SCHLESWIG-HOLSTEINISCHER LANDTAG
13. Wahlperiode

Drucksache 13/1810

24. 02. 93

100 Seiten

Bericht

des Landesbeauftragten für den Datenschutz
bei der Präsidentin des Schleswig-Holsteinischen Landtages

Sechzehnter Tätigkeitsbericht
(Berichtszeitraum: März 1993 bis Februar 1994)

SCHLESWIG-HOLSTEINISCHER LANDTAG
13. Wahlperiode

Drucksache 13/1810

24. 02. 93

Bericht

**des Landesbeauftragten für den Datenschutz
bei der Präsidentin des Schleswig-Holsteinischen Landtages**

**Sechzehnter Tätigkeitsbericht
(Berichtszeitraum: März 1993 bis Februar 1994)**

In der Anlage übersende ich gemäß § 23 Abs. 3 Satz 2 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen vom 30. Oktober 1991 den sechzehnten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz bei der Präsidentin des Schleswig-Holsteinischen Landtages.

Dr. Helmut Bäumler

Die Landtagsdrucksachen sind fortlaufend und einzeln beim Verlag Schmidt & Klaunig, Ringstraße 19, 2300 Kiel 1, Fernruf 04 31/6 20 95, zu beziehen.

Der Landesbeauftragte für den Datenschutz bei der Präsidentin des Schleswig-Holsteinischen Landtages

Düsternbrooker Weg 82, 24105 Kiel
Telefon: 0431/596-3280, Telefax: 0431/596-3300

Der Landesbeauftragte für den Datenschutz:	**Dr. Helmut Bäumler**
Dienstzimmer:	24105 Kiel, Düsternbrooker Weg 82
Dienstanschluß:	0431/596-3280
Vorzimmer:	Monika Harks App. 3281
Vertreter des Landesbeauftragten für den Datenschutz:	**Eckhard Beilecke** App. 3285

Referat LD 1

Dr. Helmut Bäumler App. 3280	
Silke Molt App. 3284	Grundsatzfragen des Datenschutzes Vorbereitung der Sitzungen der Konferenz der Datenschutzbeauftragten Haushalt, Beschaffung Allgemeine Verwaltungsangelegenheiten der Dienststelle Betreuung der DATENSCHUTZAKADEMIE
Monika Harks App. 3281	Öffentlichkeitsarbeit, Vorbereitung von Veranstaltungen Vorbereitung von Publikationen Fortbildung

Referat LD 2

Eckhard Beilecke App. 3285	
Jürgen von der Ohe App. 3287	Datenschutz im Bereich des Personal-, Wahl-, Melde-, Ausweis-, Kataster-, Ausländer-, Kommunal-, Gewerbe-, Bau- und Wirtschaftswesens Datenschutz im Bereich der Parlamentsverwaltung
Holger Brocks App. 3289	Datenschutz im Bereich des Statistik-, Verkehrs-, Umweltschutz-, Planungs-, Zivil- und Katastrophenwesens und im Kultusbereich sowie in Bereichen, für die keine andere Zuständigkeit festgelegt ist, fachübergreifende Fragen der Wissenschaft und der Forschung

Dörte Neumann App. 3237	Dokumentation, Registratur, Sekretariat
Sandra Meier App. 3299	
Anke Tuschik App. 3299	

Referat LD 3

Uwe Jürgens App. 3295	
Heiko Behrendt App. 3294	Datenschutz im Bereich der Steuer- und Landwirtschaftsverwaltung sowie innerhalb der Dienststelle des Landesbeauftragten Grundsatzfragen der Datensicherung und der ordnungsgemäßen Anwendung der DV-Programme (§§ 7, 8 LDSG), Prüfungen von Rechenzentren, Prüfung von Behörden, soweit Fragen der automatisierten Datenverarbeitung berührt sind, Mitwirkung bei der Erstellung von Gutachten Neue Medien und Informationstechniken, Medienrecht EDV-Einsatz der Dienststelle Führung und Veröffentlichung der Dateienübersicht, § 24 LDSG

Referat LD 4

Herbert Neumann App. 3290	
Gabriele Meyer-Bettyn App. 3286	Datenschutz im Sozial- und medizinischen Bereich
Hans-Jürgen Strasdat App. 3296	Datenschutz im Justiz-, Polizei- und Verfassungsschutzbereich

SECHZEHNTER TÄTIGKEITSBERICHT

des Landesbeauftragten für den Datenschutz
bei der Präsidentin
des Schleswig-Holsteinischen Landtages

nach § 23 Absatz 3 des
Schleswig-Holsteinischen Gesetzes
zum Schutz personenbezogener Informationen
vom 30. Oktober 1991

(Berichtszeitraum: März 1993 bis Februar 1994)

Inhaltsverzeichnis

		Seite
1.	**Zur Lage des Datenschutzes in Schleswig-Holstein**	9
1.1	Das neue Landesdatenschutzgesetz in der Praxis	9
1.2	Beratung und Kontrolle	10
1.3	Die Situation der Dienststelle	10
1.4	Die DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN	11
2.	**Das Recht auf informationelle Selbstbestimmung in der Bewährung**	12
2.1	Die Entwicklung seit dem Volkszählungsurteil	12
2.2	Neue Risiken für den Datenschutz	13
3.	**Datenschutz im Parlament**	16
3.1	Datenschutz bei parlamentarischen Untersuchungsausschüssen	16
3.2	„Gläserne" Abgeordnete?	18
3.3	Die Behandlung des Tätigkeitsberichts im Parlament	19
4.	**Datenschutz in der Verwaltung**	19
4.1	**Allgemeine und innere Verwaltung**	19
4.1.1	**Personalwesen**	19
4.1.1.1	Bewerberauswahl für die Besetzung von Schulratsstellen: Verstöße gegen das Datenschutzrecht	19
4.1.1.2	Datenverarbeitung bei den Personalräten	21
4.1.1.3	Mitteilung einer Schwangerschaft an den Personalrat?	22
4.1.1.4	Kauf eines Jobtickets: Parkberechtigung weg!	23
4.1.1.5	Konsequenzen aus der Prüfung von Personalakten im Kultusministerium	23

		Seite
4.1.2	**Verfassungsschutz**	25
4.1.2.1	Amtshilfe des Bundesgrenzschutzes für die Geheimdienste	25
4.1.2.2	Neufassung der NADIS-Richtlinien	26
4.1.3	**Öffentliche Sicherheit**	27
4.1.3.1	Konsequenzen aus der Datenschutzprüfung bei der Polizei	27
4.1.3.2	Neuregelung der Vorgangsverwaltung bei der Polizei	29
4.1.3.3	COMPAS	30
4.1.3.4	Auskunftsrecht und Akteneinsicht Betroffener gegenüber der Polizei	31
4.1.3.5	Lauschangriff gegen die Polizei kein Problem	32
4.1.4	**Bau- und Wohnungswesen**	33
4.1.4.1	Entwurf für neue Landesbauordnung berücksichtigt auch Datenschutz	33
4.1.4.2	Übermittlung vollständiger Kaufverträge zur Ausübung des gemeindlichen Vorkaufsrechts?	34
4.1.5	**Umweltschutz**	35
4.1.5.1	Entwurf eines Landesumweltinformationsgesetzes	35
4.1.5.2	Abfallgebührenerhebung durch Einzugsermächtigung	36
4.1.5.3	Der „Gelbe Wertstoffsack" als Datenspeicher?	37
4.2	**Kommunalbereich**	37
4.2.1	Probleme einer Stadtverwaltung bei der Umsetzung des neuen Datenschutzrechts	37
4.2.2	Die Kommunalwahl und ihre Vorbereitung	40
4.2.3	Direkter Zugriff des Rechnungsprüfungsamtes auf Verwaltungsdaten?	42
4.3	**Justizverwaltung**	43
4.3.1	Noch ein Jubiläum: 10 Jahre Übergangsbonus für GAST	43
4.3.2	Konsequenzen aus der Prüfung in den Justizvollzugsanstalten	45
4.3.3	Wahrung der Persönlichkeitsrechte bei der Häftlingsüberwachung	48
4.4	**Steuerverwaltung**	49
4.4.1	Datensicherheit bei der Aktenverwaltung in den Finanzämtern noch nicht garantiert	49
4.4.2	„Aufbewahrung vorbehalten"	50
4.4.3	Es geht doch: Fairneß bei Kontrollmitteilungen	51
4.5	**Wirtschaft, Technik und Verkehr**	52
4.5.1	Automatisierte Zahlungssysteme im Verkehr	52

		Seite
4.5.2	Auskünfte über Halter von Kraftfahrzeugen: Mal zu einfach – mal zu schwer	54
4.6	**Sozialwesen**	55
4.6.1	Intime Fragen an Sozialhilfeempfänger	55
4.6.2	Neugierige Fragen im Rahmen der Anerkennung der Vaterschaft	57
4.7	**Gesundheitswesen**	58
4.7.1	Datenschutz bei der Beratung vor Schwangerschafts-abbruch	58
4.7.2	Offenbarung von Daten im berufsgerichtlichen Ermittlungsverfahren	59
4.7.3	Aufklärung der Leukämiefälle in der Elbmarsch	59
4.7.4	Datenschutzrechtliche Kontrolle von Krankenakten	62
4.8	**Kultusbereich**	63
4.8.1	Datenschutz an der Schule	63
4.8.2	Wenn die Verwaltung anonyme Hinweise erhält	64
5.	**Datenschutz bei den Gerichten**	66
5.1	Prozeßkostenhilfe hätte teuer werden können	66
5.2	Wenn der Gutachter kommt ...	67
6.	**Ordnungsmäßigkeit der Datenverarbeitung**	68
6.1	Leitaussagen zur Informationstechnik in der öffentlichen Verwaltung – IT-Szenario –	68
6.2	Entwurf der Datenschutzverordnung in der Anhörung	71
6.3	Automatisierte Textbearbeitung „verführt" zu überflüssigen Datenbeständen	72
6.4	„Spätfolgen" bei Telefax-Anschlüssen	73
6.5	Von der Realität eingeholt	75
6.6	Ergebnisse von Prüfungsmaßnahmen im Bereich der automatisierten Datenverarbeitung	76
6.6.1	Datenzentrale meldet Abschluß der Maßnahmen-umsetzung	76
6.6.2	Beanstandungen akzeptiert – Abhilfe auf die lange Bank geschoben?	77
6.6.3	Die automatisierte Datenverarbeitung in einer anderen Großstadt – wie die Probleme sich gleichen	79
6.6.4	EDV im Krankenhaus – technischer Fortschritt pro oder contra Patienten-geheimnis?	81
6.6.5	Verdeckte Videoüberwachung – der Datenschutz-„Skandal" des Jahres 1993	84

		Seite
7.	**Neue Medien und Technologien**	86
7.1	Mobilkommunikation	86
7.2	„Rasterfahndung" durch die Gebühreneinzugszentrale der Rundfunkanstalten (GEZ)?	92
8.	**Was es sonst noch zu berichten gibt**	93
9.	**Rückblick**	97

1. Zur Lage des Datenschutzes in Schleswig-Holstein

1.1 Das neue Landesdatenschutzgesetz in der Praxis

Mit Ende des Berichtsjahres sind die Übergangsfristen im Landesdatenschutzgesetz abgelaufen. Das Gesetz ist jetzt auch im konventionellen Bereich in vollem Umfang zu beachten.

Die Kontrollen im vergangenen Jahr haben verschiedene **Mängel** bei der Umsetzung des Gesetzes gezeigt. Dies gilt vor allem für die **Transparenzvorschriften,** die bei der Datenerhebung zu beachten sind (vgl. Tz. 4.2.1), für die **Datensicherung** und generell für die **Ordnungsmäßigkeit der Datenverarbeitung** (Tż. 6.6). Es wird automatisiert, ohne daß klare **fachliche Konzepte** vorliegen, die den Technikeinsatz steuern. Auch der Prozeß der Automatisierung selbst wird nur in Ausnahmefällen von **stringenten Verfahrensregeln** begleitet.

Immer wieder stellen wir bei den Kontrollen fest, daß selbst die **Geräteverzeichnisse,** d.h. der Überblick, welche Computer überhaupt in der Behörde vorhanden sind, nicht vorliegen (Tz. 6.6.4). Auch die Meldung der Dateien erfolgt eher schleppend. Die uns bislang vorliegenden **Dateibeschreibungen** decken nur einen Bruchteil der im Land betriebenen Verfahren ab.

Viele Behörden warten ebenso dringend wie wir auf die **Verordnung der Landesregierung** zu den Einzelheiten einer **ordnungsgemäßen automatisierten Datenverarbeitung.** Nach umfangreichen Vorarbeiten im Berichtsjahr besteht Hoffnung, daß die Verordnung noch im Jahre 1994 in Kraft treten könnte (Tz. 6.2).

Generell zeigt sich, daß vom Erlaß eines fortschrittlichen Datenschutzgesetzes zur konsequenten Umsetzung seiner Regelungen ein weiter Weg ist. Dabei die Balance zwischen **Stringenz** und **Flexibilität** zu finden, ist mitunter deshalb so schwer, weil einerseits eine übermäßige Bürokratisierung und Formalisierung der Datenschutzpraxis vermieden werden soll und weil außerdem davon ausgegangen werden kann, daß auf Dauer tatsächlich nur solche Datenschutzbestimmungen eingehalten werden, deren Sinnhaftigkeit für die Verarbeiter einsehbar ist. Andererseits ist eine allgemeine Aussage, welche Daten als besonders sensibel anzusehen sind, ohne Kenntnis des **Verwendungszusammenhanges** kaum möglich. Die Adresse mögen z.B. viele als triviales Datum ansehen. Solange nur Post, Blumen o.ä. geschickt werden sollen, mag dies gelten. In den Händen eines aggressiven Neonazis kann die Anschrift eines ,,ausländerfreundlichen" Politikers aber ein höchst sensibles Datum sein.

Wir sind bei unseren Kontrollen und Beratungen bemüht, die Umsetzung des neuen Datenschutzrechts auf allen Ebenen behutsam und mit **Fingerspitzengefühl,** zugleich aber mit **Konsequenz** und **Engagement,** zu betreiben.

1.2 Beratung und Kontrolle

Auch im Berichtsjahr hatte die Beratung in der Praxis ein deutliches Übergewicht gegenüber der Kontrolle. Es ist ein positives Zeichen, daß nicht nur die Zahl der **Eingaben,** sondern auch der **Beratungsersuchen** deutlich gestiegen ist. Viele **Behörden** entdecken mehr und mehr, welche Vorteile es hat, sich in datenschutzrechtlichen Zweifelsfragen beraten zu lassen, bevor Entscheidungen und Maßnahmen getroffen werden. Von einer durch rechtzeitige Beratung abgesicherten richtigen Verfahrensweise bei der Datenverarbeitung (vgl. dazu Tz. 6.1) profitieren am Ende natürlich nicht nur die Behörden, sondern in erster Linie die **Bürgerinnen und Bürger.**

Eine besondere Form der Beratung sind die **regionalen Datenschutztage.** Gemeinsam mit den Landräten wurden derartige Veranstaltungen im Berichtsjahr in **Itzehoe, Ratzeburg, Plön** und **Eutin** durchgeführt. In Vorträgen, Diskussionen, Arbeitskreisen und Einzelgesprächen wurden die Fragen der praktischen Umsetzung des Datenschutzes mit Bürgerinnen und Bürgern, Schülern, Datenverarbeitern und Mitarbeitern der Verwaltung diskutiert. Parallel dazu wurden in einer Ausstellung Einzelheiten der Datenverarbeitung und Datensicherung in Schleswig-Holstein gezeigt. Obwohl man nicht gerade sagen kann, daß das Thema Datenschutz derzeit besonders in Mode ist, waren die Veranstaltungen durchweg sehr gut besucht und die Vorträge fanden vor vollen Sälen statt.

Die **Kontrolltätigkeit** hatte im vergangenen Jahr ihren Schwerpunkt bei den Fragen der Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung (Tz. 6.6). Die dabei gefundenen Mängel zeigen seit Jahren ein fast konstantes Bild. Andere Kontrollen befaßten sich mit der Umsetzung des neuen Datenschutzrechts in der Kommunalverwaltung (Tz. 4.2.1), der Verarbeitung von Personaldaten (Tz. 4.1.1.1) und mit dem Datenschutz in der Schule (Tz. 4.8.1).

Erstmals wurde auch in dem besonders sensiblen Bereich der Datenverarbeitung in der Psychiatrie geprüft.

Fast überall zeigte sich ein **durchwachsenes Bild.** Der Datenschutz hat in den Behörden zweifellos Fuß gefaßt und Wirkung erzielt. Die ganz großen Skandale haben wir deshalb nicht gefunden. Ein „einwandfrei" war aber ebensowenig zu vergeben. Vielmehr haben die geprüften Stellen weitere Verbesserungen vorzunehmen.

1.3 Die Situation der Dienststelle

In der Dienststelle sind derzeit 14 Mitarbeiterinnen und Mitarbeiter tätig. Im Berichtsjahr konnte ein neuer Sachbearbeiter eingestellt werden, für 1994 ist eine weitere neue Sachbearbeiterstelle bewilligt. Dies sind nur **Tropfen auf den heißen Stein.** Im gleichen Zeitraum ist nämlich auch die elektronische Datenverarbeitung in der Verwaltung weiter zügig ausgebaut worden. Zugleich wurde das Datenverarbeitungsrecht

im vergangenen Jahr spürbar komplizierter. Mit den neu geschaffenen Übermittlungs- und Datenabgleichsmöglichkeiten sind neue Risiken für das Recht auf informationelle Selbstbestimmung entstanden, mit denen eine Verstärkung der Kontrollkapazität einhergehen müßte.

Kurzfristige Verstärkungen der Dienststelle sind angesichts der finanziellen Situation der öffentlichen Hand wohl nicht zu erwarten. Daraus folgt, daß auch weiterhin mit **Defiziten** bei der **Datenschutzkontrolle** zu rechnen ist. Wenn Staat und Gesellschaft dieses auf die Dauer nicht in Kauf nehmen wollen, wird man Überlegungen anstellen müssen, auf welchem Wege eine vernünftige und verantwortbare Korrelation zwischen dem Ausbau der elektronischen Datenverarbeitung in der öffentlichen Verwaltung und einer entsprechenden Kontrollkapazität hergestellt und kontinuierlich aufrecht erhalten werden kann.

1.4 Die DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN

Eine Möglichkeit, für den Datenschutz möglichst breite Wirkung zu erzielen, sehen wir in der Öffentlichkeitsarbeit, Vortragstätigkeit und insbesondere in der **DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN.** Dort können sich alle, die in der öffentlichen Verwaltung für Fragen des Datenschutzes zuständig sind, fortbilden lassen. Die DATENSCHUTZAKADEMIE versteht sich als **praxisorientierte Fortbildungsstätte,** die Wissen vermittelt, das unmittelbar an den Arbeitsstellen umgesetzt werden kann. Deshalb kommen auch die Referenten der DATENSCHUTZAKADEMIE in erster Linie aus der Praxis.

Die bisher dort abgehaltenen Kurse waren gut besucht. Referenten und Teilnehmer haben sich zufrieden geäußert. Verschiedentlich wurde der Wunsch nach einer **Erweiterung** und weiteren **Spezialisierung** des **Kursangebotes** laut. Soweit die vorhandenen Kapazitäten ausreichen, soll diesen Wünschen Rechnung getragen werden.

Einen entscheidenden Vorteil der DATENSCHUTZAKADEMIE sehen wir darin, daß zu ihrer Einrichtung nicht eine neue Behörde, Institution o.ä. ins Leben gerufen wurde, sondern vorhandene Kapazitäten sinnvoll zusammengeführt wurden. Die DATENSCHUTZAKADEMIE ist nämlich ein **Kooperationsprojekt** der **Heimvolkshochschule Leck** im **Deutschen Grenzverein** und des **Landesbeauftragten für den Datenschutz.** Erstere steuert ihre Erfahrung und Kapazität in Fragen der Erwachsenenfortbildung bei, während die inhaltliche Konzipierung und Realisierung der Kurse in unseren Händen liegt.

Einige Veranstaltungen der DATENSCHUTZAKADEMIE werden zusammen mit der **Verwaltungsschule,** der **Verwaltungsfachhochschule** und der **Polizeischule** durchgeführt.

Für die Dienststelle des Landesbeauftragten hat die DATENSCHUTZAKADEMIE neben den Vorteilen, die eine fundierte

Ausbildung von möglichst vielen Mitarbeitern der öffentlichen Verwaltung in Datenschutzfragen bietet, noch weitere positive Aspekte. Sie eröffnet die Möglichkeit, die **Vortragstätigkeit** zu **bündeln** und auf ein Kurrikulum hin zu orientieren. Das Datenschutzthema wird so in der Fortbildungslandschaft mehr und mehr von einem Aperçu zu einem eigenständigen Thema. Die Möglichkeit, in der DATENSCHUTZ-AKADEMIE **Multiplikatoren** auszubilden, **potenziert** die Wirkung der Vorträge, so daß sich der Einsatz am Ende für die Sache des Datenschutzes lohnen dürfte.

2. Das Recht auf informationelle Selbstbestimmung in der Bewährung

2.1 Die Entwicklung seit dem Volkszählungsurteil

Bereits 10 Jahre ist es her, daß das Bundesverfassungsgericht im Volkszählungsurteil den **verfassungsrechtlichen Rang** des Rechts auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts anerkannt und bekräftigt hat. Nur wenige Urteile des Gerichts sind in ihren zentralen Aussagen so klar und eindeutig und haben eine derart breite Wirkung erzielt. Das Urteil hat dem Datenschutz die Wege geebnet und ihn zu einem festen Bestandteil unserer Rechtsordnung gemacht.

Dutzende von Gesetzen sind seitdem ergangen, in denen das „Kleingedruckte" des Rechts auf informationelle Selbstbestimmung bereichsspezifisch geregelt ist. Das so entstandene **Normengeflecht** ist **engmaschig** und **kompliziert.** Dies steht der Intention des Verfassungsgerichts, der Bürger solle bereits aus normenklaren Gesetzen erkennen können, mit welcher Verarbeitung seiner Daten er zu rechnen hat, gelegentlich bereits entgegen.

Die Gründe dafür liegen auch in der **Komplexität der Datenverarbeitung** selbst. Eine Gesetzgebung, die sich über weite Strecken als Umsetzung und Beschreibung der staatlichen Datenverarbeitung versteht, weniger als deren Begrenzung, gibt ein Spiegelbild der enormen Intensität und Dichte der Datenverarbeitung. Anders ausgedrückt: Wer sich über die zunehmende Fülle und Kompliziertheit der Datenverarbeitungsnormen beklagt, meint damit letzlich die Fülle und Kompliziertheit der Datenverarbeitung selbst.

Häufig werden in der Debatte auch die Begriffe **Datenschutzrecht** und **Datenverarbeitungsrecht** nicht deutlich genug unterschieden. Letzteres stellt die Gesamtheit der Normen dar, die bei der Verarbeitung von personenbezogenen Daten zu beachten sind, sowie die Erlaubnistatbestände der Datenverarbeitung. Nun kann man zwar mit einem gewissen Recht behaupten, eine Erlaubnisnorm enthalte immer auch ein begrenzendes Element für die Datenverarbeitung, wirke sich also letztlich als Schutznorm für den Bürger aus. Viele der seit dem Volkszählungsurteil geschaffenen Verarbeitungsvorschriften sind aber derart allgemein und umfassend zugunsten

der Eingriffsseite formuliert, daß es schwerfällt, sie als „Datenschutzgesetze" im eigentlichen Sinn zu verstehen.

Noch fehlt der Datenschutzgesetzgebung das **krisensichere verfassungsrechtliche Fundament.** Die **Gemeinsame Verfassungskommission** des Bundestages und des Bundesrates hat zwar ausdrücklich die Aufnahme eines Grundrechts auf Datenschutz in die Verfassung mit absoluter Mehrheit befürwortet, nicht aber mit der notwendigen 2/3-Mehrheit. Derzeit liegen dem Deutschen Bundestag entsprechende Anträge der SPD-Fraktion und der Gruppe Bündnis 90/DIE GRÜNEN vor. Eine Aufnahme des **Grundrechts auf Datenschutz** in die Verfassung hätte eine positive Signalwirkung, würde das Grundrecht auch bei sich ändernder Rechtsprechung des Bundesverfassungsgerichts sichern und dem Anspruch einer Verfassung für die Informationsgesellschaft entsprechen. Erstmals würde damit überdies der **Grundrechtskatalog erweitert,** statt, wie häufig in den vergangenen Jahren, eingeschränkt.

Trotz umfänglicher Gesetzgebung seit Erlaß des Volkszählungsurteils klaffen im **Recht der Datenverarbeitung** noch **beträchtliche Lücken.** So ist die **Strafprozeßordnung** in den vergangenen Jahren zwar mehrfach um neue Eingriffsinstrumente erweitert worden. Die dringend notwendige datenschutzrechtliche Ergänzung steht aber noch aus. Dabei geht es um weit mehr als nur die Erfüllung einer lästigen Pflicht. Informationen, die im Zusammenhang mit **Strafermittlungen** erhoben worden sind, gehören zu den **sensibelsten,** über die staatliche Stellen verfügen. Regelungen zum Umgang mit diesen Daten sind alles andere als trivial. Wenn wir schon, um nur einen wichtigen Aspekt herauszugreifen, in Gestalt des Bundeszentralregistergesetzes detaillierte und wohlabgewogene Regelungen für die Speicherung und Nutzung von Informationen über Strafurteile haben, um wieviel mehr benötigen wir vor dem Hintergrund der Unschuldsvermutung derartige Vorschriften für den Umgang mit Strafermittlungsdaten, wenn die Schuld noch gar nicht gerichtlich festgestellt ist.

Das Fehlen von Datenschutzvorschriften in der Strafprozeßordnung macht sich besonders nachteilig in einem Land bemerkbar, das wie **Schleswig-Holstein** die Datenverarbeitung bei den Staatsanwaltschaften in Form des **GAST-Verfahrens** automatisiert hat (Tz. 4.3.1). Andere wichtige **Gesetzgebungsdefizite** bestehen beim Bund vor allem im **Polizei- und Justizbereich,** beim **Arbeitnehmerdatenschutz** und besonders beim **Datenschutz in der Privatwirtschaft.**

2.2 Neue Risiken für den Datenschutz

Diese Defizite wirken um so schwerer, als dem Recht auf informationelle Selbstbestimmung beständig **neue Gefahren** erwachsen. Wer die **Datenverarbeitungstechnik** zur Zeit des Volkszählungsurteils mit dem heutigen Stand der Entwicklung vergleicht, bekommt einen Eindruck von der ungeheuren Dy-

namik der Materie. Die bloße Umsetzung des Volkszählungsurteils durch Schaffung von Rechtsgrundlagen reicht nicht mehr aus. Der Blick muß sich stärker auf die **Technik des Verarbeitungsprozesses** selbst richten. Zwar war es richtig, nach dem Volkszählungsurteil auch die konventionelle Datenverarbeitung außerhalb der Dateien in den Datenschutz einzubeziehen. Die Befassung mit Akten, Listen, Notizbüchern etc. darf aber nicht den Blick auf die Risiken einer auf der Oberfläche immer einfacher, in Wirklichkeit aber immer komplizierter werdenden Technik versperren. Die **sichere Beherrschung** des **automatisierten Verarbeitungsprozesses,** die Garantie seines ordnungsgemäßen Ablaufs und die notwendigen organisatorischen Konsequenzen innerhalb der Verwaltung haben dabei Bedeutung weit über den Datenschutz hinaus.

Neue Risiken drohen dem Datenschutzrecht der Bürgerinnen und Bürger aber nicht nur aus der Technik, sondern aus den sich ändernden **gesellschaftlichen Rahmenbedingungen.** Sie sind gekennzeichnet durch steigende Kriminalität und wachsende öffentliche Finanznot. Einer stärkeren Unterordnung von Einzelinteressen unter das Gemeinwohl wird, häufig unspezifiziert, das Wort geredet.

Der **große Lauschangriff** ist zwischen den großen Parteien dem Grunde nach offenbar nicht mehr umstritten. Prompt ist die öffentliche Diskussion zum Thema merklich abgeflaut. Wo früher leidenschaftlich für die Einführung des großen Lauschangriffs gestritten wurde, so als sei er das alles entscheidende Wundermittel zur Bekämpfung der organisierten Kriminalität, wird nunmehr zwei Nummern kleiner argumentiert. Gewiß, wichtig sei der Lauschangriff schon, aber er sei nur eine Verbesserungsmöglichkeit unter anderen. Man solle keine Wunderdinge von ihm erwarten usw., zusätzlich brauche man mindestens noch ...

Die Kritiker des großen Lauschangriffs müssen sich durch derlei Wechsel in der Tonart bestätigt fühlen: Einen so gravierenden Einschnitt wie die Zulassung des Lauschangriffs vorzunehmen, ohne daß er wirklich unabweisbar notwendig ist, ist **unverhältnismäßig.** Das Recht auf Privatheit wird einen entscheidenden Einbruch erleiden, wenn man sich nicht einmal mehr in den eigenen vier Wänden unbeobachtet bewegen kann. Und das alles nur, um das polizeiliche Ermittlungsinstrumentarium zu komplettieren und abzurunden? Ohne daß sich am Ansteigen der Kriminalität oder der Aufklärungsquote irgend etwas spürbar ändern würde?

Die nächsten Forderungen liegen bereits auf dem Tisch. Das **Bundeskriminalamt** soll erweiterte Befugnisse erhalten zu Lasten des föderalen Aufbaus der Polizeibehörden. Die **Schwelle** für **strafprozessuale Ermittlungen,** in der bestehenden Strafprozeßordnung bereits auf denkbar niedrigem Niveau, soll noch weiter abgesenkt werden. Obwohl die Aufklärungsquote der begangenen Straftaten in den letzten Jahren gesunken ist, sollen die Ermittlungskapazitäten stärker in das

Vorfeld von Straftaten gelenkt werden. Welche Rechtssicherheit wird noch verbleiben, wenn Polizei und Staatsanwaltschaft bereits beim **Verdacht eines Anfangsverdachts** mit den Ermittlungen beginnen dürfen?

