung als unzulässig beanstandet.

Als Folge meiner Beanstandung hat der Staatsschutz über 40 Merkblätter über den Betroffenen aus seiner Kriminalakte ausgesondert und vernichtet. Der Staatsschutz insgesamt bleibt aufgerufen, die dort gespeicherten Kriminalakten auf eine vergleichbare Speicherpraxis durchzusehen und entsprechend ebenfalls zu bereinigen.

3.7 Polizeiliche Datenverarbeitung - Spiel ohne Grenzen?

Die internationale Zusammenarbeit im Bereich der Strafverfolgung, der vorbeugenden Kriminalitätsbekämpfung und der Einreisekontrolle ist in den letzten Jahren erheblich verstärkt worden. Aus datenschutzrechtlicher Sicht haben die hierzu aufgebauten Informationssysteme, die länderübergreifend Daten sammeln und zum Abruf bereitstellen, besondere Bedeutung.

3.7.1 Schengener Informationssystem (SIS)

3.7.1.1 Schengener Abkommen und Schengener Durchführungsübereinkommen (SDÜ)

Mit dem "Schengener Abkommen" - benannt nach dem Ort Schengen in Luxemburg, in dem der Vertrag geschlossen wurde - hatten im Jahre 1985 die Benelux-Staaten, Frankreich und die Bundesrepublik Deutschland vereinbart, die Kontrollen an den gemeinsamen Grenzen nach und nach abzubauen. Am 19. Juni 1990 folgte per Staatsvertrag das sogenannte "Schengener Durchführungsübereinkommen" (SDÜ), das der Deutsche Bundestag am 15. Juli 1993 ratifizierte und das in den genannten Ländern sowie in Portugal und Spanien am 26. März 1995 in Kraft getreten ist. Nach dem späteren Beitritt von Griechenland, Italien, Österreich, Dänemark, Finnland und Schweden sind inzwischen 14 europäische Staaten am SDÜ beteiligt, wenden es aber teilweise noch nicht in vollem Umfang an.

3.7.1.2 Zweck des SDÜ

Ziel des Schengener Abkommens war und ist der freie Personenverkehr zwischen den Gebieten der Vertragsstaaten. Infolge des Wegfalls der Kontrollen an den Binnengrenzen befürchteten die beteiligten Länder jedoch

einen Verlust an Sicherheit, insbesondere in den Bereichen der Einreise aus Nicht-Vertragsstaaten, der Strafverfolgung, der vorbeugenden Bekämpfung der Kriminalität sowie der Fahndung nach Personen und Sachen. Es wurden daher Kompensationsmaßnahmen für erforderlich gehalten, die den wesentlichen Gegenstand des SDÜ bilden: Verstärkte Kontrollen an den Außengrenzen, abgestimmte Regelungen über die Visumserteilung und die Behandlung von Asylanträgen, Zusammenarbeit der Polizei- und der Strafvollstreckungsbehörden.

3.7.1.3 Datenverarbeitung im SIS

Kernstück der im SDÜ vereinbarten Regelungen ist ein in elektronischen Dateien geführtes polizeiliches Fahndungsinstrument, das "Schengener Informationssystem" (SIS). Mit ihm kann in allen Vertragsstaaten gleichzeitig nach bestimmten Personen oder Gegenständen gesucht werden. Das SIS besteht aus einem zentralen System (CSIS) in Straßburg und den nationalen Teilen (NSIS) der beteiligten Länder. Das deutsche NSIS wird beim Bundeskriminalamt in Wiesbaden geführt. Die NSIS tauschen Informationen nicht direkt untereinander, sondern über das CSIS aus. Durch ständigen Abgleich sollen Identität und Aktualität der Bestände gewährleistet werden.

Das SIS enthält Informationen zu Menschen und Sachen, die gesucht werden oder unter Beobachtung stehen. Die Speicherung personenbezogener Daten im SIS ist insbesondere in folgenden Fällen vorgesehen:

- Verurteilte, die eine Haftstrafe antreten sollen;
- Personen, die von der Polizei überwacht oder zur Festnahme oder Auslieferung gesucht werden;
- Personen, die nicht die Staatsangehörigkeit eines Vertragsstaates haben und denen die Einreise verweigert werden soll;
- gesuchte Zeuginnen und Zeugen;
- vermißte Personen.

Im SIS werden folgende Daten verarbeitet: Namen und Vornamen, Geburtsdatum und Geburtsort, Geschlecht, Staatsangehörigkeit, besondere unveränderliche körperliche Merkmale, der Ausschreibungsgrund und gegebenenfalls die Hinweise "bewaffnet" oder "gewalttätig". Falls nach einem Menschen gefahndet wird, der einen Aliasnamen benutzt, wird unter diesem Namen ein getrennter Datensatz in das System eingestellt.

Die Anzahl der in das SIS eingestellten Ausschreibungen hat sich seit der Aufnahme des Betriebs ständig erhöht. Insgesamt waren 5 592 240 Datensätze im Jahre 1997 gespeichert.

3.7.1.4 Datenschutzkontrolle

Die Kontrolle des CSIS wird durch ein unabhängiges Gremium ausgeübt, die sogenannte Gemeinsame Kontrollinstanz, die aus Mitgliedern der nationalen Datenschutzbeauftragten der Vertragsstaaten zusammengesetzt ist. Deutschland ist durch den Bundesbeauftragten für den Datenschutz und den Hessischen Datenschutzbeauftragten vertreten. Das Gremium hat 1997 und 1998 jeweils Tätigkeitsberichte vorgelegt, aus denen gravierende Datenschutzmängel hervorgehen.

3.7.1.4.1 Unrichtige Daten infolge von Abweichungen zwischen nationalen und internationalen Beständen

Die Datenbestände im CSIS sind keineswegs stets identisch mit den Inhalten der nationalen Dateien im NSIS, wobei die Abweichungen in einigen Fällen monatelang bestanden.

Offenbar fehlt es an einem sicheren und effektiven Verfahren zur Aufdeckung von Divergenzen und zur schnellen Anpassung der gespeicherten Informationen. Dieser Mangel beeinträchtigt nicht nur Funktion und Zweck des Systems. Er ist vielmehr auch aus datenschutzrechtlicher Sicht nicht hinnehmbar und kann erhebliche Nachteile für die Betroffenen haben. Wenn beispielsweise eine Ausschreibung zurückgenommen wurde und daher die Löschung des Datensatzes zu erfolgen hat, muß sichergestellt werden, daß die personenbezogenen Daten der betroffenen Person unverzüglich aus sämtlichen Teilen des SIS entfernt werden. Geschieht dies nicht, so liegt in der weiteren Speicherung der Daten ein unzulässiger und damit rechtswidriger Eingriff in das Recht auf informationelle Selbstbestimmung. Dieser Eingriff ist nicht nur abstrakter Natur, sondern kann höchst unangenehme Folgen haben, etwa die aufgrund einer Abfrage erfolgende vorläufige Festnahme, möglicherweise in einem Land, in dem wegen etwaiger Sprachschwierigkeiten die Aufklärung des Fehlers besonders lange dauert. Auch wird der jedem betroffenen Menschen zustehende Anspruch auf Richtigkeit der gespeicherten Daten nicht gewährleistet, wenn unterschiedliche Informationen verarbeitet werden oder Berichtigungen nicht zeitnah in allen Dateien erfolgen.

3.7.1.4.2 Zweckwidrige Verwendung von Ausschreibungsunterlagen

Zu beanstanden ist auch der Umgang mit schriftlichen Fahndungsunterlagen, die im Verlauf der Fahndung bei der nationalen Stelle im NSIS angefallen sind. Es wurde festgestellt, daß Unterlagen - etwa erkennungsdienstliches Material, Hinweise auf mögliche Aufenthaltsorte, Meldungen über Ort und Umstände des Antreffens - nach Erledigung der Fahndung weiterhin aufbewahrt werden.

Das Bundeskriminalamt (BKA) vertritt den Standpunkt, die Unterlagensammlung dürfe unter bestimmten Voraussetzungen in eine Kriminalakte umgewandelt werden, um sodann im polizeilichen Informationssystem nachgewiesen zu werden. Demgegenüber hat die gemeinsame Kontrollinstanz in ihrer Stellungnahme vom 03.02.1998 zutreffend ausgeführt, daß sich die Weiterverwendung der Unterlagen als Zweckänderung darstellt, die nach Artikel 102 SDÜ unzulässig ist. Die Praxis nationaler Strafverfolgungsbehörden, die im Rahmen einer SIS-Ausschreibung gelieferten personenbezogenen Daten zweckwidrig für eigene Aufgaben zu verarbeiten, ist ein weiteres Beispiel für die Tendenz, den Schutz des informationellen Selbstbestimmungsrechts der betroffenen Bürgerinnen und Bürger zugunsten der Effizienz polizeilicher Aufklärungs- und Präventionsarbeit kurzerhand hintanzustellen. Nachdrücklich zu unterstützen ist daher die Forderung der Gemeinsamen Kontrollinstanz: "Bei Löschung einer Ausschreibung zur Personenfahndung ist jede Vertragspartei gemäß Artikel 112 SDÜ verpflichtet, die personenbezogenen Daten zu löschen und alle zugehörigen Begleitpapiere umgehend zu vernichten."

Das Prinzip der Zweckbindung der Daten ist in den Schengener Gremien durchzusetzen.

3.7.1.4.3 Unzureichender Schutz der Menschen, deren Namen von anderen mißbräuchlich benutzt werden

In der Praxis des SIS tritt nicht selten folgendes Problem auf: Eine Person benutzt gefälschte oder gestohlene Ausweispapiere und wird mit diesen falschen Personalien im System ausgeschrieben. Zwangsläufig führt das für die echten Inhaberinnen oder Inhaber zu großen Schwierigkeiten, wenn sie aufgrund einer polizeilichen Überprüfung mit SIS-Abfrage festgehalten werden. Eine Lösung dieses Problems ist dringend erforderlich, läßt aber auf sich warten, weil es der derzeitige Datensatz des SIS nicht zuläßt, bei der Ausschreibung mit einer Alias-Personalie einen Hinweis auf den wahren Sachverhalt hinzuzufügen. Das BKA arbeitet mit einer "Notlösung": Den

Betroffenen wird angeboten, sich freiwillig einer erkennungsdienstlichen Behandlung (Fotos, Fingerabdrücke) zu unterziehen. Mit diesen Unterlagen wird die Identität überprüft. Stellt sich heraus, daß die betroffene Person nicht mit der gesuchten und im SIS ausgeschriebenen Person identisch ist, wird ihr ein Dokument ausgestellt, das diese Tatsache bescheinigt und bei Kontrollen vorgelegt werden kann. Dieser Behelf wird natürlich keineswegs den berechtigten Interessen der Menschen gerecht, deren Personaldaten nur deshalb international ausgeschrieben sind, weil ein anderer sie unrechtmäßig benutzt. Denn es bleibt dabei, daß die echten Inhaber der Personalien in erheblichen Schwierigkeiten sind, weil ihnen die Beweislast aufgebürdet wird. Sie müssen sich einer genauen Überprüfung ihrer Person einschließlich einer erkennungsdienstlichen Behandlung unterziehen und in die Speicherung der hierbei anfallenden Unterlagen einwilligen. Solange sie das klarstellende Dokument nicht haben oder es nicht bei sich führen, werden sie bei einer Kontrolle in arge Beweisnot kommen. Selbst wenn sie das Papier vorweisen können, wird ihnen wegen der auch insoweit aus Sicht der Polizei nicht völlig fernliegenden Fälschungsmöglichkeit Mißtrauen entgegenschlagen, das wiederum eine unangenehme und vielleicht auch langwierige Überprüfung zur Folge haben kann.

Es ist dringend erforderlich, daß zum Schutz von Personen, deren Personalien nur deshalb im SIS ausgeschrieben sind, weil ein anderer sie unrechtmäßig führt, ein effektives Verfahren entwickelt wird. Der Hinweis auf die Notwendigkeit einer Änderung der eingesetzten Software kann die Verzögerung bis zur Fertigstellung der zweiten Systemstufe (SIS II) nicht rechtfertigen.

3.7.1.4.4 Kein wirksamer Schutz vor Mißbrauch der Daten

Große Unruhe haben Meldungen darüber ausgelöst, daß in einem der nationalen Büros, die für die Abwicklung der SIS-Ausschreibungen zuständig sind, durch einen Mitarbeiter in erheblichem Umfang personenbezogene Daten an Außenstehende, vermutlich organisiert handelnde Straftäter, weitergegeben wurden. Im Bericht des Schengen-Exekutivausschusses vom 22.06.1998 heißt es dazu, dieser Vorfall sei der ausschlaggebende Faktor gewesen "für einen Bewußtwerdungsprozeß über die Gefahren, denen Organisationen im Besitz geheimer Daten ständig ausgesetzt sind"; er habe die Schengen-Staaten zu verstärkter Aufmerksamkeit und zu einer "Neubelebung der Aktivitäten im Bereich des Datenschutzes veranlaßt". In diesen Ausführungen ist leider das Eingeständnis bisheriger Inaktivität und geringer Sensibilität gegenüber dem Stellenwert des Datenschutzes zu sehen. Mögen der Einsicht Taten folgen.

3.7.2 Europol - Strafrechtliche Immunität der Europol-Angehörigen

Im 13. Datenschutzbericht wurden die datenschutzrechtlichen Bedenken gegen die Kompetenzen des europäischen Polizeiamtes Europol aufgezeigt (Seiten 65/66). Diese Bedenken sind keineswegs verringert, sondern durch die Entwicklung im Berichtszeitraum verstärkt worden. Der Bundestag hat das Europol-Zustimmungsgesetz am 10.10.1997 verabschiedet. Der Bundesrat hat am 07.11.1997 zugestimmt. Inzwischen ist auch in allen anderen Teilnehmerstaaten die Europol-Konvention ratifiziert worden.

Voraussetzung für die Aufnahme der Tätigkeit von Europol "nach den Bestimmungen des Übereinkommens" (das heißt: über die bisher bestehenden Datenverarbeitungsbefugnisse der seit 1994 arbeitenden Behörde hinaus) ist gem. Artikel 45 Abs. 4 der Konvention das Inkrafttreten verschiedener Ausführungsbestimmungen. Zu ihnen gehört das in Artikel 41 vorgesehene sogenannte Immunitätenprotokoll. Es bestimmt, daß die Mitglieder der Organe und des Personals von Europol "Immunität von jeglicher Gerichtsbarkeit hinsichtlich der von ihnen in Ausübung ihres Amtes vorgenommenen mündlichen und schriftlichen Äußerungen sowie Handlungen" genießen (Artikel 8 Abs. 1), auch nach Beendigung ihrer Tätigkeit. Danach können auch Datenschutzverstöße nicht geahndet werden.

Bundestag und Bundesrat haben der Immunitätsregelung inzwischen zugestimmt und sich damit über vielfach geäußerte Kritik hinweggesetzt. Auch ich halte die Freistellung der Europol-Bediensteten von jeglicher strafrechtlicher Verantwortlichkeit für verfassungsrechtlich äußerst bedenklich und zudem für rechtspolitisch verfehlt. Europol hat zwar (noch) keine eigenen operativen und exekutiven polizeilichen Befugnisse; es handelt sich aber um eine Institution, deren Aufgabenerfüllung grundlegende Rechte vieler europäischer Bürgerinnen und Bürger beeinträchtigen kann. Rechtsstaatliche Sicherungen sind als Korrelat zu Eingriffsbefugnissen unverzichtbar und in allen modernen Demokratien vorhanden. Es ist nicht einzusehen, weshalb Unionsbürgerinnen und -bürgern, die Rechtsschutz gegen Straftaten nationaler Polizeikräfte haben, dieser Rechtsschutz versagt bleibt, wenn dieselben Straftaten von Europol-Angehörigen begangen werden.

Mit der Immunitätenregelung ist ein weiterer Schritt in Richtung auf ein von Kontrollen weitgehend befreites europäisches Polizeiamt getan. Eine wirksame parlamentarische Kontrolle ist ebensowenig vorgesehen wie eine hinreichende gerichtliche Überprüfung der Tätigkeit von Europol. Die Zulässigkeit der Speicherung und Weiterverarbeitung personenbezogener Daten - einschließlich der für Betroffene kaum vorhersehbaren und nachzuvollzie-

henden internationalen Übermittlung, auch an Drittstaaten - kann von keinem Gericht untersucht werden. Vielmehr entscheidet abschließend ("rechtskräftig", Artikel 24 Abs. 7 der Europol-Konvention) ein Ausschuß der gemeinsamen Kontrollinstanz.

Die Frage der Immunität der Europol-Angehörigen muß weiterhin in der Diskussion bleiben. Derzeit wird den Argumenten, die gegen die Immunität sprechen, entgegengehalten, Europol nehme bislang "nur" Aufgaben einer Daten-Zentralstelle wahr; falls Europol in der Zukunft operative Befugnisse erhalte (wie im neuen Artikel 30 des EU-Vertrages vorgesehen), gelte Artikel 17 des Immunitätenprotokolls, wonach die jetzt gewährten Vorrechte im Falle der Übertragung neuer Aufgaben und Kompetenzen nicht automatisch erhalten bleiben. Das bedeutet aber lediglich, daß über die Immunitätsregelungen zwischen den Vertragsstaaten neu zu verhandeln ist. Erfahrungsgemäß ist es schwer, einmal gegebene Privilegien zurückzunehmen.

Die Freistellung einer in der Zukunft vielleicht mit vollen polizeilichen Befugnissen ausgestatteten Europol-Behörde von strafrechtlicher Verantwortlichkeit ist zu verhindern. Die Polizei steht in unserer Rechtsordnung nicht über, sondern unter dem Gesetz. Ein funktionierender Rechtsstaat ist ohne umfassende gerichtliche Kontrolle nicht denkbar.

3.7.3 INPOL - Neukonzeption

Nicht nur im internationalen Bereich, sondern auch im nationalen Raum verarbeitet die Polizei zentral in großem Umfang personenbezogene Daten, um einen schnellen und effektiven Informationsaustausch unter den verschiedenen Polizeibehörden zu ermöglichen. Beim Bundeskriminalamt (BKA) wird das bundesweite polizeiliche Informationssystem "INPOL" geführt. Seit Jahren arbeitet eine Projektgruppe der Polizei an einem neuen, erweiterten Konzept für dieses System. Unter der Bezeichnung INPOL-neu soll das neue System um die Jahrtausendwende in Betrieb genommen werden. Anlaß für die Neukonzeption sind neben den modernen technischen Möglichkeiten insbesondere auch veränderte Anforderungen, die aus polizeifachlicher Sicht an ein solches Informationssystem gestellt werden. Durch das neue Bundeskriminalamtgesetz (BKAG), das am 01.08.1997 in Kraft getreten ist, wurden konkrete gesetzliche Vorgaben für die Datenverarbeitung des BKA in seiner Funktion als Zentralstelle formuliert.

Ein abgeschlossenes Konzept für das neue System liegt bislang nicht vor. Daher ist derzeit eine umfassende datenschutzrechtliche Bewertung nicht möglich. Die Projektgruppe der Polizei erarbeitet, bedingt durch die Komplexität des zu entwickelnden Systems, in verschiedenen Teilbereichen

Konzepte, die erst in abschließenden Schritten zusammengeführt werden sollen. Hierdurch entstehen auch Schwierigkeiten für die Datenschutzbeauftragten des Bundes und der Länder, das Projekt kritisch zu verfolgen und beratend zu begleiten. Zu einzelnen Teilkonzepten kann allerdings bereits Stellung genommen werden. Hierbei handelt es sich um Entwürfe, aus denen sich die **Gefahr falscher Weichenstellungen** ergibt, die nachdrückliches Gegensteuern notwendig macht: Zum einen ist eine gewisse **Tendenz** erkennbar, **Datenverarbeitungskompetenzen und insbesondere Regelungsbefugnisse** hinsichtlich der Art und des Umfangs der Datenverarbeitung **von den Ländern auf die Bundesbehörde BKA zu verlagern**; zum anderen geht es um **die auf polizeifachlichen Wünschen beruhende Implementierung von Erfassungs- und Verarbeitungsmöglichkeiten, die nicht mehr von den gesetzlichen Ermächtigungsnormen getragen werden.**

Im einzelnen ist folgendes aufzugreifen: In Deutschland ist die Polizei im wesentlichen Ländersache. Die Rechtsgrundlagen für die Datenverarbeitung der Polizei ergeben sich aus den jeweiligen Landesgesetzen. Durch Bundesgesetz können Regelungen für die Zusammenarbeit aufgestellt, nicht aber materielle Aufgaben- und Befugnisnormen des Landesrechts verdrängt werden. Im Zusammenhang mit der Konzeption verschiedener Datensammlungen, die beim BKA geführt werden sollen, hat das Bundesministerium des Inneren (BMI) die Ansicht vertreten, aufgrund der Zentralstellenfunktion des BKA sei für die Datenverarbeitung im Zentralsystem allein das BKAG maßgeblich; daher richte sich die Zulässigkeit der Datenverarbeitung insoweit ausschließlich nach dem BKAG. Diese Auffassung des BMI wird nicht geteilt. Vielmehr enthält das BKAG lediglich die Beschreibung der Aufgaben und Befugnisse des BKA in seiner Funktion als Zentralstelle. Erhebungsnormen für die Polizei enthält es nicht. **Welche Informationen durch die Landespolizei in INPOL eingestellt werden dürfen und welche Fristen für Prüfungen und Löschungen gelten, richtet sich primär nach Landesrecht.** Auch kann entgegen der Ansicht des BMI kein Land durch das BKAG verpflichtet werden, Daten ins System einzustellen, die nach Landesrecht nicht verarbeitet werden dürfen. Für die Zulässigkeit der Datenverarbeitung im Zentralsystem sind die Regelungen des BKAG nur insoweit maßgebend, als sie rechtliche Obergrenzen aufstellen.

Für Art und Umfang der Protokollierung automatisierter Abfragen aus den Verbunddateien gibt es bislang kein zufriedenstellendes Konzept. § 11 Abs. 1 Satz 1 BKAG bestimmt: "Werden beim Bundeskriminalamt Daten abgerufen, hat es bei durchschnittlich jedem zehnten Abruf für Zwecke der Datenschutzkontrolle den Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Abruf

verantwortliche Dienststelle zu protokollieren." Diese Regelung legt lediglich einen Mindeststandard fest und verbietet, entgegen der Auffassung des BMI, nicht die Protokollierung sämtlicher Abrufe. **Eine Vollprotokollierung ist auch erforderlich, damit bei Kontrollen eine realistische Chance der Aufdeckung von unberechtigten Abrufen besteht.** Ferner müssen konkrete Festlegungen zum Inhalt der Protokolldateien erfolgen, einschließlich der Feststellung, von welcher Person auf den Datensatz zugegriffen wurde, und nicht nur, durch welche Behörde oder von welchem Terminal aus.

Die in § 11 Abs. 6 Satz 2 BKAG unter bestimmten Voraussetzungen erlaubte Zweckentfremdung der Protokolldateien muß von vornherein abschließend, restriktiv und eindeutig geregelt sein. Erforderlich sind Genehmigungsvorbehalte und die Pflicht zur Dokumentation der Gründe der Zweckänderung. Schließlich muß auch die nachträgliche Überprüfung der Rechtmäßigkeit des Zugriffs auf die Protokolldaten möglich sein. Es ist deshalb zu fordern, daß jede Verwendung der Protokolle vom System automatisiert aufgezeichnet wird - also unabhängig von einer Einzelfallentscheidung.

Die Projektgruppe der Polizei hat verschiedene **Vorschläge** vorgelegt, die darauf hinauslaufen, **die Funktion des Kriminalaktennachweises (KAN) zu erweitern.** Unter anderem wurde ein Modell vorgestellt, nach dem zusätzlich die Fallgrunddaten abrufbar gespeichert werden sollen - das heißt, alle aus polizeifachlicher Sicht interessierenden Sachverhaltsinformationen, die bisher erst aus der im System indizierten Akte ersichtlich waren. Das kann nicht akzeptiert werden, weil es eine Rechtsgrundlage für die Verarbeitung dieser Falldaten nicht gibt. **Der KAN ist ein Aktenhinweissystem, kein Forum zum Austausch von Informationen über Einzelheiten einer Straftat. Der maximal zulässige Inhalt des KAN ist in § 8 Abs. 1 und Abs. 2 BKAG abschließend aufgezählt.**

Ein anderer Vorschlag zur Erweiterung des Datensatzes im KAN betraf die **Abbildung der gesamten kriminellen Historie jeder im KAN gespeicherten Person.** Dazu wurden alternativ zwei Modelle zur Diskussion gestellt, auf die hier nicht näher einzugehen ist, weil beide aus Rechtsgründen unzulässig sind. Es geht um folgendes: Auch die Länder führen für ihren Bereich einen KAN. Nicht alle dort erfaßten Fälle werden in den Bundes-KAN (INPOL) eingestellt, sondern nur solche, die von sogenannter INPOL-Relevanz sind. Die INPOL-Projektgruppe strebt nun folgendes an: Enthält die Zentraldatei zu einer Person einen Eintrag, sollen sämtliche anderen Informationen zu dieser Person, also auch diejenigen, die nicht die Schwelle der INPOL-Relevanz erreichen, durch die Länder eingestellt werden. Dies ist mit der Gesetzeslage nicht vereinbar. In § 2 Abs. 1 BKAG sind die Vorausset-

zungen für die Einspeicherung in das Verbundsystem festgelegt: Nur "Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung" sind INPOL-relevant. Der Wortlaut der Vorschrift ist eindeutig.

Daten zu Straftaten, die unterhalb der Schwelle einzuordnen sind, dürfen nicht in INPOL zur Verfügung gestellt werden. Zulässig ist die Verarbeitung in INPOL nur dann, wenn im Einzelfall die in § 2 Abs. 1 BKAG genannten Kriterien erfüllt sind.

3.7.4 Datenübermittlung durch die Polizei

Eine Polizeibehörde versandte nach Einleitung eines Ermittlungsverfahrens unaufgefordert komplette Kopien des Vorgangs an Arbeitsamt, Sozialamt und Untere Landschaftsbehörde.

Der Betroffene war in den Verdacht geraten, in Wohnung und Garten illegal Canabispflanzen anzubauen. Er wurde vorläufig festgenommen, verhört (er machte keine Angaben zur Sache) und nach Fertigung einer Anzeige entlassen. Die Polizei stellte Kopien der bis dahin entstandenen Ermittlungsakte her und schickte diese an die genannten örtlich zuständigen Ämter. Auf Anfrage teilte die Kreispolizeibehörde mit, "durch die Übersendung der Unterlagen sollten die originär für die Auszahlung von Sozialleistungen zuständigen Behörden in die Lage versetzt werden, unter Berücksichtigung aller strafrechtlichen relevanten Feststellungen der Polizei rechtlich einwandfreie Entscheidungen zu treffen".

Die Versendung der Unterlagen des Ermittlungsverfahrens war mangels Rechtsgrundlage unzulässig. Die Voraussetzungen, unter denen die Polizei personenbezogene Daten an andere öffentliche Stellen übermitteln darf, sind im Polizeigesetz des Landes Nordrhein-Westfalen bereichsspezifisch geregelt (§§ 26, 28 PolG NW). Keine dieser Voraussetzungen lag hier vor. Auch kann die Übermittlung nicht auf § 14 Abs.1 Satz 1 in Verbindung mit § 13 Abs.2 Buchst. d DSG NW gestützt werden (wie die Polizeibehörde anfangs geltend machte), weil es hier nicht um die Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit im Sinne dieser Vorschriften ging. Die Kreispolizeibehörde wurde über die Rechtswidrigkeit der Übermittlung der personenbezogenen Daten des Betroffenen aufgeklärt. Sie hat sich meiner Auffassung angeschlossen, für Löschung der übermittelten Daten sowie Vernichtung der übersandten Unterlagen bei den angeschriebenen Behörden gesorgt und durch entsprechende Anweisungen einer Wiederholung gleichartiger Verstöße gegen das Datenschutzrecht in ihrem Bereich vorgebeugt.

Es gibt keine konkreten Anhaltspunkte für die Vermutung, daß sich ähnliches in Nordrhein-Westfalen häufig zuträgt, ich kann es allerdings auch nicht ausschließen. Aus den zahlreichen Fällen, in denen meine Dienststelle im Berichtszeitraum im Bereich der Polizeibehörden Mängeln bei der Verarbeitung personenbezogener Daten nachgegangen ist, habe ich dieses, vielleicht etwas außergewöhnliche Beispiel aus zwei Gründen herausgegriffen. Zum einen macht der Sachverhalt exemplarisch deutlich, daß noch keineswegs in allen öffentlichen Bereichen eine datenschutzfreundliche Grundhaltung fest verankert ist, eine - im positiven Sinne zu verstehende - Voreingenommenheit zugunsten des Persönlichkeitsrechts der Bürgerinnen und Bürger (auch derjenigen, die einer Straftat verdächtig sind) auf Respektierung ihrer informationellen Selbstbestimmung. Zum anderen hat die Darstellung einen präventiven Zweck. Sie soll - nicht nur im Bereich der Polizei - zur Sensibilisierung gegenüber den Belangen des Datenschutzes beitragen.

Jedes staatliche Handeln muß begleitet sein von dem Bewußtsein, daß die Verarbeitung personenbezogener Daten - und das gilt in besonderem Maße für die Übermittlung an Dritte - einen Eingriff in die Rechte der Betroffenen darstellt. Dieser Eingriff ist grundsätzlich unzulässig, soweit er nicht durch eine Rechtsvorschrift erlaubt ist. Unerläßlich ist daher in jedem Fall die sorgfältige Prüfung der Frage, ob es eine spezifische Erlaubnisnorm für die Datenverarbeitung gibt. Erst wenn hierüber Gewißheit besteht, darf gehandelt werden.

3.8 Überwachung auf Schritt und Tritt?

3.8.1 Videoüberwachung

Auf die wachsenden Verkehrsprobleme wird mit Hilfe der Telekommunikations- und Informationstechnik reagiert, kurz der Telematik. Diese Wortverbindung steht für eine Vielzahl neuer Techniken im Verkehrsbereich, wie elektronische Verkehrsleitsysteme, satellitengestützte Navigationssysteme und für Videoüberwachung. Aus Datenschutzsicht ist gegen technische Lösungen nichts einzuwenden, wenn keine personenbezogenen Daten anfallen. So messen die hauptsächlich an Autobahnbrücken installierten **Staumelder** mit ihren Infrarotsensoren lediglich Anzahl und Art der Fahrzeuge sowie deren Geschwindigkeit. Diese Daten werden vornehmlich an Mobilfunkbetreiber zum Abruf schneller Verkehrsinformationen weitergeleitet.

Demgegenüber stellt sich die **Verkehrsüberwachung mit Videotechnik** datenschutzrechtlich dann als problematisch dar, wenn dabei personenbezogene oder personenbeziehbare Daten gewonnen werden. Zwar ist die Ver-

kehrsbeobachtung eine Aufgabe der Straßenverkehrsbehörden (§ 44 Abs. 1 StVO). Keine Antwort gibt das Straßenverkehrsrecht aber auf die Frage, welche Medien mit welchem Eingriffsgrad bei der Verkehrsbeobachtung zum Einsatz kommen dürfen. Daher bleibt nur der Rückgriff auf die Generalklausel des § 9 PolG NW, die nach § 24 Nr. 1 OBG im Bereich der gefahrenabwehrenden Tätigkeit der Ordnungsbehörde entsprechend Anwendung findet. Daraus folgt, daß die Beobachtungskameras offen sichtbar aufgestellt werden müssen und grundsätzlich lediglich Übersichtsaufnahmen erstellt werden dürfen, auf denen weder Kfz-Kennzeichen noch Gesichter erkennbar oder auswertbar sind. Dies sowie weitere Hinweise zur Bedienung der Geräte und zur Auswertung der Videoaufnahmen sind in einer Dienstanweisung verbindlich festzulegen. Entsprechendes gilt, wenn Videobilder als Übersichtsaufnahmen aus den Videobeobachtungssystemen der Verkehrsbehörden an Fernsehsender für die Übertragung eines Verkehrsgeschehens im sogenannten **Staufernsehen** weitergegeben werden. Dabei muß auch sichergestellt sein, daß der Fernsehsender keine Zugriffsmöglichkeit auf die Kameras - etwa zur Veränderung der Aufnahmebereiche - hat und die Bilder nur in einem beschränkten Zeitfenster zur Verfügung gestellt werden.

Videokameras begegnen uns jedoch an allen möglichen Plätzen und Stellen immer öfter. Die **Zulässigkeit** ihres Einsatzes durch öffentliche Stellen ist **unterschiedlich** zu beurteilen. Maßgebliche Kriterien dafür sind nicht nur der Zweck der Überwachung, sondern insbesondere auch die Fragen, ob lediglich beobachtet oder ebenfalls aufgezeichnet wird, ob Personen gezielt identifiziert werden und wie lange das gegebenenfalls gewonnene Material aufbewahrt wird. Zur Verdeutlichung einige Praxisbeispiele:

In vielen Gebäuden öffentlicher Stellen sitzt im Eingangsbereich eine Pförtnerin oder ein Pförtner, um Personen Auskünfte zu geben, aber durchaus auch um einen Beitrag zur Sicherheit der im Gebäude befindlichen Personen zu leisten. Verhindern nun zum Beispiel bauliche Gegebenheiten solche Pfortenfunktionen unmittelbar am **Hauseingang**, so können keine Einwände gegen das Anbringen einer Kamera erhoben werden, mit der auf einem Monitor an der eigentlichen, aber eben räumlich entfernteren Pforte erkannt werden kann, wer das Haus betreten möchte. Für die Zulässigkeit solcher Maßnahmen, die auf das Hausrecht gestützt werden können, ist allerdings wichtig, daß tatsächlich nur eine Art **"Fernglas"** benutzt wird. Das heißt, mit der Kamera und dem Monitor darf lediglich verbunden sein, der Person, die an der Pforte sitzt, den Weg zur Haustür und zurück zu ersparen. Aufzeichnungen sind insoweit unzulässig. Außerdem ist es unerläßlich, die mit dem "Fernglas" beobachteten Personen davon in Kenntnis zu setzen, also die Kamera **gut wahrnehmbar** zu installieren.