Mehr und mehr droht das Gespür für den **„Mut zur Lücke"** verloren zu gehen. Kennzeichnend für den demokratischen Rechtsstaat ist aber nicht seine Allwissenheit, sondern die bewußte Beschränkung seiner Informationsherrschaft.

Die **öffentliche Finanznot** fügt den Gefährdungen für den Datenschutz neue hinzu. Wo alle sparen müssen, besteht für den unberechtigten Bezug von Leistungen keinerlei Verständnis mehr. Die Jagd nach Steuer-, Subventions-, Sozialleistungs- oder Gebührensündern drängt die Diskussion über die Ursachen der Finanznot in den Hintergrund. Nunmehr zeigt sich, daß die Möglichkeiten der EDV auch tatsächlich genutzt werden. Wo der schnelle Datenabgleich die manuelle Prüfung ersetzt, geht leicht der Blick für einen **schleichenden Erosionsprozeß** verloren. Solange Vergleiche „per Hand" durchgeführt werden mußten, war notgedrungen die Beschränkung auf die Verdachtsfälle unabdingbar. Der **elektronische Datenabgleich** schafft mühelos die Prüfung von Zehntausenden in kürzester Frist. Wozu sich auf die Verdächtigen beschränken, wenn jeder überprüft werden kann?

So wächst die Zahl der Wünsche nach „Abgleich" und pauschaler Überprüfung. Das Gesetz zur Umsetzung des föderalen Konsolidierungsprogramms beispielsweise schafft Rechtsgrundlagen für einen Abgleich der unterschiedlichen **Sozialleistungen,** ohne daß ein Verdacht bestehen müßte. Die **Gebühreneinzugszentrale der Rundfunkanstalten (GEZ)** möchte gerne die Daten aller Meldeveränderungen abgleichen, egal ob die Betreffenden ein Rundfunkgerät besitzen oder ihre Gebühren bezahlt haben (vgl. Tz. 7.2). Auf die Idee der **Überprüfung aller Wahlberechtigten** eines Bundeslandes schließlich wäre früher niemand gekommen, wenn dies per Hand, Karteikarte für Karteikarte, hätte erfolgen müssen.

Alle diese Abgleiche und Kontrollvorgänge mögen für sich gesehen eine gewisse Berechtigung haben. Am Ende tragen sie aber bei zu einem **Netz** von **Überwachungs-** und **Überprüfungsmöglichkeiten. Jeder Bürger** wird zum **potentiell Verdächtigen,** dessen Korrektheit es erst zu überprüfen gilt. Wenn das keine grundlegende Änderung im Verhältnis des Staates zum Bürger ist?

Neues Material für Überprüfungen aller Art entsteht an allen Ecken und Enden. Der zunehmende Gebrauch von **Kreditkarten** führt zu breiten Datenspuren, aus denen das **Konsum-** und **Freizeitverhalten** der Kartenbenutzer abgelesen werden kann. Bei der Einführung **kartengestützter Zahlungssysteme** im **öffentlichen Nahverkehr** und im Bereich der **Autobahngebühren** steht erneut eine grundsätzliche Weichenstellung an (vgl. Tz. 4.5.1): Noch ist nicht entschieden, ob in diesem Zusammenhang nach Ablauf einer bestimmten Zeit abgerechnet wird **(Post-paid)** oder im vorhinein **(Pre-paid).**

Bei Post-paid-Verfahren muß zunächst aufgezeichnet werden, wer wann wo welche Leistungen beansprucht hat. Würde die Entscheidung für diese Variante fallen, so würden die Bürgerinnen und Bürger unfreiwillig selbst ein **detailliertes Bewegungsprofil** liefern.

Es besteht also gerade beim Recht auf informationelle Selbstbestimmung auch zehn Jahre nach dem Volkszählungsurteil kein Anlaß, sich zurückzulehnen und das Erreichte selbstzufrieden zu betrachten. Zu **dynamisch** ist die **Technik,** auf die der **Datenschutz** nur **reagiert.** Noch ist die Frage nicht entschieden, ob sich die Bundesrepublik nicht doch auf dem **Weg in den Überwachungsstaat** befindet.

3. Datenschutz im Parlament

3.1 Datenschutz bei parlamentarischen Untersuchungsausschüssen

Der erste Untersuchungsausschuß der 13. Wahlperiode hat sich auch mit Fragen des Datenschutzes zu befassen. Durch eine sachgerechte Verfahrensgestaltung können der Datenschutz Betroffener und eine effektive Sachverhaltsaufklärung in Einklang gebracht werden.

Der Vorsitzende des **„Schubladen"-Untersuchungsausschusses** bat um eine gutachterliche Stellungnahme zu einigen Beweiserhebungs- und Beweissicherungsanträgen sowie generell zur Frage des Verhältnisses der Untersuchungsrechte des Ausschusses zum **Persönlichkeitsrecht Betroffener.** Die Anträge waren auf Sicherstellung gerichtlicher, staatsanwaltschaftlicher und ministerieller Unterlagen, z. B. von Posteingangsbüchern des Justizministers und der Staatskanzlei, Personalakten, Aufzeichnungen über Telefongespräche und Terminkalendern gerichtet. Wir haben dargelegt, daß nach Art. 18 der Landesverfassung der Untersuchungsausschuß in erster Linie selbst über **„die erforderlichen Beweise"** bestimmt. Die näheren Einzelheiten hierzu ergeben sich aus dem Gesetz zur Regelung des Rechts der parlamentarischen Untersuchungsausschüsse. Eingeschränkt wird dieses Bestimmungsrecht nur durch den Untersuchungsauftrag selbst. Beweisanträge ohne Beziehung zum Untersuchungsauftrag wären von der Landesverfassung nicht mehr gedeckt.

Zur Wahrung der **Persönlichkeitsrechte Dritter** sollte die Beweiserhebung stufenweise erfolgen. Durch Anträge auf **Sicherstellung** möglicher Beweismittel sollten diese aus dem Verantwortungsbereich der abgebenden Stellen in den des Untersuchungsausschusses überführt und dort zunächst unter Verschluß gehalten werden. Eine inhaltliche Auswertung der Unterlagen in Form der **Beweisaufnahme** sollte erst in einem zweiten Schritt, nach Konkretisierung der Beweisthemen, erfolgen.

Für die Zuleitung von Unterlagen der Landesregierung auf **Anforderung des Untersuchungsausschusses** bestehen

demnach, auch wenn der Beweisantrag noch nicht hinreichend konkretisiert ist, schon dann ausreichende Rechtsgrundlagen in der Landesverfassung, wenn

- nach dem zunächst noch pauschalen Beweisantrag die Unterlagen von ihrem Inhalt her Feststellungen oder weiterführende Hinweise zum Untersuchungsauftrag enthalten können,
- die Unterlagen deshalb zunächst nur sichergestellt, aber noch nicht ausgewertet werden,
- von der abgebenden Stelle keine durchgreifenden Weigerungsrechte grundsätzlicher Art (Art. 23 Abs. 3 Landesverfassung) geltend gemacht werden und
- hinreichende organisatorisch-technische Sicherungsmaßnahmen für die Unterlagen geschaffen werden.

Soll auf den **Inhalt der Unterlagen** zugegriffen werden, so muß zuvor die **Beweisfrage konkretisiert** sein. Auf ihrer Grundlage muß sodann das erforderliche Maß für die Auswertung der Beweismittel nach Art und Umfang festgelegt werden. Dabei können **Einschränkungen** erforderlich werden, indem z. B.

- Aufzeichnungen nur in bezug auf einen **bestimmten Zeitraum ausgewertet** werden, als er den ursprünglichen Anträgen zugrunde lag (z.B. Auswertung nicht einer Personalakte insgesamt, sondern nur von Unterlagen ab einem bestimmten Zeitpunkt),
- sensible Daten vor ihrer Auswertung nach der **Geheimschutzordnung** des Landtages kategorisiert und entsprechend als **Verschlußsache** behandelt werden,
- die Auswertung nur von bestimmten Mitgliedern des Ausschusses oder dem **Vorsitzenden** und seinem **Stellvertreter** vorgenommen wird,
- die **Öffentlichkeit** bei der Beweisaufnahme **ausgeschlossen** wird,
- das Anfertigen von **Kopien** aus den Unterlagen eingeschränkt und ggf. **dokumentiert** wird.

Durch die zur Vorlage von Beweismitteln verpflichteten öffentlichen Stellen können Datenschutzrechte Dritter nur in eingeschränktem Maße geltend gemacht werden. Nach der **Rechtsprechung des Bundesverfassungsgerichts** sind das Aufklärungsrecht des Untersuchungsausschusses und das Persönlichkeitsrecht der Betroffenen als verfassungsmäßige Rechte prinzipiell gleichwertig. Sie sind so aufeinander abzustimmen, daß beide die größtmögliche Wirkung entfalten.

Soweit sich die Beweisanträge also im **Rahmen des „Erforderlichen"** halten, stehen Datenschutzbelange einer Datenübermittlung an den Untersuchungsausschuß in der Regel nicht entgegen. Ausgeschlossen wären allerdings Fragen, die den Kernbereich des Persönlichkeitsrechts betreffen, etwa aus der engsten persönlichen oder familiären Sphäre.

Den schützenswerten Interessen einzelner ist dadurch Rechnung zu tragen, daß eine unbefugte Kenntnisnahme Außenstehender vom Inhalt der Unterlagen ausgeschlossen wird. Dazu können folgende **Datensicherungsmaßnahmen** dienen, die wir dem Untersuchungsausschuß empfohlen haben:

- Die Beweisunterlagen sollten in einem **Verzeichnis** erfaßt und die Herausgabe und Einsichtnahme mit Datum und Namen der Beteiligten vermerkt werden.
- Das Verzeichnis und die Akten sollten in einem **verschließbaren Raum** und dort in einem **besonderen, verschlossenen Behältnis** verwahrt werden.
- **Verschlußsachen** und nach der Geheimschutzordnung des Landtages eingestufte Unterlagen sollten entsprechend diesen Regelungen behandelt werden.
- Besonders sensible Unterlagen sollten zusätzlich in **verschlossenen Umschlägen** aufbewahrt werden. Hierzu wären z.B. Personalakten sowie jene Terminkalender zu zählen, die auch private Termine enthalten.
- Bei der Frage besonderer Geheimhaltungsstufen oder besonderer Sensibilität von Unterlagen sollte weitgehend den **Anregungen der abgebenden Stellen** gefolgt werden.
- Die **Grundzüge des Verfahrens sollten schriftlich festgehalten** werden.

Die bisherigen Erfahrungen des „Schubladen"-Untersuchungsausschusses haben gezeigt, daß bei Beachtung dieser Aspekte die datenschutzrechtlichen Probleme zu bewältigen sind.

3.2 „Gläserne" Abgeordnete?

Die Verhaltensregeln für Abgeordnete sind in Kraft getreten. In ergänzenden Verwaltungsvorschriften sollen die Einzelheiten des Umgangs mit den Abgeordnetendaten geregelt werden.

Im 15. Tätigkeitsbericht (S. 20) war angeregt worden, in Ausführungsbestimmungen zu den **„Verhaltensregeln für Abgeordnete"** möglichst umgehend die Einzelheiten festzulegen, die den **Umgang mit den Daten der Abgeordneten** regeln. Wir haben der Landtagspräsidentin empfohlen festzulegen, welche Personen Einblick in die Daten der Abgeordneten erhalten,

- wer für ihre Verarbeitung und Kontrolle zuständig ist,
- welche Verarbeitungsschritte dabei ablaufen und
- wie sie dokumentiert werden.

Zu bestimmen ist auch, wie und von wem die Unterlagen mit den Abgeordnetendaten aufzubewahren sind und wer die datenschutzrechtliche Verantwortung zu tragen hat.

3.3 Die Behandlung des Tätigkeitsberichts im Parlament

Der 14. und der 15. Tätigkeitsbericht wurden vom Parlament gemeinsam beraten. Erstmals fand eine **Debatte im Plenum** vor der Ausschußberatung und eine weitere nach deren Abschluß statt. Die Beratungen im **Innen- und Rechtsausschuß** wurden in mehreren Besprechungsrunden der **datenschutzpolitischen Sprecher der Fraktionen** vorbereitet. Da bei diesen Vorgesprächen auch die Vertreter der Regierung anwesend waren, konnten eine Reihe von Detailfragen mit der gebotenen Gründlichkeit beraten werden. In einigen Punkten konnten daraufhin konkrete Fortschritte in datenschutzrechtlichen Streitfragen erzielt werden.

Die Vorbereitung der Detaildiskussion in **Berichterstattergesprächen** hat sich deshalb aus der Sicht des Datenschutzbeauftragten **bewährt.** An dieser Praxis könnte deshalb auch künftig festgehalten werden. Insgesamt fand die Sache des Datenschutzes auch im Berichtsjahr im Parlament stets ein offenes Ohr und erfuhr die notwendige Unterstützung.

4. Datenschutz in der Verwaltung

4.1 Allgemeine und innere Verwaltung

4.1.1 Personalwesen

4.1.1.1 Bewerberauswahl für die Besetzung von Schulratsstellen: Verstöße gegen das Datenschutzrecht

Im Rahmen der Bewerberauswahl für die Besetzung von Schulratsstellen in den Jahren 1991 und 1992 ist gegen Datenschutzrecht verstoßen worden. Neue Verfahrensregelungen, die dies für die Zukunft verhindern sollen, sind noch nicht ergangen.

Aufgrund von Eingaben wurde die **Bewerberauswahl** für die Besetzung von **Schulratsstellen** in den Jahren 1991 und 1992 bei der Bildungsministerin datenschutzrechtlich überprüft. Von den Petenten war insbesondere kritisiert worden, daß als Grundlage für die Auswahlentscheidung Eignungsvermerke über die einzelnen Bewerber gefertigt wurden, von denen die Betroffenen keine Kenntnis erhielten. Nach Mitteilung der Bildungsministerin wurden diese Vermerke, die angeblich nur Auszüge aus den Personalakten darstellten, nach Abschluß des jeweiligen Auswahlverfahrens vernichtet.

Kopien der **Eignungsvermerke** waren jedoch im Rahmen des Beteiligungsverfahrens auch den zuständigen **Hauptpersonalräten** als Entscheidungsgrundlage für die Bewerberauswahl zur Verfügung gestellt worden. Dort waren sie noch nicht gelöscht und konnten für die datenschutzrechtliche Prüfung herangezogen werden. Auf diese Weise konnte auf Unterlagen über insgesamt 51 Bewerber zurückgegriffen werden.

Aus den Personalakten der Bewerber ergab sich, daß diese bei negativen Entscheidungen ein **Ablehnungsschreiben** erhalten hatten, in dem lediglich darauf hingewiesen wurde, daß auf die Ausschreibung hin sehr viele qualifizierte Bewerbungen eingegangen seien und daß dieser hohen Anzahl von Bewerbungen nur sehr wenige zu besetzende Stellen gegenübergestanden hätten. Deshalb sei eine Berücksichtigung der Bewerberin oder des Bewerbers leider nicht möglich gewesen. Der Inhalt der Eignungsvermerke war nicht Gegenstand der Ablehnungsschreiben.

Aus datenschutzrechtlicher Sicht war vor allem zu prüfen, ob die **Vernichtung der Vermerke** in Einklang mit den Löschungsregelungen des Landesdatenschutzgesetzes stand. Danach dürfen personenbezogene Daten, die nicht mehr benötigt werden, u.a. dann nicht gelöscht werden, wenn Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange Betroffener beeinträchtigt werden.

Jeder **Beamte** hat ein **Recht** auf **Einsicht** in seine **vollständige Personalakte.** Sie muß alle Unterlagen enthalten, die den Beamten in seinem Rechtsverhältnis zum Dienstherrn betreffen und die zur Dokumentation dieses Rechtsverhältnisses erforderlich sind. Dies ergibt sich auch aus der **Schutzfunktion,** die die **Personalakte** für den Beamten hat. Das Einsichtsrecht des Beamten soll gewährleisten, daß er die ihm aus dem Dienstverhältnis zustehenden Rechte wahrnehmen kann.

Die geprüften Vermerke enthielten der Sache nach **Anlaßbeurteilungen** für die Entscheidung über die Besetzung von Schulratsstellen. Im einzelnen wurde zu dem beruflichen Werdegang, zu Prüfungen und dienstrechtlichen Beurteilungen, zum Umfang und zur Qualität der bisherigen Tätigkeit Stellung genommen und schließlich in einer „zusammenfassenden Bewertung" eine Beurteilung der Tätigkeit des Betroffenen in der Funktion des Schulleiters abgegeben. Aus dem Gesamtbild wurde dann die **Prognoseentscheidung** hinsichtlich der Eignung als Schulrat mit der jeweiligen Feststellung „gut geeignet", „geeignet", „noch nicht geeignet" bzw. „nicht geeignet" abgeleitet. Der Inhalt dieser Vermerke war die maßgebliche Entscheidungsgrundlage für die Bewerberauswahl.

Nach dem Landesverwaltungsgesetz ist ein schriftlicher Verwaltungsakt auch schriftlich zu begründen. In der Begründung sind die wesentlichen tatsächlichen und rechtlichen Gründe mitzuteilen, die die Behörde zu ihrer Entscheidung bewogen haben. Die Begründung von Ermessensentscheidungen soll auch die Gesichtspunkte erkennen lassen, von denen die Behörde bei der Ausübung ihres Ermessens ausgegangen ist. **Die Dokumentation der Entscheidungsgrundlagen** gehört deshalb in die über das Verwaltungsverfahren zu führende Verwaltungsverfahrensakte.

Für den Bereich des Beamtenrechts sind diese Maßgaben in dem neuen Beamtenrechtsrahmengesetz weiter konkretisiert

worden. Danach sind die Vermerke als **materielle Bestandteile der Personalakte** zu qualifizieren. Sie hätten deshalb auch zur Personalakte genommen werden müssen, um den Betroffenen über ihr Akteneinsichtsrecht ggf. den Rechtsweg für eine Konkurrentenklage zu öffnen. Die Vernichtung der Vermerke hätte somit aus Rechtgründen unterbleiben müssen. Daß sie gleichwohl vorgenommen worden war, war **förmlich zu beanstanden.**

Gleichzeitig haben wir die Duplikate der Kopien aus den Unterlagen des Personalrats an die Bildungsministerin übersandt. Sie sind dort nachträglich wieder **zu den** jeweiligen **Personalakten genommen** worden und konnten von diesem Zeitpunkt ab von den Betroffenen eingesehen werden. Um im Fall einer negativen Beurteilung, zu der sie zeitnah nicht hatten Stellung nehmen können und die insoweit mit einem Verfahrensmangel behaftet war, für die Bewerber keine Nachteile entstehen zu lassen, hat sich die Bildungsministerin bereit erklärt, die Unterlagen nach Kenntnisnahme durch die Betroffenen auf ausdrücklichen Antrag wieder aus der Personalakte zu entfernen.

Für **künftige Auswahlverfahren** zur Besetzung derartiger Stellen wurden in Gesprächen mit dem Ministerium **Verfahrensgrundsätze** entwickelt, die den datenschutzrechtlichen Belangen der Betroffenen gerecht werden. Die entsprechenden Verwaltungsanweisungen waren eigentlich für den Herbst 1993 angekündigt. Bis zum Redaktionsschluß dieses Berichtes war aber noch kein entsprechender Eingang zu verzeichnen.

4.1.1.2 Datenverarbeitung bei den Personalräten

Personalräte sind für die Daten, die ihnen im Rahmen der Mitbestimmung übermittelt werden, datenschutzrechtlich verantwortlich. Art und Umfang der Speicherung und weiteren Verwendung der Daten sollten verbindlich festgelegt werden.

Die Prüfung des Verfahrens bei der Besetzung von Schulratsstellen (vgl. Tz. 4.1.1.1) hat deutlich vor Augen geführt, daß grundsätzlich geklärt werden muß, in welchem Umfang und auf welche Weise Personalräte nach geltendem Recht Personaldaten der Mitarbeiter speichern dürfen. Die in Rede stehenden Unterlagen waren bei der Personalverwaltung nicht mehr vorhanden, wohl aber beim Personalrat. Nach unserer Rechtsauffassung handelt es sich bei den **Personalräten um selbständige datenverarbeitende** Stellen. Daraus folgt, daß ihnen auch die Beachtung der Pflichten nach dem LDSG in eigener Zuständigkeit obliegt. Gegenüber den Betroffenen tragen sie die **rechtliche Verantwortung** für die durch sie verarbeiteten Personaldaten. Sie sind somit auch **Adressat** für **Auskunfts-, Berichtigungs- und Löschungsansprüche** der Mitarbeiter.

Personalräte haben also unter Beachtung der gesetzlichen Vorgaben des Landesdatenschutzgesetzes, des Mitbestimmungs-

gesetzes und der allgemeinen für die Verarbeitung von Personaldaten geltenden Rechtsvorschriften **selbst** die näheren Einzelheiten ihrer Datenverarbeitung **zu verantworten.** Das Landesdatenschutzgesetz schreibt z.B. die **Löschung** personenbezogener Daten vor, wenn ihre Kenntnis für die datenverarbeitende Stelle zur Aufgabenerfüllung **nicht mehr erforderlich** ist und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange der oder des Betroffenen beeinträchtigt werden. Nur im Rahmen der Erforderlichkeit kann die datenverarbeitende Stelle allgemeine Regelungen über die Aufbewahrung von Daten erlassen. Gleiches gilt für die Frage, wie intern der **Zugang zu diesen Daten** geregelt wird.

Es empfiehlt sich daher, in einer **„Aktenordnung für Personalräte"** für die Betroffenen nachvollziehbar festzulegen:

- welche Daten beim Personalrat gespeichert werden sollen,
- zu welchen Zwecken die Daten genutzt werden sollen,
- für welchen Zeitraum die Daten gespeichert bleiben sollen,
- welche technischen und organisatorischen Datensicherungsmaßnahmen zu treffen sind.

4.1.1.3 Mitteilung einer Schwangerschaft an den Personalrat?

Mitteilungen über Schwangerschaften an den Personalrat sind unzulässig, wenn nicht die Einwilligung der Betroffenen vorliegt.

Von **Personalräten** wird immer wieder der Wunsch geäußert, von ihrer Dienststelle über **bestehende Schwangerschaften unterrichtet** zu werden. Als Rechtsgrundlage wird das Mitbestimmungsgesetz angeführt, wonach der Personalrat umfassend über alle Personalangelegenheiten der Dienststelle zu unterrichten ist, soweit es für die Erfüllung seiner Aufgaben erforderlich ist. Schließlich habe der Personalrat zu überwachen, daß die besonderen Schutzvorschriften für werdende Mütter vom Dienstherrn beachtet werden.

Dabei wird allerdings übersehen, daß das **Mitbestimmungsrecht** den Umfang der Mitbestimmung und damit auch die dafür notwendigen Datenübermittlungen beschränkt, soweit **schutzwürdige persönliche Interessen** von Beschäftigten entgegenstehen. Schutzwürdig sind in diesem Zusammenhang die persönlichen Interessen von Beschäftigten, wenn sie an der Geheimhaltung bestimmter Daten ein besonderes Interesse geltend machen können. Diese Voraussetzung ist in der Regel bei **Angaben** über die **persönlichen** und **wirtschaftlichen Verhältnisse** oder bei **ärztlichen Gutachten** erfüllt, sie läßt sich aber auch aus den im Mutterschutzgesetz enthaltenen Regelungen zum Schutz schwangerer Frauen herleiten.

Gerade für die Behandlung von Fällen, in denen das Persönlichkeitsrecht der Betroffenen im Einzelfall den generellen Auftrag des Personalrats zur Interessenvertretung der Mitarbeiter überwiegen kann, ist der **Zustimmungsvorbehalt** im Mitbestimmungsrecht geschaffen worden. Daraus folgt, daß

für die Bekanntgabe einer Schwangerschaft gegenüber dem Personalrat ohne Einwilligung der Betroffenen keine gesetzliche Befugnis besteht.

4.1.1.4 Kauf eines Jobtickets: Parkberechtigung weg!

Daten, die im Rahmen eines Vertragsverhältnisses freiwillig offenbart wurden, dürfen ohne Einwilligung des Betroffenen zu keinem anderen Zweck verwendet werden.

In einer kreisfreien Stadt hatten sich die örtlichen Verkehrsbetriebe entschlossen, verbilligte **Jobtickets** anzubieten, um Berufspendlern einen finanziellen Anreiz zum Umsteigen auf öffentliche Nahverkehrsmittel zu bieten. Um Mißbrauch zu verhindern, war ein Kauf der Jobtickets nur über die jeweiligen Arbeitgeber möglich.

Bei der Stadtverwaltung sah man darin die günstige Chance, anhand der Verkaufsunterlagen die **Anerkennung von Privatwagen** für **dienstliche Zwecke** sowie die Vergabe **städtischer Parkplätze** zu überprüfen. Bei den Mitarbeitern, die aus dienstlichen Gründen häufig auf ihren Pkw angewiesen waren, an außendienstfreien Tagen jedoch öffentliche Verkehrsmittel benutzen wollten, stieß diese Aktion auf wenig Verständnis. Sie baten um datenschutzrechtliche Überprüfung.

Das **Landesdatenschutzgesetz** erlaubt eine Verarbeitung personenbezogener Daten für **andere Zwecke** als den, für den sie erhoben worden sind, nur, soweit dafür eine **besondere gesetzliche Befugnis** vorhanden ist. Bei den Daten über den Kauf des Jobtickets handelte es sich um Angaben, die im Rahmen eines Vertragsverhältnisses offenbart worden waren. Sie hätten deshalb **nur mit Einwilligung** der jeweiligen Mitarbeiter für einen Abgleich mit Daten aus anderen Verwaltungsbereichen genutzt werden dürfen.

Nach dem von uns festgestellten Sachverhalt sind die Beschäftigten beim Kauf der Jobtickets über den beabsichtigten Datenabgleich aber nicht einmal unterrichtet worden. Der Vorgang mußte deshalb als Verstoß gegen geltendes Datenschutzrecht **beanstandet** werden. Außerdem waren die aus dem rechtswidrigen Abgleich entstandenen **Daten zu löschen.**

4.1.1.5 Konsequenzen aus der Prüfung von Personalakten im Kultusministerium

Erste Konsequenzen aus der Prüfung von Lehrerpersonalakten sind gezogen, weitere stehen an. Eine mittlerweile erlassene Ausbildungs- und Prüfungsordnung steht im Widerspruch zu den Prüfungsergebnissen und soll erneut geändert werden.

Über die Feststellungen, die wir bei unserer Prüfung der Lehrerpersonalakten in den Jahren 1990/1991 getroffen haben, ist bereits ausführlich berichtet worden (13. TB, S. 11). Eine erste, noch nicht abschließende **Stellungnahme** der damals zuständigen Ministerin für Bildung, Wissenschaft, Kultur und

Sport schien eine **weitgehende Übereinstimmung** deutlich zu machen und beschränkte die weitere Diskussion auf wenige grundsätzliche Fragen. Die anschließende mündliche Erörterung der offenen Probleme ergab weiteren Entscheidungs- und Handlungsbedarf für das Ministerium, ließ jedoch einen zügigen Abschluß des Prüfungskomplexes im Jahre 1993 erwarten. Die Hoffnung, im vorliegenden Tätigkeitsbericht das Einvernehmen mit der Ministerin feststellen und damit einen endgültigen Schlußstrich unter die Prüfung ziehen zu können, trog jedoch.

Zum 01.08.1993 ist eine von der Ministerin für Bildung, Wissenschaft, Kultur und Sport erarbeitete „Landesverordnung über die Ordnung des Vorbereitungsdienstes und die Zweiten Staatsprüfungen der Lehrkräfte (OVP)" in Kraft getreten, die zum Teil bereits erzielten übereinstimmenden Ergebnissen aus der Prüfung widerspricht. Die seinerzeit zuständige Ministerin für Bildung, Wissenschaft, Kultur und Sport fühlte sich an das Muster einer **Ausbildungs-** und **Prüfungsordnung** gebunden, das der Innenminister als Arbeitshilfe für solche Stellen entworfen hat, die für ihren Zuständigkeitsbereich eigene Ausbildungs- und Prüfungsordnungen zu entwickeln haben. Eine solche Bindung besteht – auch nach Auskunft des Innenministeriums – jedoch nicht. Das Innenministerium hat weiter darauf hingewiesen, daß trotz wünschenswerter Abstimmung und Koordinierung in Grundsatzfragen der Personalverwaltung die Selbständigkeit der einzelnen Ressorts für ihre Entscheidungen bestehen bleibt.

Mit der **OVP** besteht nunmehr zwar eine Rechtsgrundlage für die Datenverarbeitung bei Bewerbungen für den Vorbereitungsdienst der Lehrkräfte. Sie **widerspricht** allerdings materiellen Anforderungen des **Datenschutzes,** wie wir sie im Rahmen unserer Prüfung herausgearbeitet haben. Mit Rücksicht auf die noch andauernden Diskussionen hierüber hätte es deshalb nahe gelegen, den Landesbeauftragten seinerzeit in die Vorbereitung der OVP einzuschalten. Dies ist nicht geschehen.

Trotzdem konnte – infolge der Zuständigkeitsänderung und Umorganisation im Schulbereich verzögert – mit der inzwischen zuständigen Ministerin für Frauen, Bildung, Weiterbildung und Sport in einem weiteren Gespräch in weitem Maße Einvernehmen erzielt werden. Von den Datenverarbeitungsmöglichkeiten, die die OVP eröffnet, wird die Ministerin weitgehend keinen Gebrauch machen, soweit sie im Gegensatz zu der Auffassung des Landesbeauftragten stehen, die **OVP** soll demnächst wieder **geändert** werden.

Übereinstimmung besteht auch darüber, daß im **Bewerberfragebogen** nur solche Daten erhoben werden dürfen, die den Entscheidungskriterien für die Bewerberauswahl entsprechen. Hier besteht noch ein **Abstimmungsbedarf** zwischen Fragebogen und konkretisierten Auswahlkriterien. Das Ministerium hat eine Überarbeitung zugesagt. Eine zusätzliche Abstim-

mung muß insoweit auch mit den entsprechenden Datenfeldern im Personalverwaltungssystem „PERLE" erfolgen.

Unterschiedliche Auffassungen bestehen zwischen der Ministerin für Frauen, Bildung, Weiterbildung und Sport und dem Landesbeauftragten jedoch nach wie vor zu der Frage, ob es erforderlich und damit datenschutzrechtlich zulässig ist, in jedem Fall über die Bewerberinnen und Bewerber eine **uneingeschränkte Auskunft** aus dem **Bundeszentralregister** einzuholen. Wir halten eine unterschiedliche Behandlung von Lehrern und anderen Mitarbeitern im öffentlichen Dienst, die nicht von einer obersten Landesbehörde eingestellt werden, für nicht geboten. Die Tatsache, daß vom Ministerium solche Auskünfte eingeholt werden dürfen, schafft nur eine **formale Berechtigung** gegenüber dem Bundeszentralregister dazu, **nicht** aber eine **materielle Rechtfertigung** gegenüber dem Betroffenen.

Die Ministerin für Frauen, Bildung, Weiterbildung und Sport ist dagegen der Auffassung, daß die Eignungsfeststellung im Lehrerbereich wegen der besonderen **pädagogischen Verantwortung** umfassende Auskünfte erforderlich macht. Aus dem gleichen Grunde wird vom Ministerium weiterhin die Erklärung zu der Frage für erforderlich erachtet, ob gegen einen Bewerber derzeit Strafverfahren laufen. Hierzu vertreten wir die Meinung, daß solche Erklärungen problematisch sind, weil vor einer Verurteilung der Betroffene als unschuldig zu gelten hat, das laufende Verfahren daher nicht gegen ihn zu verwenden ist, nach Verurteilung aber bei Bedarf eine Rücknahme der Beamtenernennung durchgeführt werden kann. Beide Fragenkomplexe werden noch weiter diskutiert werden müssen.

Schließlich wird die Ministerin **Richtlinien** über die **Behandlung der Personalakten** erarbeiten, möchte diese aber mit der Gesetzgebung zum Landesbeamtengesetz abstimmen und versuchen, landeseinheitliche Maßstäbe für alle personalaktenführenden Stellen zu erreichen.

4.1.2 Verfassungsschutz

4.1.2.1 Amtshilfe des Bundesgrenzschutzes für die Geheimdienste

Bundesweit gültige Dienstanweisung animiert den Bundesgrenzschutz, Daten für die Geheimdienste zu erheben.

Zur Problematik der **Amtshilfe,** die seitens des **Bundesgrenzschutzes** gegenüber den **Geheimdiensten** geleistet wird, finden sich bereits Ausführungen im 12. Tätigkeitsbericht (S. 17). Zwischenzeitlich ist das neue schleswig-holsteinische **Verfassungsschutzgesetz** in Kraft getreten, in dem das Gebot der strikten Trennung von Polizei und Verfassungsschutz festgeschrieben ist. Danach darf der Verfassungsschutz Polizeibehörden auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen er selbst nicht befugt ist.

1992 ist nun eine bundesweit gültige **Dienstanweisung des Bundes** in Kraft getreten, die die Durchführung der Amtshilfeersuchen der Verfassungsschutzbehörden, des Militärischen Abschirmdienstes und des Bundesnachrichtendienstes an die Grenzpolizeibehörden regelt, die bei der Wahrnehmung grenzpolizeilicher Aufgaben bekannt werden (Dienstanweisung „Amtshilfe/Grenze"). In dieser Vorschrift heißt es unter anderem: „Mit dem Ersuchen können folgende Informationen angefordert werden, die bei der Wahrnehmung grenzpolizeilicher Aufgaben bekannt werden **oder in Folge des Ersuchens erhoben werden dürfen ...".**

Diese Regelung suggeriert dem zuständigen Grenzschutzbeamten eine Befugnis, die er gerade nicht hat. Daten, die erst in Folge des Ersuchens eines Nachrichtendienstes zu erheben sind, werden nicht „bei der Wahrnehmung grenzpolizeilicher Aufgaben" bekannt. Letztlich soll dadurch der **Bundesgrenzschutz angehalten** werden, über das für die Grenzkontrolle notwendige Maß hinaus **Bürger** zu **beobachten** und die Daten an die Geheimdienste weiterzuübermitteln. Durch ein Ersuchen kann aber für die ersuchte Behörde kein Erlaubnistatbestand zu einer Datenerhebung geschaffen werden, zu der sie aus eigenem Recht keine Befugnis hat. Somit steht diese Verwaltungsvorschrift den gesetzlichen Regelungen zur Amtshilfe und insbesondere des Verfassungsschutzgesetzes entgegen und sollte schnellstmöglich mit der geltenden Gesetzeslage in Einklang gebracht werden.

Der **Innenminister** teilt diese Bedenken nicht. Er verweist darauf, daß die durch den Bundesminister des Innern in Kraft gesetzte Dienstanweisung für die Länder verbindlich sei und betont, daß in Schleswig-Holstein seit 1990 von Amtshilfeersuchen an den Bundesgrenzschutz **kein Gebrauch gemacht** worden ist. Im Ergebnis bleibt es aber unbefriedigend, wenn versucht wird, mit Hilfe von Verwaltungsvorschriften vom Gesetzgeber gezogene Grenzen zu überschreiten. Auch wenn Schleswig-Holstein derzeit keine Amtshilfeersuchen gestellt hat, hätte eine Verwaltungsvorschrift dieses Inhalts u.E. nicht in Kraft gesetzt werden dürfen.

4.1.2.2 Neufassung der NADIS-Richtlinien

Die mehr als 18 Jahre alten „Richtlinien für das nachrichtendienstliche Informationssystem der Verfassungsschutzbehörden" (NADIS-Richtlinien) sollen neu gefaßt werden. Der Entwurf ist stark verbesserungsbedürftig.

Ein Kernstück der Datenverarbeitung der Verfassungsschutzbehörden ist das **Nachrichtendienstliche Informationssystem,** dessen Rechtsgrundlagen sich in den Verfassungsschutzgesetzen des Bundes und der Länder finden. Ergänzend sind in den sogenannten **NADIS-Richtlinien** nähere Einzelheiten festgelegt.

Der Entwurf zur **Neufassung** dieser **Richtlinien** begegnet unter verschiedenen Gesichtspunkten erheblichen daten-

schutzrechtlichen Bedenken. Wir haben gegenüber dem Innenminister folgende Gesichtspunkte problematisiert:

- Hinsichtlich des **Umfangs der Datenspeicherung** gehen die Richtlinien über den maßgeblichen gesetzlichen Rahmen des Bundesverfassungsschutzgesetzes erheblich hinaus. So wollen die Richtlinien zulassen, auch solche Daten in NADIS zu speichern, die **„für die Identifizierung einer Person, einer Organisation oder eines Sachverhalts erforderlich sind".** Im Gesetz sind aber nur solche Datenspeicherungen zugelassen, „die zum **Auffinden von Akten** und der **dazu** notwendigen **Identifizierung von Personen"** benötigt werden. Damit würden die Richtlinien den Verfassungsschutzbehörden einen erheblich umfangreicheren Datenkatalog zubilligen als das Gesetz es zuläßt.
- Nicht ausreichend definiert ist der Begriff **„Erkenntnis-Datum".** Von dem letzten „Erkenntnis-Datum" aus werden die Speicherfristen berechnet. Deshalb darf z. B. nicht eine bloße formale Änderung des Datensatzes dazu führen, daß die Speicherfrist neu zu laufen beginnt.
- Offen bleibt, in welchen begründeten Einzelfällen zu welchem Zweck **Protokolldaten** genutzt werden dürfen. Dies zu klären ist deshalb wichtig, weil die Protokolldaten auch nach Löschung eines Datensatzes noch einige Jahre aufbewahrt bleiben. Wenn ihre Nutzung nicht eng begrenzt wird, kann von einer wirksamen Löschung der Daten beim Verfassungsschutz nur mit Einschränkung gesprochen werden.

Der Innenminister hat in seiner Antwort ausgeführt, daß er aufgrund dieser Bedenken keine zwingende Veranlassung zu einer Änderung der Entwurfsfassung sieht.

4.1.3 Öffentliche Sicherheit

4.1.3.1 Konsequenzen aus der Datenschutzprüfung bei der Polizei

Im Berichtsjahr hat der Innenminister den Entwurf für eine Neufassung der Richtlinien für die Führung kriminalpolizeilich personenbezogener Sammlungen vorgelegt. Der Entwurf bedarf aus unserer Sicht noch der Verbesserung. Es zeichnet sich aber ab, daß ein Großteil der noch verbliebenen Kritikpunkte aus der vor fünf Jahren durchgeführten Querschnittskontrolle ausgeräumt wird.

Zu den im 15. Tätigkeitsbericht (S. 29) aufgeführten noch offenen Punkten ergibt sich nunmehr folgendes Bild:

- **Anlegen und Führen von Kriminalakten**

  Der Entwurf für neue „Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) sowie für die „Regelung für das Anlegen und Führen von Kriminalakten (KA-Regelung)" enthält präzise

Regelungen für die **Anlegung von Kriminalakten.** Über die Einzelheiten dieser Richtlinien werden wir nach Inkrafttreten berichten.

– **Polizeiliche Erkenntnisdatei PED**

Die vom Innenminister angekündigte geänderte Fassung des **PED-Handbuches** befindet sich in Vorbereitung. Sie soll nach Inkrafttreten der KpS-Richtlinien herausgegeben werden. Unserer Forderung, Personendatensätze in der PED zu klassifizieren, will der Innenminister aus **Kostengründen** sowie aus Gründen der **Kompatibilität** mit dem **INPOL-System nicht** nachkommen. Damit bleibt für eine Dienststelle, die nicht selbst die zugehörigen Kriminalakten führt, bei einer PED-Abfrage weiterhin nicht erkennbar, ob eine Person als „Beschuldigter", „Verdächtiger" oder „andere Person" gespeichert ist.

– **Modifizierung des Zugriffs auf Daten über Polizeibeamte**

Zumindest im Ansatz eingeschränkt wurde inzwischen der Zugriff auf in der PED gespeicherte Informationen über Polizeibeamtinnen/-beamte. Demnach lassen entsprechende Datensätze zumindest keinen Rückschluß auf die berufliche Einbindung der Person zu. Die entsprechenden Kriminalakten werden von der kriminalpolizeilichen Behördenleitung gesondert aufbewahrt.

– **Vorgangsverwaltung**
(dazu nachfolgende Nr. 4.1.3.2)

– **Erkennungsdienstliche Maßnahmen**

Unsere Forderung, die Gründe für erkennungsdienstliche Maßnahmen in jedem Einzelfall auf dem jeweiligen Erhebungsbogen zu dokumentieren, hat der Innenminister zum Anlaß genommen, das **Formblatt** für die Anordnung erkennungsdienstlicher Maßnahmen **neu zu gestalten.**

Nunmehr sind dieser Unterlage die Rechtsgrundlage, auf deren Basis die erkennungsdienstliche Behandlung vorgenommen wurde, die Gründe sowie Art und Umfang der getroffenen Maßnahme eindeutig entnehmbar.

– **Datenverarbeitung beim Staatsschutz**

Angekündigt hatte der Innenminister die Neufassung von Regelungen für die Führung der Sammlungen „innere/äußere Sicherheit" im Bereich des polizeilichen Staatsschutzes.

Diese Absicht ist fallengelassen worden. Für den Bereich des polizeilichen Staatsschutzes sollen **keine Sonderregeln** mehr gelten, sondern die allgemeinen KpS-Richtlinien. Dies ist aus datenschutzrechtlicher Sicht zu begrüßen. Die Datenbestände in der Datei „innere Sicherheit" sollen nach Inkrafttreten der neuen KpS-Richtlinien bereinigt werden.

– **Berücksichtigung gerichtlicher Entscheidungen**

In den neuen KpS-Richtlinien werden auch Regelungen enthalten sein, in welcher Form gerichtliche Entscheidungen bei der polizeilichen Datenverarbeitung zu berücksichtigen sind. Von Bedeutung ist insbesondere, daß die Daten bei **Wegfall der Verdachtsgründe** zu löschen sind. Um den Weg der Rückmeldung der Justiz an die Polizei über den Ausgang des Verfahrens zu erleichtern, soll ein **automatisierter Datenaustausch** eingerichtet werden. Nach Mitteilung des Innenministers ist zu erwarten, daß das Verfahren im 2. Quartal 1994 in Betrieb geht.

Positiv hat sich im Berichtsjahr auch die Bestellung eines **internen Datenschutzbeauftragten** beim **Kriminalpolizeiamt** ausgewirkt. Damit steht im Amt ein kompetenter Gesprächspartner in Datenschutzfragen zur Verfügung.

4.1.3.2 Neuregelung der Vorgangsverwaltung bei der Polizei

Nach dem Landesverwaltungsgesetz hat der Innenminister Mittel und Umfang der Vorgangsverwaltung, die von Polizei und Ordnungsbehörden betrieben wird, in einer Verwaltungsvorschrift näher zu bestimmen. Ein Entwurf hierfür ist uns vor Inkrafttreten zur Kenntnis gegeben worden.

Diese Regelung stellt darauf ab, mit Hilfe einer Vorgangsdokumentation nicht nur den Nachweis über einen laufenden Vorgang und seine Bearbeitung zu führen oder das Auffinden und Verknüpfen von Vorgängen zu erleichtern, sondern auch – **zeitlich über die Bearbeitung hinausgehend** – zu dokumentieren, daß und wie die Polizei bzw. Ordnungsbehörde aufgrund eines Sachverhaltes zum Zwecke der Gefahrenabwehr tätig geworden ist.

Jeder Vorgang besteht aus Sachverhalts- und Verwaltungsdaten, wie z.B. Vorgangsnummer, Aktenzeichen, Personalien betroffener Personen, Angaben zu Sachen, Sachbearbeiter, Bearbeitungsstand.

Neben Eintragungen in Tage- bzw. Ordnungsbüchern und konventioneller Aktenhaltung können diese Daten im Rahmen ihrer Zweckbindung und entsprechend den fachlichen Erfordernissen auch über Listen, Karteien und EDV-Verfahren erschließbar sein.

Abgeschlossene Vorgänge sind zu löschen. Vorhandene Vorgangsunterlagen sind zu vernichten oder mit einem Sperrvermerk zu versehen. Als abgeschlossen sieht die Polizei einen Vorgang dann an, wenn eine Bearbeitung nicht mehr stattfindet und auch nicht mehr erwartet wird und die weitere Dokumentation des behördlichen Handelns nicht mehr erforderlich ist.

Darüber hinaus sieht die Verwaltungsvorschrift vor, daß die datenverarbeitenden Stellen der Polizei jeweils für ihren Bereich regeln sollen, welche Daten im Rahmen der Vorgangs-

verwaltung verarbeitet werden dürfen und welchen Speicherfristen Verwaltungsdaten und Vorgangsdaten unterliegen. Es ist nicht zu verkennen, daß mit solchen **generalklauselartigen Regelungen** vermeintlich ein beträchtlicher Spielraum für die Gestaltung der Vorgangsverwaltung eröffnet wird.

Gegenüber dem Innenminister haben wir gegen die Verwaltungsvorschrift nur deshalb keine Bedenken erhoben, da die Polizeidienststellen durch die vorrangigen Bestimmungen im Landesverwaltungsgesetz über Erhebung und Speicherung personenbezogener Daten und den Grundsatz der Zweckbindung gebunden sind. Bei künftigen Kontrollen wird darauf zu achten sein, daß die Vorgangsverwaltung nicht für andere polizeiliche Zwecke verwendet wird.

4.1.3.3 COMPAS

Der Test des Pilotprojektes COMPAS hat bei der Polizei begonnen. COMPAS wird die Datenverarbeitung bei den Revieren „vor Ort" automatisieren. Die datenschutzrechtlichen Risiken müssen durch begleitende Maßnahmen minimiert werden.

Der Innenminister hat im vierten Polizeirevier in Kiel im Herbst 1993 das Pilotprojekt **COMPAS** (Computerunterstütztes polizeiliches Arbeitsplatzsystem) zum Test freigegeben. Dieser Praxistest wird nach und nach auf insgesamt fünf Polizeidienststellen in Kiel und Plön ausgedehnt. Der Einsatz moderner Informations- und Kommunikationstechnik soll das komplizierte Formularwesen der Polizei erheblich vereinfachen. Die Mitarbeiter auf dem Revier haben jetzt folgende Möglichkeiten:

- Erledigung der anfallenden schriftlichen Arbeiten mit einer modernen **graphischen Textverarbeitung**
- Nutzung von auf dem Rechner abgelegten **Vordrucken** (z.B. Strafanzeige, Vorladung, Vernehmung von Beschuldigten und Zeugen)
- Ablage und Speicherung von Vorgängen in der **zentralen Ablage** des Reviers mit der Möglichkeit der umfassenden Recherche
- Unterstützung durch eine **elektronische Wiedervorlagemappe,** z.B. für Vernehmungen
- Nutzung **sonstiger Hilfsmittel,** wie z.B. Taschenrechner, Uhr etc. auf dem Bildschirm
- Versendung und Empfang von **Telefaxen** am Arbeitsplatz sowie Austausch von Schriftstücken und **Nachrichten** innerhalb des Reviers

Das dem Projekt zugrundeliegende **Sicherheitskonzept** und die **vorläufige Dienstanweisung** wurde uns vorab übersandt. Anläßlich einer praktischen Demonstration hatten wir Gelegenheit, die eingesetzte Hard- und Software im Praxisbetrieb zu begutachten. Es gibt noch eine Reihe **offe-**

ner Fragen, die zu diskutieren sind. So haben wir den Innenminister darauf hingewiesen, daß auch für das Pilotprojekt die gesetzlichen Bestimmungen des Polizeirechts und des Datenschutzrechts zu beachten sind, daß Anweisungen für die Paßwortvergabe notwendig sind und daß die Protokollierung von Datenänderungen zu empfehlen ist. Außerdem haben wir auf die Notwendigkeit von Dateianmeldungen hingewiesen und ergänzende Fragen zur Einhaltung der Zweckbindung gestellt. Wir werden das Pilotprojekt weiter beratend und kontrollierend begleiten.

4.1.3.4 Auskunftsrecht und Akteneinsicht Betroffener gegenüber der Polizei

Das Landesverwaltungsgesetz hat den Anspruch auf Auskunft und Akteneinsicht Betroffener zwar gesetzlich festgeschrieben, in der Praxis bestehen aber gelegentlich Umsetzungsschwierigkeiten.

Ein Petent hatte mehrfach versucht, Auskunft über die bei der Landespolizei Schleswig-Holstein zu seiner Person gespeicherten Daten zu erlangen. Zwar war ihm schriftlich mitgeteilt worden, daß über ihn in Kriminalpolizeilichen Sammlungen personenbezogene Informationen gespeichert seien, die aus den ihm bekannten abgeschlossenen und noch anhängigen strafrechtlichen Ermittlungsverfahren stammten. Unter Hinweis auf ein noch anhängiges Ermittlungsverfahren wurden jedoch **nähere Angaben verweigert.** Einer solchen Argumentation vermochte der Petent zu Recht nicht zu folgen und wandte sich deshalb an uns.

Bei unseren **Nachprüfungen** stellten wir fest, daß eine umfassende Auskunftserteilung deshalb nicht erfolgte, weil nach einem **Erlaß des Innenministers** solange keine Auskunft über gespeicherte Daten gegeben werden sollte, wie noch Verfahren zu der betreffenden Person unerledigt sind. Dies stand mit der Gesetzeslage nicht in Einklang. Der Erlaß ist zwischenzeitlich außer Kraft gesetzt. Der Petent erhielt daraufhin detaillierte Auskunft. Zugleich konnte ihm mitgeteilt werden, daß die Polizei sein Ersuchen zum Anlaß genommen habe, die zu seiner Person gespeicherten Daten auch hinsichtlich der Speicherungsvoraussetzungen zu überprüfen.

Daraufhin machte auch der Petent selbst nähere Angaben zu den einzelnen Verfahren, die zur **Berichtigung** der polizeilichen Unterlagen beitrugen. Mehrere **Sachverhalte** waren sogar zu **löschen.** Gegen die Speicherung der verbliebenen Informationen bis zum Ende der gesetzlich festgelegten Speicherfrist waren keine Einwendungen zu erheben.

4.1.3.5 Lauschangriff gegen die Polizei kein Problem

Während vielerorts über verbesserte Methoden der Verbrechensbekämpfung nachgedacht wird, können Unbefugte besser denn je ungeniert den Funkverkehr abhören. Da auf diesem Wege hochsensible Daten bekanntwerden können, besteht dringender Handlungsbedarf.

Die rasante Entwicklung der Mikroelektronik hat auch bei staatlichen Vorsorgeeinrichtungen zu einem beispiellosen Boom drahtloser Kommunikation geführt. Stolz führen uns **Sicherheitsbehörden** und **Rettungsdienste** hochmoderne, rechnerunterstützte Einsatzleitstellen vor, mit denen über flächendeckende Funkverkehrsnetze ständig Kontakt zu den mobilen Einheiten gehalten wird.

Im Funkverkehr dieser Stellen wird dabei eine Fülle höchst **sensibler personenbezogener Daten** übertragen. Für Polizei und Rettungspersonal ist die Beschäftigung mit Menschen und Personalien alltägliche Praxis. Mit Hilfe des Funkgerätes wird überprüft und berichtet, z.B. wer Halter eines Fahrzeugs ist, ob jemand gesucht wird, wo ein Betroffener wohnt und vieles andere mehr. So wandern zwangsläufig brisante Informationen zumindest in Auszügen durch den Äther. Vom Einsatzort wird gemeldet, was mit Betroffenen geschehen ist (z.B. Festnahme, Blutprobe, Anzeige, Einlieferung in das Krankenhaus mit Diagnose), welcher Ehestreit zu schlichten war, wer wen geschlagen hat usw.

Diese Funksprüche können jedoch prinzipiell von jedermann, auch von **Unbefugten,** empfangen werden. Während dazu früher noch spezielle technische Kenntnisse notwendig waren, existiert heute ein reichhaltiges Angebot preisgünstiger Spezialempfänger, mit denen sich ganze Frequenzbereiche lückenlos und vollautomatisch überwachen lassen. Angesichts tausender verkaufter Geräte gehen Sicherheitsexperten schon lange davon aus, daß – trotz nach wie vor bestehenden Verbots – nicht nur die Unterwelt den Funkverkehr der Sicherheitsdienste abhört, sondern auch eine unüberschaubar große Anzahl Neugieriger auf allen Bändern und bei allen Diensten ständig zuhört. **„Reality"-Funkverkehr** frei Haus gewissermaßen. Jüngstes Beispiel ist die erzwungene Vorverlegung einer Rauschgiftrazzia, weil sich bereits vor dem geplanten Termin Journalisten mit Fotoapparaten „bewaffnet" vor dem betreffenden Gelände postiert hatten.

Trotz dieser Situation wird auch heute noch fast der gesamte **Sprechfunkverkehr offen** abgewickelt. In Schleswig-Holstein, aber auch den meisten anderen Bundesländern, wurden Verschlüsselungsgeräte aus Kostengründen nur für ganz wenige Fälle beschafft. Für diese Entscheidung waren in erster Linie jedoch einsatztaktische Gründe ausschlaggebend und nicht der Datenschutz.

Zwar wird seit vielen Jahren bundesweit über **Verschlüsselungsverfahren** diskutiert. Zu konkreten Maßnahmen hat dies jedoch nicht geführt. Bis heute haben sich die Bundesländer

nicht auf ein gemeinsames Verschlüsselungssystem einigen können. Deshalb ist kein Land – auch Schleswig-Holstein nicht – bereit, auf eigene Faust in großem Umfang Verschlüsselungsgeräte anzuschaffen.

Bereits im 15. Tätigkeitsbericht (S. 94) hatten wir über dieses Problem berichtet. Geschehen ist seitdem nicht viel. Angesichts der deutlich **verschlechterten zugespitzten Situation** ist die zwischen den Bundesländern bestehende Uneinigkeit nicht mehr länger hinzunehmen. Die Innenminister sind aufgefordert, die erst kürzlich wieder aufgenommenen Beratungen zu dieser Frage energisch mit dem Ziel eines baldigen erfolgreichen Abschlusses voranzutreiben.

4.1.4 Bau- und Wohnungswesen

4.1.4.1 Entwurf für neue Landesbauordnung berücksichtigt auch Datenschutz

Der Änderungsentwurf zur Landesbauordnung begrenzt und konkretisiert die regelmäßigen Übermittlungen personenbezogener Daten aus den Bauanträgen an Dritte „von Amts wegen" und macht sonstige Datenübermittlungen von der Einwilligung der Betroffenen abhängig.

Novellierungsentwürfe zur Landesbauordnung gab es seit 1988. Zunächst war vorgesehen, die Übermittlung personenbezogener Daten „an Behörden, sonstige öffentliche Stellen und andere Stellen" zuzulassen, wenn die Daten zur rechtmäßigen Aufgabenerfüllung der Bauaufsichtsbehörde oder des Empfängers erforderlich waren. Im Baugenehmigungsverfahren zu beteiligende Stellen sollten die gesamten Bauakten zugeleitet werden dürfen.

Diese Formulierung hätte nur die Generalklausel des Landesdatenschutzgesetzes übernommen, den Datenschutz für das Baurecht aber nicht **bereichsspezifisch** ausgestaltet. Überdies bestanden erhebliche Zweifel daran, ob wirklich vollständige Bauakten dritten Stellen zugeleitet werden müssen.

Unsere **Verbesserungsvorschläge** führten zur Änderung der Datenverarbeitungsbestimmungen. „Von Amts wegen" soll die Datenübermittlung an öffentliche Stellen nur zulässig sein, soweit sie erforderlich ist, um nach anderen öffentlich-rechtlichen Vorschriften notwendige Einwilligungen einzuholen, die Vereinbarkeit mit öffentlich-rechtlichen Vorschriften zu prüfen oder das Liegenschaftskataster fortzuführen. An **private Stellen** dürfen entsprechende Daten nur übermittelt werden, soweit die Bauaufsichtsbehörde sich der besonderen Sachkunde der Empfänger bedienen und sie zu diesem Zweck über den Sachverhalt unterrichten muß. Das wird überwiegend bei Prüfaufträgen an Sachverständige der Fall sein.

In allen übrigen Fällen (z.B. für die Unterrichtung von Versorgungsunternehmen) bedarf eine Datenübermittlung der **Einwilligung** der Betroffenen, soweit nicht anderweitig gesetzli-

che Ermächtigungen bestehen. Damit sind die Datenverarbeitungsbestimmungen im Entwurf der neuen Landesbauordnung aus unserer Sicht akzeptabel.

4.1.4.2 Übermittlung vollständiger Kaufverträge zur Ausübung des gemeindlichen Vorkaufsrechts?

Die Gemeinden müssen die vollständigen Grundstückskaufverträge nur dann kennen, wenn sie ihr Vorkaufsrecht ausüben wollen. Sind sie an dem verkauften Grundstück aber nicht interessiert, so brauchen sie die Details der notariellen Verträge nicht zu erfahren.

Nach dem Bundesbaugesetz steht Gemeinden unter bestimmten Voraussetzungen ein Vorkaufsrecht an Grundstücken zu, die im Gemeindegebiet verkauft werden. Jeder Verkäufer hat der Gemeinde den Inhalt des Kaufvertrages unverzüglich mitzuteilen, um ihr die **Prüfung** und ggf. **Ausübung des Vorkaufsrechts** zu ermöglichen. Dies geschieht in der Regel durch den beurkundenden Notar. Die Gemeinden wurden bisher auch dann über vertragliche Einzelheiten unterrichtet, wenn ein Vorkaufsrecht überhaupt nicht bestand oder sie am Erwerb eines Grundstücks im Rahmen des Vorkaufsrechts gar nicht interessiert waren. Sie erhielten damit personenbezogene Daten, die für ihre Aufgabenerfüllung nicht erforderlich waren.

Wir haben für die Zukunft ein **gestuftes Verfahren** vorgeschlagen. Es genügt für die Vorprüfung der Gemeinde die Information, daß ein konkret bezeichnetes Grundstück verkauft worden ist. Kommt ein Vorkaufsrecht gar nicht in Betracht, so kann die Gemeinde schon aufgrund der Grundstücksbezeichnung die erforderlichen Erklärungen nach dem Baugesetzbuch abgeben, ohne daß sie weiter gehende Detailinformationen zur Kenntnis nehmen muß. Dieser Fall liegt bei den meisten Grundstückskaufverträgen vor.

Erst wenn die Gemeinde der Ausübung eines bestehenden Vorkaufsrechts nähertreten will, muß sie Kenntnis von dem **gesamten Kaufvertrag** erhalten, in den sie eintreten will. Die gesetzlichen Fristen für die Ausübung des Rechts beginnen erst von diesem Zeitpunkt an zu laufen. Wir sehen hierin eine **datenschutzrechtliche Verbesserung,** die nach dem Verhältnismäßigkeitsprinzip auch geboten ist. Darüber hinaus liegt darin u.E. sogar eine **Verfahrenserleichterung** für die beteiligten Stellen und damit ein Beitrag zur Entbürokratisierung.