Nicht zum Hausrecht gehörig und auch ansonsten ohne Rechtsgrundlage ist es dagegen, wenn mit einer Kamera aus einem Gebäude einer öffentlichen Stelle heraus minütliche Aufnahmen von dem davor befindlichen Platz ins Internet gestellt werden. **Bilder der Anwesenden** auf diesem Platz ungefragt zu touristischen Werbezwecken ins **Internet** zu geben, ist schlicht **unzulässig**.

Werden anlaßbezogen - beispielsweise beim Weiterfahren trotz roter Ampel - Aufnahmen durch die Polizei gefertigt, die im **Einzelfall der Beweissicherung** dienen, ist dagegen generell nichts zu sagen. Das betrifft zum Beispiel die Benutzung von sogenannten Starenkästen genauso wie Kameras in Streifenfahrzeugen. Demgegenüber wäre ein Dauerbetrieb ohne Anlaß eine unzulässige Datenerhebung auf Vorrat. Dies gilt ebenso für Videoüberwachungen, beispielsweise von Unfallschwerpunkten oder auch von Fußgängerüberwegen, wenn der Zweck lediglich darin besteht, einen Beweis führen zu können, **falls** in dem Zeitraum der **Aufzeichnung** eine Straftat oder auch Ordnungswidrigkeit begangen wird. Eine Rechtsgrundlage für die Erfassung einer Vielzahl völlig unbescholtener Personen durch Polizei, Staatsanwaltschaft und Ordnungswidrigkeitsbehörden ist nicht gegeben. § 100 c StPO macht deutlich, daß für derartige Maßnahmen stets ein Anfangsverdacht im Einzelfall vorliegen muß.

Auch polizeiliche Einsätze bei Demonstrationen werden nicht selten durch Videokameras begleitet. Dies ist jedoch nur in Ausnahmefällen gerechtfertigt. So betraf eine Beschwerde das Fertigen von Film- und Tonaufnahmen anläßlich einer friedlichen **Demonstration**. Zunächst wurde die Aktion als "polizeilicher Lehrfilm" bezeichnet, bei dem Absperrungsmaßnahmen und Raumschutz im Vordergrund gestanden hätten. Letztlich hat das zuständige Polizeipräsidium in Übereinstimmung mit der Bezirksregierung indes festgestellt, daß die von der Veranstaltung gefertigten Videoaufnahmen **rechtswidrig** waren. Das Original der Aufnahmen und eine hiervon gefertigte Kopie sind inzwischen **gelöscht**. In einem anderen Fall ging es darum, daß friedliche Demonstrantinnen und Demonstranten anläßlich einer **Wahlkampfveranstaltung** vor dem Tagungsgebäude mit einer Videokamera gefilmt worden sind. Die zuständige Kreispolizeibehörde hat inzwischen alle in diesem Zusammenhang gewonnenen Daten ausgesondert und vernichtet.

In einem ganz anderen Zusammenhang stehen wiederum **Videoüberwachungssysteme**, die auf öffentlichen Plätzen installiert sind und beispielsweise mit um 360° drehbaren Kameras und ferngesteuerter Zoom-Technik gestochen scharfe Portraits von Passantinnen und Passanten liefern und aufzeichnen können. Solche Beobachtungssysteme existieren bereits, wenn auch nicht von der Polizei installiert, der dies rechtlich verwehrt ist. Am

Düsseldorfer Hauptbahnhof beispielsweise entsteht seit Mitte November 1998 - vorsichtig ausgedrückt - eine gewisse Gemengelage. Die Deutsche Bahn AG - ein Privatunternehmen und damit außerhalb meines Zuständigkeitsbereichs - hat ein derartiges Überwachungssystem im **Bahnhof** und auf dem **Bahnhofsvorplatz** eingerichtet. Nach Presseberichten beobachten 72 Kameras rund um die Uhr das Geschehen, das auf 16 Monitoren in der "3-S-Zentrale" landet.

Der Bahnhofsvorplatz ist bahneigenes Gelände, die Kameras können ihr Sichtfeld allerdings auch auf den angrenzenden öffentlichen Straßenraum erstrecken. Die Bahn weist zwar generell durch Aufkleber an Türen und auf den Bahnsteigen auf die Videoüberwachung hin, stellt in der **Überwachungszentrale** jedoch ebenfalls einen Arbeitsplatz den **Sicherheitsbehörden** zur Verfügung. Nach einer ersten Auskunft des Polizeipräsidiums wird dieser Arbeitsplatz vornehmlich vom Bundesgrenzschutz genutzt, aber gelegentlich auch von der Polizei - insbesondere zur Bekämpfung der Drogenkriminalität bei konkreten Straf- und Gefahrenlagen. Wie sich die Alltagspraxis entwickeln wird, ist zu beobachten. Meine Dienststelle wird mit dem Polizeipräsidium weiter im Gespräch bleiben - beratend und kontrollierend.

Unabhängig davon, daß die derzeitige Rechtslage in Nordrhein-Westfalen eine rein vorsorgliche Videoüberwachung nicht ermöglicht, gibt es in der öffentlichen Diskussion um die Einführung derartiger Maßnahmen gleichwohl für einen **eng begrenzten, differenzierenden** Einsatz der Videoüberwachung Argumente, die nicht ohne weiteres von der Hand zu weisen sind. So wird eine demonstrativ plazierte reine Beobachtungskamera sicherlich nicht sämtliche Straftaten in ihrem Sichtfeld verhindern, aber mit hoher Wahrscheinlichkeit einen gewissen Abschreckungseffekt erzielen können. Zwar wird die absehbare Folge möglicherweise weniger in einer etwa geringeren Zahl von Straftaten insgesamt als vielmehr in der Verlagerung ihrer Begehungsorte liegen. Es sind aber selbstverständlich diejenigen Personen zu bedenken, die an bestimmten Orten durch einen Kameraeinsatz eventuell davor bewahrt werden, zum Opfer einer Straftat zu werden.

Die Frage, ob die mit der Videoüberwachung erhofften kriminalpolitischen Effekte nicht auch mit anderen, das informationelle Selbstbestimmungsrecht weniger beeinträchtigenden Maßnahmen - beispielsweise einer erhöhten Polizeipräsenz "vor Ort" - erreichbar wären, hat der **Landesgesetzgeber** zu entscheiden. Im Rahmen der anstehenden Novelle des Landesdatenschutzgesetzes ist über die Schaffung einer Rechtsgrundlage für die Videoüberwachung zu diskutieren. Wird beispielsweise zwischen der bloßen **Beobachtung**, einer möglichen **Speicherung** und einer personenbezogenen **Daten-**

zuordnung differenziert, ist dies datenschutzrechtlich zu begrüßen. Außerdem wären eine **Abwägungsklausel**, mit der die schutzwürdigen Interessen von Betroffenen zu berücksichtigen sind und strikte **Löschungsregelungen** erforderlich. Benachrichtigungspflichten bei der Datenverarbeitung identifizierter Personen wären ebenfalls festzulegen. Insgesamt könnte mit einer solchen Vorschrift die Videoüberwachung eng begrenzt dort ermöglicht werden, wo sie eventuell wirklich erforderlich sein könnte, ohne daß mit ihr eine flächendeckende, also lückenlose Überwachung ganzer Straßenzüge, Einkaufspassagen oder großer Plätze freigegeben würde.

3.8.2 Identifizierung mit Hilfe von Fotos

Zur Identifizierung der durch Überwachungskameras erfaßten Personen wird häufig auf die Fotos im Personalausweis- und Paßregister zurückgegriffen (vgl. hierzu auch 10. Tätigkeitsbericht, Seiten 38/39).

Nach § 46 des Gesetzes über Ordnungswidrigkeiten (OWiG) gelten für das Bußgeldverfahren, soweit dieses Gesetz nichts anderes bestimmt, sinngemäß die Vorschriften der allgemeinen Gesetze über das Strafverfahren. Die Verfolgungsbehörde hat, soweit dieses Gesetz nichts anderes bestimmt, im Bußgeldverfahren dieselben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten. Die Verfolgungsbehörde hat daher nach § 160 StPO den Sachverhalt zu erforschen. Zu diesem Zweck kann sie von allen öffentlichen Behörden Auskunft verlangen und Ermittlungen jeder Art entweder selbst vornehmen oder durch die Behörden und Bediensteten der Polizei vornehmen lassen. Die Behörden des Polizeidienstes sind verpflichtet, dem Ersuchen oder Auftrag der Verfolgungsbehörde zu genügen (§ 161 StPO). Auch bei Vorliegen einer gesetzlichen Grundlage für den Eingriff in die genannten Rechte der Betroffenen ist der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Bei mehreren zur Erreichung des Zwecks geeigneten Mitteln ist dasjenige zu wählen, das die Betroffenen am wenigsten belastet. Eine Möglichkeit zur Identifizierung ist die Einsichtnahme der Polizei in die bei der Personalausweisbehörde befindlichen Personalausweisfotos.

Die Zulässigkeit der Übermittlung personenbezogener Daten, zu denen auch Lichtbilder gehören, ist nach § 2 b Bundespersonalausweisgesetz (PAG) zu beurteilen. Die Personalausweisbehörden dürfen anderen Behörden auf deren Ersuchen Daten aus dem Personalausweisregister übermitteln. Voraussetzung ist, daß die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und die Daten bei der betroffenen Person nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können oder nach der Art der Aufgabe, zu deren Er-

füllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muß. Die strengen Anforderungen an die Erforderlichkeit einer Datenübermittlung gelten auch für die Datenübermittlung nach § 2 b PAG. Der Grundsatz der Verhältnismäßigkeit ist ebenfalls zu beachten.

Auch wenn nach § 2 b Abs. 3 Satz 1 PAG die ersuchende Behörde die Verantwortung dafür trägt, daß die Voraussetzungen des Absatzes 2 vorliegen, ist durch die Personalausweisbehörde zumindest eine Plausibilitätsprüfung durchzuführen. Die hierzu erforderlichen Angaben sind von der Ordnungsbehörde oder der Polizei zu machen. In der Regel ist davon auszugehen, daß auch bei der Durchführung von Ordnungswidrigkeitenverfahren § 2 b Abs. 2 Nr. 1 PAG erfüllt ist. Bedenken bestehen allerdings hinsichtlich des Vorliegens der Voraussetzungen von § 2 b Abs. 2 Nr. 2 und 3 PAG, wenn die Ordnungsbehörde/Polizei nicht zuvor (vergeblich) versucht hat, die betroffene Person aufzusuchen und zu identifizieren. Dies hat die Ordnungsbehörde/ Polizei schlüssig vorzutragen. Nach Nr. 10 des Runderlasses des Innenministeriums vom 06.02.1991 (MBl. NW S. 268) "Verwaltungsvorschrift zur Durchführung des Personalausweisgesetzes für das Land Nordrhein-Westfalen" wird es bei der Verfolgung von Ordnungswidrigkeiten in der Regel möglich sein, die betroffene Person auf andere Weise als durch Einsichtnahme in das Personalausweisregister zu identifizieren. Auch wenn diese Einsichtnahme eine Vorladung bei der Verfolgungsbehörde erspart, kann letztere nicht als "unverhältnismäßig hoher Aufwand" im Sinne des § 2 b Abs. 2 Nr. 3 PAG angesehen werden. Auch sind an das Kriterium "Erforderlichkeit" strenge Anforderungen zu stellen. Es reicht nicht aus, wenn zur Erfüllung einer Aufgabe die Kenntnis des Lichtbildes nur dienlich, aber nicht unbedingt notwendig ist.

Muß ausnahmsweise eine Identifizierung anhand des Personalausweisregisters vorgenommen werden, hat die Verfolgungsbehörde darzulegen, daß die in § 2 b Abs. 2 PAG genannten Zulässigkeitsvoraussetzungen vorliegen. Sie sind insbesondere gegeben, wenn bei der Verfolgung einer Verkehrsordnungswidrigkeit, die zu den Hauptunfallursachen zählt, die betroffene Person einer Vorladung nicht gefolgt und ein Identifizierungsversuch durch Befragung anderer Personen erfolglos war. Aus mehreren Beschwerden ergab sich, daß bei der Verfolgung von ordnungswidrigen Geschwindigkeitsüberschreitungen im Straßenverkehr auch dann, wenn eine juristische Person Halterin des Kraftfahrzeuges ist, schon bei der ersten Versendung des Zeugenfragebogens das Frontalfoto von Fahrzeug und Fahrerin oder Fahrer mitgeschickt wird. Dies verstößt gegen Nr. 3.1.31 des Runderlasses des Ministeriums für Inneres und Justiz (IV A 2-2510 vom 01.10.1987). Sowohl die

betroffenen Behörden als auch das Ministerium für Inneres und Justiz sind insoweit allerdings anderer Auffassung. Das Ministerium beabsichtigt eine aus seiner Sicht klarstellende Änderung des Erlasses.

4. Die Bürgerinnen und Bürger und die Justiz

4.1 Justizmitteilungsgesetz, MiStra, MiZi

Im Berichtszeitraum haben Bundestag und Bundesrat das seit langem überfällige Justizmitteilungsgesetz (JuMiG) verabschiedet. Es ist am 01.06.1998 in Kraft getreten und regelt - erstmals - gesetzlich die von Amts wegen erfolgende Übermittlung personenbezogener Daten durch Gerichte und Staatsanwaltschaften an öffentliche Stellen des Bundes und der Länder für andere Zwecke als die des Verfahrens, für das die Daten erhoben wurden. Leider ist das Gesetz in einigen Bereichen wenig datenschutzfreundlich; wichtige Forderungen und Anregungen der Datenschutzbeauftragten sind unberücksichtigt geblieben (vgl. zur Kritik den 13. Datenschutzbericht, Seite 70; s. auch 12. Tätigkeitsbericht, Seite 12).

Die bundeseinheitlichen Verwaltungsvorschriften (Anordnung über Mitteilungen in Strafsachen - MiStra - und Anordnung über Mitteilungen in Zivilsachen - MiZi -) zur Datenübermittlung durch die Justiz sind neu gefaßt worden. Es handelt sich um umfangreiche Regelungswerke mit einer schwer überschaubaren Fülle von Detailanordnungen. Die Datenschutzbeauftragten des Bundes und der Länder haben die Entstehung der Richtlinien kritisch begleitet und zu zahlreichen Einzelfragen Änderungsvorschläge unterbreitet. Leider sind die Anregungen nur teilweise befolgt worden, so daß nach wie vor in einigen Bereichen die Datenschutzgesichtspunkte vernachlässigt werden.

4.2 Zutritt zu den Gerichten

Die Erhebung und Speicherung von personenbezogenen Daten beim Betreten des Gerichtsgebäudes stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Zur Aufrechterhaltung von Sicherheit und Ordnung im Gerichtsgebäude kann dieser Eingriff jedoch erforderlich sein.

Ein juristisch interessierter Bürger nimmt gelegentlich an öffentlichen Gerichtsverhandlungen als Zuhörer teil und beschwerte sich darüber, daß in einem Verwaltungsgericht beim Betreten des Gebäudes eine Ausweiskontrolle durchgeführt würde. Die persönlichen Daten würden aufgeschrieben. Der Präsident des Verwaltungsgerichts teilte mit, daß wegen einer bestehenden Gefährdungslage nach Maßgabe polizeilicher Ratschläge ein Sicherheitskonzept umgesetzt worden sei, zu dem auch diese Maßnahme gehöre.

Gegen die Erhebung und Speicherung personenbezogener Daten zur Gefahrenabwehr beim Betreten des Gerichtsgebäudes bestehen keine durchgreifenden datenschutzrechtlichen Bedenken, wenn die Speicherung der personenbezogenen Daten zeitlich begrenzt ist - maximal bis zum Beginn des sechsten darauffolgenden Monats.

4.3 Akteneinsicht

Die Geltendmachung eines Akteneinsichtsanspruchs richtet sich nur während eines Verwaltungsverfahrens nach den Bestimmungen des Verwaltungsverfahrensgesetzes.

Der Antrag eines Bürgers auf Einsichtnahme in die zu seiner Person - außerhalb eines verwaltungsgerichtlichen Verfahrens - bei einem Verwaltungsgericht gespeicherten Daten wurde von dem Gericht unter Hinweis auf die **verfahrensrechtlichen** Vorschriften abgelehnt, soweit der Antrag sich auf ein anhängiges Verwaltungsverfahren bezog. Der Bürger habe nicht dargelegt, inwiefern die Kenntnis der Akten zur Geltendmachung oder Verteidigung seiner rechtlichen Interessen erforderlich sei. Die Ablehnung des Akteneinsichtsgesuchs entsprach der geltenden Rechtslage und war aus Sicht des Datenschutzes nicht zu beanstanden. Gleichwohl endet mit Abschluß eines Verwaltungsverfahrens die Anwendbarkeit der Vorschriften des Verwaltungsverfahrensgesetzes. Zeitlich danach beurteilt sich die Frage der Akteneinsicht nach § 18 Abs. 2 Satz 1 und 2 DSG NW. Im Gegensatz zu § 29 VwVfG NW ist dann der Anspruch auf Akteneinsicht nicht mehr an das Vorliegen und die Erfüllung weiterer Voraussetzungen gebunden.

Obwohl sich das Verwaltungsgericht dieser Rechtsauffassung nicht angeschlossen hat und die Anwendbarkeit des Verwaltungsverfahrensgesetzes auch über den Abschluß eines Verwaltungsverfahrens hinaus für gegeben hält, hat der Präsident des Verwaltungsgerichts sich bereit erklärt, dem Bürger die beantragte Akteneinsicht zu gewähren.

4.4 Angaben auf Briefumschlägen

Die Beschriftung von Briefumschlägen mit gerichtlich zuzustellenden Sendungen in der gleichen Weise wie die sich darin befindende Postzustellungsurkunde zum Zwecke der eindeutigen Identifizierung verstößt nicht gegen datenschutzrechtliche Vorschriften. Geburtsdaten haben auf Briefumschlägen allerdings nichts zu suchen.

Mehrere Beschwerden betrafen den Umstand, daß auf Umschlägen gerichtlicher Schreiben die jeweilige Geschäftsnummer des Gerichts vermerkt

war. Mit Postzustellungsurkunde zugestellte Schreiben von Gerichten erfüllen auch eine Nachweisfunktion. Um sie zu gewährleisten, genügt es nicht, lediglich den Namen der Adressatin oder des Adressaten zu benennen. Auch auf dem Umschlag ist die Angabe der **Geschäftsnummer** aus Gründen möglicher Rechtswirkungen erforderlich, um Verwechslungen definitiv ausschließen zu können. Demgegenüber ist es nicht nötig - und damit unzulässig -, andere zusätzliche personenbezogene Daten auf Briefumschlägen zu vermerken. Anläßlich einer Beschwerde wurde bekannt, daß ein von Gerichtsvollziehern verwendetes EDV-Programm im Adreßfeld automatisch auch das jeweilige Geburtsdatum der betroffenen Person benannte.

Entsprechend meiner Empfehlung hat das zuständige Amtsgericht sämtliche Gerichtsvollzieherinnen und Gerichtsvollzieher seines Zuständigkeitsbereichs gebeten, die Angabe von Geburtsdaten im Adreßfeld zu unterlassen oder sie zu schwärzen. Außerdem wurde der Programmhersteller gebeten, eine entsprechende Änderung des Programms herbeizuführen.

4.5 Formulare bei Familiengerichten

Auch die bei den Gerichten verwendeten Formulare müssen Datenschutzanforderungen genügen.

Verschiedene Familiengerichte holten in Unterhaltsverfahren ohne Wissen der Betroffenen Auskünfte über deren Einkommen beim jeweiligen Arbeitgeber ein. In dem entsprechenden Oberlandesgerichtsbezirk bestand allerdings überwiegend die Praxis, formularmäßige Auskünfte bei den Arbeitgebern im Regelfall erst dann einzuholen, wenn die unterhaltspflichtige Person der gerichtlichen Auskunftsanforderung nicht oder nur unvollständig nachgekommen war oder wenn Streit über die Richtigkeit der eigenen Einkommensangaben bestand.

Entsprechend meinem Vorschlag hat der Präsident des Oberlandesgerichts die nachgeordneten Gerichte gebeten, die Vordrucke für die Einholung von Lohnauskünften unter Berücksichtigung des Grundsatzes der Transparenz der Datenverarbeitung um den Hinweis zu ergänzen, daß bei Nichterteilung der Auskunft, bei Unvollständigkeit oder bei Zweifeln an der Richtigkeit der Auskunft damit gerechnet werden muß, daß eine Lohnauskunft bei den Arbeitgeberinnen und Arbeitgebern eingeholt wird.

4.6 Terminsaushänge

Die sogenannte eidesstattliche Versicherung wurde nach der bis zum 31.12.1998 geltenden Rechtslage beim Amtsgericht abgegeben. Obwohl die

hierzu anberaumte Sitzung nichtöffentlich ist, war es bei den meisten Amtsgerichten üblich, eine Terminsübersicht auszuhängen, in der die **Namen** der Schuldnerinnen oder Schuldner **angegeben** waren. Durch die offene Bekanntgabe der Namen wird ein unbestimmter Kreis Dritter darüber informiert, daß die genannte Person zahlungsunfähig und gegen sie ein Zwangsvollstreckungsverfahren anhängig ist. Rechtlich gesehen handelt es sich um eine Übermittlung personenbezogener Daten, die mangels Rechtsgrundlage unzulässig ist. Dasselbe gilt für alle anderen nichtöffentlichen Gerichtsverhandlungen beispielsweise Strafsachen gegen Jugendliche.

Das Ministerium für Inneres und Justiz teilt erfreulicherweise die datenschutzrechtlichen Bedenken grundsätzlich. Es hat den anderen Ländern eine Änderung der - bundesweit einheitlichen - Aktenordnung vorgeschlagen, mit der unter anderem folgendes geregelt wird: **Bei nichtöffentlichen Sitzungen werden in der sogenannten Terminsrolle die Namen der beteiligten Bürgerinnen und Bürger in Zukunft nicht mehr aufgeführt.** Das Ministerium hat ferner die Gerichte des Landes aufgefordert, bereits jetzt - also schon vor Änderung der Aktenordnung - entsprechend zu verfahren. Allerdings sind aus der Gerichtspraxis insofern Bedenken laut geworden, als in Familiensachen die Sitzungen - je nach Gegenstand der Verhandlung - teils öffentlich, teils nichtöffentlich sind. Die Familiengerichte sehen erhebliche praktische Schwierigkeiten, weil die Terminsaushänge unterschiedlich gestaltet und/oder im Laufe eines Sitzungstages geändert werden müßten. Das Ministerium beabsichtigt daher, außerhalb der Aktenordnung per Erlaß für die Familiensachen eine **Sonderregelung** zu treffen: Hier soll die Terminsrolle die Namen der Parteien stets enthalten dürfen, also auch dann, wenn es in der Sitzung um einen nichtöffentlichen Verhandlungsteil geht. Trotz nicht ganz ausgeräumter datenschutzrechtlicher Bedenken ist diese Sonderbehandlung der Familiensachen akzeptabel. Anders als bei Terminen zur Abgabe der eidesstattlichen Versicherung oder in Jugendstrafsachen ist die Öffentlichkeit hier nämlich nicht generell, sondern nur für bestimmte Teile des Verfahrens ausgeschlossen, und das Urteil wird stets öffentlich verkündet. Die Abweichung vom Prinzip der Öffentlichkeit jeder Gerichtsverhandlung schützt die Beteiligten davor, bestimmte ganz persönliche Angelegenheiten vor Zuhörerinnen und Zuhörern erörtern zu müssen; sie dient hingegen nicht der Geheimhaltung der Tatsache, daß die Parteien ein Familienrechtsverfahren führen.

5. Bürgerämter

5.1 Bürgerämter - Service nur mit Datenschutz

Mit Begriffen wie "Bürgeramt", "Bürgerbüro", "Bürgerservice" und "Zentrale Anlauf- und Beratungsstelle" werden Datenverarbeitungen in den Kommunen umschrieben, mit denen zahlreiche unterschiedliche Aufgabenstellungen der Verwaltung zur Erledigung in einer Stelle vereinigt werden. Bei sogenannten neuen Steuerungsmodellen, die die überkommenen Ämter- und Dezernatsstrukturen in der Verwaltung auflösen, finden sich die unterschiedlichen Aufgabenstellungen in anderen Organisationseinheiten mit anderen Bezeichnungen wieder. Nach einer Reihe von Kontrollbesuchen bleibt allerdings festzuhalten, daß eine **Vergleichbarkeit** derartiger Einrichtungen in ihrer Datenverarbeitung **nicht** gegeben ist. Selbst dort, wo eine Gemeinde sich die Organisation und Aufgabenstellung des Bürgeramtes einer anderen Gemeinde zum Vorbild genommen hatte, war aufgrund der anderen räumlichen Verhältnisse und des anders gewählten Aufgabenzuschnitts eine Vergleichbarkeit nicht vorhanden. Das einheitliche "Bürgeramt" gibt es nicht. Gleichwohl wird aus Vereinfachungsgründen im folgenden für alle derartigen Einrichtungen synonym der Ausdruck "Bürgeramt" verwandt. Auffällig war, wie gering vor lauter Umorganisation und Serviceorientierung oft das Bewußtsein für den Datenschutz in den Bürgerämtern war. Allerdings gehört zu einem ganzheitlichen Service für die Bürgerinnen und Bürger auch eine Datenverarbeitung, die dem Recht auf informationelle Selbstbestimmung Rechnung trägt.

5.1.1 Das neue Melderecht

Kernbereich der Datenverarbeitung der Bürgerämter sind stets die Aufgaben der bisherigen Einwohnermeldeämter. Durch die im Jahre 1997 vorgenommene Novellierung des Meldegesetzes für das Land Nordrhein-Westfalen (Meldegesetz NW – MG NW) sind in erfreulichem Umfang Datenschutzgrundsätze und klarstellende Datenverarbeitungsregelungen in das Gesetz aufgenommen worden.

- So ist beispielsweise zu begrüßen, daß die Übermittlung von Daten der Einwohnerinnen und Einwohner an **Adreßbuchverlage** ab dem 01. Januar 1999 nur noch mit schriftlicher Einwilligung der Betroffenen möglich ist (§ 35 Abs. 4 MG NW).

- Weiter ist die Handhabung der gesetzlichen **Auskunftssperren** klarstellend geregelt worden (vgl. § 34 Abs. 8 MG NW).

- Außerdem ist eine Nutzung der Meldedaten zur Information der betroffenen Einwohnerinnen und Einwohner **über Veranstaltungen** Dritter, wie etwa Caritas, AWO, Heimatvereinen und ähnlichen Einrichtungen, nunmehr ausdrücklich im Gesetz vorgesehen (§ 34 Abs. 4 MG NW).

- Schließlich ist der **Umfang des Auskunftsrechts** der Einwohnerinnen und Einwohner deutlich erweitert worden. Die Betroffenen erhalten auch Auskunft über den Zweck und die Rechtsgrundlage der Datenspeicherung, sowie - außer in den Fällen der einfachen Melderegisterauskunft - über die Empfängerinnen und Empfänger von Übermittlungen (§ 9 Abs. 1 MG NW).

Allerdings sind damit nicht alle Datenschutzprobleme des Melderechts gelöst worden.

- Die Datenschutzbeauftragten des Bundes und der Länder fordern in ihrer Entschließung vom 5./6.10.1998 zur Weitergabe von Meldedaten an Adreßbuchverlage und Parteien (Abdruck im Anhang, Nr. 10) gesetzliche Änderungen, nach denen **Gruppenauskünfte** an **politische Parteien** nur mit schriftlicher **Einwilligung** der betroffenen Einwohnerinnen und Einwohner zuzulassen sind. Die derzeit vorhandene Widerspruchsmöglichkeit ist den Betroffenen zumeist nicht bekannt und kann deshalb auch nicht wahrgenommen werden (vgl. § 35 Abs. 1 MG NW). Es bleibt den Gemeinden allerdings unbenommen, das ihnen gesetzlich eingeräumte Ermessen in der Weise auszuüben, daß sie - unter Wahrung des Gleichbehandlungsgrundsatzes - **keiner** Partei Melderegisterauskünfte zukommen lassen. Bedauerlicherweise hat das Ministerium für Inneres und Justiz in seiner Antwort auf eine kleine Anfrage (Drs. 12/3292) die Rechtsauffassung vertreten, Datenschutzgesichtspunkte dürften bei dieser Ermessensausübung keine Rolle spielen, da es ja das Widerspruchsrecht gäbe. Dies überzeugt nicht und steht auch nicht in Einklang mit der verwaltungsgerichtlichen **Rechtsprechung**: "Die Behörde darf dem Datenschutz gleichwohl Vorrang einräumen, weil sie damit auch die Bürger zu schützen vermag, die mangels Kenntnis der Rechtslage keinen Widerspruch haben eintragen lassen" (OVG Magdeburg, RDV 1998, 219).

- Auf die Datenerhebung durch Meldescheine von **inländischen** Besucherinnen und Besuchern in **Beherbergungsstätten** für polizeiliche Zwecke (vgl. § 27 MG NW) könnte als letztes Relikt polizeistaatlicher Datenverarbeitung durchaus verzichtet werden.

- Wenig überzeugend ist weiter die Regelung über die **Hauptwohnung** von den in Ausbildung befindlichen Bürgerinnen und Bürgern, denen der Staat zumutet, bei der Aufnahme der Ausbildung und bei jedem Wechsel der Ausbildungsstätte eine Veränderung der Hauptwohnung vorzunehmen, obwohl ein fester Lebensmittelpunkt in der Heimatgemeinde vorhanden ist. Diese letztlich auch für die beteiligten Stellen überflüssige Datenverarbeitung wird ärgerlich, wenn gleichzeitig der Staat seine Bediensteten bei Aus- und Fortbildung in der Frage der Hauptwohnung durch eine Sonderregelung (§ 24 Abs. 2 MG NW) privilegiert.

Bedauerlich ist weiterhin, daß durch die Erweiterung des Kreises der onlineabrufberechtigten öffentlichen Stellen in der Verordnung über die Zulassung der regelmäßigen Datenübermittlung von Meldebehörden an andere Behörden oder sonstige öffentliche Stellen (**Meldedatenübermittlungsverordnung NW** - MeldDÜV NW) vom 16. September 1997 die Tendenz fortgesetzt wurde, das Einwohnermelderegister zum Mittelpunkt eines vom Landesgesetzgeber so nicht geplanten übergreifenden Einwohnerinformationssystems zu machen. Zu begrüßen ist demgegenüber die Anlage zur **Verordnung zur Durchführung** des **Meldegesetzes** für das Land Nordrhein-Westfalen (DVO MG NW) vom 16. September 1997. Die Formblätter für die Datenerhebung und weitere Datenverarbeitung der Meldebehörden wurden völlig neu gestaltet. Durch ausführliche Belehrungen wurde die Transparenz der Datenverarbeitung der Meldebehörden erhöht und eine ausreichende Unterrichtung der Betroffenen über ihre Datenschutzrechte sichergestellt. Mit dem Erlaß der **Verwaltungsvorschriften zur Durchführung des Meldegesetzes NW** (VV MG NW; RdErl. d. Ministeriums für Inneres und Justiz vom 02.10.1998 - I A 6/41.12 -, MBl. NW. 1998, S. 1149) ist es endlich gelungen, die für die Praxis der Datenverarbeitung der Einwohnermeldeämter seit 1983 fehlenden erläuternden Hinweise zum Meldegesetz zu schaffen. Zahlreiche Datenschutzprobleme aus der Anwendung des Melderechts in der Vergangenheit sind damit gelöst und einer landesweit einheitlichen Handhabung zugeführt worden.

- So ist etwa der Wahrung des **Adoptionsgeheimnisses** große Aufmerksamkeit geschenkt worden. Damit ist die Gefahr, daß durch fehlerhafte Datenverarbeitung ein Adoptionsverhältnis oder ein Adoptionspflegeverhältnis aufgedeckt wird, deutlich verringert worden.

- Weiter wurde klargestellt, daß Melderegisterauskünfte grundsätzlich aus dem **aktuellen Melderegisterbestand** zu erteilen sind. Auskünfte aus dem gesonderten (Alt-)bestand des Einwohnermelderegisters sind mit einem entsprechenden Hinweis zu kennzeichnen.

- Auch die Unsicherheiten in der Praxis bei der Eintragung einer **Auskunftssperre,** ihrer Dauer, der Rechtswirkungen und des Verfahrens bei der Aufhebung sind für viele Fallkonstellationen in begrüßenswerter Klarheit beseitigt worden.