Der Bundesminister für Raumordnung, Bauwesen und Städtebau erachtet ein solches „gestuftes Mitteilungsverfahren" als im Einklang mit den Rechtsvorschriften. Auch der **Innenminister** betrachtet unseren Vorschlag als unterstützenswert. Er beabsichtigt, den Gemeinden vorzuschlagen, ein solches zweistufiges Verfahren zu akzeptieren. Die kommunalen Landesverbände haben keine grundsätzlichen Einwände dagegen erhoben. Wir werden unsererseits an die Notarkammer heran-

treten und anregen, es für die Praxis in den Notariaten zu empfehlen.

4.1.5 Umweltschutz

4.1.5.1 Entwurf eines Landesumweltinformationsgesetzes

Der Entwurf für ein Landesumweltinformationsgesetz sieht weitreichende Informationszugangsrechte vor. Vor seiner Verabschiedung muß die Abgrenzung der Gesetzgebungskompetenz des Landes zu der des Bundes geklärt werden.

Aufgrund einer Richtlinie der Europäischen Union hat seit 1992 jedermann ein Recht auf Einsicht in umweltrelevante Unterlagen der Verwaltung. Ein vom SSW und der Fraktion der F.D.P. eingebrachter **Gesetzentwurf** über den freien Zugang zu Informationen über die Umwelt **für das Land Schleswig-Holstein** sieht präzisierende Regelungen der Einzelheiten vor.

Der Entwurf eröffnet in Ausführung der EU-Richtlinie für jedermann den **freien Zugang zu Umweltinformationen,** die bei Behörden im Land Schleswig-Holstein gespeichert sind. Für den Schutz von Betriebs- und Geschäftsgeheimnissen sowie personenbezogener Daten sieht der Entwurf Ausnahmen vor.

Wir haben uns in unserer **Stellungnahme grundsätzlich positiv** zu diesem Gesetzentwurf geäußert, da nach unserer Auffassung auch der Zugang zu Informationen ein Aspekt des Rechts auf informationelle Selbstbestimmung ist. Um sicherzustellen, daß einerseits der **Schutz personenbezogener Daten** nicht unangemessen hinter dem Informationsinteresse Dritter zurücksteht, andererseits aber zu verhindern, daß berechtigte Informationsbegehren mit dem Hinweis auf Datenschutz abgelehnt werden, haben wir **ergänzende Formulierungsvorschläge** unterbreitet.

Mittlerweile liegt auch ein **Kabinettsentwurf des Bundes** zur Ausführung der EU-Richtlinie vor. Die Frage, wie im Bereich der Informationszugangsrechte die **Gesetzgebungskompetenz** zwischen Bund und Ländern verteilt ist, ist umstritten. Derzeit wird über entsprechende **Öffnungsklauseln** im Bundesumweltinformationsgesetz diskutiert, damit den **Ländern** die Möglichkeit gelassen wird, **eigene Vorstellungen** über den Zugang zu Umweltinformationen zu verwirklichen. Es ist zu wünschen, daß der Gestaltungsspielraum der Länder, ähnlich wie im Verwaltungsverfahrens- oder im Datenschutzrecht, nicht unnötig eingeengt wird.

4.1.5.2 Abfallgebührenerhebung durch Einzugsermächtigung

Die Gebührenerhebung im Lastschriftverfahren mit der Bank bedarf auch aus datenschutzrechtlichen Gründen der schriftlichen Einwilligung des Zahlungspflichtigen.

Welche Bedeutung es hat, daß das Landesdatenschutzgesetz für die Einwilligung Betroffener in die Verarbeitung ihrer personenbezogenen Daten die Schriftform vorsieht, erfuhr ein schleswig-holsteinischer Zweckverband. Ein Bürger hatte sich an uns gewandt und darüber Beschwerde geführt, daß der Zweckverband die von ihm zu zahlenden Abfallgebühren ohne seine Einwilligung im **Lastschriftverfahren** von seinem Bankkonto abrief.

Die Nachforschungen ergaben, daß **Banken** schon dann Überweisungen vornehmen, wenn der Gläubiger die Kontonummer des Betroffenen mitteilt und erklärt, er verfüge über eine Einwilligung des Schuldners zum Lastschrifteinzugsverfahren. Zwar lasse die Bank nicht jeden Gläubiger für dieses Verfahren zu, habe aber bei öffentlich-rechtlichen Körperschaften keine Bedenken. Der Kunde müsse sich mit dem Gläubiger auseinandersetzen und sei dadurch gesichert, daß er ein Widerspruchs- und Rückrufsrecht innerhalb von sechs Wochen hat. Dieses Verfahren sei Bestandteil der allgemeinen Geschäftsbedingungen und damit Gegenstand des Bankvertrages mit dem Kunden.

Der Zweckverband teilte auf Anfrage mit, der Mitarbeiter, der den konkreten Fall bearbeitet habe, sei mittlerweise aus dem Dienst des Verbandes ausgeschieden und könne nicht mehr befragt werden. Eine **schriftliche Einwilligungserklärung** des Betroffenen liege allerdings nicht vor. Man müsse aber aufgrund der vorhandenen Unterlagen und der bestehenden internen Verfahrensregeln davon ausgehen, daß eine mündliche bzw. telefonische Einwilligung vorgelegen habe.

Wenn im vorliegenden Fall auch manches dafür spricht, daß der Betroffene in die Abbuchungen und damit in die Verarbeitung seiner personenbezogenen Daten (Datenübermittlung) eingewilligt hat, so kann endgültige Klarheit für alle Beteiligten erst durch eine schriftliche Einwilligung erreicht werden. Der Zweckverband hat mitgeteilt, daß er dies **künftig** im Lastschrifteinzugsverfahren entsprechend **beachten** wird.

Die Regelung der Bank in ihren allgemeinen Geschäftsbedingungen, die einen Verzicht auf Vorlage einer schriftlichen Einwilligung in das Lastschriftverfahren zuläßt, wirkt nur zwischen Kunden und Bank und gehört überdies einem anderen Rechtskreis, nämlich dem Zivilrecht, an. Sie kann öffentlich-rechtliche Vorschriften, die das Verhältnis zwischen Zweckverband und Betroffenem regeln, nicht überspielen.

4.1.5.3 Der „Gelbe Wertstoffsack" als Datenspeicher?

Die Sammlung von Verpackungsmüll im transparenten „gelben Sack" läßt zwar Lebensgewohnheiten erkennen, jedoch handelt es sich nicht um eine verbotene Verarbeitung personenbezogener Daten.

Wie sensibel Bürgerinnen und Bürger gelegentlich auf Sachverhalte reagieren, hinter denen sie datenschutzrechtliche Relevanz vermuten, zeigt eine Eingabe in besonderem Maße. Ein Petent wies darauf hin, daß bei Verwendung des „gelben Wertstoffsacks" für die Entsorgung von Verpackungsmüll im Rahmen des „dualen Systems" durch die **transparenten Säcke** hindurch ihr Inhalt erkennbar sei. Aus ihm könne auf **Konsumgewohnheiten** der betreffenden Haushalte und unter Umständen – bei Bevorzugung gewisser Waren – sogar auf ihre **Einkommens- oder Vermögensverhältnisse** geschlossen werden. Diese Möglichkeit habe bei der Benutzung der üblichen Abfalltonnen bisher nicht bestanden. Er bat um datenschutzrechtliche Stellungnahme.

Bei allem Verständnis für seine Überlegungen mußte dem Petenten doch mitgeteilt werden, daß die Benutzung des „gelben Sacks" **datenschutzrechtlich ohne Bedeutung ist.** In der Mehrzahl der Fälle fehlt es schon an einem Personenbezug, da es für Außenstehende kaum möglich ist, das zu entsorgende Verpackungsmaterial einer natürlichen Person zuzuordnen. Mangels einer konkreten „Phase" der Datenverarbeitung (Erhebung, Speicherung, Übermittlung usw.) ist auch kein Ausgangspunkt für weitere datenschutzrechtlich relevante Vorgänge ersichtlich. Schließlich bleibt es den Benutzern unbenommen, „Peinlichkeiten" bei der Müllabfuhr dadurch zu vermeiden, daß sie für bestimmte Abfälle **undurchsichtige Zwischenverpackungen** verwenden.

4.2 Kommunalbereich

4.2.1 Probleme einer Stadtverwaltung bei der Umsetzung des neuen Datenschutzrechts

Als Rechtsgrundlagen für die Datenverarbeitung kommen auch kommunale Satzungen in Betracht. Der Beachtung der datenschutzrechtlichen Transparenzgebote kommt dabei besondere Bedeutung zu.

Anfragen und Eingaben haben gezeigt, daß die neuen Bestimmungen des LDSG im kommunalen Bereich noch nicht ausreichend umgesetzt worden sind. Zur aktuellen Standortbestimmung haben wir deshalb bei einer Stadtverwaltung eine Prüfung durchgeführt, die ausschließlich die Verarbeitung personenbezogener Daten zur Erfüllung von Selbstverwaltungsaufgaben der Stadt zum Gegenstand hatte. Dabei standen zwei Problemkreise im Vordergrund:

– **Datenverarbeitungsregelungen im kommunalen Satzungsrecht**

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn entweder die oder der Betroffene eingewilligt hat oder eine Rechtsvorschrift sie erlaubt. Neben Bundes- und Landesgesetzen können auch **Satzungen der Kommunen** Befugnisse zur Datenverarbeitung enthalten.

In ihnen sind allerdings die **Zweckbindungsvorschriften des LDSG** zu berücksichtigen. Die Weiterverarbeitung personenbezogener Daten ist nämlich grundsätzlich nur für den Zweck zulässig, für den sie erhoben worden sind. Werden Daten, die zur Aufgabenerfüllung benötigt werden, nicht bei Betroffenen erhoben, sondern bereits vorhandenen Datenbeständen entnommen, liegt darin durchweg eine zweckändernde Nutzung personenbezogener Daten, zu der die Verwaltung durch eine **ausdrückliche Befugnis** in einer Rechtsvorschrift ermächtigt werden muß.

Satzungen kommen **als Eingriffsbefugnis** in Betracht, wenn festgelegt ist, welche Daten von der Verwaltung aus welchen Datenbeständen für die Erfüllung bestimmter Aufgaben verarbeitet werden dürfen. Der notwendige Inhalt einer solchen Regelung ist im einzelnen von dem konkreten Gegenstand des Verwaltungsverfahrens abhängig. Textvorschläge, wie sie inzwischen vom Innenminister herausgegeben worden sind, können deshalb nur eine Orientierungshilfe sein, die an die individuellen Bedürfnisse der einzelnen Kommune angepaßt werden müssen.

Die kommunalen Entscheidungsgremien haben durch eine Satzung der Verwaltung nicht nur die Erfüllung einer bestimmten Aufgabe zu übertragen, sondern auch zu bestimmen, in welchem Umfang zur Erfüllung dieser Aufgabe personenbezogene Daten verarbeitet werden dürfen.

Dabei können sich Beschränkungen aus **höherrangigem Recht** ergeben. So kann z. B. aufgrund einer kommunalen Satzung nicht das in der Abgabenordnung enthaltene Steuergeheimnis abgeändert werden. Außerdem muß der Grundsatz beachtet werden, daß nach dem Datenschutzrecht personenbezogene Daten nur erhoben werden dürfen, wenn ihre Kenntnis zur **rechtmäßigen** Erfüllung der Aufgaben der erhebenden Stelle **erforderlich** ist.

– **Das Aufklärungsgebot im Rahmen der Datenerhebung**

Eine zentrale Feststellung im Volkszählungsurteil des **Bundesverfassungsgerichts** besagt, daß der Bürger einen Anspruch darauf hat, zu wissen, wer welche Daten bei welcher Gelegenheit über ihn verarbeitet. Deshalb ist im Landesdatenschutzgesetz festgelegt worden, daß Betroffene bei der Erhebung ihrer Daten in geeigneter Weise über den Zweck der Datenerhebung, die vorgesehene Art der Weiterverarbeitung und bei beabsichtigten Übermittlungen auch über

den Empfängerkreis aufzuklären und auf die Rechtsgrundlage der Erhebung bzw. die Freiwilligkeit hinzuweisen sind.

Werden Daten ausnahmsweise ohne Kenntnis der **Betroffenen** bei Dritten erhoben, so sind sie in gleicher Weise zu **unterrichten,** sobald dies ohne Gefährdung der Aufgabenerfüllung der Behörde möglich ist. Zusätzlich ist bei der Speicherung der Daten sicherzustellen, daß ihre Herkunft nachvollziehbar ist. Diese Verfahrensregelungen verbessern nicht nur den Kenntnisstand des Betroffenen über die Verarbeitung seiner Daten, sie versetzen ihn auch in die Lage, die Rechtmäßigkeit des Verwaltungshandelns selbst beurteilen zu können. Nur wenn dem Bürger bekannt ist, in welchem Umfang tatsächlich seine Daten verarbeitet werden, kann er prüfen, ob dies im Einklang mit dem geltenden Recht erfolgt.

Aus diesem Grund ist auch die Einhaltung der Verfahrensvorschriften nicht nur eine bloße Obliegenheit der datenverarbeitenden Stelle, sondern eine unmittelbar verfassungsrechtlich begründete **Zulässigkeitsvoraussetzung** für die Verarbeitung personenbezogener Daten. Das Bundesverfassungsgericht hat dazu ausdrücklich klargestellt: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden."

Wird beim Erhebungsvorgang das Aufklärungsgebot nicht beachtet bzw. die gebotene Aufklärung im Falle der Datenerhebung ohne Kenntnis der Betroffenen nicht alsbald nachgeholt, stellt dies einen unzulässigen Eingriff in die vom Bundesverfassungsgericht konkretisierte Grundrechtsposition der Betroffenen dar.

Eine andere Frage ist es, bis zu welchem Zeitpunkt die Aufklärung bei einer Datenerhebung ohne Kenntnis des Betroffenen erfolgen muß. Hier mag es angehen, daß trotz der strengen Gesetzesformulierung („**sobald** die rechtmäßige Erfüllung der Aufgaben dadurch nicht gefährdet wird") im Rahmen des Verhältnismäßigkeitsprinzips **Gesichtspunkte der Praktikabilität** berücksichtigt werden können. Erfolgt beispielsweise die Verarbeitung der Daten in einem Abgabenbescheid in unmittelbarem Zusammenhang mit der Erhebung, so dürfte die Aufklärung zusammen mit dem Erlaß des Bescheides zulässig sein.

Die Ergebnisse der Prüfung

Zum Zeitpunkt der Prüfung waren im kommunalen Satzungsrecht der Stadt noch **keine Datenverarbeitungsregelungen** enthalten. Die Notwendigkeit entsprechender Regelungen bestand vor allem für folgende Bereiche:

- Führung eines Grundstückseigentümerverzeichnisses
- Erhebung der Zweitwohnungssteuer
- Erhebung von Straßenausbaubeiträgen
- Durchführung der Baumschutzsatzung
- Erteilung von Sondernutzungserlaubnissen an öffentlichen Straßen
- Erhebung der Kurabgabe
- Erhebung der Fremdenverkehrsabgabe

Es wurden hauptsächlich Daten aus den zur Prüfung des Vorkaufsrechts übersandten Kaufverträgen nach dem Baugesetzbuch sowie aus Baugenehmigungsunterlagen in zweckändernder Weise ohne Kenntnis der Betroffenen genutzt. Auf der Grundlage der Prüfungsergebnisse konnten die **notwendigen Ergänzungen des Satzungsrechts** noch vor Ablauf der Ende 1993 auslaufenden zweijährigen Übergangsfrist verabschiedet werden. Anderenfalls wäre ein Zugriff auf die genannten Datenbestände zu Selbstverwaltungszwecken unzulässig gewesen.

Ob über die festgestellten Datenverarbeitungsvorgänge hinaus weitere Datenbestände unter Umständen in zweckändernder Weise genutzt worden sind, konnte nicht abschließend beurteilt werden, da die Herkunft der Daten in den Unterlagen häufig nicht dokumentiert war. Dies zeigt, daß die Beachtung der im Datenschutzrecht festgeschriebenen **Dokumentationspflicht** eine wichtige Voraussetzung zur Erlangung prüfungsfähiger Unterlagen darstellt.

Auch die **Aufklärungspflicht** im Rahmen der Datenerhebung ist bis zu unserer Prüfung **generell nicht beachtet** worden. In Zusammenarbeit mit der Stadt konnten aber praktikable Lösungen erarbeitet werden, die eine Umsetzung des Transparenzgebotes für die Zukunft gewährleisten sollen.

In ihrer abschließenden Stellungnahme hat die Stadt inzwischen angekündigt, nunmehr nach den datenschutzrechtlichen Anforderungen zu verfahren.

4.2.2 Die Kommunalwahl und ihre Vorbereitung

Meldedaten, die einer Auskunftssperre unterliegen, kommen bei der Kommunalwahl nicht mehr ins Wählerverzeichnis. Viele Bürger fordern darüber hinaus ein Widerspruchsrecht gegen die Weitergabe ihrer Daten an politische Parteien.

Schon vor einer Reihe von Jahren haben wir darauf hingewiesen, daß bei der öffentlichen Auslegung von Wählerverzeichnissen entsprechend den verschiedenen Wahlordnungen, auch die Daten solcher Bürgerinnen und Bürger offenbart werden, für die im Melderegister zum Schutz ihres Lebens, ihrer Gesundheit, ihrer persönlichen Freiheit oder ähnlicher Rechtsgü-

ter **Auskunftssperren** vermerkt sind. Der Innenminister lehnte bisher Änderungen des Verfahrens unter Hinweis auf die Rechtslage ab. Außerdem war er der Meinung, daß von den Wählerlisten nur eine geringe Gefahr für den betroffenen Wahlberechtigten ausgehe.

Anläßlich der Beratung der **Gemeinde- und Kreiswahlordnung** haben wir das Problem erneut aufgegriffen. Die öffentliche Auslegung gesperrter Meldedaten und die fehlende Dokumentation solcher Fälle, in denen durch Dritte Auszüge aus den Wählerlisten angefertigt werden, wurde von uns als unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht bezeichnet, endlich mit Erfolg.

Die **neue Kommunalwahlordnung** untersagt die öffentliche Auslegung von Daten Wahlberechtigter, die nach dem Landesmeldegesetz gesperrt sind. Damit ist das Problem zumindest für die anstehenden Kommunalwahlen gelöst. Es ist allerdings wichtig, auch für die anderen Wahlen einen gleichen Datenschutzstandard zu erreichen. Der Innenminister wurde daher aufgefordert, entsprechende Regelungen in den Wahlrechtsbestimmungen des Landes und des Bundes und für die europäischen Wahlen zu initiieren.

In Wahlkampfzeiten versuchen Bürgerinnen und Bürger in wachsendem Maße, sich der **Wahlpropaganda extremer Parteien** zu entziehen, deren Auftreten sie als unangemessen, belästigend oder sogar beleidigend ansehen. Das Landesmeldegesetz läßt zu, Parteien und Wählergruppen in den sechs Monaten vor der Wahl Melderegisterauskünfte über Wahlberechtigte, geordnet nach Altersgruppen, zu erteilen. Allerdings kann die **Meldebehörde nach eigenem Ermessen** entscheiden, ob solche Listen überhaupt herausgegeben werden oder nicht. Die Entscheidung kann aus Gründen der Gleichbehandlung jedoch nur für alle Parteien und Gruppen gleichmäßig getroffen werden. Das Landesmeldegesetz läßt überdies gegen die Entscheidung keinen Widerspruch betroffener Bürgerinnen und Bürger zu. Ein Unterlassungsanspruch gegen solche Auskünfte wird bei der bestehenden Rechtslage von der Rechtsprechung abgelehnt, es sei denn, im Melderegister ist eine Auskunftssperre eingetragen.

Diese **Rechtslage** empfinden wir ebenso wie viele Bürgerinnen und Bürger als **unbefriedigend.** Es sollte geprüft werden, ob nicht durch eine Änderung der melderechtlichen Bestimmungen dem einzelnen Wahlberechtigten, ähnlich wie bei der Weitergabe seiner Daten für die Erstellung von Adreßbüchern, ein **Widerspruchs- oder Abwehrrecht** eingeräumt werden sollte. Dies entspräche dem Bild des mündigen Wahlbürgers und dem Recht auf informationelle Selbstbestimmung gleichermaßen.

4.2.3 Direkter Zugriff des Rechnungsprüfungsamtes auf Verwaltungsdaten?

Ein direkter Zugriff des Rechnungsprüfungsamtes auf die Daten der Fachabteilungen ist nicht grundsätzlich ausgeschlossen. Er muß aber durch geeignete Vorkehrungen auf das notwendige Maß begrenzt werden.

Eine Kreisverwaltung wandte sich mit der Frage an uns, ob das Rechnungsprüfungsamt über seine EDV-Terminals zu Prüfungszwecken Daten aus anderen Abteilungen der Kreisverwaltung direkt abrufen dürfe.

In unserer Stellungnahme haben wir darauf hingewiesen, daß

- die Rechnungsprüfungsämter auf konventionellem Weg wie im Online-Verfahren nur insoweit **Zugriffsrechte** auf die Daten der Fachabteilungen haben dürfen, wie sie diese für Zwecke der Kontrolle **benötigen,**

- die grundsätzliche Zulässigkeit der Nutzung von gespeicherten Daten zu Prüfungszwecken durch Rechnungsprüfungsämter nicht automatisch zu einer **umfassenden** und **unkontrollierten Zugriffsberechtigung** führen darf,

- von ihrer Aufgabenstellung her den Rechnungsprüfungsämtern nur **Lese-, keine Schreibrechte** in den zu prüfenden Datenbeständen eingeräumt werden dürfen, daß es den Mitarbeitern des Rechnungsprüfungsamtes keinesfalls möglich sein darf, auf die **Betriebssystemebene** der EDV-Systeme zu gelangen,

- durch ein innerhalb der Rechnungsprüfungsämter einzusetzendes **Sicherungsverfahren** zudem sichergestellt werden muß, daß die Mitarbeiter tatsächlich nur auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können,

- die in den Rechnungsprüfungsämtern eingesetzten **Datenverarbeitungsgeräte** und **Programme** gegenüber der sonstigen Hard- und Software der Behörde keine Sonderstellung einnehmen, daß sie also entsprechend den Regelungen des LDSG **gesichert, registriert** und **dokumentiert** werden müssen,

- schließlich sichergestellt werden muß, daß die durch das Rechnungsprüfungsamt ggf. kopierten Daten nach Abschluß der Prüfung unverzüglich **gelöscht** werden.

4.3 Justizverwaltung

4.3.1 Noch ein Jubiläum: 10 Jahre Übergangsbonus für GAST

Nach wie vor fehlt der staatsanwaltschaftlichen Datei GAST eine ausreichende Rechtsgrundlage. Jüngste Gesetzentwürfe aus dem Bereich der Justizministerkonferenz waren datenschutzrechtlich inakzeptabel. Jetzt ist das Land Schleswig-Holstein gefordert.

Immer noch wird die „Geschäftsstellenautomation der Staatsanwaltschaften" (GAST) **ohne ausreichende Rechtsgrundlage** betrieben. In den Dateien der Staatsanwaltschaften werden alle in Schleswig-Holstein eingeleiteten Ermittlungsverfahren erfaßt und landesweit gespeichert. Auch im vergangenen Jahr ist es nicht gelungen, Rechtsgrundlagen dafür in die Strafprozeßordnung einzufügen. Der Entwurf einer Arbeitsgruppe der Justizministerkonferenz ist **datenschutzrechtlich höchst unbefriedigend.** Neben vielen anderen Punkten haben wir hauptsächlich folgendes kritisiert:

- Der Entwurf sieht vor, daß Strafverfolgungsakten auch anderen Behörden zu Zwecken der **„Rechtspflege"** überlassen werden sollen. Der unpräzise Begriff „Rechtspflege" umfaßt wesentlich mehr als nur strafverfolgende Maßnahmen.
- **Datenübermittlungen** sollten bereits bei einer schlichten „Erforderlichkeit zur Erfüllung einer in der Zuständigkeit der anfragenden Stelle liegenden Aufgabe" zulässig sein. Weitere einschränkende Kriterien sieht der Entwurf nicht vor. Die **besonders sensiblen Daten** aus Strafverfahren sollen so behandelt werden wie beliebige sonstige bei öffentlichen Stellen vorhandene Daten.
- **Einsicht** in die **vollständigen Akten** soll immer dann gewährt werden können, wenn die Erteilung einer Einzelauskunft mit **„unverhältnismäßig hohem Aufwand"** verbunden wäre. In der Praxis der Justizverwaltung dürfte die Gefahr bestehen, daß sehr schnell der Aufwand als unverhältnismäßig hoch empfunden würde.
- Vorgesehen ist auch, daß personenbezogene Informationen bereits dann an **Privatpersonen** hätten weitergeleitet werden dürfen, wenn diese über einen Rechtsanwalt ein **berechtigtes Interesse** darlegen. Dies wird dem hohen Stellenwert des Grundrechts auf informationelle Selbstbestimmung nicht gerecht, weil es einem nicht näher qualifizierten berechtigten Interesse untergeordnet werden soll. Allein die **„Darlegung"**, also das bloße Vortragen, eines für berechtigt gehaltenen Interesses soll genügen. Wir haben verlangt, daß die Glaubhaftmachung bei Antragstellung und in besonderen Fällen der Nachweis des berechtigten Interesses Voraussetzung der Datenübermittlung sein müssen.
- Die vorgesehene **Dateiregelung** ist ein Musterbeispiel für eine **nichtssagende Blankettvorschrift.** Der Entwurf enthält keine einschränkenden Hinweise darauf, wessen Daten

von den genannten Stellen verarbeitet werden dürfen. Die Speicherung von Informationen über **jedermann** soll erlaubt werden, wenn es bloß für „erforderlich" gehalten wird. Dies können Beschuldigte, Zeugen, Geschädigte oder Hinweispersonen sein, auch ohne daß gegen sie strafrechtlich ermittelt worden ist.

- Auch die **Art der Daten,** die gespeichert werden sollen, ist nicht näher bestimmt. Die Vorschrift schließt unterschiedslos alle Strafverfolgungsbehörden ein, so daß auch der farblose Hinweis auf die jeweilige Aufgabenerfüllung nicht weiterhilft. Eine derartige Regelung muß die Betroffenen sowie die über sie zu erfassenden Informationen präziser nennen.

Insgesamt ist festzustellen, daß die als Generalklausel für die Datenverarbeitung gedachte Vorschrift fast schrankenlos die **beliebige Verwendung** aller im Strafverfahren anfallenden Informationen zuließe. Damit würde sie das Grundrecht auf informationelle Selbstbestimmung uneingeschränkt hinter die Erfordernisse der behördlichen Aufgabenerfüllung zurückstellen. In der vorgesehenen Form würde das Gesetz eine weit **über** den derzeitigen Inhalt von **GAST hinausgehende Datenspeicherung** erlauben.

Immerhin sieht der Entwurf eine **Löschungspflicht** für unzulässig gespeicherte Daten vor. Allein zur Unzulässigkeit kann es wegen der weitgefaßten Generalklauseln kaum kommen. Überdies fehlt eine Regelung, nach welcher Frist – auch unter Berücksichtigung der Fristen des **Bundeszentralregistergesetzes** – die Daten generell gelöscht werden müssen.

Der Entwurf enthält mehrere Ausnahmen von der Löschungspflicht zu Gunsten eines **„verhältnismäßigen Aufwandes".** Sogar nach der Übermittlung falscher Informationen soll selbst beim Vorliegen eines schutzwürdigen Interesses des Betroffenen eine Richtigstellung unterbleiben dürfen, wenn sie „zu aufwendig" gewesen wäre.

Wen wunderte es dann letztlich noch, daß das **Auskunftsrecht Betroffener** geradezu **spärlich** bedacht werden soll. Anstatt den Umfang der zu erteilenden Auskunft zu regeln sowie Kostenfreiheit für Auskünfte zu gewähren, hat man nur daran gedacht, die Schriftform des Antrages im Gesetz zu regeln.

Die Vielzahl der aufgezeigten Probleme und Kritikpunkte macht überdeutlich, daß sich der Gesetzgeber keinesfalls darauf beschränken darf, ein Verfahren wie **GAST** einfach mit einigen Generalklauseln **„abzusegnen".** Bei den dort gespeicherten Daten geht es um Informationen über begangene bzw. häufig nur mutmaßlich begangene Straftaten, also um hochsensible Daten. Die Frage, wie lange auf solche Informationen zurückgegriffen werden kann, wer sie abrufen und an wen er sie weitergeben darf, kann für die Betroffenen buchstäblich von existentieller Bedeutung sein. Der Gesetzgeber steht also auch vor der Entscheidung, wie sich beispielsweise die Speicherfristen bei der Staatsanwaltschaft zu denen des Bundes-

zentralregisters verhalten sollen, ob es notwendig ist, daß jede Staatsanwaltschaft auf jedes abgeschlossene Verfahren – auch anderer Staatsanwaltschaften – zugreifen kann und wofür die abgerufenen Daten verwendet werden dürfen.

Mehrere Vorstöße des **Justizministers** des Landes mit dem Ziel, den Bundesgesetzgeber zu veranlassen, die Strafprozeßordnung entsprechend zu ergänzen, sind in den letzten Jahren gescheitert. Auch entsprechende Initiativen der Bundesregierung haben nicht zum Erfolg geführt. Nach diesen Erfahrungen kann trotz ständiger gegenteiliger Absichtserklärungen aus Bonn wohl kaum mit einer raschen und zufriedenstellenden Änderung der Rechtslage gerechnet werden.

Die Vorlage eines **eigenen Gesetzentwurfes** im **Schleswig-Holsteinischen Landtag** hat der Justizminister bislang immer mit dem Hinweis abgelehnt, bei der Strafprozeßordnung handele es sich um Bundesrecht und der Bund bereite gerade entsprechende Gesetze vor. Diese Argumentation kann nicht mehr allzulange aufrecht erhalten werden.

Unbestritten gehört das Strafprozeßrecht zum Bereich der **konkurrierenden Gesetzgebung.** Das Land kann also Rechtsvorschriften solange und soweit erlassen, wie der Bund von seiner Kompetenz keinen Gebrauch macht. Daß Landesgesetze in diesem Bereich durchaus möglich und sinnvoll sind, hat das Land Berlin unter Beweis gestellt. Ein Verfahren wie GAST wäre in Berlin durch die entsprechenden Vorschriften des Berliner **„Gesetzes zur Ausführung des Gerichtsverfassungsgesetzes"** gedeckt.

4.3.2 Konsequenzen aus der Prüfung in den Justizvollzugsanstalten

Justizminister verbessert den Datenschutz in den Justizvollzugsanstalten.

Bereits in den letzten beiden Tätigkeitsberichten (14. TB, S. 44 und 15. TB, S. 51) haben wir uns ausführlich mit den von uns festgestellten datenschutzrechtlichen Defiziten im Strafvollzug befaßt. Leider ist auch zum Ende dieses Berichtszeitraumes festzustellen, daß es trotz mehrerer Anläufe dem Bundesgesetzgeber bis heute nicht gelungen ist, datenschutzrechtliche Vorschriften in das Strafvollzugsgesetz aufzunehmen.

Bei der Behebung der von uns aufgezeigten Schwachstellen bei der Erhebung, Speicherung, Übermittlung und Löschung personenbezogener Daten Gefangener und Dritter hat es gleichwohl auch im Berichtsjahr weitere Fortschritte gegeben:

- **Die Zirkulation von Daten über Gefangene in den Justizvollzugsanstalten wird auf das notwendige Maß eingeschränkt.**

  Bei der Weitergabe sog. Basisdaten eines Gefangenen (A-Bogen) innerhalb der Justizvollzugsanstalten wird entspre-

chend der Erforderlichkeit für die Aufgabenerfüllung der einzelnen Empfänger differenziert.

Ein entsprechender Nachweis der Erforderlichkeit ist zuvor gegenüber dem Datenschutzbeauftragten der Justizvollzugsanstalt zu erbringen. An Stellen außerhalb des Vollzuges werden nur noch die zur Identifizierung erforderlichen personenbezogenen Daten mitgeteilt.

– **Gefangenenpersonalakten werden auf das für den Vollzug erforderliche Maß beschränkt.**

Kernstück der über Gefangene existierenden Datensammlungen ist die **Gefangenenpersonalakte,** deren bisherige Gestaltung und unkontrollierbare Nutzung ein Hauptkritikpunkt gewesen ist. Aufgeteilt ist diese Akte in **drei Abschnitte** und das **Urlaubsheft** (sog. Heftnadel). Darin werden nach einer bundeseinheitlichen Verwaltungsvorschrift die verschiedensten Einzelvorgänge erfaßt. **„Heftnadel" 1** enthält umfangreiche Angaben und Beschreibungen zur Person des Gefangenen auf zum Teil standardisierten Formblättern, die Aufstellung und Fortschreibung des Vollzugsplanes, Übersichten über Vollzugsmaßnahmen sowie Urlaub und Ausgang.

„Heftnadel" 2 dient zur Aufnahme der Einweisungsunterlagen (einschließlich vollständiger Urteile und/oder Anklageschriften sowie evtl. medizinischer Gutachten), über Haftersuchen und Strafzeitberechnungen.

Auch wenn an dieser Einteilung weiterhin unverändert festgehalten werden soll, wird die **3. „Heftnadel"** künftig nur noch **vollzugsrelevantes Schriftgut** enthalten und nicht mehr wie bisher alle sonstigen Schriftstücke in der Reihenfolge ihres Entstehens. Solche Schriftstücke werden in einem Ablageheft als **Beiheft** aufbewahrt. Damit ist die Gefangenenpersonalakte nicht nur im Interesse der Übersichtlichkeit von Routinevorgängen entlastet. Aus datenschutzrechtlicher Sicht wichtig ist, daß sich nun mit diesem Ablageheft eine Vielzahl von anstaltsinternen Vorgängen ohne Beiziehung der gesamten Gefangenenpersonalakte erledigen lassen.

– **Zugriff auf Gefangenenpersonalakten eingeschränkt**

Durch die Aufbewahrung der Gefangenenpersonalakten, Urlaubshefte und Ablagehefte in verschließbaren Metallschränken soll künftig eine **unbefugte Zugriffs-** oder **Einsichtsmöglichkeit verhindert** werden. Darüber hinaus ist der Personenkreis, der ein **Zugriffsrecht** auf diese Akten besitzt, erheblich **eingeschränkt** worden. Einsichtnahme und Herausgabe der Gefangenenpersonalakten werden **dokumentiert.** Der Aktenumlauf in der Justizvollzugsanstalt erfolgt nur noch in **Verschlußmappen.** Durch diese Maßnahmen dürfte sich die Gefahr der mißbräuchlichen Nutzung von Gefangenenpersonalakten verringern.

– **Daten über dritte Personen**

Unserer Forderung, die in Strafurteilen und/oder Anklageschriften enthaltenen personenbezogenen Daten Dritter unkenntlich zu machen, will der Justizminister allerdings nicht nachkommen. Zwar räumt er ein, daß es für die Erhebung und Speicherung solcher Daten derzeit an einer Rechtsgrundlage mangelt, doch hält er es zur Durchführung eines geordneten Strafvollzuges für unverzichtbar, personenbezogene Daten über dritte Personen wie **Tatopfer, Mittäter** oder **Zeugen** zu verarbeiten. Nur so könnten wirksame Schutzfunktionen gegenüber Tatopfern oder Zeugen bei dauerhaften Vollzugslockerungen wie Urlaub und Freigang wahrgenommen werden. Insoweit sehen wir noch weiteren Erörterungsbedarf. Es müßte zumindest sichergestellt werden, daß diese Daten tatsächlich nur für diese Zwecke verwendet werden.

– **Ärztliche Versorgung soll in einer Gesundheitsdienstordnung geregelt werden.**

Der gesamte Bereich der ärztlichen Versorgung in den Vollzugseinrichtungen des Landes soll in einer **Gesundheitsdienstordnung** zusammenfassend neu geregelt werden. Schon jetzt werden Gefangenenlichtbilder nicht mehr zu den Gesundheitsakten genommen. Auch die automatische Zuleitung von Gefangenenpersonalakten an den **Anstaltsarzt** unterbleibt. Gesundheitsakten werden an Ärzte außerhalb des Vollzugs nicht weitergegeben. Überweisungen erfolgen künftig unter Befundmitteilung durch Arztbrief.

Wird bei Beschwerden Gefangener, die die ärztliche Versorgung betreffen, in besonders gelagerten Einzelfällen die Einsichtnahme in Gesundheitsakten durch zuständige **Aufsichtsbeamte** erforderlich, so bedarf es einer Einwilligungserklärung der Gefangenen.

– **Informationen über HIV-Infektionen**

Hier sind die Überlegungen für eine datenschutzkonforme Lösung noch nicht abgeschlossen.

Beabsichtigt ist, jeglichen Hinweis auf HIV-Infektionen in Akten, Listen und auf andere Weise zu unterlassen. Soweit erforderlich, sollen derartige Informationen auf **ärztliche Anordnung** in einem **verschlossenen Umschlag** zur Gefangenenpersonalakte genommen werden.

Auch bei der Vorführung HIV-infizierter Gefangener zu Gerichtsterminen erhalten Richter künftig nicht mehr wie bisher drei Tage zuvor eine routinemäßige Vorabinformation.

Die endgültigen Regelungen sollten noch 1993 in einer **Änderung** des sogenannten **AIDS-Erlasses** festgelegt und vor Inkrafttreten mit uns abgestimmt werden. Bislang liegt uns dieser angekündigte Erlaß allerdings nicht vor.

– **Akten in der sozialtherapeutischen Abteilung**

Die im Rahmen von Behandlungen in der sozialtherapeutischen Abteilung offenbarten persönlichen Daten und Erkenntnisse werden speziell in der JVA Lübeck in der sog. **Behandlungsakte** festgehalten.

Unsere Auffassung, daß diese Akten dem besonderen Schutz der ärztlichen Schweigepflicht unterliegen müssen, vermag der Justizminister nicht zu teilen. Zwar werden diese Akten unter Verschluß genommen und sind ausschließlich dem Vollzugsleiter und beiden Vollzugsabteilungsleiterinnen der JVA Lübeck zugänglich, doch genießen sie in den Augen des Justizministers keinen weiter gehenden Schutz gegenüber in anderen Vollzugsbereichen erhobenen Daten und Erkenntnissen. Hierzu sind weitere Erörterungen notwendig, denn wir gehen nach wie vor davon aus, daß die dem Anstaltspsychologen anvertrauten Daten einem besonderen strafrechtlichen Schutz unterliegen.

– **Briefkontrolle**

Eingehende Post wird nur noch in **Gegenwart des Gefangenen** einer Sichtkontrolle unterzogen. Eine inhaltliche Überprüfung bleibt bei konkretisierbaren und objektivierbaren Anhaltspunkten auf Einzelfälle beschränkt.

4.3.3 Wahrung der Persönlichkeitsrechte bei der Häftlingsüberwachung

Auch bei der Überwachung inhaftierter Terroristen müssen die Persönlichkeitsrechte gewahrt bleiben. Das Verfahren wird in Schleswig-Holstein modifiziert.

Im 13. Tätigkeitsbericht (S. 27) haben wir auf Rechtsverstöße im Zusammenhang mit der Überwachung von Gefangenen aus der terroristischen Szene (sogenannte Häftlingsüberwachung) hingewiesen.

Seinerzeit hatten wir erreicht, daß eine **Übermittlung** von Daten aus der Häftlingsüberwachung an die **Verfassungsschutzbehörde** nur zur Terrorismusbekämpfung und zur Verhütung der im Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10) aufgeführten Straftaten in Betracht kommt. Unsere weiter gehenden Kritikpunkte am Verfahren der Häftlingsüberwachung blieben zunächst offen.

Sowohl der Justizminister als auch der Innenminister haben inzwischen eingeräumt, daß ausschließlich der jeweiligen **Justizvollzugsanstalt** die **Kompetenz** zukommt, eine **Überwachung** der Besucher und des Schriftwechsels mit Gefangenen aus dem Terrorismusbereich **anzuordnen.** In der alleinigen Entscheidung der Anstalt liegt es auch, ob und inwieweit bei Überwachungsmaßnahmen gewonnene Erkenntnisse verwertet und Informationen an die Polizei weitergeleitet werden

sollen. Anordnungskompetenz und die weitere Verarbeitung der bei der Häftlingsüberwachung anfallenden Daten finden ihre Rechtsgrundlage ausschließlich in den Bestimmungen des Strafvollzugsgesetzes, die der Justizminister durch Erlaß konkretisiert hat.

Die Anordnung der Besuchsüberwachung ist damit nur zulässig, soweit **Sicherheits- und Ordnungsbelange der Anstalt** berührt sind. Weiterhin wurde festgelegt, daß alle Ersuchen der Anstaltsleitung an die Polizei um Amtshilfe im Rahmen der Häftlingsüberwachung entweder in der Gefangenenpersonalakte selbst oder in einem entsprechenden Beiheft zu **dokumentieren** sind. Dies gilt auch für die Entscheidungsgründe für Mitteilungen an die Polizei aus der Besuchsüberwachung sowie aus Briefkontakten.

Eine **Ablichtung der Ausweise** von erstmaligen Besucherinnen und Besuchern sowie die Speicherung entsprechender Daten durch die Polizei erfolgt **nicht mehr.** Sichergestellt ist auch, daß **Handschriftenproben** anläßlich von Besuchskontakten nur noch im Rahmen der gesetzlichen Voraussetzungen des Landesverwaltungsgesetzes erhoben und gespeichert werden.

Dieser Erlaß des Justizministers trägt dazu bei, daß in Schleswig-Holstein die Verwaltungsvorschriften zur Häftlingsüberwachung auf das gesetzlich zugelassene Maß zurückgeführt werden.

4.4 Steuerverwaltung

4.4.1 Datensicherheit bei der Aktenverwaltung in den Finanzämtern noch nicht garantiert

Im Jahre 1992 wurden bei Kontrollen in mehreren Finanzämtern Mängel bezüglich der Datensicherheit bei der Aktenverwaltung festgestellt. Ihre Behebung scheitert bislang weniger an der fehlenden Einsicht der verantwortlichen Stellen als vielmehr an der Bereitschaft zur Finanzierung der erforderlichen Maßnahmen.

Über die Notwendigkeit,

- Steuerakten stets unter **Verschluß zu halten,** wenn sie nicht bearbeitet werden,
- den **Verbleib** von Steuerakten zu **registrieren,** wenn sie an andere Stellen herausgegeben werden,
- den **Außendienstmitarbeitern** vorzuschreiben, wie Unterlagen in ihrem **häuslichen Bereich** zu verwahren sind und
- **Büroräume** auch während der Geschäftszeiten zu **verschließen,** wenn sie nicht besetzt sind,

besteht zwischen der Oberfinanzdirektion und dem Landesbeauftragten **Einvernehmen** (vgl. 15. TB, S. 60). Wie aber und in welchem Zeitraum für Abhilfe gesorgt werden kann, ist auch nach mehr als einem Jahr noch nicht abschließend geklärt. In den Beratungsgesprächen zeigte sich nämlich, daß das

Anheben des Sicherheitsstandards auf das „erforderliche und angemessene" Niveau (so der gesetzliche Tatbestand) um so mehr **Kosten** verursacht, je „schwächer" die bisher getroffenen Maßnahmen sind. Die Schlösser in einigen Aktenschränken auszutauschen, weil die Schlüssel verlorengegangen sind, erweist sich als eine Marginalie, weil dies nur wenige DM kostet. Überhaupt erst verschließbare Schränke zu beschaffen, stellt sich dagegen als ein erhebliches Problem dar, obwohl das Ziel beider Maßnahmen das gleiche ist.

So ist es nicht verwunderlich, daß vom Minister für Finanzen und Energie bis zum Abschluß des Berichtszeitraums erst der **Entwurf einer Anweisung** an die Finanzämter zur Sicherung von Akten und sonstigen Datenträgern vorgelegt werden konnte, in dem zudem einleitend festgestellt wird, daß wegen der Haushaltslage und der verfügbaren Mittel die angewiesenen verbesserten Sicherungsmaßnahmen nicht sofort, sondern nur **schrittweise** realisierbar seien.

Sollten in der Praxis tatsächlich aufgrund fehlender Haushaltsmittel für verschließbare Behältnisse Akten auch künftig so unzureichend gesichert werden, daß es zu unbefugten Offenbarungen steuerlicher Verhältnisse kommt, wird sich die Frage nach der **Verantwortung** stellen. Spätestens dann wird deutlich werden, daß finanzielle Überlegungen eine zeitliche Hinauszögerung von Sicherungsmaßnahmen, deren Erforderlichkeit und Angemessenheit nicht bestritten wird, nicht rechtfertigen. Das gilt ganz besonders für Datenbestände, die, wie Steuerakten, einem besonderen Berufs- und Amtsgeheimnis unterliegen.

Die weitere Entwicklung der Datensicherheit in den Finanzämtern wird mithin durch erneute Kontrollen zu beobachten sein.

4.4.2 „Aufbewahrung vorbehalten"

Für bestimmte Steuerakten sehen die Richtlinien eine unbefristete Speicherdauer vor. Ein überzeugender Grund hierfür ist nicht ersichtlich.

In einer zwischen dem Bund und den Ländern abgestimmten **Richtlinie über die Aufbewahrungsfristen** für Akten ist für Vermögenssteuerakten sowie für Bilanz- und Bilanzberichtsakten, anstatt daß ein Zeitraum festgelegt wird, der Vermerk enthalten **„vorbehalten".**

Als ein Petent das für ihn zuständige Finanzamt aufforderte, die Akten nach **25 Jahren** endlich zu vernichten, teilte ihm dieses mit, es sei durch die o.a. Regelung an einer Löschung gehindert. Das war weder für den Petenten noch für uns nachvollziehbar. Es ist in der Richtlinie ja nicht vermerkt „auf Dauer aufbewahren", sondern „vorbehalten". Was aus unserer Sicht sprachlich nur bedeuten kann, daß es dem einzelnen Bundesland vorbehalten bleibt, den Löschungszeitpunkt zu bestimmen, eine Bundeseinheitlichkeit also insoweit nicht erforderlich ist.

Anders sieht es allerdings der **Finanzminister.** Diese Passage der Richtlinie sei nicht so zu verstehen, daß sich die obersten Finanzbehörden von Bund und Ländern nicht auf eine einheitliche Aufbewahrungsfrist hätten einigen können. Vielmehr sollten „die davon betroffenen Steuervorgänge ... wegen des möglicherweise steuerrelevanten Informationsgehaltes der Unterlagen für zukünftige Besteuerungszeiträume vorerst nicht vernichtet werden„. Wann und durch wen diese Vernichtungssperre beendet werden soll, ist in den geltenden Richtlinien jedoch nicht festgelegt und konnte vom Finanzminister auch nicht dargelegt werden.

Wenn man bedenkt, daß selbst hinterzogene Steuern nach 10 Jahren verjähren, fällt es schwer, in z. B. 25 Jahre alten Akten einen „steuerrelevanten Informationsgehalt für zukünftige Besteuerungszeiträume" zu vermuten. Auf diesen Aspekt angesprochen verwies der Finanzminister auf eine sich derzeit in der Schlußabstimmung befindende **Neufassung der Aufbewahrungsbestimmungen.** Der Entwurf läßt jedoch nur einen Teilerfolg erwarten. Die **Bilanz-** und **Berichtsakten** sind zwar künftig nach 15 Jahren zu vernichten. Für **Vermögenssteuerakten** gilt aber weiterhin „vorbehalten", was immer dies künftig bedeuten soll.

Im Ergebnis verstößt auch die neue Regelung gegen den datenschutzrechtlichen Grundsatz, daß Daten **zu löschen** sind, wenn ihre Kenntnis für die datenverarbeitende Stelle zur Aufgabenerfüllung **nicht mehr erforderlich** ist. Die vage Vermutung eines „möglicherweise steuerrelevanten Informationsgehaltes" begründet keine „Erforderlichkeit zur Aufgabenerfüllung".

4.4.3 Es geht doch: Fairneß bei Kontrollmitteilungen

Seit Beginn dieses Jahres erhalten die Finanzämter wieder Kontrollmitteilungen über Nebeneinkünfte von Steuerpflichtigen. Durch die gleichzeitige Unterrichtung der Betroffenen wird auch deren Belangen Rechnung getragen.

In Zeiten des knappen Geldes ist der Staat ganz besonders auf die richtige und vollständige Besteuerung seiner Bürger angewiesen. Dies war sicherlich auch ein Grund dafür, daß nach mehreren Jahren des Nachdenkens im September 1993 in einer Rechtsverordnung die Voraussetzungen festgelegt worden sind, unter denen Behörden verpflichtet sind, den Finanzämtern Mitteilungen über zu versteuernde Zahlungen, Honorare usw. an einzelne Personen zukommen zu lassen. Diese sogenannten **Kontrollmitteilungen** finden ihre Grundlage in der Abgabenordnung. Sie wurden in den letzten Jahren nur deshalb nicht erstellt, weil die besagte Verordnung noch nicht verabschiedet war (vgl. 11. TB, S. 36).

Die Anfang 1994 in Kraft getretene Regelung zeichnet sich dadurch aus, daß sie einerseits praktisch alle Zahlungen erfaßt,

die manche der „Dazuverdiener" in der Vergangenheit gerne an den Finanzämtern vorbeigeschmuggelt haben, daß sie andererseits aber das Gebot des **„Fairplay"** beachtet.

Nicht zuletzt auf Drängen der Datenschutzbeauftragten enthält sie nämlich die Anweisung, daß die zahlenden Stellen die **Betroffenen** (die Zahlungsempfänger) von ihrer Mitteilungspflicht spätestens bei der Übersendung der ersten Kontrollmitteilung an das betreffende Finanzamt zu **unterrichten** haben. Steuerpflichtige, die Nebeneinkünfte bei Behörden erzielen oder die andere steuerrechtlich relevante Vergünstigungen in Anspruch nehmen (z.B. gewerberechtliche Erlaubnisse und Gestattungen), laufen mithin nicht Gefahr, daß sie sich durch ein „Versehen" oder „Übersehen" der versuchten Steuerhinterziehung schuldig machen. Was den Finanzämtern über Honorarzahlungen und dergleichen mitgeteilt wird, erfährt auch der Betroffene und zwar so rechtzeitig, daß er die Beträge in seiner Steuererklärung berücksichtigen kann.

Im Ergebnis handelt es sich also um eine Lösung, die den Belangen des Fiskus ebenso gerecht wird, wie denen der Steuerpflichtigen.

4.5 Wirtschaft, Technik und Verkehr

4.5.1 Automatisierte Zahlungssysteme im Verkehr

Die mobile Gesellschaft verlangt Eintrittsgeld. Wer reist, muß zahlen. Moderne bargeldlose Zahlungsverfahren haben gewisse Vorteile, bergen aber die Gefahr in sich, daß Reisewege, -ziele und -zeiten Betroffener, mithin: Bewegungsbilder, aufgezeichnet werden.

„Plastikgeld" ist inzwischen ein weitverbreitetes Zahlungsmittel. Weniger bewußt dürfte den Benutzern von Scheckkarten, Kreditkarten oder anderen kartengestützten Zahlungsmitteln sein, daß sie bei der Nutzung des Plastikgeldes unter Umständen eine **breite Datenspur** hinterlassen. Je mehr das anonyme Bargeld durch bequeme Bargeldlos-Verfahren verdrängt wird, desto mehr tritt der Konsument aus seiner Anonymität heraus. Kunden- und Benutzerprofile werden möglich und unversehens findet sich der Kunde in seinen **Konsumgewohnheiten aufgezeichnet** und **transparent** gemacht. Nebenbei entsteht auch ein Bewegungsprofil darüber, wer wann wo gewesen ist.

Sofern die Kunden von diesen Risiken wissen und gleichwohl auf die Annehmlichkeiten des bargeldlosen Einkaufs nicht verzichten wollen, ist das ihre Sache. Aus **datenschutzrechtlicher Sicht** kommt es aber auf zwei Dinge ganz besonders an: Es muß immer die Möglichkeit geben, auch **weiterhin** mit **Bargeld** zu bezahlen, damit auch tatsächlich eine Wahlfreiheit

für den Kunden besteht. Außerdem ist die Qualität bargeldloser Zahlungsmittel aus der Sicht des informationellen Selbstbestimmungsrechts daran zu messen, ob auch bei ihrer Nutzung die Entstehung von Kunden- und Bewegungsprofilen möglichst vermieden wird. Wenn man nur will, ermöglicht die Technik zumeist auch eine Variante, bei der „bequem" bargeldlos bezahlt und gleichwohl die **Anonymität des Verbraucherverhaltens** gewahrt werden kann.

Im **öffentlichen Personennahverkehr** sind aber zahlreiche sogenannte **Post-paid-Verfahren** in Erprobung, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden. Diese Zahlungsweise erfordert die Speicherung umfangreicher personenbezogener Daten: Neben der Kontonummer und Bankleitzahl des Fahrgastes werden sowohl Datum und Uhrzeit des Fahrscheinkaufs bzw. des Fahrtantritts als auch Automatennummer und Preisstufe der jeweiligen Fahrt erhoben.

Auch für die künftige Erhebungsweise von **Autobahngebühren** werden Verfahren geprüft, die in ähnlicher Weise Zeiten und Strecken der Autobahnbenutzung Berechtigter aufzeichnen und in die Abrechnung einfließen lassen. Damit besteht die Gefahr, daß sehr **detaillierte Bewegungsprofile** entstehen, die z.B. auch für Strafverfolgungsbehörden, Finanzämter oder für die Werbewirtschaft von Interesse sein können. Da sämtliche Fahrten für einen gewissen Zeitraum aufgelistet werden, hat überdies jeder Kontoinhaber die Möglichkeit, Fahrten auch anderer Fahrzeugbenutzer nachzuvollziehen.

Eine solche Vorgehensweise ist um so problematischer, als **technische Alternativen** existieren, die weitaus **bürgerfreundlicher** sind. Es können, wie skandinavische und auch deutsche Projekte aufzeigen, Wertkartensysteme eingesetzt werden, bei denen im voraus bezahlt wird und die daher eigentlich gänzlich ohne personenbezogene Daten auskommen müßten.

Hierbei handelt es sich um sogenannte **Pre-paid-Verfahren,** bei denen Probleme aber dann auftreten, wenn der Kunde geltend macht, daß, aus welchen Gründen auch immer, zuviel von der Wertkarte abgebucht worden ist. Wie und durch wen ist der Nachweis zu erbringen, daß das technische System einwandfrei gearbeitet hat? Wie kann nachträglich festgestellt werden, welcher Betrag tatsächlich abgebucht worden ist? Wie kann verhindert werden, daß der Kunde die Wertkarte durch Manipulation wieder auffüllt? Eine personenbezogene Registrierung der Karteninhaber und eine Protokollierung in den Abbuchungsstellen würde zu den gleichen Effekten wie beim Post-paid-Verfahren führen.

Zusätzliche Schwierigkeiten ergeben sich bei der **Abbuchung auf Autobahnen,** wenn der Verkehrsteilnehmer nicht zum Anhalten gezwungen werden soll. Ist die Wertkarte defekt oder nicht mehr „gedeckt", muß das Fahrzeug registriert werden. Dazu muß das Fahrzeugkennzeichen und ggf. auch der Fahrer fotografiert werden. Weil es technisch schwierig ist,

dies unmittelbar beim Abbuchvorgang durchzuführen, steht der Vorschlag im Raum, zunächst alle Verkehrsteilnehmer zu registrieren und kurze Zeit später die Daten derjenigen zu löschen, die ordnungsgemäß bezahlt haben. Diese Überlegungen zeigen, daß Hersteller und Betreiber derartiger Systeme sich schwer tun, ganz ohne „Datenspuren" auszukommen. Die Datenschutzbeauftragten haben daher in einer Entschließung dargelegt, daß es dringend erforderlich ist, bei der Konzipierung und Einführung kartengestützter Zahlungssysteme mehr als bisher darauf zu achten, eine **„datenfreie Fahrt"** zu ermöglichen. Im öffentlichen Nahverkehr muß z.B. weiterhin zusätzlich alternativ die datenschutzfreundlichste Lösung angeboten werden: Der Kauf einer Fahrkarte am Automaten mit Bargeld.

4.5.2 Auskünfte über Halter von Kraftfahrzeugen: Mal zu einfach – mal zu schwer

Auskünfte der Zulassungsstellen über Halter von Kraftfahrzeugen sind einerseits leicht zu erhalten – und können dann mißbräuchlich verwendet werden –; andererseits kann es schwierig sein, sinnvolle und notwendige Angaben zu erhalten, wenn der Bezug zum Straßenverkehr nicht offenkundig ist.

In mehreren Eingaben wurde Klage darüber geführt, daß es ein Leichtes sei, Auskunft über Halterdaten zu erlangen. Ein Mann hatte z.B. über eine Auskunft bei der Kraftfahrzeugzulassungsstelle eines Kreises den Namen und die Anschrift der Halterin eines bestimmten Kraftfahrzeugs erhalten. In der Folge versuchte er, mit der Halterin Kontakt aufzunehmen und belästigte sie massiv.

Die Stellungnahme des Landrats und die Prüfung der Rechtslage zeigte, wie begrenzt die Möglichkeiten der Restriktion in solchen Fällen sind. Die **Halterauskunft** erfolgt auf der Grundlage des Straßenverkehrsgesetzes. Schon wenn jemand darlegt, daß er Daten zur **Geltendmachung von Rechtsansprüchen** im Zusammenhang mit der Teilnahme am Straßenverkehr benötigt, werden ihm Namen und Anschrift des Halters eines Kraftfahrzeugs übermittelt. Da diese Auskunft an keine weitere Voraussetzung als an die **Darlegung eines entsprechenden Sachverhalts** gebunden ist, besteht für die Zulassungsstelle keine Möglichkeit, das Vorbringen auf seine Richtigkeit hin zu prüfen. Durch einen Runderlaß des Ministers für Wirtschaft, Technik und Verkehr ist angeordnet, daß grundsätzlich nur **schriftliche Anträge** zu beantworten sind. Diese sind **aufzubewahren.** Damit werden für eine bestimmte Zeit die Umstände der Auskünfte festgehalten. Ein Mißbrauch kann so zumindest im nachhinein aufgeklärt werden. Sanktionen für den Mißbrauch kennt das Straßenverkehrsrecht allerdings nicht.

Als Reaktion auf das unberechtigte Beschaffen von Halterdaten bleiben den Betroffenen allein **Strafanzeige** und **Strafantrag.** Haben die Belästigungen beleidigenden Charakter oder

erreichen sie – etwa als massive Telefonanrufe – das Ausmaß einer Körperverletzung, so kann eine Verurteilung des Täters in Betracht kommen. Liegt Bereicherungs- oder Schädigungsabsicht beim Täter vor, ist auch eine Ahndung nach dem Landesdatenschutzgesetz möglich. Ergänzend zum Straßenverkehrsgesetz gelten nämlich die Vorschriften des LDSG. Danach sind private Empfänger von Datenübermittlungen zu verpflichten, die Informationen nur für den angegebenen Zweck zu verwenden. Halten sie die Zweckbindung nicht ein, können Freiheitsstrafen bis zu zwei Jahren, Geldstrafen oder Bußgelder (bis zu 100.000 DM) verhängt werden.