An einem Beispielsfall wird allerdings auch deutlich, daß noch so datenschutzfreundliche Regelungen im Melderecht ihre weniger datenschutzfreundliche Anwendung im Einzelfall nicht verhindern können: Ein über 80 Jahre alter Mitbürger mosaischen Glaubens hatte sich dagegen gewandt, daß - anders als früher - bei seinem Datensatz die Religionsangabe "jüdisch (israelitisch, mosaisch)" gespeichert wurde und verlangte die Löschung dieser Angaben. Das - frühere - Innenministerium vertrat den Standpunkt, daß die Verpflichtung zur Speicherung der Religionszugehörigkeit alle Bürgerinnen und Bürger des Landes Nordrhein-Westfalen in gleicher Weise träfe und hielt eine Löschung nicht für gerechtfertigt. Allerdings wäre die Befürwortung der Löschung rechtlich ebenso vertretbar gewesen. Dafür wären lediglich die Erfahrungen des Betroffenen und das Schicksal seiner Familie in der Zeit des Nationalsozialismus sowie seine Befürchtungen im Hinblick auf die Zahl von Straftaten mit antisemitischem Hintergrund als schutzwürdige Belange im Sinne des § 7 MG NW zu berücksichtigen gewesen.

Die Meldebehörden bleiben daher aufgerufen, nicht die **Einzelfallgerechtigkeit** aus den Augen zu verlieren.

5.1.2 Datenschutz im Bürgeramt

5.1.2.1 Aufgabenzuweisung

Datenschutzrechtlich problematisch ist die Zusammenfassung verschiedener Aufgabenstellungen an einem Arbeitsplatz, wenn dort vollständig die abschließende Sachbearbeitung erfolgen soll. Ist in einem Aufgabengebiet die Übermittlung von personenbezogenen Daten an andere Stellen nur bei Vorliegen bestimmter gesetzlicher Voraussetzungen möglich, so wird diese gesetzliche Vorgabe unterlaufen, wenn die Verarbeitung der unterschiedlichen Datenbestände auf einem Arbeitsplatz zusammengeführt wird. Eine beliebige Zusammenführung von unterschiedlichen Aufgabenstellungen kann auch nicht auf die **Organisationshoheit der Gemeinde** gestützt werden, da die Grenzen der Organisationshoheit von den gesetzlichen Bestimmungen gezogen werden, auch von denjenigen über die Datenverarbeitung. Wenn etwa die Zusammenführung von Aufgaben in einer Stelle erst die Notwendigkeit von Datensicherungsmaßnahmen, wie etwa Abschottung, entstehen läßt, gleichzeitig die Personalausstattung solche Maßnahmen jedoch nicht zuläßt, so stellt eine die Zusammenführung gleichwohl verfügende Organi-

sationsentscheidung der Gemeinde eine Umgehung der gesetzlichen Datenverarbeitungsvorgabe dar und dürfte damit rechtswidrig sein (vgl. hierzu auch 10. Tätigkeitsbericht, Seiten 45 - 47).

Bei einer der kontrollierten Gemeinden konnte erreicht werden, daß solche Bereiche, deren Übertragung zur vollständigen Sachbearbeitung im Bürgeramt ansonsten unzulässig gewesen wäre, nunmehr an getrennten Arbeitsplätzen im Großraumbüro des Bürgeramtes angesiedelt werden. Hierdurch wird aus der bisherigen Organisation des Bürgeramtes gleichsam ein "**Marktplatz**" , auf dem bei verschiedenen **"Ständen"** die Bürgerinnen und Bürger ihre jeweiligen Anliegen erledigen können. Wie das Besprechungsergebnis mit der Gemeinde gezeigt hat, dürfte dies wegen der nach wie vor bestehenden räumlichen Integration im Bereich Bürgeramt **keine Abstriche im Bürgerservice** bedeuten. Gleichzeitig wird jedoch eine Datenverarbeitung unter Wahrung der Datenschutzrechte der Betroffenen ermöglicht.

5.1.2.2 Rahmenbedingungen

Die Gewährleistung eines ausreichenden Datenschutzes in den Bürgerämtern erfordert entsprechende Rahmenbedingungen. So sind **innerbehördliche Regelungen zum Datenschutz** zu erlassen, also mindestens Regelungen in Form einer Dienstanweisung Datenschutz, einer Dienstanweisung ADV und einer Aktenordnung. Unverzichtbar sind auch Regelungen zur **internen Datenschutzkontrollinstanz.** Es reicht nicht aus, die genannten Vorschriften zu erlassen, ihre Einhaltung muß vielmehr auch kontrolliert werden. Deshalb ist die Bestellung einer oder eines internen Datenschutzbeauftragten wichtig. Entscheidend ist dabei allerdings nicht nur, daß es eine solche Person und Stelle gibt, sondern auch, daß der Arbeitsplatz mit dieser Aufgabenstellung so geschnitten ist, daß die Durchführung der Kontrollen auch tatsächlich möglich ist. Bei einer Stelle, bei der die genannten Regelungen gar nicht oder nur mit veraltetem Inhalt vorhanden sind, geht deshalb die Bestellung eines Datenschutzbeauftragten mit einem 10%igen Arbeitszeitanteil weit an der tatsächlichen Notwendigkeit des Arbeitsaufwandes vorbei.

5.1.2.3 Datensicherungsmaßnahmen

Die Zusammenführung unterschiedlicher Aufgaben an einem Sachbearbeitungsplatz verlangt zusätzliche technische und organisatorische Datensicherungsmaßnahmen, um eine datenschutzkonforme Datenverarbeitung gewährleisten zu können. Nur die zwei häufigsten, aber zugleich in aller Regel auch am einfachsten zu lösenden Schwierigkeiten sollen kurz benannt werden.

- Die Unterbringung von Bürgerämtern in einem **Großraumbüro** wirft datenschutzrechtliche Probleme hinsichtlich der Gewährleistung der **Vertraulichkeit von Gesprächen** auf. Es ist zu verhindern, daß Unbefugte Beratungsgespräche von Sachbearbeiterinnen und Sachbearbeitern mithören können. Dies setzt eine ausreichende akustische Isolierung der Arbeitsplätze untereinander voraus.

- Oft ist es den Besucherinnen und Besuchern nicht möglich, die für ihr Anliegen notwendigen **Formulare ausfüllen** zu können, ohne daß eine andere wartende Person von dem ausgefüllten Inhalt des Formulars Kenntnis nehmen kann.

5.2 Neue Steuerungsmodelle

Die für die Einrichtung von Bürgerämtern aufgezeigten Datenschutzprobleme treten verstärkt dann auf, wenn die Gemeindeverwaltung insgesamt und unter Verzicht auf die bisherige Ämter- und Aufgabenstruktur neu geordnet wird. Es besteht daher die Notwendigkeit, in Vorbereitung und vor Einführung eines Neuen Steuerungsmodells eine Analyse vorzunehmen, inwieweit die Organisationsentscheidungen in diesem Modell mit dem Datenschutzrecht in Einklang zu bringen sind. Ein Vergleich mit der Datenverarbeitungssituation in den (alten) Fachämtern und den (neuen) Fachbereichen ist angezeigt, um festzustellen, durch welche neuen, anderen oder zusätzlichen Maßnahmen in den veränderten Organisationsstrukturen des Neuen Steuerungsmodells ein gleichwertiger **Datenschutz-** und **Datensicherheitsstandard** zu gewährleisten ist.

Bereits das Bundesverfassungsgericht hat in seinem Beschluß vom 18. Dezember 1987 (NJW 1988, 959) ohne Beschränkung auf einzelne Aufgabenbereiche der Gemeinde herausgestellt, daß der Grundsatz der informationellen Gewaltenteilung auch innerhalb der Gemeindeverwaltung gilt; aus der Einheit der Gemeindeverwaltung folgt **keine informationelle Einheit**. Bei einem Neuen Steuerungsmodell muß daher verhindert werden, daß durch Zusammenführung von Datenverarbeitungsaufgaben auf "allzuständigen" Arbeitsplätzen die Möglichkeit entsteht, **Persönlichkeitsprofile** über die betroffenen Bürgerinnen und Bürger zu erstellen. Die wünschenswerte Ausweitung des Bürgerservices darf der Verwaltung nicht gleichzeitig die Möglichkeit verschaffen, dieselben Bürgerinnen und Bürger "gläsern" zu machen.

6. Ausländerinnen und Ausländer

6.1 Ausländerzentralregister

Das Ausländerzentralregistergesetz liegt dem Bundesverfassungsgericht zur verfassungsrechtlichen Prüfung vor.

Zentrale Sammelstelle für die personenbezogenen Daten der Ausländerinnen und Ausländer ist das Ausländerzentralregister. Die Datenschutzbeauftragten des Bundes und der Länder haben sich dagegen gewandt, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dient, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung steht (Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zum Ausländerzentralregistergesetz - abgedruckt im 12. Tätigkeitsbericht, Seite 170 f). Diese Ausweitung schwächt die datenschutzrechtliche Position der Ausländerinnen und Ausländer in besonderer Weise. Zwischenzeitlich ist gegen das Ausländerzentralregistergesetz eine **Verfassungsbeschwerde** erhoben worden, über die bislang noch nicht entschieden ist.

6.2 Der Echtheitsgrad von Ehen

Binationale Ehepaare sehen sich häufig dem Mißtrauen ausgesetzt, ihre Ehe nur wegen der damit verbundenen günstigeren aufenthaltsrechtlichen Folgen geschlossen zu haben. Bezeichnet werden solche Ehen dann als sogenannte Scheinehen. Deutschen Ehepaaren, die aus Gründen steuerlicher Vergünstigungen geheiratet haben, bleiben solche Vorwürfe erspart.

Auf die Datenverarbeitungsprobleme bei der Feststellung von sogenannten Scheinehen wurde bereits im 13. Datenschutzbericht (Seite 59/60) hingewiesen. Es gibt bundesweit in den Ländern in diesem Zusammenhang keine einheitliche Handhabung, ob und welche Daten über die betroffenen Ausländerinnen und Ausländer und ihre deutschen Ehegattinnen und Ehegatten erhoben, gespeichert und übermittelt werden.

Durch das Gesetz zur Neuordnung des Eheschließungsrechts, das am 1. Juli 1998 in Kraft getreten ist, wird durch die Neufassung der §§ 1314 und 1310 BGB der "Fahndungsdruck" auf binationale Ehen noch erhöht. So muß die Standesbeamtin oder der Standesbeamte die Mitwirkung an der Eheschließung verweigern, wenn offenkundig ist, daß die Ehe aufhebbar

wäre, weil beide Eheleute sich bei der Eheschließung darüber einig waren, daß sie keine Verpflichtung zu einer ehelichen Lebensgemeinschaft begründen wollten. Die Neuregelung wirft beispielsweise die datenschutzrechtlichen Fragen auf, welche Datenerhebungsbefugnis die Standesbeamtin oder der Standesbeamte für die Prüfung der genannten Umstände hat und welche Übermittlungsbefugnis das Standesamt hinsichtlich der Ermittlungsergebnisse gegenüber der Ausländerbehörde hat. Die Neuregelung gibt dem Standesamt **kein beliebiges Nachforschungsrecht**. Es muß sich vielmehr um äußere, konkrete tatsächliche Anhaltspunkte handeln, aus denen sich der mangelnde Wille zu einer Ehegemeinschaft unmittelbar und nachhaltig aufdrängt. Eine Datenerhebung im Standesamt nach § 5 Abs. 4 des Personenstandsgesetzes hat daher nur die Funktion, den konkreten Verdacht zu erhärten. Nur in diesen Fällen könnte auch eine Datenübermittlung nach § 76 Abs. 2 des Ausländergesetzes an die zuständige Ausländerbehörde in Betracht kommen.

Mehrere Kontrollbesuche ergaben eine unterschiedliche Praxis der Datenverarbeitung in den Ausländerbehörden. So erreichte etwa eine Ausländerbehörde die Aufklärung von Verdachtsfällen ohne zusätzliche Datenerhebung, während eine andere Ausländerbehörde binationale Ehen einer Sonderdatenverarbeitung mit Fragebögen, Hausbesuchen und Befragungen Dritter unterzog. Um insoweit landesweit zu einer datenschutzkonformen Handhabung des Problems zu gelangen, war das - frühere - Innenministerium gebeten worden, die bei den Kontrollen deutlich gewordenen diskriminierenden Auswüchse in der Überprüfungspraxis zu beseitigen und durch einen Erlaß oder Richtlinien einen einheitlichen Datenschutzstandard für Eheleute binationaler Ehen bei der Datenverarbeitung der Ausländerbehörden zu gewährleisten.

Obgleich dem Ministerium auch die kontrollierten Stellen benannt worden sind, ist - soweit bekannt - bislang nichts geschehen, um die dortige Praxis, aber auch die landesweite Handhabung datenschutzgerecht zu gestalten.

6.3 Gläserne Gastgeberinnen und Gastgeber

Besucherinnen und Besucher aus dem Ausland kamen bis vor kurzem kaum daran vorbei, regelmäßig die Höhe des Einkommens und Vermögens, den Beruf, Arbeitgeber und die Wohnverhältnisse ihrer Gastgeberinnen und Gastgeber vor Reiseantritt kennenzulernen.

Nach § 84 Abs. 2 Satz 1 in Verbindung mit Abs. 1 des Ausländergesetzes (AuslG) haben sich Gastgeberinnen und Gastgeber gegenüber der Ausländerbehörde oder einer Auslandsvertretung zu verpflichten, die Kosten für

den Lebensunterhalt ihres ausländischen Besuchs zu tragen. Dies setzt eine Prüfung der finanziellen Leistungsfähigkeit der Gastgeberinnen und Gastgeber voraus, die sogenannte **Bonitätsprüfung**. Sehr häufig handelt es sich bei diesem Personenkreis um deutsche Staatsangehörige ausländischer Herkunft, die Verwandte oder Bekannte einladen.

Während in der Vergangenheit die Angaben zur Bonität in dem Formular enthalten waren, dessen Inhalt auch dem Gast bei der Beantragung des Visums zur Kenntnis kam, ist es durch Mitwirkung des - früheren - Innenministeriums gelungen, daß nunmehr Angaben zu Beruf und Arbeitgeber der Einladenden nicht mehr in den Verpflichtungserklärungen enthalten sind, ebenso wie die Angaben über die Wohnverhältnisse, das Einkommen und das vorhandene Vermögen. Erforderlich ist inzwischen allein, daß entsprechende **Unterlagen** der Ausländerbehörde **vorgelegt** werden und diese das Vorliegen der Bonitätsanforderungen in der Akte **vermerkt** und begründet. Dieser Datenschutzfortschritt ist **ausdrücklich zu begrüßen**.

6.4 Familienzusammenführung mit unzulänglichem Datenschutz

Ausländerinnen und Ausländer, die einen Anspruch auf Familienzusammenführung haben, wird auf ihren eigenen Antrag hin ermöglicht, fehlende Standesamtspapiere über die bestehenden Verwandtschaftsverhältnisse zu ersetzen durch ein Gutachten auf der Grundlage einer **DNA-Analyse**. So werden zum Nachweis von Verwandtschaftsverhältnissen sogenannte **Speicheltests** im Heimatland der Betroffenen durchgeführt und von einem Institut einer nordrhein-westfälischen Universität untersucht. Dort werden unter anderem personenbezogene Daten wie etwa Familienname, Vorname, Geburtsdatum, Geburtsort, Wohnort, Paßnummer, Ausstellungsdatum des Passes, Ausstellungsbehörde des Passes, Gültigkeitsdatum des Passes, besondere Kennzeichen, Fingerabdrücke und Fotos der Betroffenen gespeichert.

Die Datenverarbeitung begegnet im einzelnen folgenden Bedenken: Das verwendete Antragsformular enthält nicht, wie es § 4 Satz 3 DSG NW verlangt, einen besonderen Hinweis auf die Einwilligung in die Datenverarbeitung. Auch fehlt ein Hinweis darauf, daß die Betroffenen die Einwilligung mit Wirkung für die Zukunft widerrufen können. Einwilligungserklärungen derjenigen Personen, deren Speichel in Zusammenhang mit dem Antrag auf Familienzusammenführung ebenfalls untersucht wird, fehlen ganz. Der Grundsatz der Transparenz der Datenverarbeitung ist zudem verletzt, da im Rahmen des Verfahrens keine ausreichende Information sowohl der antragstellenden als auch der anderen mitbetroffenen Personen über die weitere

Verarbeitung der personenbezogenen Daten im Institut und insbesondere deren Löschungszeitpunkt erfolgt.

Die Daten der betroffenen Personen einschließlich der personenbezogenen Daten im Gutachten werden für einen Zeitraum von 30 Jahren gespeichert. Benötigt werden diese Daten regelmäßig jedoch nur, bis die Entscheidung über die Familienzusammenführung rechtskräftig ist. Sollte ausnahmsweise eine weitere Aufbewahrung im Interesse der Betroffenen liegen, ist dafür eine wirksame Einwilligung aller Betroffenen einzuholen. Das Einwilligungserfordernis gilt auch für den Fall, daß die gespeicherten Daten von dem Universitätsinstitut oder anderen Stellen zu Forschungszwecken genutzt werden sollen.

6.5 EURODAC

Ein europaweites Fingerabdruckvergleichssystem soll alle asylbeantragenden Personen erfassen.

Im Berichtszeitraum ist der Entwurf eines Übereinkommens über die Einrichtung von "EURODAC" für den Vergleich von Fingerabdrücken vorgelegt worden. In einer europaweiten **zentralen Datenbank** sollen danach die **Fingerabdrücke aller Asylbewerberinnen und Asylbewerber** gespeichert und miteinander abgeglichen werden. Die Dauer der Speicherung beträgt in der Regel 10 Jahre ab dem Zeitpunkt der letzten Abnahme der Fingerabdrücke. Zweckbestimmung von "EURODAC" ist die Unterstützung bei der Bestimmung des Mitgliedstaates der Europäischen Union, der für die Prüfung eines in einem Mitgliedstaat gestellten Asylantrags zuständig ist. Nach einem Vorbehalt der Deutschen Delegation sollen die Mitgliedstaaten **auch** zur Abnahme der **Fingerabdrücke illegal einwandernder Personen** verpflichtet sein.

- Der Entwurf enthält zwar eine strikte Zweckbindungsregelung, Vorschriften zum umfassenden und wirksamen **Schutz vor Zweckentfremdung fehlen** jedoch.

- Die von der **Deutschen Delegation** verlangte Verpflichtung der Abnahme und Meldung von Fingerabdrücken auch der **illegal einwandernden Personen** macht deutlich, daß entgegen der ursprünglichen Zweckbestimmung der Zentraldatei "EURODAC" letztlich auch alle Ausländerinnen und Ausländer in dem System erfaßt werden sollen, deren Aufenthalt nicht im Einklang mit den innerstaatlichen Regelungen der Mitgliedstaaten steht. Denkbar wäre etwa, daß bereits Zweifel an der Gültigkeit eines Visums, die Überschreitung der Zeitdauer eines Vi-

sums oder ähnliches die betroffene Person zu einem "illegalen Einwanderer" machen könnte, dessen Fingerabdrücke in "EURODAC" 10 Jahre lang gespeichert werden könnten.

- Die Notwendigkeit der Aufbewahrung der gespeicherten Daten über einen Zeitraum von 10 Jahren ist nicht belegt. Auffällig ist allerdings, daß die **Aufbewahrungsdauer** der gespeicherten Daten von 10 Jahren in "EURODAC" übereinstimmt mit der Aufbewahrungsdauer der personenbezogenen Daten im polizeilichen Informationssystem INPOL und im Informationssystem der Verfassungsschutzbehörden NADIS.

- Eine **vorzeitige Löschung** kommt nur beim Erwerb der Staatsangehörigkeit eines Mitgliedstaates in Betracht, nicht jedoch, wenn die Asylanerkennung rechtskräftig und eine Aufenthaltserlaubnis erteilt wird. Die Erforderlichkeit einer weiteren 10jährigen Speicherung dieses Personenkreises ist nicht erkennbar.

Insgesamt ist der Entwurf des Übereinkommens für "EURODAC" nicht akzeptabel. Es bleibt zu hoffen, daß Datenschutzaspekte noch Eingang finden.

7. Sozialbereich

Das in § 35 des Ersten Buches des Sozialgesetzbuches (SGB I) verankerte **Sozialgeheimnis bröckelt**. Mit einer im Medizinproduktegesetz versteckten Vorschrift wurde eine dort völlig sachfremde Materie geregelt. Ohne nähere Prüfung der Erforderlichkeit und ohne klare Spezifizierung des Auskunftsinteresses gewährt der geänderte § 68 des Zehnten Buches des Sozialgesetzbuches (SGB X) Ordnungs- und Polizeibehörden sowie Staatsanwaltschaften, Gerichten und Justizvollzugsanstalten einen viel zu weit gefaßten Auskunftsanspruch gegenüber den Sozialleistungsträgern. Das bedeutet, daß zum Beispiel Jugend-, Sozial- oder Versorgungsämter, aber auch Krankenkassen oder Berufsgenossenschaften diesen Behörden Auskunft über die Anwesenheit oder über künftige Vorsprachetermine von Bürgerinnen und Bürgern zu geben haben. Zusammen mit anderen Datenschutzbeauftragten habe ich mich vehement gegen diese Regelung ausgesprochen und die Ministerin für Frauen, Jugend, Familie und Gesundheit sowie den Minister für Inneres und Justiz gebeten, sich im Bundesrat für eine Ablehnung dieser Regelung mit dem Ziel, den Vermittlungsausschuß anzurufen, einzusetzen. In einer mit lebhaftem Echo aufgenommenen Presseerklärung habe ich gemeinsam mit anderen Datenschutzbeauftragten vor der Einführung dieser Neuregelung gewarnt, die die Sozialleistungsträger faktisch zu "Hilfsbeamtinnen und Hilfsbeamten" der Sicherheitsbehörden macht.

Kontrolle und Überwachung von Bürgerinnen und Bürgern sind leider auch im übrigen Sozialbereich **weiter verstärkt** worden - eine unerfreuliche Tendenz. Sofern Bedürftige Leistungen nach dem Bundessozialhilfegesetz (BSHG) beziehen, müssen sie etwa damit rechnen, daß ihre gespeicherten Sozialdaten mit Daten anderer Träger der Sozialhilfe, der Bundesanstalt für Arbeit und der gesetzlichen Unfall- und Rentenversicherung in **automatisierten Abgleichsverfahren** überprüft werden. Diese Regelung beruht auf § 117 BSHG sowie der zur Ausführung dieser Vorschrift erlassenen und am 1. Januar 1998 in Kraft getretenen **Sozialhilfedatenabgleichsverordnung.** Darüber hinaus hat eine Arbeitsgruppe im Auftrag der Arbeits- und Sozialministerkonferenz von Bund und Ländern zahlreiche Vorschläge für **weitere Datenabgleichsmöglichkeiten** erarbeitet. Die Datenschutzbeauftragten des Bundes und der Länder haben ihre Bedenken dagegen in einer gemeinsamen Entschließung vom 20.10.1997 formuliert (Abdruck im Anhang, Nr. 3).

In anderen Bereichen gibt es dagegen **positive Entwicklungen.** So hat beispielsweise das - damalige - Ministerium für Arbeit, Gesundheit und Soziales erfreulicherweise frühzeitig datenschutzrechtliche Unterstützung für seine **Initiative "Jugend in Arbeit"** nachgefragt. Mit diesem Vorhaben sollten

längere Zeit beschäftigungslose Jugendliche, darunter auch viele Sozialhilfeempfängerinnen und Sozialhilfeempfänger, gezielt angesprochen werden, um Beratung, berufliche Qualifizierungsmöglichkeiten und Hilfen zum Berufseinstieg zu erhalten. Um die Betroffenen wie geplant zu erreichen, war - anders als es ein Pressebericht darstellte - keine "Datenschutz-Hürde" zu überwinden.

7.1 Sozialämter schießen über das Ziel hinaus

Hilfesuchende müssen oft bereits bei Antragstellung Unterlagen mit vorformulierten Erklärungen unterschreiben, damit das Sozialamt Auskünfte über Kontenbewegungen bei Banken oder Sparkassen einholen kann. Obwohl schon früher wiederholt auf die Unzulässigkeit solcher Ansinnen hingewiesen wurde, scheint diese Praxis wieder zuzunehmen.

Sozialhilfe erhält nicht, wer sich selbst helfen kann. Hilfesuchenden obliegt es, die Voraussetzung eines Sozialhilfeanspruchs im einzelnen nachzuweisen. Verbleibende Zweifel gehen zu Lasten der Antragstellerinnen und Antragsteller. Nur wenn es **zwingend** erforderlich ist, kann das Sozialamt verlangen, daß bei Kreditinstituten Auskünfte über etwaige Kontobelastungen oder -guthaben eingeholt werden können. Die Entscheidung darüber kann grundsätzlich **erst nach Erhalt und Auswertung der Antragsunterlagen** getroffen werden. Folglich kann frühestens zu diesem Zeitpunkt ersichtlich sein, ob und inwieweit eine über die Selbstauskunft und die bisher vorgelegten Nachweise hinausreichende besondere Mitwirkung der Betroffenen erforderlich ist. Die Praxis verschiedener Sozialämter, Hilfesuchenden im Zusammenhang mit jeder Sozialhilfebeantragung **regelmäßig** Auskunftsermächtigungen abzuverlangen, stellt daher eine überflüssige Ermittlungsmaßnahme dar. In einem solchen Zusammenhang können derartige Auskunftsermächtigungen auch nicht "auf freiwilliger Basis" erteilt werden, da die Hilfesuchenden auf die Sozialhilfe angewiesen sind und somit in eine Zwangslage geraten, in der von einer tatsächlichen freiwilligen Entscheidung keine Rede mehr sein kann. Solche "Einwilligungserklärungen" wären also unwirksam.

Zwar benötigen Sozialämter insbesondere Angaben über Höhe und Herkunft etwaiger regelmäßig wiederkehrender Geldzuflüsse, um prüfen zu können, ob Hilfesuchende ihren Lebensunterhalt aus eigenem Einkommen und Vermögen bestreiten können. Jedoch haben sie unter mehreren gleichermaßen erfolgversprechenden Möglichkeiten eines Vermögensnachweises stets diejenige zu wählen, die die Hilfesuchenden am wenigsten belastet. Dies bedeutet, daß Hilfesuchenden **zunächst** Gelegenheit gegeben werden muß,

Kontoauszüge vorzulegen, statt eine Auskunftsermächtigung zu erteilen. Insoweit ist die Anforderung von Kontoauszügen über einen zurückliegenden Zeitraum von drei bis sechs Monaten sachgerecht und verhältnismäßig. Eine **Aufbewahrung** der Kontoauszüge oder Kopien in der Akte ist nur zulässig, soweit dies zur Aufgabenerfüllung erforderlich ist. Im Regelfall dürfte ein Aktenvermerk über die getroffenen Feststellungen ausreichen. Die Soll-Posten können von Antragstellerinnen und Antragstellern grundsätzlich geschwärzt werden, worauf sie ausdrücklich hinzuweisen sind. In Einzelfällen, insbesondere bei hohen Sollbuchungen oder konkretem Mißbrauchsverdacht, mag eine Offenlegung der Soll-Posten erforderlich sein. **Auskunftsermächtigungen** müssen die **Ausnahme** bilden. Sollten sie im Einzelfall notwendig sein, haben sie eindeutig zu bezeichnen, welche Daten - zum Beispiel Kontostände einzeln aufgeführter Konten über einen bestimmten Zeitraum - bei welchem Kreditinstitut erfragt werden sollen und welche Rechtsfolgen bei einer Verweigerung eintreten können.

Das Sozialamt darf von den Hilfesuchenden erst dann eine Auskunftsermächtigung verlangen, wenn sich bei der Bearbeitung des Einzelfalles eine Auskunftserteilung durch Dritte als unumgänglich erweist. Dies kann der Fall sein, wenn die Prüfung der Antragsunterlagen ergibt, daß die eingereichten Nachweise die Angaben im Antrag nicht ausreichend belegen und Hilfesuchende nicht mehr weiter zur Aufklärung beitragen.

7.2 Prüfung von Pflegeleistungen

Auch wer auf Pflegeleistungen angewiesen ist, hat das Recht einer Intimsphäre.

Bei Gewährung von Hilfe zur Pflege nach dem Bundessozialhilfegesetz hat ein Sozialamt in bestimmten Bedarfsfällen ein besonderes Abrechnungsverfahren gewählt. Es zwingt die betroffenen Bürgerinnen und Bürger dazu, die Bekanntgabe von in ihren Intimbereich fallenden Einzelpflegeleistungen an das Sozialamt hinzunehmen. Wollen sie dies nicht, müssen sie mit der Versagung der Leistungsvergütung rechnen. Vor diesem Hintergrund fordern die Leistungsabrechnungen regelmäßig eine genaue Beschreibung jeder einzelnen körperlichen Verrichtung, die eine pflegerische Hilfestellung verlangt, sei es selbst der Gang zur Toilette. Das Sozialamt hat die Notwendigkeit sogenannter "personenscharfer Leistungsdaten" damit begründet, daß ohne diese Abrechnungsart Grauzonen und unredliche Leistungsabrechnungen zu befürchten seien. Sie entspräche der Vereinbarung gemäß § 89 SGB XI über die Vergütung ambulanter Pflegeleistungen in Nordrhein-Westfalen.

Es steht außer Frage, daß die Erbringung von Pflegeleistungen kontrollierbar sein muß. Die detaillierte Beschreibung der den Intimbereich berührenden Pflegeleistungen geht jedoch zu weit. Dem Sozialamt wurden Vorschläge gemacht, wie die Abrechnung derartiger Leistungen gesetzeskonform auch pauschaliert erfolgen kann. Um Mißbrauchsfällen (zum Beispiel Schein- oder Doppelabrechnungen) auf die Spur zu kommen, lassen die bei den Pflegebedürftigen aufzubewahrenden Pflegedokumentationen im übrigen ausreichende Kontrollen zu. Amtsärztinnen und Amtsärzte des zuständigen Gesundheitsamtes können aus gegebenem Anlaß die Pflegedokumentationen einsehen. Das Ministerium für Arbeit, Soziales und Stadtentwicklung, Kultur und Sport wurde zusätzlich gebeten, im Aufsichtswege eine Änderung der Vereinbarung gemäß § 89 SGB XI herbeizuführen, um eine generelle Lösung für alle Betroffenen zu finden.

Erbrachte Pflegeleistungen müssen zwar vor ihrer Erstattung als Sozialleistung kontrolliert werden können. Die Kontrolldichte darf aber nicht so weit gehen, daß dem Sozialhilfeträger der Tagesablauf der zu Pflegenden minutiös bekannt wird und kein Handschlag mehr verborgen bleibt. Vergleichbare Maßstäbe gelten bei der Überprüfung von Pflegeleistungen nach dem Pflegeversicherungsgesetz (SGB XI): Das Gesetz erlaubt keine Einsichtnahme in die Pflegedokumentationen durch die Pflegekassen zur Kontrolle der Abrechnung ambulanter Pflegeleistungen. Bei Anhaltspunkten für qualitativ unzureichende Pflegeleistungen besteht nach den Bestimmungen des Rahmenvertrages über die ambulante pflegerische Versorgung gemäß § 75 SGB XI für das Land Nordrhein-Westfalen die Möglichkeit einer Qualitätsprüfung bei einem Pflegedienst. Zu diesem Zweck darf der Medizinische Dienst der Krankenversicherung (MDK), nicht jedoch die Pflegekasse selbst, die Pflegedokumentation einsehen.

7.3 Datenabrufe erfordern Übermittlungsbefugnisse

Die Versorgungsverwaltung hat ein Modellprojekt mit Versorgungsämtern und Kommunen gestartet, in dem eine verbesserte Zusammenarbeit bei der Bearbeitung von Schwerbehindertenangelegenheiten getestet und das Dienstleistungsangebot für Bürgerinnen und Bürger erweitert werden soll. Geplant ist, bei Kommunen Auskunfts- und Beratungsstellen einzurichten, die im Online-Verfahren bei den Versorgungsämtern gespeicherte Sozialdaten abrufen können.

Die beteiligten Stellen wurden darauf aufmerksam gemacht, daß jeder Datenabruf eine Übermittlung von Sozialdaten darstellt, die sich grundsätzlich auf Regelungen im Zweiten Kapitel des SGB X stützen lassen muß. Das automatisierte Abrufverfahren muß zusätzlich den besonderen technischen

und organisatorischen Anforderungen genügen und die schutzwürdigen Interessen der Ratsuchenden angemessen berücksichtigen (§§ 78 a, 79 SGB X). Entgegen der Ansicht der Projektverantwortlichen scheiden Aufgabenzuweisungsnormen wie etwa die Vorschrift des § 15 Abs. 3 SGB I, die ein Gebot zur Zusammenarbeit mit den anderen Leistungsträgern enthält, als Übermittlungsbefugnis aus. Zwar besteht die gesetzliche Aufgabe der Leistungsträger darin, Auskünfte über alle sozialen Angelegenheiten zu erteilen. Die Reichweite dieser Auskunft ist aber auf eine Wegweiserfunktion begrenzt und beinhaltet keine Sachentscheidungskompetenz. Aufgabe der Kommune ist es allein, Bürgerinnen und Bürger hinsichtlich der Verfahrensabläufe und Zuständigkeiten zu beraten und ihnen bei der Einleitung von Verwaltungsverfahren behilflich zu sein. Die Prüfung der materiellen Voraussetzungen eines schwerbehindertenrechtlichen Antrags obliegt dagegen den Versorgungsämtern. Es bedarf daher einer Änderung der Regelungen in der entsprechenden Zuständigkeitsverordnung.