So leicht im vorstehenden Fall eine Halterauskunft zu erlangen war, so **schwierig** war es in einem anderen Fall, den **Halter** eines Kraftfahrzeugs **festzustellen.** Ein Unternehmen fand ein fremdes Fahrzeug auf seinem Betriebsgelände abgestellt vor und bat um Angabe des Halters, um das Fahrzeug entfernen zu lassen. Die Zulassungsstelle lehnte zunächst ab mit der Begründung, die Auskunft sei nicht zur Geltendmachung von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr notwendig, da es um rein zivilrechtliche Ansprüche im Zusammenhang mit der Benutzung des privaten Grundstücks gehe.

Nach eingehender Prüfung des Sachverhalts und Erörterungen zwischen Kreis, Minister für Wirtschaft, Technik und Verkehr und uns wurde schließlich die erbetene Auskunft doch erteilt. Es ist nämlich nicht erforderlich, daß der Anspruch auf Ereignisse zurückzuführen ist, die sich im öffentlichen Verkehrsraum unmittelbar abspielen. Ein **mittelbarer Zusammenhang** mit der Teilnahme am Straßenverkehr reicht aus, wenn der Auskunftsanspruch überhaupt einen **Bezug zum Straßenverkehr** aufweist. Das ist zum Beispiel der Fall bei unberechtigter Benutzung privater Parkplätze und Stellflächen, die nur über eine Teilnahme am öffentlichen Straßenverkehr erreicht werden.

4.6 Sozialwesen

4.6.1 Intime Fragen an Sozialhilfeempfänger

Die Datenerhebung durch Sozial- und Wohngeldämter findet ihre Grenze in der Intimsphäre der Betroffenen.

„Antragsteller mit Schnüffelbogen abschrecken?" und „Wer sortiert die Wäsche in den Schrank?", so lauteten die Schlagzeilen von Berichten über den sogenannten Überprüfungsbogen „Wohn- und Wirtschaftsgemeinschaft/eheähnliche Gemeinschaft", den eine Stadtverwaltung durch Antragsteller ausfüllen ließ. Sie wollte damit herausfinden, ob eine **Wohn- und Wirtschaftsgemeinschaft** oder eine **eheähnliche Gemeinschaft** vorlag, mit der Folge, daß bei der Berechnung der Sozialhilfe auch das Einkommen gemeinsam zu kalkulieren war wie bei Ehepaaren.

So wollte die Stadt beispielsweise wissen, wer die Räume pflegt, wie die Lebensmittel eingekauft werden, wie die Lebensmittel aufbewahrt werden, wer die Wäsche bügelt und ob der Fernseher gemeinsam genutzt wird. Für uns waren die Presseberichte Anlaß, der Wohngeldstelle der betreffenden Stadt einen **Prüfbesuch** abzustatten. Die Durchsicht einschlägiger Vorgänge ergab, daß sich betroffene Bürger durch die Fragen erheblich in ihrer Intimsphäre verletzt fühlten. Einzelne Randbemerkungen an den Anträgen machten die ganze Erbitterung über diese staatliche Neugier deutlich.

So entspann sich zwischen Antragstellern und der zuständigen Behörde folgender „Dialog": Nachdem im Antrag eine getrennte Nutzung des Schlafzimmers angegeben worden war, wurden vom Sozialamt hierzu und zu weiteren Punkten ergänzende Nachfragen gestellt. Wunschgemäß führten die Betroffenen aus:

„Eine eheähnliche Beziehung besteht zwischen uns nicht; wir kennen uns erst seit ... und außer einem "guten Verstehen" besteht keine Beziehung. Eine Änderung unserer persönlichen Verhältnisse (Beziehung etc.) teilen wir Ihnen unverzüglich mit."

In der Folge kam es zu weiteren Meinungsverschiedenheiten zwischen Betroffenen und Sozialbehörde. Schließlich teilten die Antragsteller sarkastisch mit: „.... Zu allerletzt etwas Positives für Sie: Seit gestern, sprich dem ..., haben wir ein enges, intimes Verhältnis."

Bereits im Laufe der Prüfung wurde erreicht, daß der kritisierte **Fragebogen** von der Stadtverwaltung **aus dem Verkehr gezogen** wurde. Dem schloß sich der Kreis an. Da es viele Wohngeldstellen gibt, wurde nachgefragt, wie in den Landkreisen in Schleswig-Holstein und in anderen Bundesländern verfahren wird. Die Rückläufe ergaben, daß bisher auch andere Landkreise und kreisfreien Städte ähnlich vorgegangen sind. Zwar wurden unterschiedliche Fragebogen verwandt und teilweise auch abgestufte Verfahren. Die kritischen Fragen, wie z.B. die nach dem gemeinsamen Schlafzimmer fanden sich jedoch stets wieder, zumindest in den Fällen, in denen anders eine Klärung nicht zu erreichen war.

Derart **intime Fragen** halten wir für **unzumutbar.** Sie sind auch nicht geeignet, da das Vorliegen einer Wohn- und Wirtschaftsgemeinschaft oder eheähnlichen Gemeinschaft nicht davon abhängig ist, daß die betroffenen Bewohner der Wohnung das Bett miteinander teilen. Diese Auffassung bestätigt das **Bundesverfassungsgericht,** das in einer Entscheidung zur eheähnlichen Gemeinschaft im Sinne des Arbeitsförderungsgesetzes dargelegt hat, daß die Annahme, es liege eine eheähnliche Gemeinschaft vor, nicht die Feststellung voraussetzte, daß zwischen den Partnern geschlechtliche Beziehungen bestehen. Die Betroffenen haben nach dem Urteil insoweit Anspruch auf Respektierung ihrer **Intimsphäre.** Wir wollen deshalb darauf hinwirken, daß in Schleswig-Holstein auf Fragen dieser Art künftig verzichtet wird.

Verbesserungen sollten auch bezüglich der **übrigen Fragen** angestrebt werden. Wir haben angeregt, die Antragsteller darauf hinzuweisen, daß der Gesetzgeber nach der geltenden Rechtslage vermutet, daß Personen, die gemeinsam eine Wohnung bewohnen, auch eine Wohn- und Wirtschaftsgemeinschaft bilden und dies im Einzelfall vom Antragsteller zu widerlegen wäre. Anstelle des bisher üblichen obligatorischen Fragebogens haben wir empfohlen, dem Antragsteller im einzelnen aufzulisten, welches die **maßgeblichen Kriterien** für die Beurteilung der Frage, ob eine **eheähnliche Gemeinschaft** beziehungsweise eine **Wohn-und Wirtschaftsgemeinschaft** vorliegt, sind. In diesem Zusammenhang haben wir den zuständigen Wohngeldstellen die Streichung einer Reihe von Kriterien nahegelegt, da sie nach unserer Auffassung nicht erforderlich und im Zweifelsfall auch kaum überprüfbar und damit auch nicht justitiabel sind. Es sind dies zum Beispiel die Fragen danach, wer bügelt oder die Wäsche wäscht.

4.6.2 Neugierige Fragen im Rahmen der Anerkennung der Vaterschaft

Der Umfang der Fragen der Jugendämter an junge Mütter im Zusammenhang mit der Ermittlung der Vaterschaft mußte erheblich eingeschränkt werden.

Eine junge Frau machte darauf aufmerksam, daß ein Kreisjugendamt in Zusammenhang mit der **Ermittlung der Vaterschaft** einen **Fragebogen** verwendete, der zahlreiche Fragen enthielt, deren rechtliche Zulässigkeit ihr fragwürdig erschien. So wurde z.B. wie folgt gefragt:

- Sind Sie gesund?
- Wissen die Eltern der Kindesmutter von der Geburt?
- Wie hoch ist das Einkommen Ihrer Eltern?

Außerdem enthielt der Fragebogen eine **Schweigepflichtentbindungserklärung,** in der es hieß: „Ich befreie hiermit den an der Geburt beteiligten Arzt und die Hebamme von ihrer Schweigepflicht."

Unsere Bemühungen ergaben, daß diese Klausel ersatzlos aus dem Formular gestrichen wurde. Auch der übrige **Datenumfang** des Fragebogens wurde **deutlich reduziert.** Wo erforderlich, wurde auf die Freiwilligkeit der Angaben ausdrücklich hingewiesen, z.B. bei der Frage nach dem religiösen Bekenntnis. Gestrichen wurden u.a. die Fragen nach dem Geburtsgewicht, der Länge, dem Kopfumfang sowie dem Gesundheitszustand des Kindes und der Mutter.

Die Mütter werden künftig auch nicht mehr nach ihrer Schulbildung und ihrem jetzigen Beruf befragt. Entfallen sind ferner die Fragen nach dem Beruf, dem Arbeitgeber, dem Einkommen und dem Vermögen der Großeltern. Es stellte sich nämlich heraus, daß die Angaben über die Großeltern erst dann erforderlich sind, wenn sie zu Unterhaltsleistungen herangezogen werden sollen. Nur in diesen Einzelfällen sind die Ju-

gendämter befugt, die entsprechenden Angaben zu verlangen. Der **reduzierte Datenkatalog** kommt im übrigen nicht nur den jungen Müttern zugute, sondern dürfte letztlich auch die **Verwaltung entlasten,** da die Verarbeitung überflüssiger Daten unnötig Verwaltungskapazität bindet.

4.7 Gesundheitswesen

4.7.1 Datenschutz bei der Beratung vor Schwangerschaftsabbruch

Schwangere Frauen müssen sich vor einem Schwangerschaftsabbruch beraten lassen, wenn sie sich nicht strafbar machen wollen. Sie haben einen Anspruch, daß dabei ihre Anonymität gewahrt bleibt.

Im Mai 1993 hat das Bundesverfassungsgericht die vom Bundestag beschlossene Änderung des Abtreibungsrechts für verfassungswidrig erklärt. Bis zur Vorlage eines neuen Gesetzes wurde eine **Übergangsregelung** in Kraft gesetzt, in der die zwischenzeitlich geltenden **Voraussetzungen für einen Schwangerschaftsabbruch** festgelegt sind. Danach muß die betroffene Frau u.a. eine auf ihren Namen ausgestellte Bescheinigung darüber vorlegen, daß sie sich in einer anerkannten Beratungsstelle über die Problematik einer Abtreibung hat beraten lassen. Der beratenden Person gegenüber braucht sie jedoch ihren Namen nicht zu nennen.

Die Umsetzung dieser Vorgaben stößt nun in der Praxis auf folgende **Schwierigkeit:** Einerseits haben die Beratungsstellen die **Anonymität** der Beratung **sicherzustellen,** andererseits müssen sie darüber jedoch eine mit dem Namen der Frau versehene **Bescheinigung** ausstellen.

Um für die Übergangszeit zu einem praxis- und datenschutzgerechten Verfahren beizutragen, haben wir folgende **Vorschläge** gemacht:

- In der Beratungsstelle sind deutliche schriftliche **Hinweise** darauf zu geben, daß sich Frauen anonym beraten lassen können.
- Der Beraterin oder dem Berater braucht zu keinem Zeitpunkt der **Name** genannt zu werden.
- Die beratende Person vergibt eine **Beratungsnummer** für das Protokoll und die spätere Bescheinigung.
- Wird über das Gespräch zum Schwangerschaftsabbruch hinaus **konkrete Hilfestellung** gewünscht, muß eine andere Person als die Beraterin oder der Berater tätig werden.

Alle beteiligten Personen sind untereinander und Dritten gegenüber zur **Verschwiegenheit verpflichtet** und dürfen insbesondere den Namen der Unterstützung suchenden Frau nicht weitergeben.

Diese Vorstellungen haben wir der **Sozialministerin** im Laufe des Jahres übersandt. Wie uns mitgeteilt wurde, haben dort inzwischen alle Ressorts **Zustimmung** bekundet. Unsere Vor-

schläge sollen in das Konzept für die Beratungsstellen übernommen werden.

4.7.2 Offenbarung von Daten im berufsgerichtlichen Ermittlungsverfahren

Das Sozialdatengeheimnis erlaubt es nicht, Patientendaten für Zwecke eines berufsgerichtlichen Ermittlungsverfahrens zu offenbaren. Gericht bestätigt die Rechtsauffassung des Landesbeauftragten.

Das Sozialgeheimnis soll sicherstellen, daß die gesetzlichen Krankenkassen Informationen über Versicherte nicht unbefugt an Dritte weitergeben. Nur wenn im Gesetz geregelte Ausnahmetatbestände vorliegen, dürfen **Sozialdaten offenbart** werden.

An dieser hohen Barriere scheiterte der Untersuchungsführer für die **Berufsgerichtsbarkeit der Heilberufe,** als er im Rahmen eines berufsgerichtlichen Ermittlungsverfahrens gegen Apotheker von einer gesetzlichen Krankenkasse verlangte, ihm die Namen und Adressen aller in einem bestimmten Ort wohnhaften Patienten mitzuteilen, soweit sie bei dort praktizierenden Ärzten in Behandlung waren.

Zwar dürfen im Rahmen der **Amtshilfe** Namen, Geburtsdaten, Anschrift und Arbeitgeber übermittelt werden, wenn schutzwürdige Belange des Betroffenen nicht beeinträchtigt sind. Hier wäre über diese Daten hinaus zusätzlich aber auch die **Behandlung** durch einen **bestimmten Arzt** mit **offenbart** worden. Weitere Daten sind Ermittlungsbehörden jedoch nur dann bekannt zu geben, wenn der Beschuldigte im Verdacht steht, eine Straftat begangen zu haben. Dies war jedoch nicht der Fall. Nach entsprechender Beratung durch uns lehnte die Krankenkasse deshalb eine Auskunftserteilung ab.

Dennoch verlangte die Kammer weiterhin die Herausgabe der Daten und zog mit dem Argument vor **Gericht,** die Mißachtung der standesrechtlichen Vorschriften sei in diesem Falle so schwerwiegend, daß sie der Verletzung von Strafvorschriften gleichkäme. Das Gericht war jedoch wie wir der Ansicht, zur Herausgabe der Daten genüge es nicht, daß lediglich zu klären sei, ob ein Beschuldigter gegen die standesrechtlichen Vorschriften der für ihn geltenden Berufsordnung verstoßen habe. Die **Klage** der Kammer wurde in erster Instanz **abgewiesen.** Das Berufungsverfahren ist noch nicht abgeschlossen.

4.7.3 Aufklärung der Leukämiefälle in der Elbmarsch

Auch wenn die Untersuchung von Leukämiekrankheiten in der Umgebung von Kernkraftwerken wichtige Anliegen verfolgt, dürfen dabei Patientendaten nur unter Einhaltung der gesetzlichen Bestimmungen verarbeitet werden.

Im Zusammenhang mit den Untersuchungen zur Aufklärung des **Leukämieclusters** in der Elbmarsch ist das Bremer Institut für Präventionsforschung und Sozialmedizin (BIPS) von

den Expertenkommissionen in Niedersachsen und in Schleswig-Holstein mit der Durchführung einer retrospektiven Inzidenzerhebung in den Landkreisen Harburg, Lüneburg und Herzogtum Lauenburg beauftragt. Die Studie soll eine Totalerhebung der Diagnosen Leukämien, maligne Lymphome und multiple Myelome bei Kindern und Erwachsenen für den Zeitraum 1984 bis 1991 umfassen.

Die **Datenerhebung** erfolgt aus:

- den Krankenakten der Kliniken in den Landkreisen Harburg, Lüneburg sowie im Kreis Herzogtum Lauenburg, sofern diese über Abteilungen für Innere Medizin, Pädiatrie oder Onkologie bzw. Hämatologie verfügen;
- den Krankenakten der entsprechenden Abteilungen der Universitätsklinik Hamburg-Eppendorf und einiger ausgewählter weiterer Hamburger Kliniken sowie der Medizinischen Hochschule Hannover;
- den Patientenkarteien aller niedergelassenen Ärzte für Allgemeinmedizin, Internisten und Pädiater in den drei Landkreisen;
- den Todesbescheinigungen der Gesundheitsämter der Landkreise;
- den Akten und Karteien von Pathologischen Instituten und Abteilungen, die Kliniken und niedergelassene Ärzte im Untersuchungsgebiet betreuen.

Für die Erfassung der einzelnen Fälle wird ein **Erhebungsbogen** eingesetzt, der die notwendigen Angaben zur Person des Patienten wie Geburtsdatum, Geschlecht, Beruf, die genaue Diagnose sowie Angaben zum Tod enthält. Die abgebende Stelle bekommt eine Durchschrift des Erhebungsbogens, auf der auch der Name des Patienten eingetragen wird. Eine weitere Durchschrift ist für das Gesundheitsamt bestimmt. Diese sollte nach der Konzeption des Bremer Instituts die Wohnanschrift des Patienten enthalten. Das Gesundheitsamt sollte die Wohnanschrift dann für das Institut in eine Angabe der genauen Lage mit Hilfe eines Koordinatensystems (Gauß-Krüger-Koordinaten) umwandeln, um Doppelmeldungen auszuschließen.

Dieses Verfahren erschien uns datenschutzrechtlich nicht vertretbar, weil in Einzelfällen der Personenbezug hergestellt werden könnte. Die **Auswertung** der **Krankengeschichten** in den Kliniken soll nach den Zielvorstellungen des Instituts von **Mitarbeitern** des **Krankenhauses** durchgeführt werden. Dagegen ist nichts einzuwenden, wenn man davon ausgehen kann, daß die erhobenen Daten, die dann an das Institut weitergegeben werden, ausreichend anonymisiert sind.

Die **Patientenkarteien** der niedergelassenen Ärzte – für die der Innenminister des Landes Schleswig-Holstein als Datenschutzaufsichtsbehörde zuständig ist – sollen von den Ärzten selbst bzw. ihren Mitarbeitern ausgewertet werden, die dann

die ausgefüllten, aber anonymisierten Erhebungsbogen den Mitarbeitern des BIPS übergeben.

Auch die Auswertung der **Daten** und **Karteien** der **Pathologischen Institute** ist zulässig, wenn sie durch eigene Mitarbeiter geschieht. Die Weitergabe der ausgewerteten Daten jedoch nur dann, wenn diese ausreichend anonymisiert sind. Bei der ursprünglichen Konzeption des Instituts war davon auszugehen, daß dies nicht der Fall gewesen wäre, da die relativ präzisen Angaben auf dem Fragebogen im Zusammenhang mit der Gauß-Krüger-Koordinate die Herstellung des Personenbezuges möglich gemacht hätte.

Da dies für das Institut nicht akzeptabel war, haben wir folgenden **Lösungsvorschlag** unterbreitet:

- Die Krankenhäuser, Ärzte und Pathologischen Institute stellen alle relevanten Leukämiefälle zusammen. Die „Adressen" dieser Fälle (ausschließlich Straße, Hausnummer, Wohnort) werden zusammen mit den Identifizierungsnummern an das **Gesundheitsamt als Clearingstelle** gegeben.

- Gemeinsam mit dem zuständigen Katasteramt wird die Belegenheit der Anschrift auf der Grundlage der **Gauß-Krüger-Koordinate** festgestellt. Dabei muß sichergestellt werden, daß nur ein solcher Feinheitsgrad der Koordinaten gewählt wird, der es nicht zuläßt, daß die geographische Belegenheit in der Zusammenschau mit den anderen später hinzukommenden Daten des Falles die Identifizierung einzelner natürlicher Personen ermöglicht. Dies könnte z.B. bei einzeln gelegenen Gehöften der Fall sein. In diesen Fällen ist eine Zusammenfassung von mehreren Anschriften unter einer Grobkoordinate bzw. die Bildung von Planquadraten anzustreben.

- Wenn dies nicht möglich ist, ist die Adresse über das Gesundheitsamt an die Datenquelle mit der Bitte zurückzugeben, die **Einwilligung** des betroffenen Patienten einzuholen.

- Gibt der Patient seine Einwilligung nicht, darf der Fall nur **ohne Koordinate** ausgewertet werden.

Die Auswertung der Todesbescheinigungen des Gesundheitsamtes durch eigene Mitarbeiter des Amtes ist zulässig. Die Weitergabe der Daten ebenfalls, soweit es sich um anonymisierte Daten handelt. Sind die Daten nicht ausreichend anonymisiert, kommt nur eine **Genehmigung** zur Nutzung der Daten **für Forschungszwecke** nach dem Landesdatenschutzgesetz bei überwiegendem öffentlichen Interesse in Betracht. Diese Genehmigung hat das Ministerium erteilt, so daß das BIPS trotz der schwierigen datenschutzrechtlichen Probleme in die Lage versetzt worden ist, den fraglichen Leukämiefällen in dem gewünschten Umfange nachzugehen.

4.7.4 Datenschutzrechtliche Kontrolle von Krankenakten

Patienten haben auch unabhängig vom Datenschutzrecht Anspruch auf Einblick in ihre Krankenakte. Das sog. Patientengeheimnis steht der Kontrolle durch den Datenschutzbeauftragten nur dann entgegen, wenn der Patient ausdrücklich widersprochen hat.

Wenn Patienten wissen wollen, was über sie in ihrer Krankenakte steht, kommt es immer wieder zu Meinungsverschiedenheiten mit Ärzten und Krankenhäusern. Dabei hat die Rechtsprechung längst ein **Informationsrecht des Patienten** unabhängig vom Datenschutzrecht entwickelt. Obwohl auch das nunmehr seit 1991 geltende Datenschutzgesetz keine Ausnahmevorschriften für Krankenakten enthält, wird von manchem Arzt immer noch die unzutreffende Ansicht vertreten, er allein habe frei darüber zu entscheiden, wem welcher Zugang eröffnet wird.

So verweigerte eine **Fachklinik für Psychiatrie, Neurologie und Rehabilitation** einem dort Untergebrachten die Einsichtnahme in seine Krankenakte. Nachdem sich der Petent Anfang 1993 an uns gewandt hatte, hörten wir auf unsere Aufforderung, dieses Verhalten zu begründen, zunächst drei Monate nichts. Auf mehrere Nachfragen sowie nach Übersendung einer Abschrift der ersten Anfrage teilte die Fachklinik lapidar mit, der Betroffene könne die Akten unter ärztlicher Aufsicht einsehen, allerdings nicht „Angaben von Dritten und Wertungen". Eine Begründung für diese Beschränkung wurde wiederum nicht gegeben.

Daraufhin bat uns der Petent, zu **überprüfen,** ob die teilweise Verweigerung der Akteneinsicht rechtmäßig sei. Auf die Möglichkeit, sich an uns zu wenden, hätte die Klinik von sich aus hinweisen müssen. Als wir die Unterlagen sichten wollten, schrieb uns die Fachklinik im Juli 1993 wörtlich: „Eine Überprüfung durch ... kommt nicht in Betracht und erst recht nicht – stellvertretend für ihn – durch den Landesbeauftragten für den Datenschutz".

Hinweise auf unsere im Gesetz unzweideutig verankerte **umfassende Kontrollkompetenz** fruchteten nichts. Auch nachdem die **Sozialministerin** als Fachaufsichtsbehörde die Klinik **förmlich angewiesen** hatte, die Akten vorzulegen, weigerte sich der leitende Abteilungsarzt weiterhin. Es bedurfte erst des Erscheinens des zuständigen Referenten der Sozialministerin vor Ort, bis man uns die Akten im Januar 1994 endlich vorlegte – allerdings nicht, ohne zuvor Aktenteile mit ausdrücklichem Hinweis auf die bevorstehende Kontrolle **geschwärzt** zu haben.

Dieses Vorgehen haben wir förmlich **beanstandet.**

Das Datenschutzgesetz kennt **kein „Ärzteprivileg".** Für die öffentlich-rechtlichen Krankenanstalten gelten vielmehr dieselben gesetzlichen Verpflichtungen wie für alle anderen Landesbehörden auch:

- Grundsätzlich ist **jedem Bürger kostenlos Auskunft** darüber zu erteilen, was die datenverarbeitende Stelle über ihn gespeichert hat.
- Die öffentlichen Stellen sind verpflichtet, dem **Datenschutzbeauftragten Auskunft** zu erteilen und Einsicht in **alle Unterlagen und Akten** zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Der Gesetzgeber hat sogar ausdrücklich bestimmt, daß **„besondere Amts- und Berufsgeheimnisse dem nicht entgegenstehen".**

Damit ist klargestellt, daß auch die ärztliche Schweigepflicht einer Kontrolle nicht entgegengehalten werden kann. Gelegentlich meinen allerdings Mediziner, sie besäßen ein generelles persönliches Auskunftsverweigerungsrecht gegenüber jedermann. Diese irrige Ansicht wird durch den volkstümlichen Begriff „Arztgeheimnis" unterstützt. Richtig muß es jedoch **„Patientengeheimnis"** heißen. Geschützt werden soll nämlich nicht pimär der Arzt, sondern der Patient.

Nur in **Ausnahmefällen** kann dem **Patienten** eine **Auskunft verwehrt** werden, nämlich wenn entweder einer der im Gesetz abschließend geregelten Tatbestände vorliegt oder es aus therapeutischen Gründen erforderlich ist. Gerade für den Bereich der Psychiatrie hat die Rechtsprechung derartige Einschränkungen zugelassen.

Dies gilt jedoch nicht, wenn der **Datenschutzbeauftragte,** noch dazu wie hier ausdrücklich auf Bitten des Petenten hin, dessen Krankenakte einsieht. In solchen Fällen prüfen wir den gesamten Akteninhalt, teilen jedoch dem Petenten nur dasjenige mit, was er auch selbst durch eigene Akteneinsicht erfahren dürfte.

4.8 Kultusbereich

4.8.1 Datenschutz an der Schule

Die Bestellung schulischer Datenschutzbeauftragter kann sich positiv für den Datenschutz auswirken. Die Effizienz eines Datensicherungskonzeptes hängt davon ab, daß es sowohl die automatisierte als auch die konventionelle Verarbeitung der Daten einbezieht.

Das Landesdatenschutzgesetz verpflichtet die Behörden nicht ausdrücklich, einen Datenschutzbeauftragten zu bestellen. Wo dies geschieht, so stellen wir bei unseren Kontrollen fest, wirkt sich dies häufig positiv auf den rechtmäßigen und sicheren Umgang mit personenbezogenen Daten aus.

So auch in einem großen **Berufsschulzentrum,** bei dessen Kontrolle wir keine schwerwiegenden Mängel festgestellt haben. Datenschutz und Datensicherheit hatten dort einen hohen Stellenwert, eine **schulische Datenschutzbeauftragte** überwachte die Einhaltung der Bestimmungen.

Positiv fiel beispielsweise auf, daß jede **Lehrkraft** ein eigenes, **abschließbares Postfach** besitzt, über das vertrauliche Informationen zugeleitet werden können. Die **Zugangsregelung** zur schuleigenen **EDV-Anlage** war schlüssig und wirkungsvoll.

Negativ war allerdings zu bemerken, daß „mangels ausreichenden Platzes" **Klassenarbeitshefte ungesichert** und für jedermann zugänglich in einer Ecke im Schulsekretariat aufgestapelt lagen, um irgendwann einmal archiviert zu werden. Einige Karteien und Akten mit personenbezogenen Daten über Schüler fanden sich in offenen Regalen.

Diese Mängel wurden noch im Laufe der Prüfung abgestellt. Sie verdeutlichen einmal mehr, daß ein **Sicherungskonzept** nur dann überzeugend ist, wenn es für die elektronisch wie auch für die konventionell verarbeiteten Daten gleichermaßen wirksam ist. Denn an Schulen gilt wie überall, daß ein „perfektes" Sicherungssystem für die Computer wenig nützt, wenn die gleichen Informationen relativ ungesichert in Akten vorhanden sind.

4.8.2 Wenn die Verwaltung anonyme Hinweise erhält

Vielfach besteht Unsicherheit darüber, wie mit anonymen Schreiben zu verfahren ist, insbesondere was zu beachten ist, wenn aufgrund solcher Schreiben gegen anonym Beschuldigte Maßnahmen ergriffen werden.

Über einen Lehrer gingen beim **Kultusministerium** und bei der **Kraftfahrzeugzulassungsstelle** eines Kreises **anonyme Schreiben** ein, die ihn auf übelste Weise beschimpften. Es wurde behauptet, er führe einen unsittlichen Lebenswandel und sei trunksüchtig. Deshalb sei er weder als Lehrer und damit als Vorbild für seine Schüler geeignet, noch dürfe er ohne Gefahr für die Allgemeinheit ein Kraftfahrzeug führen.

Die **Kultusministerin** hatte die Schreiben „auf dem Dienstwege" über den zuständigen Schulrat dem Betroffenen aushändigen lassen. Hinweise darüber wurden in die Personalakte des Betroffenen nicht aufgenommen.

Der **Landrat als Verkehrsbehörde** hatte nach Rückfrage beim Betroffenen bei dem Kreis Erkundigungen veranlaßt, der den Führerschein des Betroffenen ausgestellt hatte. Seine eigenen Unterlagen hatte er daraufhin überprüft, ob gegen den Betroffenen straßenverkehrsrechtliche Maßnahmen bekannt waren und schließlich – auf wiederholtes Drängen des Betroffenen – ihn im einzelnen unterrichtet und ihm mitgeteilt, daß kein Anlaß für Maßnahmen gegen ihn bestehe.

Der Betroffene wandte sich gegen die Art, in der die anonymen Beschuldigungen behandelt wurden. Nach seiner Auffassung hätten aufgrund der Schreiben überhaupt keine Prüfungen durchgeführt werden dürfen, ihm diese statt dessen unverzüglich und unmittelbar zugeleitet werden müssen. Der Eingabenausschuß des Schleswig-Holsteinischen Landtages, an

den sich der Betroffene gewandt hatte, bat uns um Stellungnahme.

Wir haben uns dabei auf den Standpunkt gestellt, daß es grundsätzlich im **pflichtgemäßen Ermessen** der empfangenden Stelle liegt, wie sie anonyme Schreiben bewertet. Im wesentlichen lassen sich folgende Möglichkeiten unterscheiden:

- Die anonyme Information wird als belanglos betrachtet und vernichtet.
- Die Nachricht ist für die empfangende Stelle belanglos, bedeutet für Betroffene jedoch eine Belästigung, Belastung, Beleidigung oder einen ähnlichen Eingriff in die Persönlichkeitssphäre. Die empfangende Stelle wird die Nachricht dem Betroffenen aushändigen, um ihm die Möglichkeit eigener Maßnahmen zu eröffnen. Eines Rückbehalts bei der empfangenden Stelle bedarf es nicht.
- Die Nachricht ist für die empfangende Stelle prüfungsrelevant. Die Prüfung ergibt jedoch keinen Anlaß zu weiteren Maßnahmen. Die Prüfungsaktivitäten werden dokumentiert und damit personenbezogene Daten gespeichert.
- Die Informationen führen zu konkreten Mäßnahmen gegen Betroffene. Die Maßnahmen vollziehen sich sodann nach den einschlägigen Fachvorschriften in Verbindung mit den Datenschutzbestimmungen. Bei dienstlichen Maßnahmen ist dem Betroffenen Gelegenheit zur Stellungnahme zu geben. Die Unterlagen sind in diesem Fall – und nur in diesem Fall – zu den Personalakten zu nehmen.

Im konkreten Fall hat das Kultusministerium die Schreiben als belanglos betrachtet und sie dem Betroffenen für eigene Maßnahmen zugeleitet. Eine gezielte Datenerhebung lag nicht vor, da die Schreiben der Ministerin unverlangt zugesandt wurden. Nach der Entscheidung zur Abgabe an den Betroffenen waren sie im Kultusministerium nicht mehr erforderlich und wurden durch die Abgabe im Ministerium „gelöscht". Die Datenübermittlung an den Schulrat war nach Auffassung der Kultusministerin aus dem Gesichtspunkt der **Fürsorge** für den Betroffenen erforderlich, um auch dem nachgeordneten Bereich deutlich zu machen, daß solche Schreiben gegen den Betroffenen nach Auffassung des Ministeriums belanglos seien. Gegen diese Form der Rückgabe einschließlich der Datenübermittlung an den Schulrat bestehen grundsätzlich keine Bedenken.

Letztlich war auch die Vorgehensweise der Verkehrsbehörde nicht zu beanstanden, wenngleich es offenbar des Drängens durch den Betroffenen bedurfte, bis ihm die anonymen Schreiben eröffnet wurden.

Wenn nach alledem formelle Datenschutzverstöße auch nicht festgestellt werden konnten, so bleibt doch ein **Unbehagen** über die tatsächlichen Verwaltungsabläufe. Zum angemessenen Umgang mit so sensiblen Informationen wie derartigen anonymen Vorwürfen gehört eine sehr sorgfältige Auswahl

und Durchführung der notwendigen Verfahrensschritte. Hier wäre u.U. eine **zügigere Bearbeitung** im Kultusministerium, eine klare Unterrichtung des Betroffenen über das Verfahren und eine zusätzliche, deutliche Information der Schulaufsichtsbehörde von der ministeriellen Bewertung der Angelegenheit vorstellbar gewesen. In der Führerscheinangelegenheit hätte von vornherein durch eine **größere Offenheit** der Verkehrsbehörde gegenüber dem Betroffenen vermieden werden müssen, daß er die Behörde mehrfach persönlich drängen mußte, ihm den Sachverhalt zu erläutern und dabei den Eindruck erhielt, das Verfahren laufe nicht in rechtlich einwandfreier Weise ab. Solche Überlegungen gehören in den Gesamtzusammenhang des **fairen** und **sachgemäßen Umganges** mit personenbezogenen Daten und unterstreichen die besondere Bedeutung der Transparenzvorschriften des LDSG.

5. Datenschutz bei den Gerichten

5.1 Prozeßkostenhilfe hätte teuer werden können

Daten, die Bürger freiwillig im Rahmen der Beantragung von Prozeßkostenhilfe machen, dürfen nicht zur Vollstreckung staatlicher Forderungen gegen sie zweckentfremdet werden.

Nichts auf dieser Welt ist umsonst – schon gar nicht das Führen von Prozessen. Damit aber auch weniger finanzstarke Bürger ihr Recht bekommen, können sie bei Gericht **Prozeßkostenhilfe** beantragen. Dazu sind genaue Angaben über persönliche und finanzielle Verhältnisse erforderlich, aufgrund derer dann entschieden wird.

Informationen über die wirtschaftliche Situation eines Betroffenen sind jedoch auch für andere Behörden interessant, besonders, wenn es ihre Aufgabe ist, Geld einzutreiben. Vor diesem Hintergrund verlangte eine **Landesbezirkskasse** vom Arbeitsgericht in Lübeck die Übersendung von Prozeßkostenhilfeunterlagen, um daraus Erkenntnisse für die **Vollstreckung** anderer Forderungen zu ziehen.

Eine solche Auswertung hätte zur Folge gehabt, daß die Angaben zur Erlangung einer staatlichen Unterstützung unerwartet und in völlig anderem Zusammenhang zum **Nachteil des Betroffenen** verwendet worden wären. Sind Daten jedoch zu einem bestimmten Zweck erhoben worden, so dürfen sie grundsätzlich auch nur dazu genutzt werden.

Im vorliegenden Fall kam noch hinzu, daß es sich um ein Antragsverfahren handelte, dessen Durchführung ausschließlich vom Willen des Betreffenden abhing und in dem er alle **Informationen** über sich **freiwillig** und nur für diesen einen **bestimmten Zweck** preisgab. Für solche Fälle sieht das Landesdatenschutzgesetz ausdrücklich vor, daß die Daten nicht gegen den Willen des Betroffenen zu anderen Zwecken verwandt werden dürfen.

Dementsprechend lehnte die Justiz nach Erörterung der Sachlage mit uns eine Herausgabe der Akten ab.

5.2 Wenn der Gutachter kommt...

Zu weit gefaßte Gutachteraufträge durch Gerichte können leicht zu einer exzessiven Erhebung sensibler Daten führen. Der Gesetzgeber sollte Regelungen für die weitere Verwendung von Sachverständigengutachten in Gerichtsakten treffen.

Neben der Zeugenvernehmung ist das Sachverständigengutachten vor Gericht eines der am häufigsten genutzten Beweismittel. Wenn um Gesundheitszustand und körperliche Schäden vor Gericht gestritten wird, kommt einem medizinischen Gutachter zumeist prozeßentscheidende Bedeutung zu. Um hier nichts falsch zu machen, erteilen die Gerichte den Gutachtern gelegentlich sehr umfassend formulierte Aufträge. Nicht selten führt dies dazu, daß eine Fülle sehr **intimer Lebensumstände** in das Gutachten und damit in die **Gerichtsakten** Eingang findet, deren Zusammenhang mit dem Streitgegenstand sich dem unbefangenen Beobachter auch bei näherem Hinsehen nicht erschließt.

So führte ein Petent Klage darüber, daß er bei einem Streit über seine Gehfähigkeit **Testfragen** zu seinem **Denkvermögen** und seiner **geistigen Verfassung** beantworten mußte. Der Gutachter befragte ihn weiter nach seinen Kinderwünschen und den Konsequenzen, die er aus einem eventuellen Verlust des Prozesses ziehen wollte. All diese Angaben sowie sämtliche im Vorgespräch erörterten Themen fanden sich dann später im Gutachten wieder. Über den Weg der **Akteneinsicht** erhielt davon auch die **Gegenpartei** Kenntnis.

Selbstverständlich entscheidet jeder Richter in Unabhängigkeit darüber, welche Beweise er in welchem Umfang für erforderlich hält, um den Sachverhalt umfassend aufzuklären. Allerdings sollte auch über der alltäglichen Routine stets berücksichtigt werden, in welch außerordentlich hohem Maße die Intimsphäre eines Menschen ausgeleuchtet wird, wenn ihn ein medizinischer Sachverständiger begutachtet. Entsprechende Aufträge sollten deshalb sorgfältig formuliert und präzise auf die prozeßrelevanten Tatsachen beschränkt werden.

Zusammen mit anderen Datenschutzbeauftragten bemühen wir uns, den Gesetzgeber zu veranlassen, in die **Prozeßordnungen** Vorschriften aufzunehmen, die eine Datenerhebung durch Gutachter auf das dem Streitgegenstand entsprechend notwendige Maß beschränken.

Erforderlich sind auch Regelungen über die **weitere Verwendung** der in **Gerichtsakten** befindlichen Informationen nach Abschluß des Verfahrens. Dies gilt insbesondere auch im Hinblick auf die oben erwähnten Gutachten. Wer als Proband freiwillig mit Blick auf den Ausgang eines Verfahrens mitarbeitet und die Arbeit des Sachverständigen so erst ermöglicht oder wesentlich erleichtert, muß Gewißheit darüber haben, ob

und wenn ja, in welchem Umfang die zur Verfügung gestellten Daten über den ursprünglichen Zweck hinaus auch nach Abschluß des Verfahrens weiter verwandt werden dürfen.

6. Ordnungsmäßigkeit der Datenverarbeitung

6.1 Leitaussagen zur Informationstechnik in der öffentlichen Verwaltung – IT-Szenario –

Der Kooperationsausschuß ADV legt ein Grundsatzpapier mit Leitaussagen zur EDV in der öffentlichen Verwaltung vor, die sich weitgehend mit Positionen des Datenschutzes decken.

Im letzten Tätigkeitsbericht (15. TB, S. 99) wurde über richtungsweisende Empfehlungen der Automationskommission der kommunalen Landesverbände zur Weiterentwicklung der technikunterstützten Informationsverarbeitung in der Kommunalverwaltung Schleswig-Holsteins berichtet. Zugleich wurde bedauert, daß die Feststellungen und Aussagen dieses Gremiums so wenig Widerhall in der Verwaltung und bei den Herstellern und Vertreibern von Informationstechnik gefunden haben.

Es bleibt zu hoffen, daß ein mindestens ebenso bedeutsames (weil bundesweit abgestimmtes) Grundsatzpapier des **„Kooperationsausschusses ADV Bund/Länder/kommunaler Bereich"** mit Leitaussagen zur Informationstechnik in der öffentlichen Verwaltung, das auch ein sogenanntes „IT-Szenario" enthält, mehr Beachtung erfährt.

Aus unserer Sicht sind folgende **Feststellungen** dieses Arbeitskreises von IT-Fachleuten aus allen Verwaltungsbereichen von **besonderer datenschutzrechtlicher Bedeutung:**

- Die Nutzung von Informationstechnik hat erhebliche **wirtschaftliche** und **soziale Folgen.** Sie bestimmt maßgebend die Aufgabenwahrnehmung öffentlicher Verwaltungen gegenüber Bürgerinnen und Bürgern sowie der Wirtschaft und hat daneben wesentliche Auswirkungen auf einen Großteil der Beschäftigten in der Verwaltung.
- Eine **Sättigung des Bedarfs** an weiterer Informationstechnik ist in der Verwaltung **nicht erkennbar.** Der gegenwärtige Ausstattungsstand dürfte sich bis zum Ende dieses Jahrzehnts mindestens verdoppeln bis verdreifachen.
- Mit jeder erreichten Technikausstattung tritt eine unumkehrbare Veränderung ein, die eine verstärkte Sicherung und Vorsorge gegen Risiken der gravierend gesteigerten **Verwundbarkeit der Verwaltung** erfordert.
- Grundlage für die Nutzung der Informationstechnik müssen **Organisations-, Technik-** und **Sicherheitskonzepte** sein, in denen die fachlichen und organisatorischen Voraussetzungen für die Nutzung von Informationstechnik analysiert sowie die potentiellen Anwendungen der betreffenden In-

formationstechnik grob beschrieben und zusammengefaßt werden.

- Wegen der Anforderungen an die Gestaltungs- und Integrationskraft werden **kleinere Verwaltungen** zunehmend außerstande sein, **komplexe IT-Anwendungen** selbst zu erstellen.

- Der Einsatz **konfektionierter IT-Anwendungen** auf der Basis übergreifender Zielsetzungen und Vorgaben sowie von Normen und Standards sollte der dem fachlichen Einzelfall optimal angepaßten IT-Anwendung vorgezogen werden. Die jeweilige Entscheidung sollte dabei im Zweifel eher im Sinne kostengünstiger, schnell verfügbarer und übertragbarer IT-Anwendungen getroffen werden. Durch die Abwägung von Qualitätsanforderungen muß jedoch zugleich deutlich werden, daß es sich **nicht um** eine **einseitige Orientierung** an den zu minimierenden **Kosten** handelt.

- Die zunehmende Nutzung der Informationstechnik bringt eine Erhöhung der Gefahr durch unrichtige, unbefugt gesteuerte, fehlende oder rechtsgutgefährdende Informationen mit sich. Deshalb kommt der **IT-Sicherheit** eine **besondere Bedeutung** zu. Hierbei geht es um den Schutz vor möglichen Bedrohungen, die die Verfügbarkeit der Informationstechnik sowie die Integrität und die Vertraulichkeit der verarbeiteten Informationen gefährden.

- Die grundlegenden Forderungen nach **IT-Sicherheit** haben zur Folge, daß dieser Anspruch als ein **gleichrangiges Ziel** neben die allgemeinen **Nutzungs- und Leistungsmerkmale** der Informationstechnik tritt. Als notwendig erkannte Maßnahmen der IT-Sicherheit sind auch dann zu treffen, wenn sie die Entwicklung einer IT-Anwendung erschweren. Dies kann sogar so weit gehen, daß im Einzelfall von der Nutzung der Informationstechnik abzusehen ist, wenn notwendige Sicherheitsforderungen nicht erfüllbar sind.

- Neue IT-Anwendungen verlangen **Aufklärung, Schulung** und **Betreuung** der Beschäftigten. Hiermit ist eine besondere Herausforderung an die Personalführung verbunden. Die Schulung und die mit ihr angestrebte Beherrschung der Technik dienen der Sicherung der Akzeptanz, eröffnen den Benutzern aber auch die Möglichkeit, den von der Anwendungssoftware gebotenen Freiraum eigenständig zu gestalten. Eine vernünftige Schulung und Einweisung schafft damit die Voraussetzung für den **„mündigen" Benutzer.**

- Akzeptanzsicherung bedeutet jedoch nicht nur, daß personelle und organisatorische Maßnahmen im Interesse der Beschäftigten zu treffen und **ergonomische Normen und Standards** zu beachten sind. Dazu gehört insbesondere auch, daß das **Recht der Bürgerinnen** und **Bürger** auf **informationelle Selbstbestimmung** gewahrt wird, so daß

sie ihre Daten bei der Verwaltung in sicheren Händen wissen.

- Auf der **Führungs-** und **Leitungsebene** sind Problembewußtsein und auch Fachkenntnis über Nutzungspotentiale und Entscheidungskriterien in bezug auf Informationstechnik nachdrücklich weiter zu fördern, damit die durch die Nutzung von Informationstechnik herbeigeführte Verwaltungsinnovation nicht allein eine Angelegenheit der hierfür eingesetzten Spezialisten bleibt, sondern von den hierfür verantwortlichen Leitungs- und Führungskräften kompetent und bewußt geplant, gesteuert und überwacht werden kann.

Der Kooperationsausschuß ADV geht davon aus, daß die folgenden **Entwicklungen** die Nutzung der Informationstechnik in den **nächsten Jahren** bestimmen werden:

- Papierloses Büro bleibt Utopie,
- elektronische Kommunikation nimmt weiter zu,
- grafische Benutzeroberflächen werden sich verbreiten,
- der integrierte Arbeitsplatz rückt näher,
- elektronische Vorgangsbearbeitung kommt,
- offene Systeme setzen sich durch,
- verteilte Anwendungen erhalten größere Bedeutung,
- grafische Informationsverarbeitung wird wichtig,
- Sprachverarbeitung steigt in der Bedeutung,
- Software-Engineering ersetzt „freies Künstlertum",
- Anforderungen an die Sicherheit der Informationstechnik nehmen zu,
- entscheidungsunterstützende Informationssysteme werden praktikabler,
- Akzeptanz steigt,
- Umgang wird selbstverständlich.

Wir halten die vorstehenden Überlegungen deshalb für so wichtig, weil sie sich nicht nur in weiten Teilen mit den Erfahrungen von Datenschutzbeauftragten decken, sondern von **professionellen Datenverarbeitern** erarbeitet worden sind. Sie sind deshalb nicht nur als abstrakte Konzeption zu verstehen, sondern eignen sich auch als ein wesentlicher Maßstab für die datenschutzrechtliche Beurteilung von Sachverhalten, die im Rahmen von Prüfungen und Beratungen bekannt werden.

Auch in den Erörterungen über die datenschutzrechtlichen Aspekte der **Sicherheit** und **Ordnungsmäßigkeit** der Datenverarbeitung werden wir uns an den Aussagen des „IT-Szenarios" orientieren.

6.2 Entwurf der Datenschutzverordnung in der Anhörung

Der Entwurf der Verordnung über die Sicherheit und Ordnungsmäßigkeit bei der automatisierten Verarbeitung personenbezogener Daten berücksichtigt inhaltlich die wesentlichen Vorstellungen des Landesbeauftragten

Trotz der wiederholt dargestellten und begründeten Dringlichkeit (vgl. 15. TB, S. 91) ist es bisher noch nicht gelungen, die Landesverordnung über die Sicherheit und Ordnungsmäßigkeit bei der automatisierten Verarbeitung personenbezogener Daten zu verabschieden.

Wegen der unbestreitbaren Schwierigkeit, technikorientierte Sachverhalte durch rechtliche Normen zu erfassen, haben wir uns zu Beginn des Berichtsjahres entschlossen, dem Innenminister einen **eigenen Verordnungsentwurf** zur Verfügung zu stellen. Diese Initiative führte immerhin dazu, daß im August ein Innenminister-Entwurf in die Ressortanhörung gehen konnte und uns gem. § 7 Abs. 4 Satz 3 Landesdatenschutzgesetz zur Stellungnahme vorgelegt wurde.

In unserer Antwort haben wir deutlich gemacht, daß sich die Verordnungsermächtigung im Landesdatenschutzgesetz gerade dadurch auszeichnet, daß dem Verordnungsgeber detaillierte Vorgaben bezüglich der **Struktur und** des **Inhalts** der zu schaffenden **Regelungen** gemacht worden sind. Deshalb hätten wir es vorgezogen, die Verordnung in **5 Regelungskomplexe** zu gliedern:

- Allgemeine Beschreibung des Begriffes „ordnungsgemäße Datenverarbeitung",
- Konkretisierung von technischen und organisatorischen Maßnahmen für bestimmte Systemkonfigurationen und Anwendungsbereiche,
- Definition von Mindestanforderungen an die Dokumentation von automatisierten Datenverarbeitungsprozessen,
- Regelungen zur formalen Darstellung von Verfahrensdokumentationen,
- Festlegung von Aufbewahrungsfristen für Dokumentationsunterlagen.

Eine solche Strukturierung hätte die Fortschreibungen von Einzelbestimmungen, wie sie in Zukunft insbesondere im Bereich „Anpassung an den Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen" in relativ kurzen Zeitabständen erforderlich sein werden, vereinfacht.

Der vom **Innenminister** zur Stellungnahme vorgelegte **Entwurf** geht von einem **anderen Aufbau** aus. Es ist versucht worden, das Textvolumen möglichst gering zu halten und sich weitgehend der Begriffe aus dem Bereich der „konventionellen" Organisation zu bedienen.

So sehr die Komprimierung auf der einen Seite Vorteile hat, so sehr befürchten wir andererseits, daß der Entwurf der vom

Verfassungsgericht geforderten Normenklarheit insoweit nicht hinreichend gerecht wird.

Da allerdings die überwiegende **Mehrzahl** unserer **Regelungsvorschläge inhaltlich** in dem Entwurf ihren Niederschlag gefunden hat und die datenverarbeitenden Stellen im Lande auf ein **kurzfristiges Inkrafttreten der Verordnung** drängen, haben wir diese grundsätzlichen Bedenken zurückgestellt und unsere Stellungnahme auf einzelne Tatbestände des Verordnungsentwurfes beschränkt.

Im Verlaufe der Anhörung zum Kabinettsentwurf der Verordnung werden wir diejenigen Punkte zur Sprache bringen, die unseres Erachtens noch nicht sachgerecht geregelt sind. Dazu gehört z. B. die Problematik der **Dokumentation automatisierter Verfahren** mit Hilfe von „CASE-Tools". In diesen Fällen ist nämlich auch die Dokumentation in einem Computer gespeichert und nur lesbar, wenn die „Sprache" des Speicherprogramms (Tool) bekannt ist.

6.3 Automatisierte Textbearbeitung „verführt" zu überflüssigen Datenbeständen

In den meisten Dienststellen kommen inzwischen „Schreibautomaten" zum Einsatz. In deren Speicher entstehen Sammlungen mit „Kopien" aller gefertigten Schreiben. Die daraus resultierenden Datenschutzprobleme werden häufig unterschätzt.

Entsprechend der technischen Entwicklung wird in den letzten Jahren in praktisch allen Behörden der **Schreibdienst** einer **grundlegenden Neuorganisation** unterzogen. Auf den ersten Blick dokumentiert sich dies lediglich in dem Austausch der Schreibmaschinen gegen Personalcomputer mit angeschlossenen Druckern und einer Reduzierung der Schreibdienst-Arbeitsplätze wegen der größeren Effektivität im Korrektur- und Änderungsdienst und der Rückverlagerung der Schreibarbeiten in die sachbearbeitende Ebene. Häufig bleibt hinter dieser Oberfläche aber verborgen, daß die automatisierte **Textbearbeitung** bisher nicht bekannte **personenbezogene Datenbestände** erzeugt.

Wurde **in der Vergangenheit** im Sekretariat ein Schreiben gefertigt, gelangte die Durchschrift in die Akte und das Original wurde abgesandt. Das **Sekretariat** arbeitete **„rückstandsfrei"**, weil die Seiten mit Tippfehlern und dergleichen spätestens abends vernichtet wurden.

Heute werden auf den Festplatten der PC von allen Schreiben Kopien angelegt, damit bei Korrekturwünschen nur die geänderten Texte einzugeben sind und das Dokument neu ausgedruckt werden kann. Wegen der praktisch **kostenlosen Speicherkapazitäten** (bereits die gängigen Minimalkonfigurationen der PC lassen die Speicherung der Inhalte ganzer Akten-

schränke zu) macht man sich über Löschungsfristen in der Regel keine Gedanken.

Das führt zu umfangreichen **Sammlungen** von Dokumenten mit teilweise **„hochbrisanten" Inhalten.** Wenn man nur wollte, könnte man diese Dateien mit „Standardwerkzeugen" der benutzten Texteditoren nach allen interessanten Merkmalen durchsuchen. Obwohl die Schreiben als „unformatiert" gelten, stellen sie in ihrer Summe eine **große Datenbank** dar.

Dies zwingt eigentlich dazu, die Daten zum frühestmöglichen Zeitpunkt zu löschen und sie bis dahin besonders wirksamen Sicherungsmaßnahmen zu unterwerfen. Der **Sicherheitsstandard** müßte sich nach den Erfordernissen des jeweils **„sensibelsten"** Schreibens richten.

Soweit die **Theorie.** Die **Praxis** zeichnet ein **anderes Bild:**

- Den Dateien der Texteditoren wird sowohl von den Datenverarbeitungsabteilungen wie auch von den Fachabteilungen in der Regel nur eine geringe Beachtung beigemessen. Für die einen geht es vorrangig um das Funktionieren der Software, für die anderen steht im wesentlichen der Änderungskomfort für die Schriftstücke im Vordergrund.

- Wegen des sehr heterogenen Inhalts der Dateien erscheint die Zuweisung einer hohen Sicherheitsstufe unangemessen und wegen der damit verbundenen Restriktionen „anwenderunfreundlich".

- Da man sich nie ganz sicher sein kann, wann man einen Text noch einmal „gebrauchen" könnte, wirken kurze Löschungsfristen vermeintlich nur störend.

Der Blick der Verantwortlichen für die Risiken (und Überflüssigkeiten) wird sich wohl erst aufgrund der zu erwartenden künftigen Datenschutzskandale und „Skandälchen" schärfen. Dies ist jedenfalls nach unseren Erfahrungen zu befürchten.

6.4 „Spätfolgen" bei Telefax-Anschlüssen

Eine sehr spezifische Form der Technikfolgenabschätzung ist erforderlich, wenn Behörden Telefaxgeräte einsetzen. Ein späterer Wechsel der Telefaxnummer muß rechtzeitig bedacht werden.

Wechselt ein Telefax-Anschlußinhaber (also jeder, der mit oder ohne Wissen der Telekom ein Faxgerät an einen normalen Telefonanschluß angeschlossen hat) seine Telefonnummer, weil er z.B. sein Büro in einen anderen Stadtteil verlegt hat, wird die alte Nummer nach einer in der Regel recht kurzen Zeit von der Post einem neuen Fernsprechteilnehmer zugewiesen. Dieser Umstand läßt zunächst keine datenschutzrechtliche Relevanz erkennen. Sie ergibt sich erst bei einem Szena-

rio, das künftig in der Praxis häufiger eintreten wird, als es den Beteiligten lieb sein dürfte:

- Eine **Behörde** schließt ein **Fax-Gerät** an und macht in ihrem Briefkopf allen Korrespondenzpartnern deutlich, daß sie bereit ist, neben Briefen und Telefonanrufen auch Telefaxe (unter der angegebenen Nummer) zu empfangen.
- Über die Jahre **„streut"** sie diese **Fax-Nummer** (mit jedem ausgehenden Brief) an tausende von Stellen und Personen.
- Die Behörde zieht um und erhält gezwungenermaßen eine **neue Telefon-/Telefax-Nummer.**
- In der ersten Zeit wundern sich einige Bürger, daß die von ihnen abgesandten **Faxe** von der Behörde **nicht ordnungsgemäß empfangen** werden können. Erst auf Nachfragen werden sie von der Behörde über die neue Fax-Nummer aufgeklärt.
- Ein Teil der Korrespondenzpartner erfährt zwar von dem Umzug durch den neuen Briefkopf der Behörde, durch unzustellbare Schreiben oder im Rahmen von Telefonkontakten. Ein anderer Teil geht aber auch nach längerer Zeit davon aus, daß die in den Unterlagen vorhandenen Angaben nach wie vor aktuell sind. Wird weiterhin „reibungslos" über Telefax kommuniziert, obwohl inzwischen ein ganz anderer Teilnehmer an die bisherige Behördennummer sein eigenes Telefax-Gerät angeschlossen hat, so merken die Absender nichts von den von ihnen erzeugten **„Irrläufern".** Wenn der falsche Adressat sie zudem nicht auf den Fehler aufmerksam macht, kann er über lange Zeiträume die an die Behörde gerichtete Korrespondenz mitlesen.

Aus diesen durchaus praxisnahen Gegebenheiten gilt es **Folgen** zu **ziehen.** Gefordert sind insbesondere die Behörden,

- bei denen ein **künftiger Rufnummernwechsel wahrscheinlich** ist (z.B. weil sie gemietete Räume nutzen),
- die mit einer so **großen Anzahl** von **Bürgern korrespondieren,** daß nicht alle von einem Fax-Nummernwechsel unterrichtet werden können (z.B. Kommunal-, Steuer- oder Sozialbehörden),
- die damit rechnen müssen, daß Bürger in Erwartung einer hinreichend abgesicherten Behandlung der Faxe im Behördenbereich auf diesem Wege **Daten** übermitteln, die einem **besonderen Berufs-** oder **Amtsgeheimnis** unterliegen oder die sonst als besonders **„sensibel"** gelten (Sicherheitsbehörden, Amtsärzte, Finanzämter, Sozialämter, Krankenhäuser).

Diejenigen, die Bürgerinnen und Bürger zu einer Korrespondenz via Telefax auffordern, können sich der **Verantwortung** für einen **ordnungsgemäßen Empfang** nicht entziehen. Ggf. muß deshalb eine Neubelegung der betreffenden Telefonnummer durch vertragliche Vereinbarungen mit der Telekom ausgeschlossen werden. Eine andere Möglichkeit wäre, die alte Telefonnummer für einen angemessenen Zeitraum noch bei

der Telekom zu mieten, was lediglich die Kosten für die Grundgebühr verursachen würde.

Behörden müssen sich, bevor sie einen Fax-Anschluß einrichten, über diese Aspekte klar werden und **rechtzeitig** an ggf. notwendige **Vorkehrungen** denken (vgl. hierzu auch 14. TB, S. 69).

6.5 Von der Realität eingeholt

Der zunehmende Einsatz tragbarer Datenverarbeitungsgeräte erhöht die Gefahr des Datendiebstahls. Die Verschlüsselung der Daten könnte das Schlimmste verhindern.

Seitdem in der Verwaltung tragbare Personalcomputer, sogenannte **Laptops,** eingesetzt werden, fordern wir die betreffenden Behörden dazu auf, nicht nur die Betriebssysteme und Programme durch Überprüfung der Identität der Benutzer (Eingabe einer Benutzerkennung und Überprüfung anhand eines zusätzlichen persönlichen Schlüsselwortes) gegen unbefugte Zugriffe zu sichern, sondern auch die **Dateien zu verschlüsseln.** Auf andere Weise ist die unbefugte Kenntnisnahme der gespeicherten Daten nämlich nicht wirksam zu verhindern, da bei diesen Geräten (wenn sie z.B. gestohlen oder auf andere Weise in fremde Hände gelangt sind) die Festplatten relativ leicht ausgebaut und in anderen Geräten (ohne Sicherheitskontrollen) gelesen werden können. Wegen der stark steigenden Tendenz der Verwendung dieser Geräte in den Behörden außerhalb der Diensträume haben wir auch vorgeschlagen, derartige Sicherungsmaßnahmen im Rahmen der **Datenschutzverordnung** (vgl. Tz. 6.2 dieses Berichtes) den datenverarbeitenden Stellen als Pflicht aufzuerlegen.