Um gleichwohl die vorgesehene Datenverarbeitung im Interesse der Betroffenen - und begrenzt auf ein befristetes **Modellprojekt** - durchführen zu können, besteht die rechtliche Möglichkeit, im Rahmen eines Vertrages zwischen dem örtlich zuständigen Versorgungsamt und der jeweiligen Gemeinde diejenigen Gemeindebediensteten, die für die Mitwirkung am Modellprojekt vorgesehen sind, ausschließlich den Weisungen des jeweiligen Versorgungsamtes zu unterstellen. Außerdem ist ein umfassendes **Datensicherheitskonzept** unverzichtbar.

Erst wenn jede Einwirkungsmöglichkeit der Gemeinde ausgeschlossen ist und die Datensicherheitsanforderungen erfüllt sind, stehen dem Modellprojekt keine datenschutzrechtlichen Bedenken mehr entgegen.

7.4 Datenschutz bei den Krankenkassen

Die Krankenkassen sind im Umbruch. Dies sollte als Chance für eine Verbesserung des Datenschutzes genutzt werden.

Auch aus Wettbewerbsgründen und zur Verbesserung der Versichertenbetreuung werden gegenwärtig Anpassungen der Organisationsstrukturen der Krankenkassen vorgenommen. Die Datenschutzbeauftragten des Bundes und der Länder haben daher ein **Datenschutzkonzept für den Einsatz der Informationstechnik der Krankenkassen** entwickelt, das durch technische und organisatorische Vorkehrungen den Schutz vor Mißbrauch der bei den Krankenkassen gespeicherten Versichertendaten erhöhen kann. Datenbanksysteme mit großen Datenmengen sind grundsätzlich für viele Anwendungen nutzbar, zum Beispiel zur Durchführung von Wirtschaftlichkeitsunter-

suchungen, Auffälligkeitsprüfungen oder zu sonstigen Datenauswertungen (§§ 294 ff. SGB V). Die Versichertendaten dürfen aber nur im Rahmen der im einzelnen gesetzlich zugelassenen Zwecke **erhoben und gespeichert** werden. Ebenso müssen der **Zweckbindungsgrundsatz** und die gesetzlichen **Löschungsvorgaben** gewährleistet sein. Mit dem Datenschutzkonzept wollen die Datenschutzbeauftragten sicherstellen, daß auch bei besonderen Kundenservice-Dienstleistungen und sonstigen Vorhaben der Krankenkassen die Rechte ihrer Kundinnen und Kunden auf Datenschutz beachtet werden. Der zulässige Umfang der Datenverarbeitung hängt dabei von der Einwilligung der Versicherten ab.

Im einzelnen bedürfen folgende Probleme einer Lösung:

- Sogenannte **freie Abfragesprachen,** die eine Auswertbarkeit und Selektierbarkeit von Versichertendatenbeständen nach beliebigen Gesichtspunkten ermöglichen, müssen durch klare Regelungen bestimmt sein. Dabei sind programmtechnische Festlegungen erforderlich, welchen Stellen in welchem Umfang und für welche Zwecke solche Abfragemöglichkeiten zur Verfügung stehen. Andere Datenauswertungen bedürfen einer besonderen Genehmigung nach vorheriger datenschutzrechtlicher Zulässigkeitsprüfung, wobei die oder der Datenschutzbeauftragte der Krankenkasse zu beteiligen ist.

- Soweit Versichertendatenbestände durch eine außenstehende Stelle - zum Beispiel ein Rechenzentrum - verarbeitet werden, müssen schriftliche Weisungen zu einer solchen Auftragsdatenverarbeitung erfolgen (§ 80 SGB X). Die Trennung der Datenbestände der einzelnen Krankenkassen ist dabei von zentraler Bedeutung, damit bestandsübergreifende Auswertungen von vornherein ausgeschlossen sind. Hier bieten sich folgende **Problemlösungen** an:
  - getrennte System- und Programmumgebungen (virtuelle Systeme) für die Anwendungen der jeweiligen Kasse,
  - Zugriffskonzept für landesspezifische und zentrale Funktionen,
  - Test- und Freigabeverfahren für Programme,
  - Revisions-, Datensicherungs-, Archivierungs- und Löschkonzept.

  Besonderer Wert ist auf die **Protokollierung** von Abfragen und Auswertungen zu legen, die eine wirksame Datenschutzkontrolle ermöglicht.

- Abfragemöglichkeiten, die den Zugriff auf alle oder einen Großteil der Versichertendaten erlauben, dürfen den Beschäftigten der Krankenkassen nicht undifferenziert (etwa durch "allgemeine Auskunftsmasken") zur Verfügung stehen. Hier kann ein **Zugriffsschutzkonzept**

sicherstellen, daß den Beschäftigten Zugriffsbefugnisse auf die Versichertendaten nur im Rahmen ihrer Zuständigkeit eingeräumt sind. Die Krankenkassen können und sollten mit einem solchen Konzept insbesondere die von den Datenschutzbeauftragten des Bundes und der Länder bereits 1995 erhobene Forderung umsetzen, einen umfassenden Zugriff auf die Daten der Versicherten - einschließlich der Angaben zu Diagnosen und Leistungen - lediglich einer Geschäftsstelle zu ermöglichen (siehe schon 13. Datenschutzbericht, Seite 86 f.).

- Bei der automatisierten Verarbeitung von Versichertendaten müssen die gesetzlichen Vorgaben zur **Löschung** dieser Daten eingehalten werden. Im Gegensatz zur Aufbewahrung von Belegen in Papierform sind Löschungsfristen bei automatisierter Speicherung dieser Daten nur zum Teil festgelegt. Ein Datenschutzkonzept kann auch insoweit Speicherungsdauer und Löschung von Versichertendaten nach Ablauf der Aufbewahrungsfristen automationsunterstützt überwachen.

Es ist wünschenswert, daß sich die gesetzlichen Krankenkassen das ihren Spitzenverbänden und dem Bundesgesundheitsministerium bereits vorgestellte Datensicherheitskonzept zu eigen machen und die erforderlichen organisatorischen und technischen Maßnahmen zügig umsetzen.

7.5 Dürfen Krankenkassen Arztberichte anfordern?

Eine Krankenkasse hat im Zusammenhang mit ihrer Anfrage über das Fortbestehen einer Arbeitsunfähigkeit bei dem behandelnden Arzt auch die Übersendung des Krankenhausentlassungsberichts eines Patienten erbeten. Dieser sollte dem Medizinischen Dienst der Krankenversicherung (MDK) zur weiteren Prüfung zugeleitet werden.

Wie verhalten sich Krankenkassen sozialdatenschutzrechtlich korrekt, wenn sie zum Beispiel Art und Ausmaß der Arbeitsunfähigkeit ihrer Versicherten oder Maßnahmen zur Wiederherstellung der Arbeitsfähigkeit zu beurteilen haben? Sie müssen beachten, daß es ihnen mangels gesetzlicher Befugnis nicht erlaubt ist, von ausschließlich für den MDK bestimmten Krankenhausentlassungsberichten oder ärztlichen Gutachten der Leistungserbringer (Vertragsärztinnen und -ärzte, Krankenhäuser) Kenntnis zu nehmen. Zwar dürfen die Krankenkassen solche Sozialdaten bei den Leistungserbringern erheben, soweit es für die Beteiligung des MDK erforderlich ist (§ 276 Abs. 1 in Verbindung mit § 284 Abs. 1 Nr. 7 SGB V). Der den Leistungserbringern mitzuteilende Erhebungszweck ist jedoch ausschließlich auf die **Weiterleitung** der Daten an den MDK begrenzt und erlaubt keine Kenntnisnahme der Patientenunterlagen durch die Krankenkasse. Dies wird auch da-

durch deutlich, daß die Leistungserbringer ohnehin gesetzlich verpflichtet sind, diese besonders sensiblen, dem Arzt-Patienten-Geheimnis unterliegenden Daten auf Anforderung des MDK unmittelbar an diesen zu übermitteln (§ 276 Abs. 2 SGB V). Briefumschläge mit Patientenunterlagen müssen als solche erkennbar und zur Weiterleitung an den MDK gekennzeichnet sein.

Sofern die Anforderung von Patientenunterlagen im Zusammenhang mit einer Begutachtung durch den MDK erfolgt, muß die Krankenkasse dies gegenüber den Leistungserbringern deutlich zum Ausdruck bringen. Diese haben dafür Sorge zu tragen, daß Krankenhausentlassungsberichte und ärztliche Gutachten nur für den MDK bestimmt sind und dies der anfordernden Krankenkasse erkennbar ist.

7.6 Mehr Bürgernähe bei den Rentenversicherungsträgern

Die Rentenversicherungsträger haben zur verbesserten Betreuung der Versicherten ein bürgernahes Dialogverfahren entwickelt. Jedoch müssen bei diesem Verfahren, in dem Versichertendaten bundesweit automatisiert ausgetauscht werden können, Datensicherheitsmaßnahmen ein hohes Schutzniveau erreichen.

Das Dialogverfahren ermöglicht den Rentenversicherten, Angaben zu ihren Versicherungsverläufen, Rentenauskünfte, Lückenauskünfte und sonstige Informationen sowohl bei den für sie zuständigen als auch bei allen anderen am Dialogverfahren beteiligten Stellen zu erhalten. Bei diesem gigantischen, alle Versicherten der angeschlossenen Rentenversicherungsträger erfassenden Informationsverbund muß ein hoher **Datensicherheitsstandard** gewährleistet sein:

- Nur eine auf das erforderliche Maß begrenzte Anzahl von Beschäftigten darf zur Dialognutzung zugelassen werden. Deren Datenzugriffsmöglichkeiten müssen durch technische Maßnahmen auf das zu ihrer Aufgabenerfüllung notwendige Maß beschränkt werden. Die Beschäftigten müssen über die datenschutzrechtlichen Erfordernisse besonders unterwiesen werden.

- Im Publikumsverkehr ist von den Beschäftigten zu beachten, daß eine Identitätsprüfung der oder des Versicherten an Hand eines Lichtbildausweises und eine (formularmäßige) schriftliche Antragstellung erfolgt.

- EDV-Zugriffe müssen sowohl bei dem anfordernden als auch bei dem zuständigen Rentenversicherungsträger protokolliert und stichprobenweise kontrolliert werden.

Die Landesversicherungsanstalten Rheinprovinz und Westfalen wurden gebeten, sich dafür einzusetzen, diesen Datensicherheitsanforderungen zu entsprechen. Sichergestellt werden muß insbesondere, daß die Rentenversicherten mit der Abrufmöglichkeit ihrer Daten bei verschiedenen Rentenversicherungsträgern einverstanden sind. Hierüber sind sie vorher aufzuklären.

Nur nach vorheriger Aufklärung können Rentenversicherte darin einwilligen, sich frei für oder gegen eine Teilnahme an dem bundesweiten Informationsverbund des Dialogverfahrens der Rentenversicherungsträger zu entscheiden. Die angesprochenen Verantwortlichen sind hier noch gefordert!

8. Gesundheit

8.1 Trotz guter Zusammenarbeit noch ungelöste Probleme

Mit dem - früheren - Ministerium für Arbeit, Gesundheit und Soziales und dem - jetzigen - Ministerium für Frauen, Jugend, Familie und Gesundheit hat es im Berichtszeitraum viele konstruktive Gespräche gegeben, die in etlichen Fragen zu datenschutzgerechten Lösungen geführt haben. So konnte beispielsweise für die **Durchführung des Psychotherapeutengesetzes** erreicht werden, daß der Personenkreis, der für die Erlangung der Approbation die bisherige Berufstätigkeit im einzelnen nachzuweisen hat, dies grundsätzlich ohne Nennung der Namen von Patientinnen und Patienten tun kann. Es wird die Vorlage anonymisierter Unterlagen über die jeweiligen Behandlungen verlangt, soweit keine Einwilligung der Patientinnen und Patienten vorliegt. Die Antragstellenden werden jedoch verpflichtet, ihre Unterlagen in nicht-anonymisierter Form mindestens noch ein Jahr nach bestandskräftigem Abschluß des Verwaltungsverfahrens vorzuhalten. Bei Anhaltspunkten für falsche Darstellungen im Einzelfall dürfen die Angaben nachgeprüft werden.

Die mit datenschutzrechtlichen Mängeln behaftete Praxis des **Kostenerstattungsverfahrens** nach dem Gesetz zur Hilfe für Frauen bei **Schwangerschaftsabbrüchen** in besonderen Fällen war ebenfalls Thema der Gespräche. Auch hier bedarf es keiner Offenbarung der Namen von Patientinnen. Die Erklärung der Krankenkasse, daß es sich um eine antragsberechtigte Person handelt, genügt. Bedenken gegen die Korrektheit einzelner Abrechnungen können ohne weiteres durch Identifikationsnummern verfolgt, dem Einzelfall zugeordnet und geprüft werden. Das Ministerium prüft zur Zeit, ob als Ersatz für die verwaltungsaufwendige Identifikationsnummer die Krankenversichertennummer der jeweiligen Patientin, ergänzt um Wohnort und Bundesland, verwendet werden kann. Dieser Lösung kann nur zugestimmt werden, wenn der Erstattungsbehörde ein Rückschluß auf die Person nicht möglich ist. Auch muß noch geklärt werden, in welchem Umfang die Kassenärztlichen Vereinigungen in das Kostenerstattungsverfahren miteinbezogen werden dürfen, denn das Gesetz sieht eine Abrechnung allein mit den Krankenkassen vor.

Die Bekämpfung von Krebserkrankungen ist seit geraumer Zeit eines der Ziele der Gesundheitspolitik der Landesregierung. Für die weiter aufzubauenden **Krebsregister** fordern Ärztinnen und Ärzte eine breitere Datengrundlage, damit Krebsforschung und onkologische Nachsorge besser vorankommen. Die behandelnden Ärztinnen und Ärzte sind dazu angehalten,

dem Krebsregister bestimmte, in § 16 Abs. 3 Gesundheitsdatenschutzgesetz (GDSG NW) genannte Erkrankungsdaten ihrer Patientinnen und Patienten mit deren **Einwilligung** zu übermitteln. Damit zusammenhängende Fragen - zum Beispiel die notwendige Information der Patientinnen und Patienten sowie die verbesserte Einbindung der Pathologinnen und Pathologen in das Meldeverfahren - wurden in Dienstbesprechungen im Ministerium für Frauen, Jugend, Familie und Gesundheit zusammen mit der Ärztekammer Nordrhein und Epidemiologen erörtert.

Anhand eines noch ungelösten Falles wurde eine gesetzliche **Regelungslücke** offenkundig, die baldmöglichst zu schließen wäre. Der Vermieter einer Arztpraxis teilte mit, daß seit dem Tod des dort früher niedergelassenen Radiologen die Unterlagen seiner ehemaligen Patientinnen und Patienten - etwa 10.000 bis 15.000 Röntgenbilder und 4.000 bis 5.000 Karteikarten - in teilweise unverschlossenen Kellerräumen lagerten. Da meiner Dienststelle mangels Zuständigkeit für die Datenschutzaufsicht im nichtöffentlichen Bereich die Hände gebunden waren, wurde umgehend die zuständige Bezirksregierung eingeschaltet. So recht verantwortlich dafür, Abhilfe zu schaffen, wollte sich aber niemand fühlen - nicht die Nachlaßverwaltung und nicht die Ärztekammer. Das städtische Ordnungsamt sicherte die Unterlagen zwar vorläufig, indem es ein privates Unternehmen mit der ordnungsgemäßen Zwischenlagerung beauftragte, doch es ist nachvollziehbar auch nicht bereit, die Unterlagen dauerhaft zu lagern. Ärztekammern in anderen Bundesländern übernehmen in derartigen Notfällen durchaus die Sicherung solcher Unterlagen. Dies hat die hiesige Ärztekammer von sich gewiesen. Das Ministerium sollte daher die Initiative ergreifen, die Ärztekammern in vergleichbaren Fällen zur Aufbewahrung von Patientenunterlagen gesetzlich zu verpflichten. Dies könnte auch im Wege einer klarstellenden Satzungsänderung durch die Ärztekammern selbst erfolgen.

In Krankenhäusern bestimmen Kostendruck, Sparzwänge, personelle und räumliche Engpässe das Geschehen. Dies führt zu Rationalisierungsüberlegungen, die auch die Aufbewahrung von Krankenunterlagen betreffen. Die **Archivierung**, insbesondere die **Mikroverfilmung und/oder Digitalisierung** von Krankenunterlagen des Krankenhauses birgt ebenso wie ein Outsourcing dieser Aufgaben Datenschutzrisiken, über die die Verantwortlichen in den Krankenhäusern informiert sein sollten. Die Datenschutzbeauftragten des Bundes und der Länder beobachten kritisch Bestrebungen im Gesundheitswesen, bei denen eine Verarbeitung medizinischer Patientendaten außerhalb des krankenhausärztlichen Bereichs - mit dem Risiko der Kenntnisnahme und des Zugriffs durch unbefugte Dritte - möglich werden kann. In ihrer Entschließung vom 17./18.04.1997 (Abdruck im Anhang, Nr. 2) haben sie daher gesetzgeberische Maßnahmen zur Sicherstel-

lung des Schutzes medizinischer Datenbestände außerhalb ärztlicher Behandlungseinrichtungen gefordert. In meiner Dienststelle kann in Kürze eine **Orientierungshilfe** zu diesem Problemkreis angefordert werden.

8.2 Gesundheitsnetze - höchste Anforderungen an Datenschutz und Datensicherheit

Das - damalige - Ministerium für Arbeit, Gesundheit und Soziales erwog die Beteiligung an der Finanzierung eines Gesundheitsnetzprojektes und fragte an, ob meine Dienststelle das Projekt unter Datenschutzaspekten beratend begleiten könne. Die aus der Beratungstätigkeit entstandenen Fragestellungen sind zum Anlaß genommen worden für die folgenden grundsätzlichen Ausführungen, die für Gesundheitsnetze jedweder Art allgemeine Gültigkeit besitzen.

8.2.1 Ziele von Gesundheitsnetzen

Netze und Dienste der Informations- und Telekommunikationstechnologie sollen dazu beitragen, die Kommunikation zwischen den Institutionen des Gesundheitswesens zu verbessern und die Leistungsprozesse zu optimieren. Mit der Einrichtung von Gesundheitsnetzen sollen unter anderem die folgenden Ziele erreicht werden:

- Schnelle Übermittlung von Patientendaten zwischen den Leistungserbringern - beispielsweise Ärztinnen und Ärzten, Krankenhäusern, Rehabilitationseinrichtungen.

- Vermeidung unnötiger Mehrfachuntersuchungen durch zeitnahen Zugriff auf Patientendaten, die an verschiedenen Orten vorliegen.

- Verkürzung der Verweildauer der Patientinnen und Patienten in Akutbehandlung und Rehabilitation durch verbesserte informationelle Koordination.

- Verbesserung der Entscheidungsrationalität in der Medizin durch eine zeitlich parallele Verständigung mehrerer Expertinnen und Experten über medizinische Sachverhalte auf der Grundlage komplexer Daten.

- Verbesserte Koordinierung bei langwierigen Erkrankungen durch Vereinfachung und Verkürzung des Prozesses der Integration der von verschiedenen Stellen erhobenen Befunde zu einem Gesamtbild.

Die Nutzung von Gesundheitsnetzen bietet gewiß Möglichkeiten zur Steigerung von Effizienz und Effektivität im Gesundheitswesen. Dabei darf aber der Blick auf die Risiken nicht verstellt werden. Solche Systeme dürfen nur betrieben werden, sofern den datenschutzrechtlichen Erfordernissen genügt ist und die Datensicherheitsfragen beantwortet sind.

8.2.2 Rechtsgrundlagen

Rechtsgrundlagen für die Verarbeitung von Patientendaten sind im allgemeinen der Arzt- oder der Krankenhausbehandlungsvertrag, die Vorschriften der ärztlichen Berufsordnung, das Gesundheitsdatenschutzgesetz und - im Rechtsverhältnis zwischen Ärztin oder Arzt und gesetzlicher Krankenkasse - die Vorschriften des SGB V. Diese Regelungen erlauben keine Übermittlung von Patientendaten in Gesundheitsnetzen, so daß eine solche Datenverarbeitung allenfalls für die Durchführung eines Pilotprojektes aufgrund einer **Einwilligung** von Patientinnen und Patienten in Betracht kommt. Besonderes Gewicht hat hierbei ihre umfassende vorherige Aufklärung, damit das Recht der Betroffenen auf informationelle Selbstbestimmung gewahrt bleibt.

Nur ein "informed consent" begründet eine rechtswirksame Einwilligung. Patientinnen und Patienten müssen sich frei und unbeeinflußt von faktischen Zwängen für oder gegen einen Austausch ihrer Daten in Gesundheitsnetzen entscheiden können.

8.2.3 Sicherheitspolitik

In den USA und Großbritannien wurden einige - zum Teil schwerwiegende - Fälle von Mißbrauch persönlicher Gesundheitsinformationen bekannt. Allgemein ist dort ein großes kommerzielles Interesse an Patientendaten zu beobachten. In einer Umfrage in den USA äußerten 80% der befragten Bürgerinnen und Bürger Besorgnis um die Privatheit ihrer Gesundheitsdaten. Vor diesem Hintergrund gab die British Medical Association die Ausarbeitung einer Sicherheitspolitik für Systeme zur Verarbeitung von elektronischen Gesundheitsinformationen in Auftrag. Die Essenz der Studie von Ross J. Anderson & British Medical Association, Security in Clinical Information Systems, sind die folgenden Grundprinzipien:

Prinzip 1: Zugangskontrolle
Ein patientenbezogenes Dokument bezeichnet einen einzelnen medizinischen Sachverhalt zu einem Patienten oder einer Patientin. Die Menge aller zu einem Patienten oder einer Patientin existierenden Dokumente ist die Patientenakte. **Jedes** patientenbezogene Dokument soll mit einer Zugangskon-

trolliste versehen sein, welche die Personen oder Personengruppen benennt, die das Dokument lesen und ihm Daten anfügen können. Das System soll verhindern, daß Personen, die nicht auf der Liste stehen, in irgend einer Weise Zugang zum Dokument finden.

Prinzip 2: Einrichten eines Dokuments
Als Kliniker werden die Beschäftigten im Gesundheitswesen bezeichnet, die unter Schweigepflicht stehen und bei deren Bruch die Berufserlaubnis verlieren können. Ein Kliniker kann ein Dokument einrichten und sich selbst und die Patientin oder den Patienten in die Zugangskontrolliste eintragen. Wurde die Patientin oder der Patient überwiesen, kann er sich selbst, die Patientin oder den Patienten und den überweisenden Kliniker in die Zugangskontrolliste eintragen.

Prinzip 3: Verantwortlichkeit
Ein Kliniker auf der Zugangskontrolliste ist als Verantwortlicher zu markieren. Nur er darf die Zugangskontrolliste verändern und ihr ausschließlich im Gesundheitswesen Beschäftigte mit ihren jeweiligen Zugangsberechtigungen hinzufügen.

Prinzip 4: Mitteilung und Einwilligung
Der verantwortliche Kliniker muß der Patientin oder dem Patienten Mitteilung von den Namen auf der Zugangskontrolliste machen:
a) wenn das Dokument eingerichtet wird,
b) bei allen nachfolgenden Hinzufügungen,
c) immer, wenn die Verantwortung weitergegeben wird.
Die Einwilligung der Patientin oder des Patienten muß ebenfalls eingeholt werden - außer im Notfall und bei gesetzlichen Ausnahmen.

Prinzip 5: Fortbestand
Niemand soll klinische Informationen löschen können, bevor der vorgesehene Zeitraum abgelaufen ist.

Prinzip 6: Zuschreibung
Jeder erfolgte Zugang zu klinischen Dokumenten soll im Dokument mit dem Namen der betreffenden Person, Datum und Uhrzeit eingetragen werden. Ein solcher "Audit-Vermerk" muß auch bei jeder Löschung erfolgen.

Prinzip 7: Informationsfluß
Informationen, die einem Dokument A entnommen werden, dürfen an ein Dokument B dann - und nur dann - angefügt werden, wenn die auf der Zugangskontrolliste von B stehenden Berechtigten auf der Zugangskontrolliste von A verzeichnet sind.

Prinzip 8: Aggregationskontrolle
Es muß effektive Maßnahmen geben, mit denen die Aggregation von persönlichen Gesundheitsinformationen verhindert wird. Insbesondere müssen Patienten und Patientinnen eine besondere Benachrichtigung erhalten, wenn eine Person der Zugangskontrolliste hinzugefügt werden soll, die bereits Zugang zu den persönlichen Gesundheitsinformationen einer großen Anzahl von Personen hat.

Prinzip 9: vertrauenswürdiges Sicherheitssystem
Computersysteme, die persönliche Gesundheitsinformationen verarbeiten, sollen ein Untersystem haben, das auf effektive Weise die obengenannten Prinzipien erzwingt. Dessen Effektivität soll Gegenstand der Evaluation durch unabhängige Experten sein.

Diese Sicherheitspolitik formuliert Sicherheitsvorgaben für patientendatenverarbeitende Systeme auf einem Abstraktionsniveau, das den Blick auf das Wesentliche lenkt und nicht durch technische Details die eigentlich zu lösenden Probleme verschleiert. Die aufgestellten Prinzipien sind geeignet, einen allgemeingültigen Rahmen für die Entwicklung von Sicherheitskonzepten für Systeme zur Verarbeitung elektronischer Patientendaten zu definieren.

Eine effektive Sicherheitspolitik ist essentielle Voraussetzung für die Entwicklung von Gesundheitsnetzen!

8.2.4 Sicherheitskonzept

Aufbauend auf den Vorgaben einer Sicherheitspolitik ist ausgehend von den Bedrohungen der Sicherheit persönlicher Gesundheitsinformationen für jedes geplante Gesundheitsnetz ein **individuelles Sicherheitskonzept** zu entwickeln. Darin werden unter Berücksichtigung der konkreten technischen Architektur die technischen und organisatorischen Maßnahmen spezifiziert, die geeignet sind, die Sicherheitspolitik durchzusetzen und die angestrebten Sicherheitsziele zu erreichen. Im folgenden werden allgemeine Sicherheitsziele für die Sicherheitskonzeption von Gesundheitsnetzen definiert und die essentiellen Maßnahmen zu deren Umsetzung angegeben. Dabei wird die in den USA und in Großbritannien gemachte Erfahrung berücksichtigt, daß neue Bedrohungen hauptsächlich von Insidern kommen.

8.2.4.1 Vertraulichkeit

Vertraulichkeit ist ein Privileg der Patientin und des Patienten. Nur sie können darauf verzichten. Ihre Zustimmung dazu kann nur auf der Basis kom-

petenter Information und Freiwilligkeit erfolgen. Aus diesem Grunde ist der Patientin und dem Patienten zum Beispiel mitzuteilen, welche Personen Zugriff auf ihre Gesundheitsdokumente haben. Der Sicherstellung dieses Vertraulichkeitsprivilegs dienen die unter 8.2.3 angeführten Prinzipien 1 bis 4 und die Prinzipien 7 und 8.

Eine grundlegende Voraussetzung für eine systemtechnische Gewährleistung dieser Prinzipien ist die Realisierung eines effektiven Zugriffsschutzkonzepts, das sicherstellt, daß auch nur die in den **Zugangskontrollisten** aufgeführten Berechtigten ausschließlich im Rahmen ihrer festgelegten **spezifischen Berechtigungen** auf klinische Dokumente zugreifen können. Andererseits sind die Kliniker, die vertrauliche Informationen aufzeichnen oder verwahren, dafür verantwortlich, daß diese wirksam gegen unzulässige Offenbarung geschützt werden. Werden Patientendokumente elektronisch verarbeitet, haben die Patientinnen und Patienten aber keinen unmittelbaren Einfluß darauf, daß dies gewährleistet ist. Für die Kliniker ist zur Wahrung ihres Berufsgeheimnisses von entscheidender Bedeutung, in jeder Phase der elektronischen Verarbeitung von patientenbezogenen Informationen darauf vertrauen zu können, daß durch effektive Sicherheitsmechanismen die Vertraulichkeit sichergestellt ist. Vor diesem Hintergrund kann Vertraulichkeit letztlich nur gewährleistet werden, wenn sowohl übermittelte als auch gespeicherte patientenbezogene Informationen mit **starken kryptographischen Verfahren** verschlüsselt werden.

Kryptographische Methoden sind ebenso geeignet zur Pseudonymisierung patientenbezogener Gesundheitsinformationen unter gleichzeitiger Beibehaltung der Zuordnungsfähigkeit. Wenn für einen klinischen Verfahrensschritt - wie etwa bei der Übermittlung von Laborwerten - die personenidentifizierenden Daten einer Gesundheitsinformation keine Relevanz haben, sind sie zu **pseudonymisieren**.

8.2.4.2 Integrität

Sind klinische Informationen verfälscht, können Kliniker falsche Entscheidungen treffen, die den Patientinnen und Patienten schaden oder gar zu deren Tod führen können. Ist bei einem System zur Verarbeitung von Gesundheitsinformationen nicht sicher auszuschließen, daß klinische Informationen **verfälscht** sein können, haben diese Informationen für die klinische Entscheidungsfindung einen verminderten oder sogar keinen Wert. Die Informationen eines solchen Systems müssen als nicht vertrauenswürdig angesehen werden, unabhängig davon, ob eine einzelne Information nun tatsächlich verfälscht ist oder nicht.

Insofern sind gespeicherte und übermittelte Informationen durch starke **Integritätssicherungsmechanismen** vor Verfälschungen zu schützen. Hierfür kommen kryptographische Mechanismen in Betracht. Darüber hinaus ist sicherzustellen, daß die informationsverarbeitende **Anwendungssoftware** korrekt die geforderten Funktionalitäten ausführt und selbst nicht verfälscht wird. Ersteres ist eine Frage der Softwarequalität und stellt hohe Anforderungen an den Softwareentwicklungsprozeß. Der Schutz der Anwendungssoftware vor Verfälschungen kann ebenfalls mit kryptographischen Mitteln erreicht werden. Die **Prüfung auf Integritätsverletzungen** sollte automatisch bei jedem erneuten Aufruf der jeweiligen Anwendungssoftware erfolgen.

8.2.4.3 Authentizität

Neben der Vertraulichkeit und Integrität von Patientendokumenten ist deren **Herkunft** ein wichtiger Faktor im klinischen Entscheidungsprozeß und Voraussetzung für eine vertrauenswürdige Kommunikation im Gesundheitswesen. Im Gegensatz zur konventionellen Verarbeitung klinischer Informationen ist bei der elektronischen Verarbeitung einem digitalen Dokument seine Herkunft zunächst nicht anzusehen. Es muß durch zusätzliche Mechanismen gewährleistet werden, daß ein elektronisches Dokument sicher seiner Urheberin oder seinem Urheber zugeordnet werden kann. Die **digitale Signatur** bietet hierfür die Möglichkeiten. Damit ist jedes patientenbezogene Dokument von dem verantwortlichen Kliniker mit seiner digitalen Signatur zu versehen.

Neben der Authentizität klinischer Dokumente ist ebenso die Authentizität der Nutzerinnen und Nutzer von Datenverarbeitungssystemen sicherzustellen. Sie müssen als Berechtigte zur Inanspruchnahme spezifischer Berechtigungen vom System **sicher identifiziert** werden. Die für den Identifizierungsprozeß gebräuchlichen Paßwortverfahren sind für Systeme, die Patienteninformationen verarbeiten, aufgrund der hohen Sensibilität der Daten nicht hinreichend sicher. Einzusetzen sind chipkartengestützte Verfahren, die auf kryptographischen Mechanismen basieren, oder biometrische Authentifizierungsverfahren.

Bei den in Gesundheitsnetzen stattfindenden Kommunikationsvorgängen müssen sich die an einer Kommunikation Beteiligten, bevor es zum eigentlichen Datenaustausch kommt, zunächst **gegenseitig** authentifizieren. Nur so kann sichergestellt werden, daß die an einer Kommunikation Beteiligten auch wirklich diejenigen sind, für die sie sich ausgeben. Hierbei ist zu unterscheiden zwischen einer Ende-zu-Ende-Kommunikation und einer Prozeß-Prozeß-Kommunikation. Bei der Ende-zu-Ende-Kommunikation werden In-

formationen unmittelbar von Kliniker zu Kliniker zum Beispiel mittels eines E-Mail-Verfahrens ausgetauscht. Bei Datenverarbeitungsverfahren, die auf dem Client/Server-Prinzip basieren, kommunizieren auf verschiedene Rechnersysteme verteilte Softwareprozesse über ein verbindendes Netzwerk miteinander. In beiden Fällen müssen sich jeweils die an der Kommunikation Beteiligten gegenseitig sicher identifizieren. Unabhängig davon, ob eine Identifikation von Kliniker gegenüber Kliniker oder von Prozeß gegenüber Prozeß erforderlich ist, sind Authentifizierungsverfahren auf der Basis kryptographischer Methoden einzusetzen. Nur kryptographische Authentifizierungsmechanismen bieten eine für Gesundheitsnetze hinreichende Sicherheit.

8.2.4.4 Nicht-Abstreitbarkeit

Eine weitere wichtige Voraussetzung für eine vertrauenswürdige, über Gesundheitsnetze stattfindende Kommunikation, ist die Nicht-Abstreitbarkeit des **Sendens** und des **Empfangs** von klinischen Informationen. Ein Kliniker, der einem anderen Kliniker eine patientenbezogene Information übermittelt, muß sicher sein können, daß die Information ihren Empfänger erreicht hat. Oder anders ausgedrückt: Es muß gewährleistet sein, daß die die Nachricht empfangende Person nicht abstreiten kann, diese Nachricht mit einem bestimmten Inhalt erhalten zu haben. Gleiches gilt auch für die sendende Person.

Die Nicht-Abstreitbarkeit des Sendens und des Empfangs klinischer Informationen ist realisierbar auf der Grundlage von Quittungsverfahren unter Verwendung digitaler Signaturen.

8.2.4.5 Verfügbarkeit

Wenn die in einem Gesundheitsnetz bereitgehaltenen Informationen - etwa wegen Systemfehlern oder wegen Sabotage - nicht zeitgerecht oder unter Umständen gar nicht mehr zur Verfügung stehen, ist dieses System nicht **verläßlich** für die Verarbeitung klinischer Informationen. An die Sicherstellung der Verfügbarkeit von Gesundheitsnetzen sind hohe Anforderungen zu stellen. Dazu bedarf es einer Vielzahl von **technischen** und **organisatorischen Maßnahmen,** die abhängig von der konkreten Architektur des Systems individuell im Rahmen eines Sicherheitskonzepts zu ermitteln sind. In diesem Zusammenhang sind beispielsweise Recovery-Konzepte, Back-up/Restore-Konzepte und Konzepte für den Betrieb und die Administration zu entwickeln.

8.2.4.6 Revisionssicherheit

Die in einem Gesundheitsnetz ablaufenden Vorgänge müssen **nachvollziehbar festgehalten** werden. Insbesondere ist zu gewährleisten:

- Jeder Zugang zu einem Patientendokument ist benutzerbezogen mit der Zugangsart, dem Zugangsdatum und der Zugangszeit zu protokollieren. Für die Protokolldaten ist die Vertraulichkeit, Integrität und Authentizität sicherzustellen. Sie unterliegen einer strengen Zweckbindung.

- Der Stand einer Patientenakte (als Menge von Dokumenten) muß für jeden beliebigen Zeitpunkt rekonstruierbar sein.

- Es sind entsprechende Mechanismen bereitzustellen, die die Patientin und den Patienten in die Lage versetzen, ihr Recht auf Einsicht in ihre oder seine Patientenakte ausüben zu können.

Bei der Planung eines Gesundheitsnetzes ist ein individuelles Sicherheitskonzept zu erstellen. Die notwendige Voraussetzung für die Erreichung der Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Nicht-Abstreitbarkeit bilden kryptographische Verfahren.

8.2.5 Zusammenfassung

Eine gesetzliche Grundlage für die Verarbeitung von Patientendaten in Gesundheitsnetzen ist nicht gegeben. Allenfalls für die Durchführung eines Pilotprojektes ist eine solche Informationsverarbeitung auf Einwilligungsbasis möglich. Dies setzt voraus, daß den Patientinnen und Patienten vollkommen transparent ist, was mit ihren Daten geschieht und sie sich frei und unbeeinflußt für oder gegen eine Verarbeitung in dieser Form entscheiden können. Im Vordergrund müssen die **informierten Patientinnen und Patienten** stehen, die die Kontrolle über ihre Daten haben.

Sehr hohe Risiken in Gesundheitsnetzen bergen elektronische Patientenakten, die zum Beispiel durch eine Vernetzungssoftware gebildet werden und durch die eine Fülle sensibler Gesundheitsdaten zum Abruf bereitgehalten werden kann. Dies kann zur Entstehung **zentraler medizinischer Datensammlungen** führen, die ungewisse Risiken und Gefährdungen für die **Persönlichkeitsrechte** der Betroffenen zur Folge haben können. Die Wahrscheinlichkeit, daß Patientendaten in unzulässiger Weise offenbart werden, hängt von ihrem Wert und von der Anzahl der Personen ab, die Zugang zu ihnen haben. Das Aggregieren von Patientendaten erhöht beide **Risikofaktoren** zugleich.

Gesundheitsnetze stellen höchste Anforderungen an Datenschutz und Datensicherheit. Die Planung solcher Systeme kann nur auf der Grundlage einer Sicherheitspolitik und individuellen Sicherheitskonzepten erfolgen, welche die hohe Sensibilität der zu verarbeitenden Daten und die besondere Bedrohungslage berücksichtigen. Erst durch Verfahren zur **Verschlüsselung** und **digitalen Signatur** eröffnen sich Möglichkeiten zur Gewährleistung einer hinreichenden Datensicherheit. Beim Einsatz solcher Verfahren dürfen die organisatorischen Probleme, die mit der **Schlüsselverwaltung und -verteilung** verbunden sind, nicht unterschätzt werden. Ansonsten entsteht an dieser Stelle ein **systemisches Sicherheitsrisiko**. In diesem Zusammenhang ist noch zu untersuchen, ob die mit einem zentralen Schlüsselmanagement verbundenen zentralen Datensammlungen ein neues, nicht hinnehmbares Gefährdungspotential hervorrufen. In diesem Fall ist über die Entwicklung effektiver dezentraler Schlüsselmanagementstrukturen nachzudenken.

9. Statistik – Kommt wieder eine Volkszählung?

Die Europäische Union (EU) hat ihren Mitgliedstaaten vorgeschlagen, im Jahre 2001 eine gemeinschaftsweite Volks- und Wohnungszählung durchzuführen. Ob dies in der Bundesrepublik Deutschland geschieht, ist noch offen.

Von einer verbindlichen Zensusverordnung mit einem ebenso umfangreichen wie kostenträchtigen Erhebungsprogramm in Form eines Rechtsaktes ist das Statistische Amt der Europäischen Gemeinschaften (EuroStat) nach verschiedenen, auch von deutscher Seite vorgebrachten Einwänden mittlerweile abgerückt. Die Überlegungen zur Durchführung eines gemeinschaftsweiten Zensus beruhen nunmehr auf von EuroStat vorgelegten unverbindlichen "Leitlinien für das gemeinschaftliche Programm der Volks- und Wohnungszählungen im Jahre 2001". Diese empfehlen als Verfahren für die Datengewinnung

- Vollerhebungen oder repräsentative Stichprobenerhebungen,
- die Nutzung von Verwaltungsregistern oder anderen Verwaltungsquellen oder
- eine Kombination dieser beiden Verfahren.

Eine von der Innenministerkonferenz beauftragte Arbeitsgruppe prüft derzeit Schritte zur Entwicklung eines Modells, den herkömmlichen Zensus zu ersetzen. Diskutiert wird, ob und inwieweit zur Durchführung der Erhebungen auf Daten in bereits bestehenden Registern zugegriffen werden kann. Die Überlegungen orientierten sich zunächst an dem Datenbedarf des Bundes und führten zum sogenannten **Bundesmodell**. Mit Rücksicht auf den insbesondere von Nordrhein-Westfalen betonten Informationsbedarf der Länder und Kommunen wurde alternativ das sogenannte **Ländermodell** erarbeitet.

Das **Bundesmodell** setzt sich zusammen aus einem Modul, mit dem aus Melderegistern die **demographischen Grunddaten** gewonnen werden, einem weiteren **erwerbsstatistischen Modul**, das den Großteil der Erwerbstätige und Pendelnde betreffenden Daten liefert, sowie dem Modul eines **erweiterten Mikrozensus**. Die Module sollen nicht, auch nicht personenbezogen, verknüpft werden.

Das **Ländermodell** beinhaltet zwei Module. Durch das **Grundmodul** mit Daten aus der Gebäude- und Wohnungszählung sowie Melderegisterdaten der Gemeinden sollen unter anderem die demographischen und gebäude- sowie wohnungsstatistischen Grunddaten einschließlich Daten zur Struktur der Haushalte und der Wohnungsversorgung gewonnen werden. Im **Ergänzungsmodul** mit verschiedenen Komponenten - Dateien der Bundesanstalt für Arbeit sowie anderer Behörden und Gebietskörperschaften, einer Ergänzungsstichprobe im Erwerbsbereich und einer Zusammenführung mit den Dateien des Grundmoduls - sollen die erwerbsstatistischen Daten einschließlich Pendlerdaten sowie Ergebnisse, wie sie von einer Volkszählung erwartet werden, gewonnen werden. Bestandteil des Ländermodells ist darüber hinaus eine datenschutzrechtlich problematische Zusammenfassung verschiedener Einzelregisterdaten mit Primärerhebungen in bestimmten Fachgebieten zu personenbezogenen Einzeldatensätzen.

Soll eine künftige Volkszählung "registergestützt" erfolgen, ist hierzu wie bei jedem anderen Zensus eine gesetzliche Grundlage erforderlich. Sie muß für die Bürgerinnen und Bürger und die rechtsanwendenden Verwaltungen klar und deutlich regeln, welche Daten aus welchen Registern genutzt, wo und durch wen sie gespeichert und gegebenenfalls auch verknüpft werden dürfen. Insbesondere bedarf es spezieller Regelungen zur Übermittlung der notwendigen Daten und ihrer Löschung.

Bei Realisierung sowohl des Bundesmodells als auch des Ländermodells sind die im Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1/55) festgelegten Grundsätze zu beachten. Eine Totalerhebung war damals deshalb nicht beanstandet worden, weil Alternativen noch mit zu großen Fehlerquoten behaftet waren. Zugleich hat das Gericht - mit Blick auf die sich stetig weiterentwickelnden Methoden der amtlichen Statistik und der Sozialforschung - verdeutlicht, daß sich der Gesetzgeber vor künftigen Entscheidungen für eine Erhebung erneut mit dem dann erreichten Stand der Methodendiskussion auseinanderzusetzen habe. Zu prüfen ist damit, welche der zur Erreichung des angestrebten Zwecks zur Verfügung stehenden statistischen Methoden mit dem geringsten Eingriff in die Rechte der Bürgerinnen und Bürger verbunden sind.

Beiden Modellen ist eine weitgehende Auskunftspflicht eigen. Selbst das Bundesmodell sieht Ortsbegehungen vor, um Zweifelsfälle und Doppelerhebungen aufzuklären. Weiter wollen die Modelle eine Übermittlung von Meldedaten aller Einwohnerinnen und Einwohner an das Statistische Bundesamt, um länderübergreifend Mehrfachmeldungen zu erkennen und zu bereinigen. Es ist fraglich, ob dieser immense Datentransfer durch den damit verfolgten Zweck gerechtfertigt und verhältnismäßig ist. Es bestehen bereits

Zweifel, ob das angestrebte Ziel in der Praxis überhaupt erreicht werden kann, weil die Führung eines fehlerfreien Einwohnermelderegisters zu den Kernproblemen der Datenverarbeitung in diesem Bereich gehört. Deshalb muß noch gründlich geprüft werden, ob eine Bereinigung der Statistik um Mehrfachmeldungen nicht auf anderem, weniger einschneidendem Weg erreicht werden kann oder ob sie nicht verzichtbar ist und eine statistische Ungenauigkeit damit hingenommen werden muß.

Die Modelle lassen zudem nicht erkennen, wie eine Zusammenführung aus verschiedenen Verwaltungsregistern ohne **Registernummer oder Personenkennzeichen** erfolgen soll. Soweit ein solches Kennzeichen eine Verknüpfung der erhobenen Daten mit den bei Verwaltungsbehörden vorhandenen Datenbeständen oder sogar die Erschließung eines Datenverbundes zuläßt, ist dies mit den im Volkszählungsurteil aufgestellten Grundsätzen nicht vereinbar. Auf keinen Fall darf die beabsichtigte Zusammenführung von Daten die Erstellung von Persönlichkeitsprofilen der Bürgerinnen und Bürger ermöglichen.

Eine erheblich geringere Eingriffstiefe in das Recht auf informationelle Selbstbestimmung würde mit einer **Qualitätsverbesserung bestehender Register und Statistiken** erzielt, um sie für die jeweiligen Fachgebiete effektiver statistisch nutzen zu können. Untersucht werden sollte ebenfalls, ob die gegebenenfalls verbesserten, bestehenden Register und Statistiken für den statistischen Bedarf nicht ohne personengenaue Zuordnung der Datensätze zur Erreichung des angestrebten Zwecks nutzbar sind.

Schließlich muß der Grundsatz beachtet werden, daß die bei der statistischen Bearbeitung der Daten gewonnenen Erkenntnisse nicht in den Verwaltungsbereich zurückfließen dürfen. Die im Ländermodell vorgesehene Gebäude- und Wohnungszählung soll zum Beispiel in Gebäude- und Wohnungsregistern fortgeführt werden. Wenn die Kommunen die Führung der Register übernähmen, wäre kaum noch erkennbar, wie die Zweckbindung der Erhebung für statistische Zwecke eingehalten werden könnte.

"Eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger ist auch in der Anonymität statistischer Erhebungen unzulässig" (BVerfGE 65, 1/53).

10. Bildung und Wissenschaft

Der Einzug neuer Informations- und Kommunikationstechniken im Bildungsbereich verändert auch hier die Datenverarbeitung grundlegend. Besonders weit entwickelt sind die Anwendungen im **Hochschulbereich.** Dort wird der Informationsaustausch für Forschung und Lehre mit elektronischer Kommunikation über hochschulinterne Netze, über das Breitband-Wissenschaftsnetz unter den Hochschulen und über das Internet weltweit bewältigt. Die Nutzung der neuen Medien setzt umfangreiche Datenflüsse in Gang. Das bewirkt nicht nur Zufriedenheit über die neuen Dimensionen der Recherche- und Kommunikationsmöglichkeiten, sondern löst auch **Unsicherheiten** bei der Bewältigung neuer Probleme im Umgang mit personenbezogenen Daten und Befürchtungen hinsichtlich etwaiger **Beeinträchtigungen des Persönlichkeitsschutzes** aus. Dasselbe passiert im **Schulbereich,** allerdings hier überwiegend noch im Anfangsstadium und deshalb mit der Chance, die neuen Medien selbstverantwortlich nutzen zu lernen und **Datenschutzaspekte von Anfang an einzubeziehen.**

10.1 Die Schulen und das Internet

Die bisherige Entwicklung:
Ausstattung mit Hardware, Anschaffung von Software, Sponsoring mit Übernahme der Kosten für die Internet-Nutzung, Ausbildung von Mentorinnen und Mentoren, Bildungsserver und Projekte, Selbstversuche mit Homepages.

Unterrichtsziel:
medienkompetente, selbstverantwortliche Schülerinnen und Schüler.

Rahmenbedingungen:
weitgehend offene Nutzung, Vertrautmachen mit dem Internet, Erfahrung mit den Risiken sammeln und den sicheren Umgang mit dem Medium erarbeiten.

Die Nutzung des Internet wird vor Ort vorbereitet. Dabei gilt es aber gerade auch, den Datenschutzanforderungen gerecht zu werden. Meine Dienststelle **arbeitet** in der Projektgruppe **"NRW-Schulen ans Netz" mit,** um dazu beizutragen, praktisch umsetzbare Lösungen für die damit verbundenen Fragen zu finden.

10.1.1 Basisinformation der Schülerinnen und Schüler

Im Internet können Schülerinnen und Schüler "surfen", sich informieren, spielen und Nachrichten austauschen. Der dabei von ihnen preisgegebenen personenbezogenen Daten und hinterlassenen Spuren müssen sie sich allerdings **bewußt** sein. Neben einer umfassenden **Information** über die Funk-

tionsweise des Internet und dessen Möglichkeiten der weltweiten Kommunikation sind die Schülerinnen und Schüler daher auch über **Risiken** und **Schutzmaßnahmen** zu unterrichten. Dabei sollten folgende Gesichtspunkte einbezogen werden:

- Eine vollständig anonyme Nutzung ist dem Internet bereits aus abrechnungstechnischen Gründen bis heute grundsätzlich fremd. In aller Regel wird es personenbezogen, personenbeziehbar - über die sogenannte User-ID - oder unter Gruppenkennungen genutzt. Daher hinterläßt etwa jedes Aufblättern von Homepages **Datenspuren**, aus denen Nutzungs- und Kommunikationsprofile erstellt werden können - beispielsweise welches Diskussionsforum von wem wie oft aufgesucht wurde.

- Bei Kommunikationsvorgängen - etwa per E-Mail - werden Daten in der Regel nicht gesichert, so daß sie auf ihrem Weg durch das öffentliche Netz **ausgespäht** werden können.

Aus der **unsicheren Infrastruktur** des Internet erwachsen Gefahren für die Vertraulichkeit und inhaltliche Integrität der übertragenen Daten. Zudem können bestehende Schwachstellen der Endgeräte ausgenutzt werden, um sich mit relativ wenig Aufwand unbemerkt einen unberechtigten Zugang zu dem kommunizierenden Rechner zu verschaffen. So können Daten **ausgespäht**, aber auch **manipuliert** oder **gelöscht** werden. Unverschlüsselte und nicht digital signierte Nachrichten sind so leicht les-, veränder- und unterdrückbar wie eine **maschinengeschriebene Postkarte,** die außerdem auch eine **andere Person** geschrieben haben kann. **Gewißheit** über die Richtigkeit von Inhalt und Herkunft gibt es also nicht. Wie sie sich nach dem heutigen Stand der Erkenntnisse **herstellen** läßt, findet sich unter 2.2.

Beispiele für die "gläserne" Internet-Nutzung:

- Mit Suchprogrammen wie etwa "deja news" lassen sich **Profile** aller in Newsgroups Kommunizierenden erstellen. Auf diese Weise können zum Beispiel Hobbys und persönliche Neigungen erfaßt werden.

- Im Internet können digitale **"cookies"** auf der Festplatte des eigenen Rechners hinterlassen und bei der nächsten Einwahl automatisch wieder aufgerufen werden. Ohne Einwilligung ist das unzulässig.

- Wer sich in die Homepage der Schule - selbst unter so harmlosen Rubriken wie etwa dem "Treffpunkt" oder ähnlichem - mit Namen, Adresse

oder anderen Erreichbarkeitsdaten **aufnehmen läßt,** sollte damit rechnen, daß dies auch **unerwünschte Werbung** zur Folge haben kann.

Bei einem Internet-Zugang über einen Schul-PC bleibt die individuelle Nutzung nach draußen meist ohnehin anonym, da in aller Regel nur die Kennung des Schul-PC in Erscheinung tritt. Die Verwendung eines Pseudonyms - etwa in Chatrooms - schadet jedoch nie. Ebenso sollten Nachrichten verschlüsselt werden, wenn ihr Inhalt niemanden etwas angeht.

10.1.2 Nutzungsordnungen

Die schulische Internet-Welt setzt verbindliche Spielregeln voraus, die den Nutzungsumfang, Art und Weise der Nutzung und die Kontrolle von Mißbrauch festlegen.

Solche Nutzungsordnungen werden folgendes zu regeln haben:

- Genaue Festlegung der an der Schule zugelassenen **Internetdienste** und der **Nutzungsrechte** von Schülerinnen und Schülern, aber auch der Lehrkräfte.

- Bestimmungen darüber, in welchem Rahmen die Lehrkräfte **weisungsbefugt** sein sollen und wann den Schülerinnen und Schülern **unbeobachtete Kommunikation** außerhalb des Unterrichts möglich ist.

- Festlegungen darüber, **wer** zu welchem Zweck temporäre Internet-Dateien einsehen darf und wann diese zu löschen sind.

Einem höheren Maß an Klarheit könnte es auch dienen, in die Nutzungsordnung **Hinweise** auf medienrechtliche **Bestimmungen** und deren datenschutzrechtliche **Grundsätze** aufzunehmen - etwa, daß das **Fernmeldegeheimnis** zu beachten ist, und daß Kontrollen zur Feststellung von unerlaubten Nutzungen außerhalb des Unterrichts nur mit **Kenntnis** der Betroffenen und **stichprobenartig** durchgeführt werden dürfen.

Weder die Schule noch das Internet sind rechtsfreie Räume. Die den Schülerinnen und Schülern zu vermittelnde Medienkompetenz sollte auch Datenschutzkompetenz umfassen.

10.2 Keine Wahl beim Studierendenausweis mit Chip?

Mit der anstehenden Gesetzesnovelle wird den Hochschulen ermöglicht, zwangsweise einen Studierendenausweis in Form einer Chipkarte einzuführen.

Der Referentenentwurf für ein neues Hochschulgesetz sieht in § 65 Abs. 1 Satz 3 vor, daß die Einschreibungsordnungen der Hochschulen diejenigen Daten der Studierenden festzulegen haben, die zur Aufgabenerfüllung der Hochschulen erforderlich sind, insbesondere für einen mit **maschinellen Verfahren und Datenträgern unterstützten Studierendenausweis**. Der Entwurfsbegründung ist zu entnehmen, daß davon auch **Chipkarten** erfaßt sein sollen. Die Chipkarte soll zudem nicht auf die Ausweisfunktion begrenzt sein, sondern ihre Dienste beispielsweise auch für Rückmeldungen, Hochschulwechsel, Bibliotheks- und Mensanutzung sowie Gebührenzahlungen leisten. Solche **multifunktionalen** Chipkarten sind nicht unproblematisch. Anläßlich eines Modellversuchs an einer Universität hatte sich schon der 13. Datenschutzbericht (Seite 102 f.) unter der Fragestellung: "Bequeme Welt oder gläserne Studierende?" mit ihren Vor- und Nachteilen auseinandergesetzt. Die dort vorsorglich formulierten **Anforderungen** an die Rahmenbedingungen und an die konkrete Ausgestaltung eines Karteneinsatzes haben ihre Gültigkeit nicht verloren und angesichts des Referentenentwurfs noch an Aktualität gewonnen. Eine **gesetzliche Regelung** muß mindestens folgende Festlegungen treffen:

- Den Studierenden ist ein **Wahlrecht** einzuräumen; sie müssen ohne Benachteiligung auf die Chipkarte insgesamt oder auf einzelne Funktionen verzichten können.

- Die von der Chipkarte umfaßten **Funktionen** müssen **abschließend** festgelegt sein.

- Bestimmt werden muß, **wer** verarbeitende Stelle und **verantwortlich** für Speicherung, Veränderung und Löschung der Daten auf der Chipkarte sein soll.

- Festzulegen ist, wer auf die Daten lesend zugreifen und Daten aus der Chipkarte für eigene Zwecke speichern und nutzen können soll; die jeweiligen **Zwecke** müssen im einzelnen **bestimmt** werden.

- Die Studierenden müssen die Möglichkeit haben, die auf der Chipkarte gespeicherten Daten an dafür bereitgestellten Lesegeräten **kostenlos** und **jederzeit überprüfen zu können**.

- Es sind Regelungen über die technischen und organisatorischen Maßnahmen zu treffen, mit denen die datenschutzgerechte Datenverarbeitung gewährleistet wird. Vor allem betrifft dies die fälschungssichere **Authentifizierung** der Karteninhaberin oder des Karteninhabers, die Steuerung der Zugriffs- und Nutzungsberechtigung sowie die **Vertraulichkeit** und **Integrität** der gespeicherten Daten.

- Die Erstellung von **Nutzungsprofilen** ist zu verbieten.

- Aufzunehmen sind Vorschriften zum Schutz gegen **mißbräuchliche Verwendung** der Daten durch Dritte bei Verlust der Chipkarte.

Die gesetzliche Festlegung der Bedingungen für die Datenverarbeitung mit der Chipkarte bedeutet natürlich keinen absoluten Schutz vor Mißbrauch der gewonnenen Daten oder auch nur vor Versehen bei der Datenverarbeitung. Wer sich freiwillig für den Kartengebrauch mit allen oder auch nur einigen Funktionsmöglichkeiten entscheiden möchte, muß - um eine wirksame Einwilligungserklärung abgeben zu können - vorher umfassend unterrichtet sein über Art, Umfang und Zweck der mit der Chipkarte möglichen Datenverarbeitung und die beteiligten Stellen. Je **komplexer** die Chipkarte gestaltet ist, desto **unüberschaubarer** wird die damit erfolgende Datenverarbeitung. Problematisch sind insbesondere alle Online-Nutzungen, eine größere Zahl unterschiedlicher lese- und schreibberechtigter Stellen sowie umfangreiche Datensätze. Wird nicht bei jeder Nutzung für die Betroffenen erkennbar, welche Daten an einer Stelle gespeichert und eventuell weitergegeben sowie welche Daten neu auf der Chipkarte gespeichert werden, sind erteilte Einwilligungen unwirksam; die Datenverarbeitung ist dann unzulässig.

Die Chipkarte darf kein Zwang sein. Bei ihrem Einsatz müssen Transparenz und Sicherheit gewährleistet sein.

10.3 Forschung

Forschung kann das Recht der Betroffenen auf informationelle Selbstbestimmung beeinträchtigen, wenn datenschutzrechtliche Anforderungen nicht bereits in der Projektplanung berücksichtigt werden.

Da bei vielen Forschungsvorhaben im Grunde vergleichbare Datenschutzprobleme zu lösen sind, beantwortet der **Leitfaden "Selbstbestimmung und Erkenntnisdrang"** die Fragen, die sich im Forschungszusammenhang am häufigsten stellen und gibt Tips für die Gestaltung von **Merkblättern** und **Einwilligungserklärungen**. Der Leitfaden zu Datenschutz und Forschung kann bei meiner Dienststelle **angefordert** oder unter **"www.**

lfd.nrw.de" oder **"www.nordrhein-westfalen.datenschutz.de"** abgerufen werden.

Oft bedarf es nur einiger Ideen im organisatorischen Ablauf eines Forschungsprojektes, um von vornherein sicherzustellen, daß **gar keine** personenbezogenen Daten **verarbeitet** werden müssen. Dann entsteht auch kein Datenschutzproblem. Wenn im Rahmen der Forschung allerdings personenbezogene Daten zur Kenntnis genommen werden sollen, ist **vorher grundsätzlich** die **Einwilligung** der betroffenen Personen einzuholen. Unter welchen Voraussetzungen dies ausnahmsweise unterbleiben kann, regeln beispielsweise § 6 Abs. 2 GDSG NW und § 28 Abs. 2 DSG NW.

Die Daten sind in jedem Fall so frühzeitig wie möglich von ihrem **Personenbezug zu trennen**. Konkret bedeutet dies zum Beispiel folgendes: Besteht das Untersuchungsziel darin, Ergebnisse über die Entwicklung der Rechtsprechung zu gewinnen - etwa in Schuld- oder Strafzumessungsfragen -, so müssen einzelne Strafverfahrensakten ausgewertet werden. Da es für das Erkenntnisziel - Rechtsprechungsentwicklung - bedeutungslos ist, wer die betroffenen Personen sind, können schon die einzelnen Akten in **anonymisierter** oder **pseudonymisierter Form ausgewertet** werden. Dafür kann entweder auf mögliche Identifikationsdaten vollständig verzichtet werden, oder es werden Pseudonyme vergeben und die Informationen darüber, wer sich hinter den Pseudonymen verbirgt, getrennt von der Auswertung des Akteninhalts aufbewahrt. Eine **getrennte Aufbewahrung** von Identifikationsdaten vereinfacht zudem ihre frühestmögliche Löschung.

Etwas komplizierter wird es allerdings dort, wo es um qualitative Aussagen geht, die etwa auf der Grundlage mehrstündiger **Befragungen** zur individuellen Lebensgeschichte oder zu spezifischen Vorfällen gewonnen werden sollen. Hier muß schon bei der **Information** der Betroffenen über den Forschungszweck, das Forschungsziel, die vorgesehene Verarbeitung ihrer Daten und insbesondere über die gegebenenfalls unter Darstellung der Gesprächsinhalte erfolgende Veröffentlichung der Forschungsergebnisse darauf geachtet werden, daß keine **Mißverständnisse** entstehen. Bei derartigen Vorhaben ist nämlich eine vollständige Anonymisierung kaum leistbar. Gemeint ist mit der vollständigen Anonymisierung nicht lediglich das Weglassen unter anderem des Namens, sondern die Möglichkeit, daß nicht einmal das engere soziale Umfeld oder auch andere Personen, die über Zusatzwissen verfügen, die betreffende Person identifizieren können. Die in solchen Forschungsprojekten tätigen Personen können und sollten sich also in ihren Darstellungen um die größtmögliche Anonymität **bemühen**, eine **vollständige Anonymität** im eben genannten - datenschutzrelevanten - Sinne **ga-**

rantieren können sie den betroffenen Personen **nicht**. Die Betroffenen müssen über dieses verbleibende **"Restrisiko" informiert** sein.

Soweit **Forschungsergebnisse** mit personenbezogenen Daten nicht nur in althergebrachter Form veröffentlicht, sondern auch ins **Internet** eingestellt werden sollen, bedarf es angesichts der Netzrisiken auch einer **Einwilligung** der betroffenen Personen in diese **spezifische Form** der Veröffentlichung. § 28 Abs. 4 b DSG NW macht auch **ohne Einwilligung** die Veröffentlichung personenbezogener Daten dann möglich, wenn dies für die Darstellung von Forschungsergebnissen über Ereignisse der **Zeitgeschichte** unerläßlich ist. Da der Gesetzgeber derartigen Forschungsergebnissen ein besonderes Gewicht zugemessen hat, und da die Veröffentlichungsvoraussetzungen gleichwohl streng sind, dürften bei ihrem Vorliegen im Regelfall keine durchgreifenden Bedenken gegen eine Publikation im Netz bestehen.

11. Öffentlicher Dienst

Die in meiner Dienststelle erarbeiteten Vorschläge zu dem Entwurf einer **Verwaltungsverordnung zur Ausführung des Landesbeamtengesetzes** - unter anderem präzisere Regelungen für Datenerhebungen im Bewerbungsverfahren und Hinweise zu den neuen personalaktenrechtlichen Vorschriften des Landesbeamtengesetzes - wurden leider nur in geringem Umfang berücksichtigt. Daß die ebenfalls vorgeschlagene Präzisierung der Vorschriften über die Datensicherheit bei Transport und Versand von Personalakten notwendig ist, um Datenschutzpannen vorzubeugen, zeigt der im nächsten Unterpunkt zu schildernde Fall recht plastisch.

11.1 "Ihre Personalakte konnte trotz umfangreicher und wiederholter Bemühungen nicht wieder aufgefunden werden ..."

Diesen Satz mußte eine Bezirksregierung 15 Beschäftigten der Arbeitsschutzverwaltung mitteilen, die sich um den Aufstieg vom mittleren in den gehobenen Dienst beworben hatten und deren Personalakten deshalb der obersten Dienstbehörde vorzulegen waren.

Die bei der Bezirksregierung befindlichen Personalakten sollten dem - damaligen - Ministerium für Arbeit, Gesundheit und Soziales durch Kurier überbracht werden. Der Kurier hatte die Sendungen der Poststelle der Staatskanzlei zu überbringen, die als Verteilerstelle fungiert. Feststellbar war noch, daß das an das Ministerium adressierte Aktenpaket in der Poststelle der Staatskanzlei abgegeben wurde, allerdings **ohne Empfangsbestätigung**. Trotz umfangreicher Recherchen verlor sich dort die Spur der Personalakten. In den fraglichen Zeitraum fiel gerade ein Umzug des Ministeriums.

Die Betroffenen wurden von der Bezirksregierung gebeten, bei der Rekonstruktion ihrer Personalakten zu helfen, um die dienstlichen Werdegänge wieder lückenlos dokumentieren zu können. Dabei galt es, überflüssige Datenerhebungen im Einvernehmen mit den Betroffenen zu vermeiden. Die erkennbar gewordenen Datenschutzdefizite wurden auch mit dem Ministerium sowie der Staatskanzlei erörtert und ergänzende Sicherheitsregelungen empfohlen.

Pannen dieser Art lassen sich nur vermeiden, wenn die Einhaltung der getroffenen Sicherheitsvorschriften auch kontrolliert wird.

11.2 Bewerbungsverfahren

Bei Bewerbungen gibt es keinen Dienstweg - hieß es im 13. Datenschutzbericht 1995/96 (Seite 111/112). Erfreulicherweise halten sich die öffentlichen Stellen jetzt an diese Regel und verzichten in Ausschreibungstexten auf die Anforderung, Bewerbungen auf dem Dienstweg vorzulegen. Darüber hinaus achtet auch das Ministerium für Inneres und Justiz darauf, daß die in der Stellenbörse der Landesverwaltung veröffentlichten Ausschreibungstexte dieser Datenschutzregel entsprechen.

In einem anderen Bereich läßt der Umgang mit Daten von Bewerberinnen und Bewerbern dagegen noch immer zu wünschen übrig: Bei **polizeiärztlichen Einstellungsuntersuchungen,** deren unverhältnismäßige Intensität bereits im 13. Datenschutzbericht 1995/96 (Seite 112) kritisch kommentiert wurde, wird immer noch nach der in etlichen Punkten datenschutzrechtlich bedenklichen Polizeidienstvorschrift "Ärztliche Beurteilung der Polizeidiensttauglichkeit und der Polizeidienstfähigkeit" (PDV 300) verfahren. Eine dem Gebot der Erforderlichkeit entsprechende Überarbeitung ist dringend anzumahnen.

11.3 Befragungen von Mitarbeiterinnen und Mitarbeitern - zuverlässige Ergebnisse sind gefragt

Arbeitsplatzuntersuchungen und Mitarbeiterbefragungen sind häufig Bestandteile von Organisationsuntersuchungen zur Erprobung neuer Steuerungsmodelle.

Zur Teilnahme an einer Befragung von Mitarbeiterinnen und Mitarbeitern sind Beschäftigte öffentlicher Stellen verpflichtet, soweit die Datenerhebung zur Aufgabenerfüllung der Dienststelle erforderlich ist (§ 29 Abs. 1 DSG NW). Die Erhebung von Beschäftigtendaten im Rahmen einer Organisationsuntersuchung stellt keine Zweckänderung dar.

Anders verhält es sich mit Fragestellungen, deren Erforderlichkeit für Zwecke der Organisationsuntersuchungen nicht bejaht werden kann - zum Beispiel allgemeine Einschätzungen oder nicht objektivierbare Angaben. Im Hinblick darauf, daß Vorstellungen und Ideen von Mitarbeiterinnen und Mitarbeitern bei der Umsetzung neuer Steuerungsmodelle in den öffentlichen Stellen zweckmäßig sein dürften, werden solche Informationen oft in Mitarbeiterbefragungen einbezogen. Sie dürfen aber nur auf **freiwilliger Grundlage** erhoben werden.

Bei Mitarbeiterbefragungen ist Transparenz geboten. Sie wird durch ausführliche Informationen über die verfolgten Zwecke erhöht.

11.4 Tele-Heimarbeit - Hinweise für eine datenschutzgerechte Einführung

Im Informations- und Kommunikationszeitalter gewinnt die Telearbeit als Arbeitsform auch in der öffentlichen Verwaltung zunehmend an Bedeutung. Dies zeigt sich auch darin, daß im Berichtszeitraum mehrere Kommunen über die datenschutzgerechte Einführung von Telearbeit beraten werden wollten. Darüber hinaus wurden die Modellprojekte "Telearbeit in NRW - Das virtuelle Büro" und "Arbeit zu Hause" der Bezirksregierungen Düsseldorf und Münster beratend begleitet. Nicht zuletzt durch die im Rahmen der TaskForce Telearbeit der Landesinitiative "media NRW" stattfindenden Aktivitäten ist mit einer Zunahme von Telearbeitsprojekten zu rechnen. Aus diesem Grunde bietet es sich an, datenschutzrelevante Hinweise einmal zusammenfassend als Leitfaden zur datenschutzgerechten Planung und Einführung von Telearbeit darzustellen.

> Telearbeit ist jede auf Informations- und Kommunikationstechnik gestützte Tätigkeit, die an einem Arbeitsplatz verrichtet wird, der außerhalb der Diensträume der öffentlichen Stelle liegt und mit dieser durch elektronische Kommunikationsmittel verbunden ist.

Telearbeit kann in verschiedenen Ausprägungen erfolgen. Zu nennen sind beispielsweise die mobile Telearbeit, die Telearbeit im Telecenter in Form von Satellitenbüros oder Nachbarschaftsbüros sowie die On-Site-Telearbeit. Die Tele-Heimarbeit ist die Form der Telearbeit, mit der sich die öffentliche Verwaltung in ihren Planungen und unmittelbaren Aktivitäten zur Zeit vordringlich beschäftigt. Bei der **Tele-Heimarbeit** verrichten die Beschäftigten ihre Arbeit an einem Arbeitsplatz in ihrer heimischen Umgebung. Steht ihnen zusätzlich noch ein Arbeitsplatz in den Diensträumen der öffentlichen Stelle zur Verfügung und wechseln sie zwischen dem heimischen und dem dienstlichen Arbeitsplatz, kann von alternierender Tele-Heimarbeit gesprochen werden.

Die (alternierende) Tele-Heimarbeit ist eine Arbeitsform, die den Beschäftigten sowie den öffentlichen Stellen einige Vorteile bietet. Festzustellen ist, daß in nicht wenigen Fällen die Initiative für die Einführung von Tele-Heimarbeit von den Beschäftigten ausgeht. Für sie dürften für ihr Interesse an dieser Arbeitsform unter anderem die folgenden Aspekte von Bedeutung sein:

- Bessere Vereinbarkeit von Beruf, Familie und Freizeit.
- Größere Flexibilität und Zeitsouveränität bei der Arbeit.
- Erleichterung der Wiedereingliederung in das Erwerbsleben für bestimmte Gruppen, wie Beschäftigte mit Familie, Alleinerziehende und Behinderte.
- Reduzierung der Fahrten zur Dienststelle.

11.4.1 Allgemeines

Der Tele-Heimarbeit stehen keine grundsätzlichen datenschutzrechtlichen Bedenken entgegen. Allgemein gilt aber, daß bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen die gesetzlichen Vorschriften über den Datenschutz einzuhalten sind, und zwar unabhängig von der Art und dem Ort der Verarbeitung. Die Besonderheit der Tele-Heimarbeit liegt darin begründet, daß die öffentliche Stelle die unmittelbare **Verfügungsgewalt** über die Daten verliert, die an Tele-Heimarbeitsplätzen verarbeitet werden. Jede Bürgerin und jeder Bürger hat aber das Recht auf eine ordnungsgemäße Verarbeitung ihrer oder seiner personenbezogenen Daten, so daß die Bedingungen dafür auch in der häuslichen Umgebung der Beschäftigten zu gewährleisten sind. Deshalb hat die öffentliche Stelle sicherzustellen, daß ihre Organisationshoheit nicht an der Haustür der Dienststelle endet. Da sie in den häuslichen Bereich ihrer Beschäftigten nur durch verbindliche vertragliche Vereinbarungen hineinwirken kann, sind die erforderlichen Voraussetzungen und Bedingungen dafür explizit festzulegen. Eine Dienstvereinbarung oder eine Dienstanweisung ist notwendige Voraussetzung und damit Grundlage, um die Sicherstellung von Datenschutz und Datensicherheit bei der Verarbeitung personenbezogener Daten an Tele-Heimarbeitsplätzen gewährleisten zu können.

11.4.2 Grundsätzliche Anforderungen/Hinweise

Bei der Planung und Einführung von Tele-Heimarbeit ist insbesondere folgendes zu beachten:

- Vor der Einrichtung eines Tele-Heimarbeitsplatzes ist zu prüfen, ob die Verarbeitung personenbezogener Daten zwingend erforderlich ist oder ob eine Bearbeitung von Vorgängen auch **ohne Personenbezug** oder in **pseudonymisierter** Form möglich ist.

- Personenbezogene Daten, die Berufs- oder besonderen Amtsgeheimnissen unterliegen, sollten **nicht** in Tele-Heimarbeit verarbeitet werden. Hierzu zählen insbesondere Sozial-, Personal- und Steuerdaten sowie Beihilfedaten und medizinische Daten.

- Die Tele-Heimarbeit ist **keine Auftragsdatenverarbeitung**. Die Tele-Heimarbeiterinnen und Tele-Heimarbeiter bleiben Beschäftigte der Dienststelle.

- Die Dienststelle, der die in Tele-Heimarbeit Beschäftigten angehören, ist als öffentliche Stelle im Sinne des § 7 DSG NW **verantwortlich** für die Sicherstellung des Datenschutzes.

- Die Dienststelle ist und bleibt **weisungsbefugt** und bestimmt die Art und Weise, wie die Aufgaben der Tele-Heimarbeit zu erledigen sind.

- In einer Dienstanweisung oder Dienstvereinbarung sind die Tele-Heimarbeiterinnen und Tele-Heimarbeiter auf die Einhaltung aller vorgegebenen Sicherheitsmaßnahmen zu **verpflichten**. Gravierende Verstöße sollten eine fristlose Beendigung des Tele-Heimarbeitsverhältnisses zur Folge haben.

- Die Beschäftigten, die Tele-Heimarbeit verrichten, sind schriftlich über ihre **Pflichten** nach § 6 DSG NW zu belehren. Eine Durchschrift dieser Belehrung ist der Personalakte beizufügen.

- Die Dienststelle muß für sich selbst und für die Landesbeauftragte für den Datenschutz ein **Kontrollrecht** in der Wohnung der Tele-Heimarbeiterin oder des Tele-Heimarbeiters ausbedingen. Wegen des Grundrechts auf Unverletzlichkeit der Wohnung bedarf dies der Zustimmung der Betroffenen. Wird die Einwilligung abgelehnt, kann die Tele-Heimarbeit nicht stattfinden. Der Widerruf einer bereits erteilten Einwilligung muß die Beendigung der Tele-Heimarbeit zur Folge haben.

- Damit die Landesbeauftragte für den Datenschutz ihre Kontrollaufgaben wahrnehmen kann, muß sie über die Einrichtung von Tele-Heimarbeitsplätzen, an denen personenbezogene Daten verarbeitet werden, rechtzeitig **unterrichtet** werden.

- Die Dienststelle, die personenbezogene Daten in Tele-Heimarbeit verarbeitet, hat sicherzustellen, daß die Betroffenen in der Wahrnehmung ihrer **Rechte** durch diese Arbeitsform nicht eingeschränkt werden.

- Beim Einsatz von Tele-Heimarbeitsplätzen ist nicht auszuschließen, daß auch Daten aus dem privaten Bereich über die in Tele-Heimarbeit Beschäftigten anfallen. So könnte beispielsweise festgestellt werden, zu welcher Zeit welche Arbeitsergebnisse per Datenübertragung an die Dienststelle weitergeleitet wurden. Insofern muß festgelegt werden, ob überhaupt und gegebenenfalls welche **Arbeitszeitdaten** und **-ergebnisse** der Beschäftigten mit welchen technischen Einrichtungen im Rahmen der Dienst- und Fachaufsicht zu welchen Zwecken durch die Dienststelle verarbeitet werden dürfen. Daten der Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 DSG NW gespeichert werden, dürfen gemäß § 29 Abs. 5 DSG NW nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

11.4.3 Anforderungen an technische und organisatorische Maßnahmen

Grundsätzlich sind bei der Planung von Tele-Heimarbeitsplätzen Sicherheitskonzepte zu erstellen, welche die **tatsächlichen örtlichen und personellen** Gegebenheiten berücksichtigen. Die umzusetzenden technischen und organisatorischen Maßnahmen sind dabei daraufhin auszurichten, daß jederzeit die Vertraulichkeit, Integrität und Authentizität der Daten sichergestellt ist und deren Verfügbarkeit im Rahmen der von der öffentlichen Stelle zu erfüllenden Aufgaben gewährleistet ist. Die Maßnahmen sind dem jeweiligen **Stand der Technik** entsprechend anzupassen. Die im folgenden aufgeführten Anforderungen an technische und organisatorische Maßnahmen stellen eine **generelle** Leitlinie bei der Einrichtung von Tele-Heimarbeitsplätzen dar und ersetzen nicht ein individuelles Sicherheitskonzept:

- Alle an Tele-Heimarbeitsplätzen zum Einsatz kommenden IT-Komponenten - Geräte, Datenträger, Systemsoftware, Standard- und Anwendungssoftware, Einrichtungen zur Datenfernverarbeitung und -übertragung etc. - stehen grundsätzlich im **Eigentum der Dienststelle**, werden von ihr beschafft, freigegeben, installiert, konfiguriert und administriert. Eine Verwendung privater IT-Komponenten sollte untersagt werden. Die Nutzung nicht freigegebener Software ist durch technische Maßnahmen zu verhindern.

- Die Dienststelle hat für jeden Tele-Heimarbeitsplatz ein **Inventariatsverzeichnis** mit allen jeweils eingesetzten IT-Komponenten und deren Konfigurationen zu führen. Die Verzeichnisse sind auf dem neuesten Stand zu halten.

- Es sind geeignete Maßnahmen in den **Privaträumen** der Beschäftigten zu treffen, die eine Kenntnisnahme, Nutzung und Manipulation von personenbezogenen Daten durch Mitbewohnerinnen und Mitbewohner oder Besuchspersonen ausschließen.

- Für die Verwahrung von dienstlichen Unterlagen - etwa elektronische Datenträger, papierene Unterlagen - im häuslichen Bereich sind von der Dienststelle verschließbare **Behältnisse** zur Verfügung zu stellen, die auch einen ausreichenden Schutz gegen den Verlust und die Zerstörung von Daten bieten.

- Dienstliche Unterlagen, die nicht mehr benötigt werden, müssen einer sachgemäßen **Entsorgung** zugeführt werden können, um Rückschlüsse auf personenbezogene Daten auszuschließen.

- Der Aktentransport und der **Transport** von elektronischen Datenträgern zwischen der Dienststelle und dem häuslichen Arbeitsplatz sollte in verschlossenen Behältnissen erfolgen, die von der Dienststelle zur Verfügung gestellt werden. Die Daten auf den zu transportierenden elektronischen Datenträgern sind zu **verschlüsseln**. Die Transportwege und alle sonstigen Umstände des Transports sind so zu wählen, daß die Akten und Datenträger ihr Bestimmungsziel sicher und zeitgerecht erreichen.

- Die am Tele-Heimarbeitsplatz auf elektronischen Datenträgern vorgehaltenen personenbezogenen Daten sind zu verschlüsseln. Die **Verschlüsselungsmethode** und die Schlüssel sind von der Dienststelle vorzugeben.

- Werden Daten mittels **Datenfernübertragung** zwischen Tele-Heimarbeitsplatz und Dienststelle transferiert, so haben sich die beteiligten Systeme vor Aufnahme einer jeden Kommunikation gegenseitig zu **authentifizieren**. Die im Anschluß an die Authentifikation zu übertragenden Daten sind zu **verschlüsseln**. Darüber hinaus ist die Integrität und Authentizität der zu übertragenen Daten sicherzustellen. Die hierfür zum Einsatz kommenden technischen Verfahren sind abhängig von der Schutzbedürftigkeit der Daten auszuwählen. Für den Austausch sensibler personenbezogener Daten sollten digitale Signaturverfahren eingesetzt werden.

- Im Einzelfall ist zu prüfen, ob durch entsprechende **Quittungsverfahren** sicherzustellen ist, daß transferierte Daten ihre Empfängerin oder ihren Empfänger auch erreicht haben.

- Beim Einsatz elektronischer Rechner ist sicherzustellen, daß sich die Tele-Heimarbeiterin oder der Tele-Heimarbeiter gegenüber dem System authentifizieren muß und die Daten nur im Rahmen der festgelegten **Berechtigungen** verarbeiten kann. Zur **Authentifizierung** sollte ein Chipkarten-basiertes Verfahren gewählt werden. Sollen sensible personenbezogene Daten verarbeitet werden, ist im Einzelfall zu prüfen, ob biometrische Authentifizierungsverfahren - wie zum Beispiel Fingerabdruckverfahren oder Verfahren zur Handschriftenerkennung - einzusetzen sind. Da bei diesen Verfahren personenidentifizierende Merkmale ausgewertet werden, muß gewährleistet sein, daß das zur Wahl stehende biometrische Verfahren datenschutzgerecht ausgestaltet ist. Hinweise dazu enthält der "Kriterienkatalog zur Bewertung der Vergleichbarkeit biometrischer Verfahren" der TeleTrust Deutschland e.V. Außerdem muß das Verfahren eine technische Reife besitzen, die einen praktikablen Einsatz ermöglicht.

- Bei elektronischen Rechnern ist sicherzustellen, daß der eingeschaltete **Bildschirm** automatisch **gesperrt** wird, wenn die Tele-Heimarbeiterin oder der Tele-Heimarbeiter in einem bestimmten Zeitraum keine Aktivität mehr entwickelt. Die Entsperrung erfolgt erst wieder nach der Authentifizierung.

- Verändernde **Zugriffe** auf die Betriebssystemebene und auf die Konfigurationen sonstiger IT-Komponenten des Tele-Heimarbeitsplatzes durch die Tele-Heimarbeiterin oder den Tele-Heimarbeiter sind zu untersagen und soweit möglich **technisch zu verhindern.** Sie bleiben ausschließlich der Systemadministration der Dienststelle vorbehalten.

- Auf den eingesetzten elektronischen Rechnern dürfen keine anderen als die von der Dienststelle vorgegebenen **Aufgaben** zum Ablauf gebracht werden. Die Dienststelle hat sicherzustellen, daß personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden.

- Der elektronisch gespeicherte **Datenbestand** ist so **gering** wie möglich zu halten.

- Es sind geeignete und für die Tele-Heimarbeiterin und den Tele-Heimarbeiter leicht handhabbare, möglichst automatisierte Verfahren zur **Sicherung** und **Wiedereinspielung** des elektronischen Datenbestandes zu implementieren. Die Intervalle zur Datensicherung sollten abhängig von den anfallenden Daten festgelegt werden. Mindestens ist jedoch einmal täglich eine Sicherung durchzuführen.

- Zur Gewährleistung der Revisionssicherheit sind entsprechende **Protokollierungen** durchzuführen. Die Protokolldaten sollen der Nachvollziehbarkeit aller maßgeblichen Ereignisse dienen, die im Rahmen der automatischen Verarbeitung personenbezogener Daten eintreten und im Hinblick auf Sicherheitsverstöße und die Datenschutzkontrolle auswertbar sein. Der Protokollumfang, die Protokolldichte und die Löschfristen für die Protokolldaten sind abhängig von der Sensibilität der zu verarbeitenden personenbezogenen Daten festzulegen. Die Protokolle sind manipulationssicher und nur von Berechtigten auswertbar zu erstellen. Sie sind gesichert aufzubewahren und entsprechend festgelegter Vorgaben der Dienststelle zugänglich zu machen. Die Auswertung der Protokolle unterliegt einer strikten Zweckbindung.

- Bei einem Online-Anschluß des elektronischen Rechners eines Tele-Heimarbeitsplatzes an das Rechnersystem der Dienststelle sind auf **beiden Seiten Sicherheitsmaßnahmen** zu implementieren, welche die Integrität, Vertraulichkeit und Verfügbarkeit der Daten beider Systeme gewährleisten.

- Es ist sicherzustellen, daß die Administration der Tele-Arbeitsplätze bedarfs- und zeitgerecht durch die **Systemadministration** der Dienststelle wahrgenommen werden kann.

- Für den Vertretungsfall - etwa aus Urlaubsgründen - ist durch geeignete Maßnahmen die zeitgerechte **Verfügbarkeit** der hierfür erforderlichen Unterlagen und Daten des Tele-Heimarbeitsplatzrechners für die Vertretung sicherzustellen.

- Die Ausgestaltung der Tele-Heimarbeit muß sicherstellen, daß bei einer Beendigung des Arbeitsverhältnisses die **Rückabwicklung** so erfolgt, daß nachweisbar weder Daten noch Datenträger oder sonstige Unterlagen an dem Arbeitsplatz zurückbleiben. Alle eingeräumten Berechtigungen sind zuverlässig außer Kraft zu setzen.

Abschließend sei noch darauf hingewiesen, daß das Bundesamt für Sicherheit in der Informationstechnik (BSI) in das IT-Grundschutzhandbuch 1998 die Kapitel "Telearbeit" und "Häuslicher Arbeitsplatz" aufgenommen und den Band "Sichere Telearbeit" in der Schriftenreihe zur IT-Sicherheit veröffentlicht hat. Über das Bundesministerium für Arbeit und Soziales ist das Buch "Telearbeit - Ein Leitfaden für die Praxis" erhältlich, welches einen umfassenden Überblick über das Thema Telearbeit bietet.

12. Verkehr, Wirtschaft und öffentliche Unternehmen

12.1 Führerschein im neuen Gewand - was verbirgt sich dahinter?



Seit dem 1. Januar 1999 ist der neue EU-Führerschein zu haben; handlich klein, im Scheckkartenformat und fälschungssicher soll er sein.

Einen **Zwangsumtausch** der alten Führerscheine wird es **nicht** geben. Dagegen hatten sich die Datenschutzbeauftragten des Bundes und der Länder gewehrt, weil dies de facto zu einer bedenklichen bundesweiten Zusammenführung aktueller Meldedaten in einer zentralen Datei - dem Zentralen Fahrerlaubnisregister beim Kraftfahrt-Bundesamt - geführt hätte.

Zu begrüßen ist, daß in dem neuen Straßenverkehrsgesetz die langjährigen Forderungen nach Verbesserungen des Datenschutzes für die Führerscheininhaberinnen und -inhaber umgesetzt worden sind. Vor allem konnte erreicht werden:

- Die unentgeltliche **Auskunft** aus den Registern der Fahrerlaubnisbehörden sowie dem Zentralen Fahrerlaubnisregister und dem Verkehrszentralregister in Flensburg.

- Keine lebenslange **Aufbewahrung** von belastenden Unterlagen in der Führerscheinakte. Die neue Regelung sieht vor, daß grundsätzlich Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse spätestens nach 10 Jahren zu vernichten sind.

- Genaue Festlegung im Gesetz, zu welchen **Zwecken** an welche Behörde welche Fahrerlaubnisdaten übermittelt werden dürfen.

- Keine **regelmäßige** Übermittlung von Angaben durch die Polizei über nur vorübergehende Mängel der Fahrtauglichkeit.

Neu ist auch das **Bonus-System.** Durch den Besuch eines sogenannten Aufbauseminars oder - je nach Punktestand - einer verkehrspsychologischen Beratung sollen Verkehrsteilnehmerinnen und Verkehrsteilnehmer veranlaßt werden, Mängel in ihrer Einstellung zum Straßenverkehr und im verkehrssicheren Verhalten zu erkennen und abzubauen.

Die Sinnhaftigkeit und der Nutzen solcher Schulungen sollen hier gar nicht angezweifelt werden. Klar sollte aber sein, daß mit der Teilnahme wiederum ein Stückchen Persönlichkeitsbild festgehalten wird.

12.2 Bekämpfung von mißbräuchlicher Betätigung in Verwaltung und Wirtschaft

12.2.1 Korruptionsregister

In Nordrhein-Westfalen sind auf Landesebene Regeln für die öffentlichen Vergabeverfahren unter meiner Beteiligung erarbeitet worden.

Die kritische Bewertung der Errichtung eines landesweiten Korruptionsregisters (13. Datenschutzbericht, Seite 119) hat dazu beigetragen, daß gegenüber der ursprünglichen, in anderen Bundesländern umgesetzten Absicht, eine Datenbank mit allen Informationen über Fehlverhalten von korruptionsverdächtigen Unternehmen einzurichten, eine zentrale Meldestelle für ausgesperrte Wettbewerberinnen und -bewerber datenschutzgerecht ausgestaltet wurde. Gemäß dem Grundsatz der **Datenvermeidung** werden nur noch Angaben über einen Ausschluß und die Dauer des Ausschlusses gespeichert. Insbesondere konnte vermieden werden, daß auch die einzelnen Ausschlußgründe vorgehalten werden. Es kann deshalb keine Entscheidung aufgrund der dort gespeicherten Daten, sondern nur im **Einzelfall** allein durch die **jeweilige Vergabestelle** und unter Würdigung aller Umstände getroffen werden. Die Vergabestelle kann aber vorher bei der Meldestelle **Auskunft** darüber einholen, ob und durch welche Vergabestelle der Bewerber oder die Bewerberin bereits ausgeschlossen worden ist. Dort können dann gegebenenfalls Einzelheiten zu einer Ausschlußentscheidung abgefragt werden.

Bereits bei der Ausschreibung wird auf die Möglichkeit einer Meldung hingewiesen und im Entscheidungsfall der oder die Betroffene über die Meldung konkret unterrichtet. Außerdem muß mit der Bewerbung die Erklärung unterschrieben werden, daß keine Verfehlungen vorliegen, die einen Ausschluß von der Teilnahme am Wettbewerb rechtfertigen könnten.

12.2.2 Bekanntgabe von Wettbewerbsverstößen

Zum Schutz ihrer Mitglieder können Industrie- und Handelskammern, Handwerkskammern und bestimmte Verbände wettbewerbsrechtliche Unterlassungsansprüche geltend machen. Im Vordergrund steht dabei die Verfolgung unzulässiger Gewerbeausübung.

Zur Koordinierung, Vereinheitlichung und Vereinfachung des Vorgehens gegen den unlauteren Wettbewerb wurde die Zentrale zur Bekämpfung unlauteren Wettbewerbs e.V. Frankfurt am Main (Wettbewerbszentrale) gegründet. Ihr gehören alle Industrie- und Handelskammern, Handwerkskammern und eine Vielzahl von Verbänden an. Zunächst war zu vermuten, daß die Kammern in Nordrhein-Westfalen regelmäßig die Wettbewerbszentrale bei Wettbewerbsverstößen einschalten und damit auch personenbezogene Informationen übermitteln würden. Dem ist allerdings nicht so. Eine Information an die Wettbewerbszentrale erfolgt nur in den Fällen, in denen unzulässige Wettbewerbshandlungen allgemein an die **Öffentlichkeit gerichtet** sind. Dabei werden in der Regel nur veröffentlichte Daten übermittelt, die ihrer Qualität nach ein Vorgehen durch die Wettbewerbszentrale rechtfertigen.

Um schwarzarbeitende Unternehmen wirksam bekämpfen zu können, plante ein Landesinnungsverband die Überwachung dadurch zu verbessern, daß die entsprechenden Firmen in einem **landesweiten Mitgliederrundschreiben** bekanntgemacht werden sollten. Den Mitgliedsbetrieben sollte damit ermöglicht werden, die Einhaltung der strafbewehrten Unterlassungserklärungen vor Ort überwachen zu können. Es ist allerdings **nicht erforderlich,** daß landesweit alle Betriebe informiert werden, wenn es ausreicht, Unterlassungserklärungen mit Namen und konkretem Verstoß nur den Mitgliedsunternehmen mitzuteilen, in deren Tätigkeitsbereich der Wettbewerb stattgefunden hat. Zusätzlich dürfen je nach Sachlage auch die Mitglieder der unmittelbar benachbarten Innungen des betreffenden Handwerks unterrichtet werden. Meiner Auffassung hat sich der Landesinnungsverband angeschlossen.

Eine **räumliche Begrenzung** der Mitteilung war bei den nordrhein-westfälischen Steuerberaterkammern **nicht zu erreichen.** Deren Ahndungen von Wettbewerbsverstößen werden in den jeweiligen Mitteilungsblättern der Kammern veröffentlicht. Eine Beschränkung der Mitteilung lediglich auf die Kammermitglieder, die den Verstoß gegenüber der Kammer angezeigt hatten, wird für nicht ausreichend erachtet, weil wettbewerbsverstoßende Tätigkeiten häufiger in einem größeren Wirtschaftsraum angeboten werden. Die lediglich anonymisierte Bekanntgabe im Mitteilungsblatt erfüllt den Zweck der Veröffentlichung nicht. Außerdem fällt demgegenüber ein schutzwürdiger Belang der wettbewerbswidrig handelnden Personen nicht ins Gewicht; deshalb besteht keine Veranlassung, die Veröffentlichung zu beanstanden.

Allerdings sollten die Personen, die eine strafbewehrte Unterlassungserklärung abgeben, darauf hingewiesen werden, daß dieser Umstand im Mitteilungsblatt der Kammer veröffentlicht wird.

12.2.3 Geldwäsche

Ebenso risikoreich wie zentrale Datensammlungen sind Abgleiche neuer Daten mit vorhandenen Dateien, die ursprünglich einem anderen Zweck dienen sollten.

Kreditinstitute dürfen über ihre gesetzliche Pflicht zur Anzeige von Verdachtsfällen von Geldwäschevorgängen hinaus nicht etwa eine permanente Überwachung aller Kunden- und Kontobeziehungen vornehmen. Instrumente, die einen automatisierten Datenabgleich von typisierten geldwäscheträchtigen Indikatoren mit dem gesamten Datenbestand eines Kreditinstitutes ermöglichen, um vermeintliche Geldwäschesachverhalte herauszufiltern, kommen einer Rasterfahndung gleich, die das Geldwäschegesetz nicht zuläßt.

Im übrigen ist zu konstatieren, daß von den seit Inkrafttreten des Geldwäschegesetzes im Jahr 1993 erstatteten 1156 Verdachtsanzeigen in Nordrhein-Westfalen nur etwa 3% als Geldwäschefälle konkretisiert werden konnten. Dabei wächst die Anzahl der unerledigten Fälle stetig (Quelle: Landeskriminalamt, Lagebild Finanzermittlungen NRW 1997, Nr. 3.1).

12.2.4 Warndateien der Versicherungen

Seit Jahren schon unterhält die Versicherungswirtschaft zentrale Hinweissysteme, mit denen unzulässige Doppelversicherungen sowie Fälle von Versicherungsbetrug aufgedeckt und Risikoerhöhungen wie etwa erhöhte gesundheitliche Risiken im Bereich der Lebensversicherung erkannt werden sollen.

Bei dem Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) in Berlin besteht ein automatisiertes Hinweissystem. Darin wird beispielsweise in der Rechtsschutzversicherung die Kündigung durch die Versicherung nach mindestens zwei Versicherungsfällen innerhalb von 12 Monaten aufgenommen. In der Sachversicherung werden Fälle von Brandstiftung oder Kündigung wegen Verdachts von Versicherungsmißbrauch festgehalten. In der Kraftfahrzeugversicherung erfolgt eine Registrierung von auffälligen Schadensfällen, Diebstählen sowie von Personen, bei denen der Verdacht des Versicherungsmißbrauchs besteht. Dieses Hinweissystem funktioniert so, daß das jeweilige Versicherungsunternehmen den Sachver-

halt, sogenannte Volltexte, an den GDV meldet. Dort wird der Datensatz codiert und auf Datenträgern an die Mitgliedsunternehmen weitergegeben.

Verfahrenstechnisch ist sichergestellt, daß nur der jeweiligen Versicherungsgesellschaft, bei der eine Person einen Versicherungsantrag stellt oder einen Anspruch anmeldet, ausschließlich zu dieser Person ein personenbezogener Abgleich mit der codierten Hinweisdatei möglich ist.

12.3 Direktmarketing von Sparkassen und öffentlichen Versicherungen

War das Direktmarketing zunächst eine Domäne des Versandhandels, so versuchen heute fast alle Branchen, hierüber an Kundschaft heranzukommen.

Wie der Adressenhandel funktioniert und welche Rechte die Betroffenen haben, wenn sie von unerwünschter Werbung verschont bleiben wollen, ist in der Broschüre **"Tips zum Adressenhandel"** dargestellt, die bei meiner Dienststelle **angefordert** und unter **"www.lfd.nrw.de"** oder **"www.nordrhein-westfalen.datenschutz.de"** abgerufen werden kann.

Direktmarketing:
Alle Aktivitäten, die es ermöglichen, die Kundinnen und Kunden unmittelbar und persönlich durch Post, Telefon oder andere Medien anzusprechen und ihnen Dienstleistungen und Produkte anzubieten.

Die öffentlichen Unternehmen, hier insbesondere die Sparkassen und Versicherungsunternehmen, nutzen diese Methoden zur Anknüpfung und Erweiterung ihrer Geschäftsbeziehungen ebenfalls. Versicherungsunternehmen und Sparkassen unterbreiten ihre Produkte den Kundinnen und Kunden häufig in einem Komplettangebot. So kooperieren Sparkasse, Versicherungsunternehmen, Bausparkasse, Immobiliengesellschaft und deren Außendienstteams seit jeher in der Weise, daß von allen jeweils die **gesamte Produktpalette** des Verbundes vermittelt wird. Neu ist nunmehr die Absicht, die Daten aus einem Vertragsverhältnis dazu zu nutzen, für die anderen Finanzdienstleistungsprodukte zu werben und diese Daten untereinander auszutauschen. Da jeder **Datenaustausch** im Verbund grundsätzlich nur mit einer wirksamen **Einwilligung** der Kundinnen und Kunden zulässig ist, wird dazu die sogenannte Allfinanz-Klausel geschaffen. Mit entsprechender Einwilligung soll eine Übermittlung bestimmter Daten an einen Verbundpartner zulässig sein, ohne im Einzelfall die Zustimmung der Betroffenen hierzu einholen zu müssen. Insbesondere weil auch sensible Daten wie Kontostände übermittelt werden, kommt der **Transparenz** und der **Freiwilligkeit**

der Einwilligungserklärungen besondere Bedeutung zu. Die kombinierte Einwilligungs- und Hinweisklausel für die Datenübermittlung lautet wie folgt:

> *"Ich bin damit einverstanden, daß der Vermittler die Daten darüber hinaus für die Beratung und Betreuung auch in sonstigen Finanzdienstleistungen nutzen darf. Soweit hiernach eine Datenübermittlung erfolgen kann, entbinde ich/entbinden wir die (Name der Bausparkasse/Name des Kreditinstituts) vom Bankgeheimnis."*

Die Einwilligungserklärung wird drucktechnisch hervorgehoben und mit dem Hinweis verbunden, daß die Erklärung ohne Folgen für den Vertrag gestrichen oder jederzeit für die Zukunft widerrufen werden kann. Weitere Präzisierungen der Klausel etwa zur Auswahl der zu übermittelnden Daten oder das Ausklammern bestimmter Datenempfängerinnen oder -empfänger konnten nicht durchgesetzt werden.

Um eine praktikable, zugleich aber datenschutzgerechte Lösung zur Einbeziehung der Klauseln in bestehende Verträge zu erzielen, wird als Mindestvoraussetzung eine Benachrichtigung der Betroffenen angesehen. Sie erhalten damit die Möglichkeit, gegebenenfalls Widerspruch gegen eine Verwendung ihrer Daten zu Marketingzwecken zu erheben.

12.4 Datenspuren, Datenschatten im elektronischen Zahlungsverkehr

Die Informationen und Ankündigungen der Kreditwirtschaft sind voll des Lobes für die neuen Techniken: Vielseitigkeit, Bequemlichkeit und Sicherheit für die Kundinnen und Kunden durch den Einsatz von ec-Karte mit Chip, GeldKarte, Homebanking und elektronischem Geld.

Wenn aber die Fachleute bei der Einführung neuer Techniken im Zahlungsverkehr unter sich bleiben, stehen ausschließlich bankfachliche und technische Überlegungen zur Realisierung an. In diese Denkprozesse findet selten die Überlegung Zugang, ob die Gestaltung neuer Techniken **datenschutzfreundlicher** ausfallen kann. Zu fragen ist beispielsweise danach, in welchem elektronischen Zahlungssystem Abbilder der einzelnen Transaktionen durch gespeicherte Datenspuren oder -schatten geschaffen und nutzbar gemacht werden können, etwa für Zwecke, die außerhalb der für den Zahlungsverkehr notwendigen Speicherungen liegen, und wie dies vermieden werden kann.

12.4.1 Elektronisches Lastschriftverfahren

Durch den Einsatz der ec-Karte mit Chip hat sich im wesentlichen nichts gegenüber dem bisherigen Verfahren geändert.

Alle notwendigen Daten werden aus dem Speicher im Chip über dieselbe Schnittstelle im Händlerterminal ausgelesen, die auch für das Lesen der elektronischen Geldbörse bestimmt ist. Dabei kann allerdings immer nur auf die jeweiligen Speichersegmente getrennt zugegriffen werden. Also sind bei jeder Kauftransaktion die Kartendaten wie Bankleitzahl, Kontonummer und Schlüsseldaten mit den Händlerdaten für das automatisierte Lastschriftverfahren in einem Datensatz zusammengefaßt. Weiter wird die Transaktion auch im Protokollfile der ec-Karte gespeichert. Die **Datenspuren** des Einkaufs sind damit **gelegt**, der Zahlvorgang bleibt an mehreren Stellen nachvollziehbar. Außerdem ist es technisch möglich, die Kundinnen- und Kundendaten im Händlerterminal auf einem anderen Speicherplatz - etwa zusammen mit Daten des gekauften Produktes - abzulegen, ohne daß dies von der Kundin oder dem Kunden bemerkt wird. Zusammen mit dem von jeder ec-Karte ablesbaren Namen läßt sich also recht einfach ein personenbezogenes **Kauf- und Verhaltensprofil** erstellen. Wird zu dem Namen noch die Anschrift aus der Telefonbuch-CD-ROM gesucht, dann ist der perfekte Marketingdatensatz hergestellt, der auf dem Markt des Adressenhandels zusätzliches Geld einbringt.

Damit liegt das Risikopotential des Einsatzes einer ec-Karte mit Chip nicht zuvorderst im Bereich der Kreditinstitute, sondern in dem Informationszuwachs, der auf der Seite der Handelsunternehmen entsteht.

12.4.2 Elektronische Geldbörse - GeldKarte

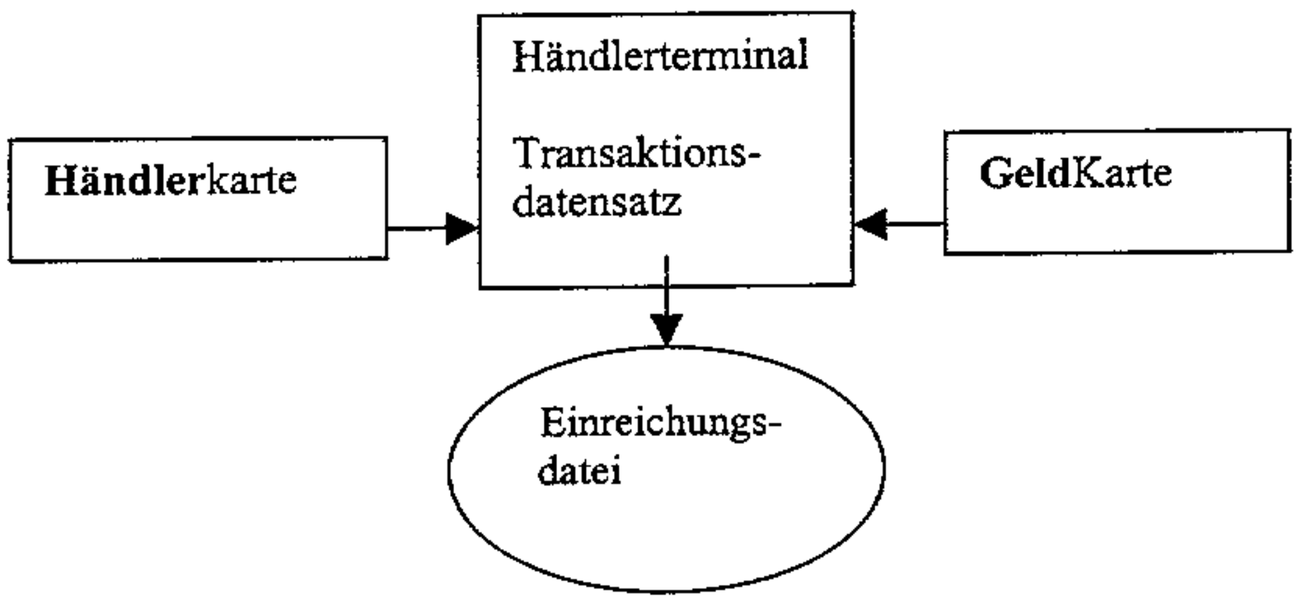
Mit der millionenfach ausgegebenen kontogebundenen GeldKarte können prinzipiell sämtliche Zahlungsvorgänge abgebildet und den Kontoinhaberinnen und -inhabern zugeordnet werden, sofern die im Zahlungssystem der GeldKarte beteiligten Stellen zu diesem Zweck zusammenwirken. Dabei ist die anonyme Bezahlung mit einer GeldKarte, die mit Bargeld aufgeladen wird und nicht an ein Bankkonto gebunden ist, durchaus möglich.

Das institutsübergreifende Zahlungssystem beruht auf einer Vereinbarung der vier Spitzenverbände der deutschen Kreditwirtschaft (unter anderem dem Deutschen Sparkassen- und Giroverband sowie dem Verband öffentlicher Banken), die jede Sparkasse anerkennen muß, wenn sie ihren Kundinnen und Kunden die Teilnahme an dem System GeldKarte ermöglicht. Im

Verhältnis der Sparkassen zu diesen gelten die "Bedingungen für die Verwendung der ec-Karte" und im Verhältnis zu den angeschlossenen Händlerinnen und Händlern die "Bedingungen für die Teilnahme am System GeldKarte". Alle von den Sparkassen herausgegebenen eurocheque-Karten tragen inzwischen den GeldKarten-Chip. Er enthält, außer den Personalisierungs- und Schlüsseldaten, Betriebssysteme und Speicherkapazitäten. Diese ec-Karten sind ausnahmslos als sogenannte **kontogebundene** Karten ausgelegt. Sie können an den Ladeterminals mit einem Geldbetrag - bis 400 DM - geladen werden. Der geladene Geldbetrag wird sofort von dem kartenbezogenen Girokonto abgebucht. Der Ladevorgang verläuft für die Kundinnen und Kunden in gleicher Weise wie bei der Auszahlung von Bargeld am Geldautomaten.

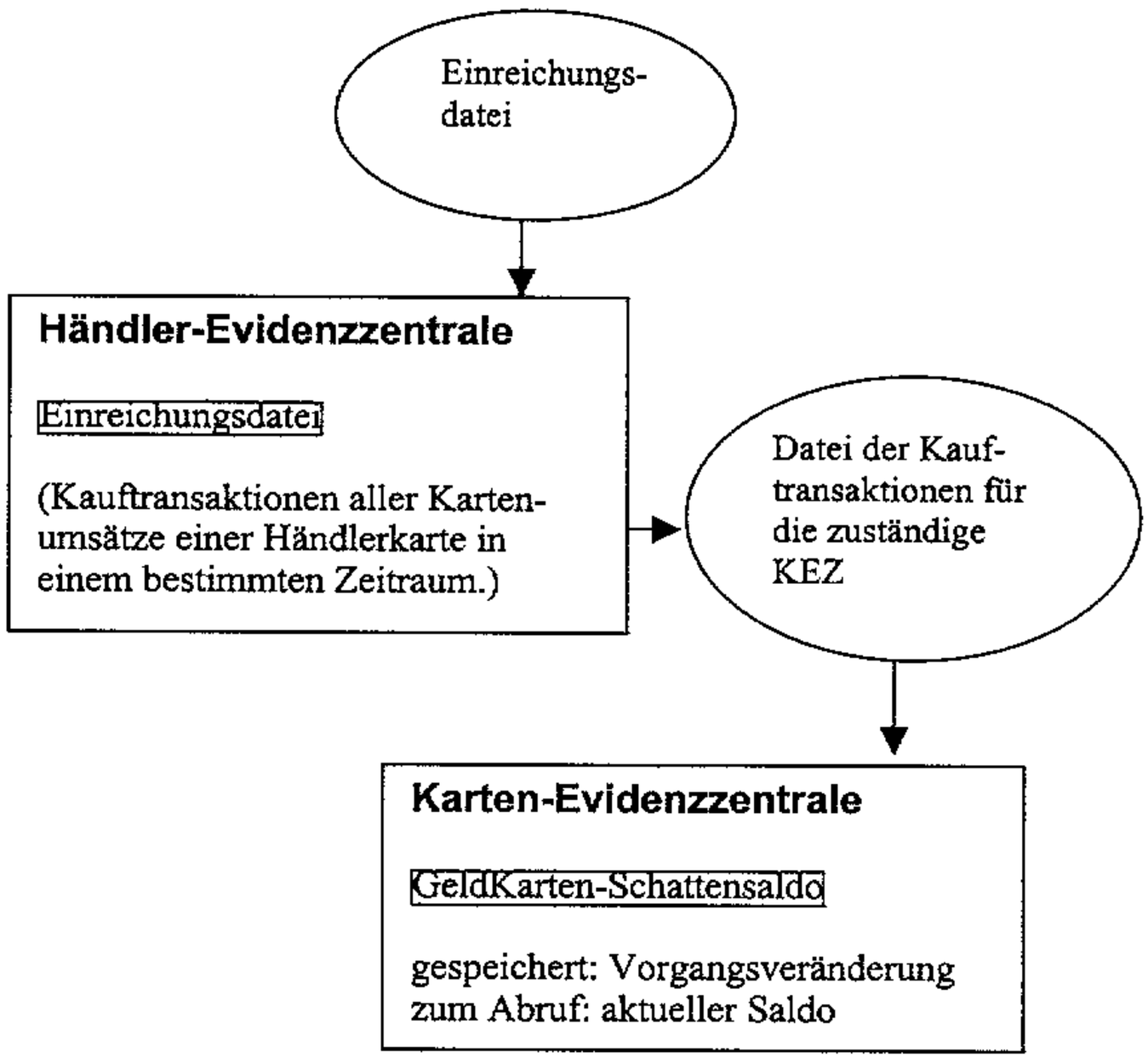
Neu ist, daß der Vorgang des Ladens mit den Kartendaten, Betrag und Datum in der zuständigen Karten-Evidenzzentrale (KEZ) - für alle deutschen Sparkassen ist sie in Münster eingerichtet - in einem unter der jeweiligen Kartennummer eingerichteten **Schattensaldo** festgehalten wird.

Beim Zahlvorgang - Einschieben der GeldKarte und Bestätigen des Betrages durch die Kundin oder den Kunden - werden im Händlerterminal die aus der GeldKarte gelesenen Daten zusammen mit den Daten aus der Händlerkarte in einem Transaktionsdatensatz gespeichert. Dieser wird dann mit allen anderen Kauftransaktionen eines bestimmten Zeitraumes in einer Einreichungsdatei erfaßt.



Die Einreichungsdatei wird an die zuständige Händler-Evidenzzentrale (HEZ) übermittelt, dort geprüft, gespeichert und bis zu **sieben** Jahren archiviert. Außerdem sortiert die HEZ die einzelnen Kauftransaktionen anhand

der Bankleitzahl und gibt sie mit den Angaben über Kartennummer, Datum, Buchungszeit und Betrag an die zuständige KEZ weiter. Dort wird vor allem der zur entsprechenden Kartennummer gespeicherte Schattensaldo reduziert, so daß ein neuer aktueller Saldo lesbar ist. Jede Veränderung des Schattensaldos wird protokolliert und ebenfalls bis zu **sieben** Jahren gespeichert. Der **aktuelle** Schattensaldo wird mit der nächstfolgenden Transaktion überschrieben. Bei Anfrage der kartenausgebenden Sparkasse - im Reklamationsfalle - teilt die KEZ jeweils nur den aktuellen Schattensaldo mit.



Somit entsteht in der KEZ eine kartenbezogene Abbildung aller Lade- und Kauftransaktionen der letzten Jahre. Dieses Abbild trägt keinen Namen, sondern die Kartennummer; es ist deshalb für die KEZ aus sich heraus nicht personenbezogen. Dasselbe gilt für das Abbild aller händlerbezogenen Umsätze in der HEZ. Aber die hinter dem Abbild stehende Person, auf deren Konto die GeldKarte bezogen ist, wird namentlich dann bekannt, wenn die

GeldKarte mit den Daten aus der KEZ zusammengeführt wird. Auf der GeldKarte kann abgelesen werden, bei welcher Sparkasse welche namentlich genannte Person unter welcher Kontonummer ihr Konto hat. Aber auch ohne im Besitz der GeldKarte zu sein, können Kartennummer und Kontonummer von der Ladezentrale und der Sparkasse einer bestimmten Person zugeordnet werden.

Es ist also prinzipiell denk- und realisierbar - ohne den Sparkassen oder ihren Rechenzentren solche Verknüpfungen unterstellen zu wollen -, durch automatisierte Datenabgleiche in der KEZ und der HEZ nach den Kauftransaktionen einer bestimmten Kartennummer zu suchen - etwa welche Beträge wann geleistet worden sind oder welcher Händlerkartennummer ein Einkauf zuzuordnen ist. Die archivierten Daten erlauben noch nach längerer Zeit, die Spuren einer bestimmten GeldKarte zurückzuverfolgen, wenn Kundeninstitut, Ladezentrale und KEZ auf der einen Seite oder HEZ und Händlerinstitut auf der anderen Seite Daten zusammenführen. Eine solche Möglichkeit kann in einem Rechenzentrum, das die Funktionen der Ladezentrale, der KEZ und der HEZ zugleich wahrnimmt, einfacher realisiert werden.

Die aufgezeigten Möglichkeiten einer Verknüpfung - technisch und organisatorisch - müssen für das gesamte Zahlungssystem betrachtet werden. Da die Datensätze mit der Kartennummer versehen sind, sind sie zwar pseudonymisiert, doch kann die Pseudonymisierung mittels des Zusatzwissens der kartenausgebenden Sparkasse aufgehoben werden.

Bedenkenswert wäre zumindest eine **Verkürzung der langen Speicherdauer**. Zwar wird sie mit der aufsichtsrechtlichen Verpflichtung zur lückenlosen Überwachung durch das Bundesaufsichtsamt begründet (§ 25 a Gesetz über das Kreditwesen). Ob diese Vorschrift aber auch dann Anwendung findet, wenn es um die Speicherung von technischen Kontrollmaßnahmen - Protokollierung der Veränderungen des Schattensaldos - geht, die keine ausgeführten Geschäfte belegen, kann bezweifelt werden. Die eigentlichen Buchungsvorgänge finden bei den Verrechnungsbanken statt. Somit könnte die Aufbewahrungsfrist auf eine für Sicherheitskontrollen erforderliche Zeitdauer beschränkt werden und damit erheblich kürzer ausfallen.

Schließlich ist für eine datenschutzrechtliche Bewertung noch von Bedeutung, ob die Sparkassen von ihren Evidenzzentralen eine Datenverarbeitung im Auftrag durchführen lassen, oder ob etwa den Evidenzzentralen im Rahmen der Abwicklung dieses Zahlungssystems **selbständige Funktionen übertragen** worden sind. Im ersten Fall wären die in den Evidenzzentralen verarbeiteten - pseudonymisierten - Daten einer Einflußnahme der Sparkas-

sen nicht entzogen, die Sparkassen wären als Auftraggeberinnen weisungsbefugt, aber auch verantwortlich für eine zulässige Datenverarbeitung durch die Evidenzzentralen. Dies wäre im Hinblick auf den Ausgangspunkt des Zahlungssystems - die Sparkassen geben die GeldKarten aus - auch interessengerecht. Im zweiten Fall würden die Evidenzzentralen die bei ihnen gespeicherten Daten in alleiniger Verantwortung verarbeiten, ohne daß die Verarbeitung, insbesondere die Zweckbindung der Daten abschließend geregelt wäre. In der Vereinbarung der Spitzenverbände der deutschen Kreditwirtschaft ist hierzu nämlich keine eindeutige Festlegung getroffen.

Verbindliche Festlegungen und organisatorische Vorkehrungen müssen sicherstellen, daß ein Zusammenwirken der zentralen Funktionen und der Kreditinstitute nur im festgelegten Ausnahmefall und nur in der Abfrage des aktuellen Schattensaldos erfolgt.

Klärungsbedürftig ist noch:

- Sind die Evidenzzentralen (Karten- und Händler-Evidenzzentrale) sowie Ladezentralen im Zahlungssystem jeweils voneinander getrennte datenverarbeitende Stellen? Welcher Kontrolle unterliegen sie?

- Mit welchen verbindlichen Festlegungen ist die Zweckbindung der verarbeiteten Daten in der jeweiligen Evidenzzentrale bestimmt?

- Ist eine Speicherdauer für die Daten in den Evidenzzentralen nach den bankrechtlichen Vorgaben notwendig oder kann sie kürzer sein, weil die Evidenzzentralen keine Bankgeschäfte führen?

- Wie wird den Kundinnen und Kunden die Datenverarbeitung im Zahlungssystem transparent gemacht - Art und Umfang der Datenverarbeitung sowie beteiligte Stellen?

- Wo und wie können die Betroffenen ihre Rechte auf Auskunft und Löschung geltend machen?

Keine Datenschutzprobleme bereitet dagegen eine mit Bargeld aufladbare GeldKarte ohne Bindung an ein Bankkonto, wenn Ausgabe und Clearing ohne Personenbezug erfolgen.

12.4.3 Homebanking mit dem HBCI-Verfahren

Gegenüber dem bisher über T-Online oder gar das Internet praktizierten Homebanking mit seinen unzulänglichen Vorkehrungen der PIN-

und TAN-Listen erreicht das vom Zentralen Kreditausschuß ausgewählte HBCI-Verfahren wesentliche Verbesserungen für eine sicherere Übermittlung der Kundinnen- und Kundendaten.

Durch das **HBCI-Verfahren** werden die Daten unter Wahrung des Bankgeheimnisses verschlüsselt übermittelt: PIN und elektronische Unterschrift - allerdings keine Signatur entsprechend dem Signaturgesetz - gewährleisten nach heutigem Erkenntnisstand außerdem die Authentizität der übermittelnden Person. Das Verfahren wird von den Sparkassen erprobt, so daß noch nicht abschließend beurteilt werden kann, ob die Rahmenbedingungen den datenschutzrechtlichen Anforderungen entsprechen. Dabei wird es vor allem darauf ankommen, wie die Kundinnen und Kunden **informiert** werden, wie die Einbindung des HBCI-Verfahrens in das Vertragsverhältnis erfolgt und wie die Datenverarbeitung im Sparkassenbereich **organisiert** ist.

HBCI - Homebanking Computer Interface
Standard für die Nutzung moderner Endgerätetechnik bei Bankkundinnen und Bankkunden mit einheitlichen Schnittstellen (multibankfähig), verschiedenen Übertragungsverfahren und den Sicherheitsmedien Chipkarte / Diskette und PIN.

Fragen der sicheren Kommunikation mit der Sparkasse, der Abschirmung des Zugangs vom Internet zum Sparkassen-Rechenzentrum sowie eines gesicherten Betriebssystems, das bankintern vor unberechtigtem Zugriff auf Kontodaten schützt, und der Schlüsselverwaltung sind insoweit von Bedeutung.

12.4.4 Elektronisches Geld - Netzgeld

Die letzte Lücke der online-Zahlungsmittel wird das Netzgeld schließen.

Netzgeld besteht aus digitalen Informationen, etwa einer Reihe verschlüsselter Seriennummern, und kann virtuell übertragen werden. Soweit bekannt, laufen **Pilotprojekte** für die Einführung von Netzgeld nur bei privaten Banken, nicht aber bei nordrhein-westfälischen Sparkassen.

Maßgeblich ist, daß die Anonymität der Zahlung mit realem Bargeld auch beim virtuellen Geld erhalten bleibt.

Anhang

Arbeitsergebnisse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Entschließungen der Datenschutzbeauftragten des Bundes und der Länder

Nr. 1 vom 17./18. April 1997 - 53. Konferenz

Achtung der Menschenrechte in der Europäischen Union

Die DSB-Konferenz ist gemeinsam der Überzeugung, daß hinsichtlich nicht Verdächtiger und hinsichtlich nicht kriminalitätsbezogener Daten die Forderung des Europäischen Parlaments vom 17.09.1996 zu den Dateien von Europol unterstützt werden soll.

Das Europäische Parlament hat in seiner Entschließung zur Achtung der Menschenrechte gefordert, "alle Informationen persönlichen Charakters, wie Angaben zur Religionszugehörigkeit, zu philosophischen oder religiösen Überzeugungen, Rasse, Gesundheit und sexuellen Gewohnheiten, von der Erfassung in Datenbanken von EUROPOL auszuschließen."

Nr. 2 vom 17./18. April 1997 - 53. Konferenz

Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen

Die Datenschutzbeauftragten des Bundes und der Länder halten es für sehr problematisch, daß in Folge technischer und gesellschaftlicher Veränderungen in einer zunehmenden Anzahl von Konstellationen personenbezogene medizinische Patientendaten außerhalb des ärztlichen Bereiches verarbeitet werden. Sie fordern, daß zunehmend die Möglichkeiten einer anonymen oder pseudonymen Datenverarbeitung mit Verschlüsselung genutzt werden. Soweit dennoch Patientendaten personenbezogen weitergegeben werden, ist ein wesentliches Problem, daß außerhalb des ärztlichen Gewahrsams der von der Strafprozeßordnung vorgesehene Schutz personenbezogener Patientendaten vor Inanspruchnahme als Beweismittel durch Zeugeneinvernahme oder Beschlagnahme nicht mehr zweifelsfrei sichergestellt ist bzw. überhaupt nicht existiert.

Die folgenden Beispiele machen dies deutlich:

1. Ärzte bzw. Krankenhäuser haben z.B. keinen Gewahrsam an den personenbezogenen Patientendaten, die der Patient auf einer (freiwilligen) Patientenchipkarte bei sich

trägt/besitzt oder die von einer dritten Stelle außerhalb des ärztlichen Bereichs im Auftrag verarbeitet werden, wie z.B. bei Mailbox-Systemen, externer Archivierung oder der Vergabe von Schreibarbeiten an selbständige Schreibbüros.

Fraglich ist auch die Aufrechterhaltung des ärztlichen Gewahrsams, wenn Hilfspersonal des Arztes oder Krankenhauses Patientendaten in der Privatwohnung bearbeitet.

2. Zunehmend werden einzelne Unternehmensfunktionen bzw. fachliche Aufgaben ausgelagert und einer externen Stelle - in der Regel einem Privatunternehmen - übertragen (sog. Outsourcing), - z.B. bei Einschaltung eines externen Inkassounternehmens, bei externem Catering für stationäre Patienten, bei externer Archivierung oder bei Vergabe von Organisationsanalysen an externe Beratergesellschaften.

3. Medizinische Daten mit Patientenbezug sollen an Forscher oder Forschungsinstitute zu Zwecken wissenschaftlicher Forschung übermittelt werden. Je umfassender und komplizierter der Einsatz automatisierter Datenverarbeitung für Forschungszwecke vorgesehen wird, desto weniger werden die personenbezogenen Patientendaten ausschließlich durch ärztliches Personal verarbeitet. Hier setzt sich vielmehr die Verarbeitung durch Informatiker und Statistiker immer mehr durch. Aber auch bei Verarbeitung durch Ärzte, die in der Forschung tätig sind, ist keineswegs sichergestllt, daß die personenbezogenen Patientendaten diesen Ärzten "in ihrer Eigenschaft als Arzt" bekannt geworden sind, wie dies durch die Strafprozeßordnung für den Beschlagnahmeschutz als Voraussetzung festgelegt ist.

Die zunehmende Verlagerung personenbezogener Patientendaten aus dem Schutzbereich des Arztgeheimnisses nach außen verstößt nach Ansicht der Datenschutzbeauftragten massiv gegen Interessen der betroffenen Patienten, solange nicht ein gleichwertiger Schutz gewährleistet ist.

Die Datenschutzbeauftragten des Bundes und der Länder bitten daher den Bundesgesetzgeber - unabhängig von weiteren Fragen des Datenschutzes, die mit der Verarbeitung medizinischer Daten im Rahmen der Telemedizin verbunden sein können - für die sich zunehmend entwickelnden modernen Formen der Auslagerung medizinischer Patientendaten sowie für die Weitergabe medizinischer Patientendaten für Zwecke wissenschaftlicher medizinischer Forschung einen dem Arztgeheimnis entsprechenden Schutz der Patientendaten zu schaffen.

Nr. 3 vom 20.10.1997

zu den Vorschlägen der Arbeitsgruppe der ASMK "Verbesserter Datenaustausch bei Sozialleistungen"

Mit dem von der ASMK-Arbeitsgruppe vorgeschlagenen erweiterten Datenaustausch bei Sozialleistungen wird die Bekämpfung von Leistungsmißbräuchen angestrebt. Soweit dieses Ziel der Arbeitsgruppe mit einer Veränderung der Strukturen der Verarbeitung personenbezogener Daten im Sozialleistungsbereich - insbesondere mit veränderten Verfahren der Datenerhebung - erreicht werden soll, muß der verfassungsrechtlich gewährleistete Grundsatz der Verhältnismäßigkeit beachtet werden.

Die gegenwärtigen Regelungen der Datenerhebung im Sozialleistungsbereich sehen unterschiedliche Verfahren der Datenerhebung vor, vor allem

- Datenerhebungen beim Betroffenen selbst

- Datenerhebungen bei Dritten mit Mitwirkung des Betroffenen

- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen aus konkretem Anlaß

- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen ohne konkreten Anlaß (Stichproben/Datenabgleich)

Diese Verfahren der Datenerhebung sind mit jeweils unterschiedlich schwerwiegenden Eingriffen in das Persönlichkeitsrecht der Betroffenen verbunden. So weiß z.B. bei einer Datenerhebung beim Betroffenen dieser, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritte erhalten keine Kenntnis von diesen Datenerhebungen.

Im Gegensatz dazu wird bei einer Datenerhebung bei Dritten ohne Mitwirkung des Betroffenen dieser darüber im unklaren gelassen, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritten werden Daten über den Betroffenen zur Kenntnis gegeben (z.B. der Bank die Tatsache, daß der Betroffene Sozialhilfeempfänger ist).

Dieses System der Differenzierung des Verfahrens der Datenerhebung entspricht dem Grundsatz der Verhältnismäßigkeit. Ferner ist zu differenzieren, ob Daten aus dem Bereich der Sozialleistungsträger oder Daten außerhalb dieses Bereichs erhoben werden.

In dem Bericht der Arbeitsgruppe wird dieses System zum Teil aufgegeben. Es werden Verfahren der Datenerhebung vorgesehen, die schwerwiegend in die Rechte der Betroffenen eingreifen, ohne daß hinreichend geprüft und dargelegt wird, ob minder schwere Eingriffe in das Persönlichkeitsrecht zum Erfolg führen können. Die Datenschutzbeauftragten wenden sich nicht um jeden Preis gegen Erweiterungen des Datenaustauschs, ge-

hen aber davon aus, daß pauschale und undifferenzierte Änderungen des gegenwärtigen Systems unterbleiben.

Datenabgleichsverfahren sollen nur in Frage kommen bei Anhaltspunkten für Mißbrauchsfälle in nennenswertem Umfang. Deshalb müssen etwaige neue Datenabgleichsverfahren hinsichtlich ihrer Wirkungen bewertet werden. Daher ist parallel zur ihrer Einführung die Implementierung einer Erfolgskontrolle für das jeweilige Abgleichsverfahren vorzusehen, die auch präventive Wirkungen erfaßt. Dies ermöglicht, Aufwand und Nutzen zueinander in das verfassungsmäßig gebotene Verhältnis zu setzen.

Soweit unter Beachtung dieser Prinzipien neue Kontrollinstrumente gegen den Leistungsmißbrauch tatsächlich erforderlich sind, muß für den Bürger die Transparenz der Datenflüsse sichergestellt werden. Diese Transparenz soll gewährleisten, daß der Bürger nicht zum bloßen Objekt von Datenerhebungen wird.

Bezugnehmend auf die bisherigen Äußerungen des BfD und von LfD bestehen gegen folgende Vorschläge im Bericht gravierende Bedenken:

1. **Mitwirkung bei der Ahndung des Mißbrauchs (für alle Leistungsträger) und Verbesserungen für die Leistungsempfänger (zu D.II.10.1 und B.I)** (S. 30 u. S. 2)

   Die vorgeschlagenen Möglichkeiten von anlaßunabhängigen Mißbrauchskontrollen beinhalten keine Klarstellung der gegebenen Rechtslage, sondern stellen erhebliche Änderungen des bisherigen abgestuften Systems der Datenerhebung dar.

   Die mit der Datenerhebung verbundene Offenlegung des Kontaktes bzw. einer Leistungsbeziehung zu einem Sozialleistungsträger stellt einen erheblichen Eingriff für den Betroffenen dar, u.a. da sie geeignet ist, seine Stellung in der Öffentlichkeit, z.B. seine Kreditwürdigkeit, wesentlich zu beeinträchtigen. Anfragen bei Dritten ohne Kenntnis des Betroffenen lassen diesen im unklaren, welche Daten wann an wen übermittelt wurden.

   Derartige Datenerhebungen werden vom geltenden Recht deshalb mit Rücksicht auf das verfassungsrechtliche Verhältnismäßigkeitsprinzip nur in begrenzten und konkretisierten Ausnahmefällen zugelassen. Von dieser verfassungsrechtlich gebotenen Systematik würde die vorgeschlagene Neuregelung grundlegend abweichen. Die Datenschutzbeauftragten betonen bei dieser Gelegenheit den allgemeinen Grundsatz, daß Datenerhebungen, die sowohl pauschal und undifferenziert sind, als auch ohne Anlaß erfolgen, abzulehnen sind.

   Die Datenschutzbeauftragten weisen schließlich darauf hin, daß gegen eine Ausnutzung der technischen Datenverarbeitungsmöglichkeiten zugunsten des Betroffenen

(B.I des Berichts) nichts spricht, solange die Betroffenen davon informiert sind und soweit sie dem Verfahren zugestimmt haben.

2. Nachfrage beim Wohnsitzfinanzamt des Hilfesuchenden zu Schenkungen und Erbschaften (zu D.I.1.1) (S. 6)

Die Datenschutzbeauftragten teilen nicht die Auffassung, daß Stichproben nach der geltenden Rechtslage zu § 21 Abs. 4 SGB X möglich sind. § 21 Abs. 4 SGB X ist eine Auskunftsvorschrift für die Finanzbehörden, die über die Datenerhebungsbefugnis der Sozialleistungsträger nichts aussagt. Die Leistungsträger dürfen diese Auskünfte bei den Finanzbehörden als Dritten nur nach Maßgabe des § 67a SGB X einholen, soweit das erforderlich ist: Diese Erforderlichkeit setzt Anhaltspunkte für Leistungsmißbrauch im Einzelfall voraus.

3. Auskunftspflicht der Banken und Lebensversicherungen (zu D.II.1.6) (S. 13)

Die Datenerhebung im Sozialbereich ist von einer möglichst weitgehenden Einbeziehung des Betroffenen gekennzeichnet. Der Vorschlag zur Einführung einer Auskunftspflicht geht auf dieses differenzierte System der Datenerhebungen im Sozialbereich überhaupt nicht ein.

Die Annahme in der Begründung des Vorschlags, ohne eine derartige Auskunftspflicht bestünden keine sachgerechten Ermittlungsmöglichkeiten, trifft nicht zu. Der Betroffene ist verpflichtet, Nachweise zu erbringen; dazu können auch Bankauskünfte gehören. Allerdings ist dem Betroffenen vorrangig Gelegenheit zu geben, solche Auskünfte selbst und ohne Angabe ihres Verwendungszwecks beizubringen. Nur soweit dennoch erforderlich, ist der Betroffene im Rahmen seiner Mitwirkungspflicht gehalten, sein Einverständnis in die Erteilung von Bankauskünften zu geben.

Die vorgeschlagene pauschale Auskunftsverpflichtung birgt deshalb die Gefahr in sich, daß dann generell ohne Mitwirkung des Betroffenen und ohne sein Einverständnis sofort an die Bank/Lebensversicherung herangetreten wird mit der Wirkung, daß der Betroffene desavouiert wird.

Die Datenschutzbeauftragten halten deshalb eine Klarstellung für dringend erforderlich, daß derartige unmittelbare Anfragen und Auskünfte erst in Betracht kommen, wenn die Ermittlungen unter Mitwirkung des Betroffenen zu keinem ausreichenden Ergebnis führen und Anhaltspunkte dafür bestehen, daß bei der fraglichen Bank/ Lebensversicherung nicht angegebenes Vermögen vorhanden ist.

4. Akzeptanz des Datenaustauschs (zu E.IV) (S. 36)

Datenabgleiche beinhalten eine Verarbeitung personenbezogener Daten, die nicht beliebig durchgeführt werden darf und anerkanntermaßen einer gesetzlichen Grundlage bedarf. Die im Papier der Arbeitsgruppe unter E.IV vertretene These, daß anlaßunabhängige Datenabgleiche keiner speziellen gesetzlichen Grundlage bedürften, trifft deshalb nicht zu.

Die Datenschutzbeauftragten wenden sich nicht gegen einzelne Veränderungen der Datenverarbeitung im Sozialleistungsbereich, soweit sie tatsächlich erforderlich und verhältnismäßig sind und die zuvor aufgezeigten Grundsätze beachtet werden. Die Datenschutzbeauftragten sind dazu gesprächsbereit.

Nr. 4 vom 23./24. Oktober 1997 - 54. Konferenz

Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Oktober 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.

Noch immer gibt es keinen Kabinettbeschluß; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

- Verbesserungen des Datenschutzes der Bürger, z.B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;

- dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

Zur Harmonisierung des europäischen Datenschutzrechts empfehlen die Datenschutzbeauftragten der Bundesregierung und dem Gesetzgeber folgende Grundsatzentscheidungen:

- weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlaßunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;

- Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;

- Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG, z.B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;

- Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen, die der EG-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen;

- Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Als ebenso vordringlich betrachten die Datenschutzbeauftragten eine Anpassung der noch von der Großrechnertechnologie der siebziger Jahre bestimmten gesetzlichen Regelungen an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft. Dazu gehören insbesondere folgende Punkte:

- Verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystem und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;

- mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutzaudits;

- Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Video-Überwachung;

- Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren;

- Einführung einer Vorabkontrolle für besonders risikoreiche Datenverarbeitung, namentlich bei Verarbeitung sensitiver Daten;

- Regelungen für Chipkarten-Anwendungen;

- Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing, unter anderem auch mindestens durch die Festlegung von Hinweispflichten hinsichtlich der Möglichkeit des Widerspruchs; vorzuziehen ist in jedem Fall eine Einwilligungsregelung;

- Verstärkung des Schutzes gegenüber der Einholung von Selbstauskünften vor Abschluß von Miet-, Arbeits- und ähnlich existenzwichtigen Verträgen;

- Datenexport nach Inlandsgrundsätzen nur bei angemessenem Schutzniveau im Empfängerstaat; Festlegung, unter welchen Voraussetzungen ein Mitgliedstaat Daten, die er im Anwendungsbereich der Richtlinie (also nach Inlandsgrundsätzen) erhalten hat, außerhalb ihres Anwendungsbereichs verwenden darf;

- möglichst weitgehende Ersetzung der Anmeldung von Dateien bei der Aufsichtsbehörde durch Bestellung weisungsfreier Datenschutzbeauftragter; Beibehaltung des internen Datenschutzbeauftragten auch bei Sicherheitsbehörden;

- Stärkung der Kontrollrechte des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz durch uneingeschränkte Kontrollbefugnis bei der Verarbeitung personenbezogener Daten in Akten einschließlich solcher über Sicherheitsüberprüfungen.

Die Konferenz weist ferner auf die Rechtspflicht der Länder hin, ihr Datenschutzrecht ebenfalls der EG-Richtlinie fristgerecht anzupassen.

Nr. 5 vom 23./24. Oktober 1997 - 54. Konferenz

Erforderlichkeit datenschutzfreundlicher Technologien

Moderne Informations- und Telekommunikationstechnik (IuK-Technik) gewinnt in allen Lebensbereichen zunehmende Bedeutung. Die Nutzer wenden diese Technik z.B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezo-

genen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z.B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der IuK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie läßt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflußt wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptographische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne daß die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff "Privacy enhancing technology (PET)" eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, daß er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, daß sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit läßt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, daß die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm "Forschung und Entwicklung" aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von IuK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

Nr. 6 vom 19./20. März 1998 - 55. Konferenz

Datenschutz beim digitalen Fernsehen

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, daß bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, daß erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, daß auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen ("Free TV" und "Pay TV") muß die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, daß die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrages vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

- Die Gestaltung technischer Einrichtungen muß sich an dem Ziel ausrichten, daß so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;

- die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;

- personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;

- wie bereits im Mediendienstestaatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d.h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die

Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug - etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen - entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten. Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

Nr. 7 vom 19./20. März 1998 - 55. Konferenz

Datenschutzprobleme der Geldkarte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen "Schattenkonten" der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese "Schattenkonten" noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluß der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene

Daten - sog. White Cards - anzubieten. Die Anwendung ist so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

Nr. 8 vom 5./6. Oktober 1998 - 56. Konferenz

Dringlichkeit der Datenschutzmodernisierung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefaßten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.

- Die anlaßfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muß in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.

- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.

- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.

- Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

Nr. 9 vom 5./6. Oktober 1998 - 56. Konferenz

Entwicklungen im Sicherheitsbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, daß die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z.B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, daß die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

Nr. 10 vom 5./6. Oktober 1998 - 56. Konferenz

Weitergabe von Meldedaten an Adreßbuchverlage und Parteien

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über veröffentlichte Daten in Adreßbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellten Betroffene fest, daß sie persönlich adressierte Wahlwerbung der Parteien bekommen. Ihnen ist unerklärlich, wie Adreßbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adreßbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert.

Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen - erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

Nr. 11 vom 5./6. Oktober 1998 - 56. Konferenz

Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlaß an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlaß an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

Thesenpapier zum Allgemeinen Informationszugangsrecht und zum Recht auf informationelle Selbstbestimmung

Die Datenschutzbeauftragten des Bundes und der Länder sehen sich zunehmend mit der Frage konfrontiert, in welchem Verhältnis das Grundrecht auf informationelle Selbstbestimmung zur Forderung nach Schaffung eines allgemeinen Informationszugangsrechtes der einzelnen Bürgerinnen und Bürger gegenüber dem Staat steht. Die Verfassung des Landes Brandenburg sieht ein Recht auf Einsicht in Akten und sonstige amtliche Unterlagen der Behörden und Verwaltungseinrichtungen ausdrücklich vor und macht eine Gesetzgebung notwendig. Im Bund und in einigen anderen Ländern diskutiert ein Teil der Parteien ebenfalls über die Gewährung solcher Rechte. In anderen Staaten gehören Informationszugangsrechte zur Rechtstradition (Schweden), oder sie wurden in den letzten Jahrzehnten eingeführt (z.B. USA, Frankreich, Kanada). Die Europäische Union hat für ihre Institutionen in den Amsterdamer Verträgen ein Akteneinsichtsrecht geschaffen. In-

ternational hat sich der Begriff "Informationsfreiheit" eingebürgert, der damit über den Begriff der Informationsfreiheit im Grundgesetz hinausgeht (s. unter I.).

Es spricht viel dafür, daß die Datenschutzbeauftragten nicht nur die Schranken eines allgemeinen Informationszugangsrechts im Hinblick auf die informationelle Selbstbestimmung aufzeigen, sondern sich auch die Forderung nach einem Informationszugangsrecht selbst zu eigen machen. Ein Teil der Datenschutzbeauftragten hat dies auch in der Vergangenheit bereits getan. Das Recht auf informationelle Selbstbestimmung und auf demokratische Teilhabe können so zu einem ausgewogenen Konzept gebracht werden, bei dessen Durchsetzung die Datenschutzbeauftragten durchaus eine aktive Rolle übernehmen können.

I. Informationsgesellschaft und Informationszugang

Anders als die eher dem Prinzip der Öffentlichkeit verpflichteten Bereiche der Legislative und der Judikative, ist das Verwaltungshandeln in der Bundesrepublik Deutschland traditionell geprägt vom Grundsatz des Amtsgeheimnisses. Das geltende Recht räumt den einzelnen Bürgerinnen und Bürgern in der Regel nur Informationsrechte zur Wahrung ihrer individuellen Rechte gegenüber dem Staat ein. Informationsmöglichkeiten bestehen insoweit wegen einer Betroffenheit in eigenen Rechten. Demgegenüber gewinnt in der Informationsgesellschaft die Frage eines darüber hinausgehenden Informationszugangs und somit die Schaffung und Verwirklichung eines allgemeinen Informationszugangsrechts auch unabhängig von einer individuellen Betroffenheit zunehmend an Bedeutung. Wesensbestimmend hierfür sind individuelle und demokratische Komponenten.

Die Freiheit, sich aus allgemein zugänglichen Quellen zu informieren, zählt für das Bundesverfassungsgericht ebenso zu den Grundvoraussetzungen des demokratischen Meinungs- und Willenbildungsprozesses wie zu den Bedingungen verantwortlichen, individuellen Handelns: "Es gehört zu den elementaren Bedürfnissen des Menschen, sich aus möglichst vielen Quellen zu unterrichten, das eigene Wissen zu erweitern und sich so als Persönlichkeit zu entfalten. Zudem ist in der modernen Industriegesellschaft der Besitz von Informationen von wesentlicher Bedeutung für die soziale Stellung des Einzelnen. Das Grundrecht der Informationsfreiheit ist wie das Grundrecht der freien Meinungsäußerung eine der wichtigsten Voraussetzungen der freiheitlichen Demokratie" (vgl. BVerfGE 7, 198 [208]). "Erst mit seiner Hilfe wird der Bürger in den Stand gesetzt, sich selbst die notwendigen Voraussetzungen zur Ausübung seiner persönlichen und politischen Aufgaben zu verschaffen, um im demokratischen Sinne verantwortlich handeln zu können" (BVerfGE 27, 71 [81 f.]).

Im Hinblick auf die Entwicklung der Informationsgesellschaft und auf die Vielzahl der allein bei der Verwaltung vorhandenen Informationen, kann die bloße Möglichkeit, sich aus allgemein zugänglichen Quellen zu unterrichten, nicht mehr genügen. Ein Kenn-

zeichen der Informationsgesellschaft ist, daß die einzelnen Bürgerinnen und Bürger in zunehmendem Maße vom Zugang zu Informationen abhängig werden. Selbst zur Durchsetzung eigener Rechte sind sie vielfach auf bisher nicht veröffentlichte Informationen angewiesen, auch wenn sie sich nicht unmittelbar auf sie beziehen, aber als Grundlage für ihre schutzwürdigen Interessen wichtig sind. Je intensiver sich Verwaltung und Bürger/-innen der Informationstechnik bedienen und deren erschließbare Informationsressourcen nutzen, um so enger müssen der Zugang zu den Daten und der Schutz der informationellen Selbstbestimmung miteinander verflochten werden. Um die Rechte der einzelnen Bürgerinnen und Bürger dabei zu gewährleisten, ist die Herstellung von Transparenz eine besonders wichtige Zielsetzung bei der humanen Gestaltung der Informationsgesellschaft.

Neben der individuellen Komponente ist Öffentlichkeit für den demokratischen Staat von zentraler Bedeutung. Der Grundsatz der Öffentlichkeit von Parlamentssitzungen und Gerichtsverhandlungen gehört zum Grundbestand unserer Rechtsordnung; ebenso unumstritten ist die Pflicht zur Veröffentlichung von Gesetzen oder von Gerichtsentscheidungen mit grundsätzlicher Bedeutung. Lediglich der Bereich der vollziehenden Gewalt ist vom Öffentlichkeitsgrundsatz bislang weitgehend ausgenommen geblieben.

Dies ist jedoch unter informationstechnischen Bedingungen, die Verwaltungshandeln zunehmend prägen, nicht mehr zeitgemäß. Vielmehr ist Transparenz der Verwaltung für die Wahrnehmung der Teilhabe unerläßlich. Hierfür kann es auf individuelle Betroffenheit oder (was auf das gleiche hinausläuft) berechtigte Interessen der Einzelnen nicht ankommen.

II. Entwicklung der Informationsrechte in Deutschland

Der Entwicklung rechtsstaatlicher Grundsätze ist es vorrangig zu verdanken, daß schon früh den Beteiligten an Gerichtsverfahren Informationsrechte zugestanden wurde, um ihnen die Möglichkeit zu geben, ihre rechtlichen Interessen wirkungsvoll verfolgen zu können. Für die verwaltungsrechtlichen Streitigkeiten zwischen Bürger/-innen und Staat brachte dies zwangsläufig auch Informationsrechte am vorangehenden Verwaltungsverfahren der Beteiligten mit sich. Der Informationszugang unterliegt in diesem Bereich allerdings nach wie vor der Voraussetzung am Verfahren beteiligt zu ein, also in aller Regel in irgendeiner Form in eigenen Rechten betroffen zu sein.

Für eine Vielzahl von Planungsentscheidungen ist mittlerweile anerkannt, daß der Kreis der Betroffenen nicht schon im vorhinein festgelegt werden kann. Aus Gründen staatlicher Informationspflichten - z.B. bei der Bauleitplanung - wurden Instrumente geschaffen, um auch potentiell Betroffene zu informieren. In diesen Verfahren sind Planungsgrundlagen öffentlich bekanntzumachen. Einwände kann aber auch in Planungsverfahren

nur geltend machen, wer individuell betroffen ist und damit zum Kreis der Beteiligten an diesem Verfahren im weitesten Sinne gehört.

In den siebziger Jahren setzte sich im Zuge der Datenschutzdebatte endgültig die Einsicht durch, daß auch außerhalb förmlicher Verfahren Auskunfts- und Einsichtsrechte der Betroffenen zu schaffen sind. Der datenschutzrechtliche Auskunftsanspruch besteht unabhängig von der Beteiligung an einem förmlichen Verfahren, bezieht sich gleichwohl jedoch nur auf die Daten zur eigenen Person.

Betroffenen- und verfahrensunabhängige Transparenz der Datenverarbeitung schaffen die bei den Datenschutzbeauftragten zu führenden Dateienregister; auch die Zugangsmöglichkeiten für alle zu staatlichem Archivgut wurden erweitert.

Mit dem Umweltinformationsgesetz hat der Gesetzgeber für einen ganzen Bereich die Regel durchbrochen, daß Informationsrechte in Form von Einsichts- und Auskunftsrechten nur Betroffenen oder Beteiligten zustehen. Dies sollte nicht nur als Angleichung an europäisches Recht im Prozeß der europäischen Integration verstanden werden. Vielmehr muß es als Teil einer die Bürgerrechte stärkenden generellen Rechtsentwicklung eingeordnet werden. Umweltveränderungen betreffen in besonderem Maße potentiell alle Bürgerinnen und Bürger. Die Zusammenhänge können infolge der Langzeitwirkung oft nur schwer nachvollzogen werden, und dies setzt auch genaue Kenntnisse der Umweltsituation und der Umweltfaktoren voraus. Würde die Darlegung der Betroffenheit als Voraussetzung für die Erteilung von Auskünften und Informationen verlangt werden, würde dies häufig den Informationszugang unmöglich machen.

Diese Entwicklungslinie sollte konsequenterweise zu einer Öffnung aller Verwaltungsbereiche für den Informationsanspruch der Bürgerinnen und Bürger führen.

III. Grenzen eines allgemeinen Informationszugangsrechts

Ein schrankenloses allgemeines Informationszugangsrecht würde jeder Bürgerin und jedem Bürger die Möglichkeit eröffnen, Einsicht in alle Verwaltungsakten zu nehmen oder Auskunft darüber zu erhalten. Es steht außer Frage, daß ein derart schrankenloses Recht mit dem Grundrecht auf informationelle Selbstbestimmung - aber auch z.B. in die Forschungsfreiheit - unvereinbar sein würde. Grundsätzlich macht jedes personenbezogene Datum in einem Vorgang eine Abwägung mit diesem Grundrecht erforderlich.

Ein Großteil der für den Informationszugang relevanten Unterlagen enthält jedoch einen solchen Personenbezug nicht. Soweit das Zugangsrecht ausschließlich die Grundlagen des grundsätzlichen Verwaltungshandelns (z.B. Erlasse, Rundschreiben und andere Verwaltungsvorschriften, Dienstanweisungen und Grundsatzakten) betrifft, dürfte demzufolge einem solchen Anliegen aus der Sicht des Datenschutzes nichts entgegenstehen.

Auch die weiteren Bereiche sachbezogenen Verwaltungshandelns (z.B. Haushaltswesen, Straßenbau, Bildungswesen) werfen keine datenschutzrechtlichen Fragen auf. Selbst wenn solche Unterlagen einzelne personenbezogene Daten enthalten, lassen sie sich nach Anwendung bekannter und bewährter Verfahren (Schwärzung, Kodierung, Pseudonymisierung) zugänglich machen.

Beziehen sich Verwaltungsvorgänge im wesentlichen auf personenbezogene Daten von Betroffenen, bedarf die Offenbarung der Daten im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung einer ausdrücklichen normenklaren Rechtsgrundlage, soweit nicht ebenfalls eine Anonymisierung in Betracht kommt. Derartige Rechtsgrundlagen auf Bundes- und Landesebene liegen in Spezialgesetzen bereits vor oder sind gegebenenfalls zur Ausweitung des Informationszugangsrechts noch zu schaffen. Für Trivialdaten oder andere Daten, bei denen schutzwürdige Interessen der Betroffenen nicht berührt sein können (z.B. weil der oder die Betroffene - wie beim Telefonbuch - selbst der Verbreitung zugestimmt hat), ermöglichen die Datenschutzgesetze in der Regel bereits jetzt die Offenbarung.

Denkbar wäre außerdem, daß der Gesetzgeber im Gesetz über den freien Informationszugang selbst einen Katalog typisierender Beispiele festlegt, in welchen Fällen darüber hinaus das Recht auf informationelle Selbstbestimmung hinter dem Informationszugangsrecht zurücktritt und - in Umkehrung des normalerweise geltenden Verhältnisses - der Zugang nur bei besonderer Schutzwürdigkeit der personenbezogenen Daten verweigert werden kann. In einen solchen Katalog könnten beispielsweise mit dem Vorgang befaßte Personen, also Amtsträgerinnen und Amtsträger oder beauftragte Beschäftigte, aber auch Sachverständige, die Beiträge bei oder zu der Bearbeitung der Angelegenheit geleistet haben, aufgeführt werden. Die Offenlegung von Verantwortlichkeiten für Verwaltungsentscheidungen oder für Sachbearbeitung gehört zu einer transparenten Verwaltung und dient den überwiegenden Interessen der Öffentlichkeit. Einer besonders sorgfältigen Abwägung bedarf die Frage, ob und in welchen Fällen der freie Zugang zu Identdaten von an Verwaltungsverfahren beteiligten Personen und möglicherweise zu solchen personenbezogenen Daten zu gewährleisten ist, zu deren Bekanntgabe, Auskunft oder Mitteilung betroffene Personen gegenüber einer Behörde verpflichtet waren.

Generell wäre auch daran zu denken, im Einzelfall eine Einwilligung der Betroffenen in die Offenbarung ihrer Daten einzuholen und sie damit zugleich über das Vorliegen eines Informationsbegehrens zu unterrichten. Wird die Einwilligung nicht innerhalb einer bestimmten Frist erteilt, wäre von Amts wegen zu prüfen, ob dem Begehren der oder des Informationssuchenden durch die Mitteilung der Geheimhaltungsverpflichtung und der lediglich sachbezogenen Auskunftserteilung, durch Schwärzung der Daten für die Akteneinsicht oder durch Abtrennung von Aktenteilen nachgekommen werden kann. Jedenfalls würde eine vom Gesetzgeber in dieser Weise zum Ausdruck gebrachte Festlegung für die Öffentlichkeit erhöhte Anforderungen an die behördliche Begründung einer endgültigen Informationsverweigerung zur Folge haben.

Gegen die Gewährung eines Informationszuganges können darüber hinaus im Einzelfall Aspekte sprechen, die sich aus staatlichen Sicherheitsinteressen ergeben oder auch aus dem Interesse an einer effizienten Erfüllung der öffentlichen Aufgaben der Verwaltung. Diesen Aspekten kann im Rahmen eines Informationszugangsgesetzes Rechnung getragen werden. Dabei ist jedoch auch hier zu beachten, daß Abweichungen vom Grundsatz des allgemeinen Informationszugangs im Gesetz hinreichend konkret und bestimmt zu fassen sind. Um die Gefahr zu vermeiden, daß ein Katalog von Ausnahmetatbeständen den Grundsatz des Informationszugangs letztlich doch wieder in sein Gegenteil verkehrt, müßten auch diese Ausnahmetatbestände (z.B. Wohl des Bundes oder eines Landes, Beeinträchtigung der Strafverfolgung und Vollstreckung der Gefahrenabwehr oder andere Belange der inneren Sicherheit sowie Offenbarung von Akten zur Durchführung eines Gerichtsverfahrens) selbst eng ausgelegt werden. Dasselbe gilt für Aktenvorgänge, die bei der laufenden Verwaltungsarbeit anfallen, insbesondere wenn es sich um personenbezogene Daten handelt.

Eine weitere explizite Einschränkung erfährt das Informationszugangsrecht dort, wo gesetzliche Vorschriften ausdrücklich die Geheimhaltung bestimmter Umstände fordern. Daneben hat ein Informationszugangsgesetz in seinen Ausnahmetatbeständen beispielsweise Betriebs- und Geschäftsgeheimnisse zu berücksichtigen; ein ausgewogener Ausgleich zwischen Informationszugang und den durch die Geheimhaltung geschützten Interessen ist zu schaffen.

IV. Abwehr und Durchsetzung des Informationszugangs

Grundsätzlich sollten vor der Erfüllung eines Informationsanspruchs, der mit der Preisgabe personenbezogener Daten verbunden wäre, Betroffene von dem Informationsbegehren unterrichtet werden, um Einwände geltend machen zu können. Wird ihren Einwänden nicht stattgegeben, und kann der Informationsanspruch nicht ohne Eingriff in ihr Recht auf informationelle Selbstbestimmung erfüllt werden, so müssen sie Gelegenheit haben, Abwehrrechte gerichtlich prüfen zu lassen und gegebenenfalls durchsetzen zu können. Auch dann, wenn ein Informationsanspruch verweigert wird, müssen die Anspruchsteller die Möglichkeit haben, den Anspruch mit gerichtlicher Hilfe durchzusetzen und zumindest prüfen zu lassen.

Zusätzlich zum Rechtsweg bietet es sich an, den Bürgerinnen und Bürgern die Möglichkeit zu eröffnen, sich mit ihrem Anliegen an eine unabhängige Stelle zu wenden (Beauftragter oder Beauftragte für Informationsfreiheit). Umfangreiche positive Erfahrungen aus anderen europäischen und aus außereuropäischen Ländern lassen erwarten, daß eine solche unabhängige Stelle die Mehrheit der Fälle klären könnte, Für die unabhängige Stelle bietet sich eine rechtliche Konstruktion an, die derjenigen der Datenschutzbeauftragten des Bundes und der Länder vergleichbar ist. Ihre Tätigkeit hat gezeigt, daß eine unabhängige Stelle auch dann, wenn sie keine Sanktionen verhängt, sondern lediglich

über das Instrument der Beanstandung verfügt, dennoch befriedigend und ausgleichend wirken kann. Übertragbar wäre beispielsweise das kanadische Modell, bei dem Datenschutz- und Informationszugangskontrolle unter einem Dach vereint sind.

Das Verhältnis zwischen unabhängiger Verwaltungskontrolle und Verwaltungsgerichtsbarkeit könnte durch eine geeignete Regelung des Vorverfahrens und der zu wahrenden Fristen geklärt werden. Das nach der derzeitigen Rechtslage bestehende Problem, daß das Anliegen der Verwaltung an einer Verweigerung der Akteneinsicht mit der Klage faktisch unterlaufen würde, ließe sich beispielsweise nach amerikanischem Vorbild mit der Einführung eines in-camera-Verfahrens lösen, bei dem der streitbefangene Aktenvorgang nur dem Gericht zur Kenntnis zu bringen wäre.

V. Fazit

Unserem Rechtssystem widerspricht es nicht, den einzelnen Bürgerinnen und Bürgern Rechte einzuräumen, die bei staatlichen Stellen den Zugang zu vorhandenen Informationen ohne den Nachweis der Betroffenheit in eigenen Rechten eröffnen. Das moderne Staatsverständnis geht von mündigen und informierten Bürgerinnen und Bürgern aus. Eine Erweiterung der Informationszugangsrechte ist dafür eine der Voraussetzungen, wobei dem verfassungsrechtlichen Rang des Rechts auf informationelle Selbstbestimmung Rechnung getragen werden muß.

Anlage: Informationszugangsrechte in anderen Ländern

Die Informationszugangsrechte sind in anderen Ländern in unterschiedlicher Weise geregelt:

- Dänemark (kein Verfassungsanspruch, Gesetz über die Öffentlichkeit in der Verwaltung vom 19.12.1985),
- England (kein Verfassungsanspruch, jedoch Absichtserklärungen in dem Regierungsprogramm der britischen Labour Party vom 14.05.1997),
- Frankreich (kein Verfassungsanspruch, durch Gesetz vom 17.07.1978),
- Niederlande (Art. 110 Niederländische Verfassung von 1983, Openness of Administration Act von 1978),
- Österreich (Art. 20 Abs. 4 Österreichische Verfassung vom 15.05.1987, Bundesgrundsatzgesetz vom 15.05.1987),
- Portugal (Art. 268 Portugiesische Verfassung von 1976, einfachgesetzliche Zugangsansprüche),
- Spanien (Art. 105 Spanische Verfassung, einfachgesetzliche Ansprüche nur in speziellen Bereichen),

- Schweden (seit 1766 mit Verfassungsrang im Grundsatz, Einschränkungen durch Act on Secrecy von 1980),
- Ungarn (Verfassungsanspruch, Act on Protection of Personal Data and Disclosure of Data of Public Interest von 1992),
- Kanada (kein Verfassungsrang, sowohl auf Bundesebene durch Informationszugangsgesetz vom 28.06.1982 als auch in einzelnen Bundesstaaten wie Ontario, Quebec und British Columbia Informationszugangsgesetze),
- USA (keine verfassungsrechtliche Gewährleistung, Freedom of Information Act von 1966),
- Recht für jeden Unionsbürger auf freien Zugang zu Informationen bei den Organen der EU (Art. 191 a EGV als Bestandteil des Vertrags von Amsterdam vom 16./17. Juni 1997).

Stichwortverzeichnis

A

Abfragesprachen 103
- freie 103
- Protokollierung von 103
Abgleichsverfahren
- automatisierte 98
Abhörbefugnisse 32
Abhörmaßnahmen 56
Abrufverfahren
- automatisierte 101
Adreßbuchverlage 87
Adressenhandel 141
Akteneinsicht 84
Aliasnamen 67, 69
Allfinanz-Klausel 141
Anbieterkennzeichnung 44
Anonyme Nutzung 9, 29
Anonymisierung 5
Auskunftsanspruch 56
- Sozialleistungsträger 98
Auskunftsermächtigungen 100
Auskunftssperre 87
Ausländerzentralregister 93
Ausschreibungsunterlagen 69
Authentifikation 47
Authentizität 20, 114

B

Beherbergungsstätte 88
Benachrichtigung 56
Beschäftigtendaten 40
Bewerbungen 129
Bonitätsprüfung 95
Briefgeheimnis 49
Briefumschläge 84
Bundesgrenzschutz 54

Bundeskriminalamt (BKA) 72
Bundeskriminalamtgesetz 72
Bundesnachrichtendienst 51
Bürgeramt 87

C

Chipkarten
- multifunktionale 124
Cookies 38

D

Datenintegrität 46
Datenreduzierung 9
Datensammlungen
- zentrale medizinische 116
Datenschutzaudit 36
Datenschutz durch Technik 35
Datenschutzfreundliche Technologien 8
Datenschutzkontrolle 5
Datenschutzrecht
- modernes 5
Datensicherheitskonzept 102
Datenübermittlung 75
Datenvermeidung 8, 29, 36
Digitale Signatur 19, 47
Digitale Signaturverfahren 17
Direktmarketing 141
DNA-Analysedatei 52
DNA-Identitätsfeststellungsgesetz 52
DNA-Profil 52

E

Eidesstattliche Versicherung 85
Einstellungsuntersuchungen
- polizeiärztliche 129
Einwilligung 38, 108, 110
- elektronische 39

Elektronischer Zahlungsverkehr 142
EURODAC 96
Europäische Telekommunikationsdatenschutzrichtlinie 29
Europol 71

F

Fahndungsunterlagen 69
Familiengerichte 86
Fernmeldeanlagengesetz 32, 55
Fernmeldegeheimnis 30, 49
Firewallsysteme 22
Formulare 85
Führerscheinakte 137

G

Gästebücher 42
Geburtsdaten 84
GeldKarte 143
Geldwäsche 140
Gemeinsame Kontrollinstanz 68, 72
Gerichte 83, 85
Gerichtsakten 84
Gerichtsgebäude 83
Gerichtstermin 85
Geschäftsnummer 84
Gesundheitsnetze 109
Gewaltenteilung
- informationelle 5

H

Hash-Funktionen 17
Hauptwohnung 89
Homebanking 147
Homepage 40
Hybridverschlüsselung 16

I

Identifizierung	80
Immunität	71, 72
IMSI-Catcher	32, 33
Info-City NRW	28
Informationelle Selbstbestimmung	3
Informationsmacht	4
Informations- und Kommunikationsdienstegesetz	35
INPOL	72
Integrität	20, 113
Internet	2
Internetdienste	23
Internetnutzung	21
- Diensteauswahl	21
- Administration	21
- Protokollierung	21
- Kontrolle	21
- Direktanschluß	21

J

Justiz	83
Justizmitteilungsgesetz	83

K

Kommunikationsteilhabe	4
KOM-ON	45
Korruptionsregister	138
Krankenhausentlassungsbericht	104
Krankenkassen	
- Datenschutzkonzept für Einsatz der Informations-technik	102
Krankenunterlagen	108
- Aufbewahrung	108
- Archivierung	108
- Mikroverfilmung	108
- Digitalisierung	108
- Outsourcing	108
Krebsregister	107

Kriminalaktennachweis (KAN) 74
Kryptographie 11
Kundendaten 51
Kundendatei 31

L

Lauschangriff 50, 51
Löschung 104
- Vorgaben 103

M

Mediendienste 34
Mediendienstestaatsvertrag 34
MiStra 83
Mitarbeiterbefragungen 129
Mixe 10
MiZi 83

N

Nachrichtendienste 49
NADIS 61
Nebenstellenanlage 31
Negativauskunft 56
Neue Steuerungsmodelle 92
Nicht-Abstreitbarkeit 115
Nichtöffentliche Gerichtsverhandlung 86
Nutzungsanalysen 48
Nutzungsordnungen 123
Nutzungsprofile 37

O

Observationssysteme 50
Öffentlichkeit 86
Öffentliche Schlüssel 13
Outsourcing 108

P

Patientenakte	110
Personalakten	
- Verlust von	128
Persönlichkeitsprofile	8, 37
Persönlichkeitsrecht	116
Pflegeleistungen	
- Prüfung	100
Politische Parteien	88
Polizei	49, 73, 75
Postgeheimnis	49
Private Schlüssel	13
Privatsphäre	51
Protokollierung	73
Pseudonyme Nutzung	29
Pseudonymisierung	5
Psychotherapeutengesetz	107

Q

Quittungsverfahren	48

R

Rasterfahndung	50
Registergestützte Volkszählung	119
Rentenversicherungsträger	105
- Dialogverfahren	105
Revisionssicherheit	116
Risikoanalyse	23

S

Schattensaldo	144
Scheinehen	93
Schengener Durchführungsübereinkommen (SDÜ)	66
Schengener Informationssystem (SIS)	66
Schleierfahndung	54
Schleppnetzfahndung	49

Schulen ans Netz	121
Schwarzes Brett	42
Screened Gateway	22, 25
Sicherheitsbehörden	49
Sicherheitskonzept	23, 112
Sicherheitspolitik	110
Sicherheitsüberprüfung	59
Sicherheitszertifikat	24, 46
Signaturgesetz	39
Signaturverordnung	39
Sozialgeheimnis	98
Sozialhilfedatenabgleichsverordnung	98
Speicheltest	95
Staatsschutz	57, 62
Steuerberaterkammern	139
Systemdatenschutz	5

T

Teleantrag	45
Telearbeit	130
Teledienst	34
Teledienstedatenschutzgesetz	34
Telefonüberwachung	49, 54
Tele-Heimarbeit	130
Telekommunikation	29, 34
Telekommunikationsdatenschutz	29
Telekommunikationsgesetz	30, 34
Telekommunikationsüberwachungsverordnung	34
Terminsrolle	86
Transparenz	38

U

Unbeobachtbare Kommunikation	37
Unterrichtung	38
Unversehrtheit	20
Urheber- und Empfängernachweis	47

V

Verbindungsdaten	26, 55
Verbot mit Erlaubnisvorbehalt	38
Verdachtsunabhängige Kontrollen	54
Verfassungsschutz	49, 57
- Löschung	58
Verfügbarkeit	115
Versammlungen	63
Verschlüsselung	
- asymmetrische	13
- symmetrische	12
Verschlüsselungsverfahren	12
Vertrauenswürdige Dritte	15, 19
Vertraulichkeit	17, 46, 112
Verwaltungsverfahren	44
Verwaltungsverordnung zur Ausführung des Landesbeamtengesetzes	128
Videoüberwachung	76
Volks- und Wohnungszählung - 2001	118

W

Warndateien	140
Weitervermittlung	44
Wettbewerbsverstöße	138
Wohnung	49, 51

Z

Zertifikate	19
Zugriffsschutzkonzept	103
Zurechenbarkeit	20
Zweckbindung	38, 103

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:

_____ den neuesten Datenschutzbericht

_____ den ..... Datenschutzbericht

_____ 20 Jahre Datenschutz - Individualismus oder Gemeinschaftssinn?

_____ Die Bedeutung der EG-Datenschutzrichtlinie für öffentliche Stellen

_____ Neue Instrumente im Datenschutz

_____ Tips zum Adressenhandel

_____ Datenscheckheft

_____ Selbstbestimmung und Erkenntnisdrang - Datenschutz und Forschung in Nordrhein-Westfalen

_____ Handys - Komfort nicht ohne Risiko

_____ Schulen ans Netz

_____ Orientierungshilfe Behördlicher Datenschutzbeauftragter

_____ Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

_____ Orientierungshilfe Telefax

_____ Orientierungshilfe Unterlagenvernichtung

Mit freundlichen Grüßen