Auf eine besondere Resonanz sind diese Aktivitäten bisher nicht gestoßen. Die Gesprächspartner hielten das Risiko des Diebstahls oder Verlustes für so gering, daß der Verschlüsselungsaufwand (gemeint waren offenbar die Kosten in Höhe von wenigen hundert Markt pro Gerät, denn die Verschlüsselung selbst führt zu kaum meßbaren Zeitverlusten) nicht gerechtfertigt sei. Daß eine solche Einschätzung sehr schnell von der **Realität** überholt werden kann, wird durch nachstehende Annonce (durch uns anonymisiert) belegt:

> **1000,– Belohnung** für die Wiederbeschaffung eines IBM Laptops. Wurde am 18.11.93 aus einem gelben Mercedes in der str. entwendet. Keine Anzeige. Keine Fragen.
> Infos bei
> (Die. 9–18 Uhr, Mi. 9–12 Uhr, Do. 9–13 Uhr)

Unsere Nachforschungen haben ergeben, daß das **Gerät aus** einem **Pkw gestohlen** worden ist, der nur eine kurze Zeit unbeaufsichtigt war. Der Schaden lag weniger im Verlust des Gerätes als vielmehr im Verlust der Daten, da nicht einmal Sicherheitskopien der Dateien angefertigt worden waren. Aber auch die Dateninhalte waren nicht für Dritte bestimmt. Für den Bestohlenen (eine Privatperson) steht nach diesem Erlebnis außer Frage, daß er künftig von der Möglichkeit der Dateiverschlüsselung Gebrauch machen wird.

Wir haben aus diesem Fall die Erkenntnis gewonnen, daß die Behauptung „es ist ja bisher noch nichts passiert" kein tragfähiges Argument für den Verzicht auf **logisch sinnvolle Sicherungsmaßnahmen** sein kann.

6.6 Ergebnisse von Prüfungsmaßnahmen im Bereich der automatisierten Datenverarbeitung

6.6.1 Datenzentrale meldet Abschluß der Maßnahmenumsetzung

Die Umsetzung unserer Beanstandungen und Verbesserungsvorschläge gegenüber der Datenzentrale ist abgeschlossen.

Die datenschutzrechtlichen Beanstandungen und Verbesserungsvorschläge datieren vom Oktober 1990. Mit Schreiben vom Dezember 1993 hat die Datenzentrale Schleswig-Holstein nunmehr **„Vollzug gemeldet".** Sie hatte zwar in einem Halbjahresrhythmus stets über den Fortgang der Arbeiten zur Umsetzung der Forderungen und Anregungen aus einer Prüfungsmaßnahme im Jahr 1990 unterrichtet (vgl. 13. TB, S. 73, 14. TB, S. 25), es bedurfte aber eines Zeitraumes von fast 40 Monaten, um zu einem Abschluß zu gelangen. Auf die grundsätzlichen Probleme der Zeitkomponente bei der Behebung von festgestellten Mängeln haben wir bereits an anderer Stelle hingewiesen (vgl. 15. TB, S. 8 und Textziffer 6.6.2 dieses Berichtes).

Unabhängig davon ist in bezug auf die Aktivitäten der Datenzentrale festzustellen, daß unsere Forderungen und die neue Unternehmensphilosophie der Datenzentrale einige **grundlegende Veränderungen** bewirkt haben. Es besteht nunmehr Übereinstimmung darin, daß auch sicherheitstechnisch zwischen den Funktionen der Datenzentrale als Hardware-Lieferant, als Software-Haus und als Rechenzentrum unterschieden werden muß. Hieraus ergibt sich z.B. die praktische Konsequenz, daß Mitarbeiter aus den Verkaufs-und Entwicklungsbereichen nicht im Rechenzéntrum und Kundendaten nichts in den Verkaufs- und Entwicklungsbereichen „zu suchen haben". Außerdem darf das Rechenzentrum grundsätzlich nur mit solchen **Programmen** arbeiten, die von den Auftraggebern der Datenzentrale ein **Freigabetestat** erhalten haben.

Die Realisierung allein dieser beiden Forderungen hat die Datenzentrale offenbar vor signifikante Probleme gestellt. Immerhin spricht sie auch in ihrem Abschlußbericht davon, daß in einzelnen Bereichen „wegen Überbeanspruchung unserer Programmierkapazitäten noch keine weiteren Fortschritte gemacht worden sind"; seit Oktober 1993 habe sie deshalb eine **Interimslösung** realisiert.

Die Optimierung von Maßnahmen zum **Datenschutz** und zur **Datensicherheit** sehe sie aber als **Daueraufgabe** auch im Zusammenhang mit Änderungen in der Organisationsstruktur aufgrund der Realisierung des neuen Unternehmenskonzeptes an.

Wir werden die tatsächlichen Auswirkungen der getroffenen Maßnahmen in den nächsten Jahren im Rahmen von **punktuellen Prüfungsmaßnahmen** untersuchen und bewerten.

6.6.2 Beanstandungen akzeptiert – Abhilfe auf die lange Bank geschoben?

Die Stadt Kiel hat umfangreiche Konsequenzen aus der datenschutzrechtlichen Kontrolle angekündigt. Konkrete Maßnahmen und präzise Terminvorstellungen wurden aber noch nicht genannt.

Im letzten Tätigkeitsbericht (15. TB, S. 89) haben wir über die Ergebnisse einer umfassenden Überprüfung der automatisierten Datenverarbeitung bei der **Landeshauptstadt Kiel** berichtet und angekündigt, wir würden die von der Stadt konkret getroffenen Maßnahmen demnächst darstellen.

Hierzu sehen wir uns leider noch nicht in der Lage, weil die geprüfte Stelle bisher lediglich **Absichtserklärungen** abgegeben hat. Die Auswertung der sechs Monate nach Übersendung der Prüfungsniederschrift eingegangenen Stellungnahme der Stadt hat zwar ergeben, daß in allen **wesentlichen Punkten Übereinstimmung** in der datenschutzrechtlichen Bewertung der im Rahmen der Prüfung festgestellten Sachverhalte besteht. Hierin ist ein positiver Ansatz für die konkrete Behebung der festgestellten datenschutzrechtlichen Defizite und die Realisierung der Verbesserungsvorschläge zu sehen.

Trotz der als Grund für die Verzögerung genannten organisatorischen Umstellungen im Bereich des Amtes für Organisation und Verwaltungsreform erscheint es uns aber angesichts der rechtlichen Tragweite der festgestellten Mängel **unumgänglich,** daß die Absichtserklärungen der betroffenen Ämter und Personen in einem **definierten Zeitrahmen** umgesetzt werden. Wir haben die Stadt deshalb aufgefordert mitzuteilen, wann jeweils mit der Umsetzung begonnen wird und wann mit einem Abschluß zu rechnen ist.

Die Bandbreite der erforderlichen Aktivitäten ergibt sich aus folgender Zusammenstellung der **„offenen Posten":**

- Überarbeitung der Geschäftsanweisung für die EDV-Abteilung,
- Schaffung eines Gesamtkonfigurationsplanes und eines einheitlichen, vollständigen und aktuellen Geräteverzeichnisses,
- Regelung der Funktionen der EDV-Verbindungsleute in einer Dienstanweisung,
- Überarbeitung der Geschäftsanweisung zum Schutz der Datenträger,
- Neuerstellung der Dateibeschreibungen,
- Anonymisierung von Testdaten,
- Veränderung bzw. Vervollständigung des Testdatenbestandes im Einwohnerwesen,
- Protokollierung von Zugriffen der Programmierer auf „Echtbestände",
- schriftliche Fixierung der Konventionen für die Behandlung von Meldedaten,
- Erstellung einer Dienstanweisung für Systemkoordinatoren,
- Verbesserung der Eingabekontrolle,
- Verbesserung der Raumsituation im Einwohnermeldeamt,
- Erstellung von Dienstanweisungen und Erarbeitung spezifizierter Datensicherungsmaßnahmen in mehreren Bereichen der Stadtverwaltung,
- Erstellung eines Schulungskonzeptes,
- Verabschiedung eines von allen Beteiligten akzeptierten Konzeptes für die Fortentwicklung der automatisierten Datenverarbeitung,
- Neuregelung der Aufgabenabgrenzung zwischen den Fachabteilungen und der EDV-Abteilung,
- Verhandlung über Vertragsänderung mit einem Service-Rechenzentrum.

Der Oberbürgermeister der Landeshauptstadt Kiel hat daraufhin seine terminlichen Vorstellungen in einigen Punkten konkretisiert, aber keine definitiven Zeitpunkte für das Wirksamwerden konkreter Maßnahmen genannt. Formulierungen wie „der Erledigungszeitpunkt ist bisher noch nicht abzusehen", „ein konkreter Termin kann nicht festgelegt sein" und „.... -Konzept wird erarbeitet" lassen befürchten, daß damit ein Hinausschieben „auf die **lange Bank**" nicht anzuschließen ist. Wir werden deshalb darauf drängen, daß den guten Absichten bald auch Taten folgen. Denn angesichts der umfangreichen Automatisierungsvorhaben bei der Stadt Kiel kommt der rechtzeitigen datenschutzgerechten Gestaltung der Abläufe eine besondere Bedeutung zu.

6.6.3 Die automatisierte Datenverarbeitung in einer anderen Großstadt – wie die Probleme sich gleichen

Die Kontrollen der automatisierten Datenverarbeitung in mittleren und größeren Kommunalverwaltungen haben im Berichtsjahr sowie in den vergangenen Jahren zur Feststellung übereinstimmender Mängel geführt.

Überprüfungen **„vor Ort"** haben in erster Linie den Zweck, Mängel und Schwachstellen bei den betreffenden datenverarbeitenden Stellen aufzudecken und ihre Behebung, zumindest aber eine Verbesserung des Datenschutzes zu bewirken. Daneben dienen sie aber auch dazu, über den Einzelfall hinausgehende Grundsatzfragen und -probleme aufzuzeigen sowie allgemeine sicherheitstechnische Fragestellungen im Zusammenhang mit dem Einsatz von Informationstechnik in der öffentlichen Verwaltung einer vergleichenden Analyse zu unterziehen.

Aus diesem Grunde haben wir unmittelbar im Anschluß an die Nachschau bei der Stadt Kiel (vgl. 15. TB, S. 85 und Tz. 6.6.2 dieses Berichts) mit einer gleichartigen Prüfungsmaßnahme bei der **Stadt Flensburg** begonnen. Die Ergebnisse zeigen eine **weitgehende Übereinstimmung** bezüglich der **datenschutzrechtlichen** Mängel und Schwachstellen im Bereich der technischen und organisatorischen Sicherheitsmaßnahmen. Faßt man diese und die Ergebnisse aus anderen Prüfungen zusammen, können folgende Sachverhalte als generelle Probleme beim Einsatz von Informationstechnik in mittleren und großen Kommunalverwaltungen angesehen werden:

- Es mangelt an klaren **aufbauorganisatorischen Maßnahmen.** Die Einbettung der Organisationseinheiten, die als „Dienstleister" auf dem Gebiet der Informationstechnik fungieren, in das Gesamtgefüge der Behörde ist nicht frei von Schnittstellenproblemen. Bezüglich der konkreten Verantwortung für Mängel und Sicherheitsrisiken verweist nicht selten die EDV-Abteilung auf die Fachabteilung und umgekehrt (**Beispiel:** Wer entscheidet über die sicherheitstechnische Minimalausstattung von Personalcomputern in einem Gesundheitsamt, der Amtsarzt oder der EDV-Leiter? Wer trägt die Verantwortung für sicherheitstechnische „Restrisiken"? Wer ist gegenüber den Systemadministratoren weisungsberechtigt?).

- Aus den aufbauorganisatorischen Schwachstellen folgen **ablauforganisatorische Mängel.** Die entsprechenden Anweisungen und Regelungen sind unvollständig oder so veraltet, daß eine Nichtbeachtung „in der Natur der Sache" liegt (**Beispiel:** Wenn eine Dienstanweisung zwar die DV-Organisation von vor fünf Jahren durchaus sachgerecht reglementiert, auf die Besonderheiten des aktuellen PC-Einsatzes aber nicht eingeht, ist es nicht verwunderlich, wenn sie insgesamt nicht mehr beachtet wird.).

- Einzelnen Mitarbeitern in den Fachabteilungen werden EDV-orientierte Funktionen übertragen, ohne daß sie ent-

sprechend ausgebildet sind und schriftlich festgelegt ist, welche **Verantwortung** und **Befugnisse** damit verbunden sind (**Beispiel:** Bevor jemand zum EDV-Koordinator, Systembetreuer oder zum Datenschutzbeauftragten ernannt wird, muß ihm gesagt werden, welche Arbeitsergebnisse von ihm erwartet werden und auf welche Art und Weise sie erbracht werden sollen.).

- Werden Fachabteilungen erstmals mit informationstechnischen Systemen ausgerüstet und die Verfahrensabläufe automatisiert, wird aus Zeit- und Kostengründen die **Schulung** der Mitarbeiter **auf die verfahrensspezifischen Aspekte begrenzt** (**Beispiel:** Vorgesetzte und Sachbearbeiter erfahren zwar, wie Daten einzugeben sind, nicht aber wann und wie eine Löschung zu erfolgen hat; in der Fachabteilung bleibt weitgehend unbekannt, welche Konsequenzen sich ergeben, wenn ein IT-Gerät nicht so benutzt wird, wie es eigentlich vorgeschrieben ist oder was passiert, wenn – was an sich verboten ist – doch eine Diskette in das entsprechende Laufwerk eingeschoben wird oder welche Folgen ein „Programmabsturz" hat.).

- „Durchgängige", gleichwohl „angemessene" **Sicherheitskonzepte** für die gesamte datenverarbeitende Stelle sind insbesondere bei großen Behörden sehr selten zu finden. Einerseits gibt es immer wieder Fachabteilungen, die für sich Sonderrechte reklamieren und zugestanden bekommen, so daß **Insellösungen** toleriert werden. Andererseits werden die Fachabteilungen nicht grundsätzlich in die Pflicht genommen, ihre spezifischen (rechtlich begründeten) Sicherheitsanforderungen selbst zu definieren und der EDV-Abteilung als Vorgabe für die Hardware- und Softwareauswahl zur Verfügung zu stellen (**Beispiel:** Die zweckgebundene Bereitstellung von Haushaltsmitteln für bestimmte IT-Projekte durch politische Gremien befreit nicht von einer „professionellen" Erarbeitung eines Sicherheitskonzeptes: das Problem der Zugriffsberechtigung auf Datenbestände in einem Gesundheitsamt oder in einem Krankenhaus ist mit Rechtsfragen verbunden, deren Klärung nicht von der EDV-Abteilung erwartet werden kann.).

- Der Übergang von der Entwicklung (Erprobung) der automatisierten Verfahren in die Produktionsphase erfolgt fast immer „fließend". Ein **systematischer Verfahrenstest** und eine **schriftliche Freigabe** zum Einsatz ist weder beim ersten Einsatz noch nach Änderungen gängige Praxis. (**Beispiel:** Änderungsbefugnisse der EDV-Abteilung für Datenbestände sind in der Testphase eines Verfahrens unbedingt notwendig, im Echtbetrieb aus der Sicht der Fachabteilung jedoch nicht zu verantworten – im wahrsten Sinne des Wortes.).

- Die sicherheitstechnisch „brisantesten" Aktivitäten in einem informationstechnischen System, die verändernden **Zugriffe auf das Betriebssystem** und die **systemnahe Software** werden **nicht revisionsfähig protokolliert** (**Bei-**

spiel: Wenn der Verdacht auftaucht, ein Systembetreuer habe manipuliert, kann er den Gegenbeweis nicht antreten, da er zweifellos die Möglichkeit gehabt hätte, aber nicht registriert ist, was er und was er nicht getan hat.).

- Obwohl es seit vielen Jahren gesetzlich vorgeschrieben ist, mangelt es an der korrekten **Dokumentation** der eingesetzten **Hardware** und **Software** sowie der Datenbestände (**Beispiel:** Aussage eines Mitarbeiters in der EDV-Abteilung: „Mir fehlt die Zeit, das Verfahren vernünftig zu dokumentieren".).
- In dem Maße, wie die Anzahl der informationstechnischen Systeme in der Verwaltung steigt, wächst die **Abhängigkeit von externen Dienstleistern;** deren Tätigkeit führt fast zwangsläufig zur Kenntnisnahme geschützter personenbezogener Daten (**Beispiel:** Speicherfehler auf einer Magnetplatte werden in der Regel in der Weise behoben, daß die betreffende Platte zur Fehleranalyse „eingeschickt" wird; zum Nachweis von Programmfehlern wird die Kopie eines Bildschirminhalts übergeben.).

Über die spezifischen Problemstellungen bei der Stadt Flensburg und ihre Lösung kann erst im nächsten Jahr berichtet werden, da eine Stellungnahme bis zum Redaktionsschluß dieses Tätigkeitsberichtes noch nicht vorlag.

6.6.4 EDV im Krankenhaus – technischer Fortschritt pro oder contra Patientengeheimnis?

Im Jahre 1993 haben wir uns im Rahmen unserer Prüfungsmaßnahmen einem Bereich zugewandt, in dem der Wunsch bzw. der Zwang, die technische Entwicklung auf dem Gebiet der Informationsverarbeitung voll auszuschöpfen, zu erheblichen Rechtsproblemen führen wird.

Krankenhäuser gehören zu den wenigen öffentlichen Stellen, die nach **kaufmännischen** und nicht nach kameralistischen **Grundsätzen** zu **kalkulieren** haben. Dies führt vor dem Hintergrund des Drängens der Sozialleistungsträger (Krankenkassen), die Behandlungskosten (Tagesätze) zu reduzieren, zur Offenlegung von Kostenstrukturen (Kostenstellen- und Kostenträgerrechnung). Da **erscheint** der konsequente Einsatz von **Datenverarbeitungssystemen** im Bereich der Krankenhausverwaltung, aber auch unmittelbar im medizinischen Bereich ein probates Mittel zur **Effizienzsteigerung** und zur **Rationalisierung.** Wie schnell bei einem nur an den Kosten orientierten Ansatz die rechtlichen Voraussetzungen und die sicherheitstechnischen Rahmenbedingungen zu einer Nebensache werden können, haben Prüfungen in einem Kreiskrankenhaus und in einem Universitätsklinikum gezeigt.

Folgende **Feststellungen** in dem **Kreiskrankenhaus** dürften auch für andere kommunale Krankenhäuser zutreffend sein:

- **Ausgangspunkt** für die automatisierte Datenverarbeitung waren Verfahren im Bereich **der Krankenhausverwal-**

tung. Es handelte sich dabei um die Abrechnung der Behandlungen, die Fakturierung, die Debitoren- und Kreditorenbuchhaltung sowie die Finanz- und Anlagenbuchhaltung. Aber auch in den rein **medizinischen Bereich** hat die Informationstechnik Einzug erhalten, zunächst bei der Labormedizin, sodann auch zur Unterstützung der Behandlungen.

- Die Tatsache, daß es sich auch bei den Verwaltungsdaten zumindest zum Teil um solche handelt, die einem besonderen Berufs- und Amtsgeheimnis unterliegen (Name des Patienten, Dauer der Behandlung und Diagnose, therapeutische Maßnahmen), fand in der Praxis keine entsprechende Beachtung. So war es nahezu selbstverständlich, daß die **Hard-** und **Softwaretechniker** der **Computerlieferanten und Softwarehäuser** bei Routinearbeiten am System, insbesondere aber bei Systemfehlern, **Kenntnis** von diesen **Patientendaten** bekamen.

- Für die **Administration** der technischen Systeme und der Software waren in der Verwaltung des Krankenhauses Mitarbeiter zuständig, deren Aktivitäten durch die Vorgesetzten mangels Fachwissen auf dem Gebiet der automatisierten Datenverarbeitung **nicht überwacht** werden konnten. Eine Protokollierung ihrer Aktivitäten fand nicht statt.

- Der automatisierten Datenverarbeitung lag **kein** schriftlich formuliertes **Sicherheits-** und **Verfahrenskonzept** zugrunde, das als Basis für detailierte Anweisungen für die beteiligten Systemadministratoren und Systembenutzer hätte dienen können.

- Die **Verantwortungsaufteilung** zwischen dem medizinischen-, dem pflegerischen- und dem Verwaltungsbereich korrespondierte nicht mit der Datenverarbeitungsorganisation. Es war z.B. nicht geklärt, ob und ggf. welche Befugnisse bzw. Verantwortung eine im Krankenhausverwaltungsamt des Kreises eingerichtete, jedoch nur mit einem Mitarbeiter besetzte, Stabsstelle bezüglich des medizinischen und des pflegerischen Bereichs hatte.

- Dementsprechend unzureichend war auch die **Administration** der **datenverarbeitungstechnischen Systeme** im medizinischen Bereich. Teilweise lag die ausschließliche Verantwortung beim leitenden Arzt, in einem anderen Fall hatte dieser die Systembetreuung an einen anderen Arzt delegiert. Beide verfügten jedoch nicht über eine entsprechende Ausbildung. Der ärztliche Direktor übte keine unmittelbare Kontrollfunktion aus.

- Die gesetzlich vorgeschriebenen **Dateibeschreibungen** und **Geräteverzeichnisse** wurden **nicht geführt.** Insbesondere im medizinischen Bereich bestanden Unklarheiten bezüglich der Inhalte der gespeicherten Daten und der Löschungsfristen.

Aufgrund unserer **Beanstandungen** hat sich die Krankenhausleitung veranlaßt gesehen, mit der Behebung der

Schwachstellen und Mängel zu beginnen. Als erster Schritt ist der **Entwurf einer Dienstanweisung** formuliert worden. Dieser konnte allerdings noch nicht überzeugen. Dies mag an dem von der Krankenhausleitung gewählten Ansatz gelegen haben, daß in der Dienstanweisung (Zitat) „nur solche Vorgaben gemacht werden, die letztendlich die Datenverarbeitung nicht deutlich beeinträchtigen". An anderer Stelle heißt es: „Bei der Einführung neuer automatisierter Verfahren werden die Sicherheitskonzepte stärker berücksichtigt werden. Hierzu muß jedoch angemerkt werden, daß aufgrund der personellen Ausstattung sich diese Konzepte auf das unbedingt vertretbare Maß beschränken müssen." oder „Die Überlegung, den Zugriff von echten Daten für Mitarbeiter der Systemhäuser auszuschließen, ist theoretisch".

Wir haben den Kreis auf die rechtliche und **sicherheitstechnische Brisanz,** die in derartigen Aussagen liegt, hingewiesen und auf wirksame Verbesserungen gedrängt.

Die als eine vergleichende Analyse gedachte Prüfung in einem **Universitätsklinikum** mußte abgebrochen werden, da keine ausreichend prüffähigen Unterlagen über die installierten Datenverarbeitungssysteme und benutzte Software vorgelegt werden konnten.

Gleichwohl hat bereits eine erste Nachschau „vor Ort" ergeben, daß einheitliche konzeptionelle Vorgaben (EDV-Konzept, EDV-Dienstanweisungen, Mindestanforderungen an die Datensicherung, Form und Inhalt von Dokumentationen) weder für die automatisierten Verfahren, die von der Universitäts-bzw. Klinikverwaltung eingesetzt werden, noch für solche, die aufgrund der Initiative der einzelnen Kliniken und Institute in eigener Verantwortung realisiert worden sind, bestehen.

Allerdings sind im August 1993 (die schriftliche Ankündigung der Prüfung erfolgte im Juli) sogenannte **„Datenschutzrichtlinien"** in Kraft gesetzt worden, die jedoch bis zum Prüfungszeitpunkt (September) noch **keine wesentlichen Wirkungen** entfaltet hatten. Trotz der komplexen Struktur des Universitätsklinikums enthalten sie keine konkrete schriftliche Fixierung der personellen Zuständigkeiten bezüglich der Administration der eingesetzten Hardware, der Software und der Datenbestände. Festgeschrieben ist allerdings, daß die Abteilungsdirektoren für die Einhaltung des Datenschutzes als „Herren der Daten" die Verantwortung tragen. Eine Differenzierung dieser Verantwortung im Hinblick auf die innere Organisation einerseits und die Verantwortung im Außenverhältnis andererseits ist nicht vorgenommen worden. Ein im Jahr 1988 erstelltes Konzept für ein Datenschutz- und Datensicherheitssystem läßt weder den Auftraggeber noch den Verfasser erkennen. Es hat offenbar nicht die Absicht bestanden, es in die Praxis umzusetzen.

Besondere Schwierigkeiten ergaben sich daraus, daß die gesetzlich vorgeschriebenen **Dateibeschreibungen** und das **Ge-**

räteverzeichnis seit einigen Jahren nicht mehr fortgeschrieben bzw. nicht erstellt worden sind und daß es der Klinikverwaltung nicht gelang, in dem Zeitraum zwischen der Ankündigung der Prüfung und ihrer Durchführung die entsprechenden Daten nachzuerheben. Von den fünfzig Kliniken, Instituten und Verwaltungsstellen, in denen personenbezogene Daten verarbeitet werden, hatten bis zum Zeitpunkt der Prüfung trotz schriftlicher Aufforderung neunzehn Stellen keine Angaben gemacht, vierzehn Stellen haben mitgeteilt, daß sie keine Dateien mit personenbezogenen Daten führen, in den übrigen siebzehn Stellen sind ca. 150 Rechnersysteme und Einzelplatzrechner sowie 25 Bildschirmarbeitsplätze mit acht unterschiedlichen Betriebssystemen und vierzig verschiedenen Software-Paketen zum Zweck der personenbezogenen Datenverarbeitung im Einsatz. Diese Zahlen geben allerdings nur einen ungefähren Anhaltspunkt über die Vielzahl der in diesen Bereichen vorhandenen automatisierten und nichtautomatisierten Dateien.

Zu den entsprechenden datenschutzrechtlichen Beanstandungen hat der **Rektor der Universität** in einer **ersten Stellungnahme** mitgeteilt, daß er zu vielen Punkten eine abweichende Position vertrete. Die Registrierung der Dateien und der Hardware sei aus seiner Sicht vollständig. Die ablauforganisatorischen Regelungen seien im Hochschulgesetz des Landes Schleswig-Holstein abschließend dargestellt. Darüber hinaus existierende Regelungen würden jedoch aufgrund unserer Vorschläge grundsätzlich überarbeitet. Zudem würde eine Stabsstelle zur Erarbeitung eines DV-Gesamtkonzeptes und eine **Datenschutzkommission eingerichtet** werden. Über den Fortgang der Prüfung werden wir im nächsten Tätigkeitsbericht berichten.

6.6.5 Verdeckte Videoüberwachung – der Datenschutz-„Skandal" des Jahres 1993

Nicht böser Wille, sondern Unkenntnis des Rechts und der datenverarbeitungstechnischen Möglichkeiten waren Ursache von gravierenden Fehlentscheidungen. Dies führte zur Installation einer verbotenen geheimen Videoüberwachung.

Kaum ein anderer „Datenschutzunfall" im Lande Schleswig-Holstein hat in den vergangenen Jahren ein solches Presseecho hervorgerufen, wie eine **verdeckte Videoüberwachung** in der Amtsverwaltung Bargteheide-Land. „Video-Skandal", „Bespitzelung im Amt", „Bargteheide-Gate" lauteten nur einige der Überschriften in praktisch allen regionalen und einigen überregionalen Zeitungen, Rundfunk und Fernsehen berichteten mit ähnlichem Inhalt.

In der Tat, es war zu einer **rechtlich unzulässigen Datenverarbeitung** gekommen. Aber was war die **Ursache,** was die **Wirkung?** Der **Sachverhalt** stellte sich wie folgt dar:

Im Oktober 1992 wurden von den Mitarbeitern des Amtes **Manipulationen** an der **EDV-Anlage** im Kämmereiamt bemerkt. Es waren **Haushaltsdaten** offenkundig **verfälscht** worden. Da es sich vermeintlich nur um einen Einzelfall handelte, wurden die falschen Angaben wieder richtiggestellt. Ein Manipulationsverdacht kam erst auf, als man auch von Unstimmigkeiten in anderen Bereichen der Verwaltung zu früheren Zeitpunkten hörte. Auf dem PC im Vorzimmer des Leitenden Verwaltungsbeamten waren Zahlen geändert worden. Im Bereich der technischen Abteilung hatte es Unstimmigkeiten mit der automatisierten Abwasserabgabenberechnung gegeben und ein ganzes Programm war zeitweise verschwunden. Später wurde dann festgestellt, daß ein Lehrling es mit nach Hause genommen und dort privat bearbeitet hatte.

Wegen dieser **Unstimmigkeiten** wandte sich eine Mitarbeiterin des vom Amt beauftragten EDV-Beratungsunternehmens seinerzeit auch an uns und ließ sich – ohne die Sachverhalte darzulegen – ganz allgemein bezüglich der Ausgestaltung von Dienstanweisungen beraten.

Später ist auch die Beschaffung einer speziellen **Sicherheitssoftware** erwogen, aber **nicht realisiert** worden. Auf Anraten der Unternehmensberatungsfirma wurde **statt dessen** die **Videoüberwachung** durch den Amtsvorsteher veranlaßt. Man wollte auf diese Weise feststellen, wer sich unbefugt an den Datenverarbeitungsgeräten zu schaffen machen würde. Auf die Rechtswidrigkeit der Maßnahme ist der Amtsvorsteher von der Unternehmensberatungsfirma und von den Mitarbeitern der Amtsverwaltung, die eingeweiht waren, nicht aufmerksam gemacht worden. Nach anderen Sicherungsmöglichkeiten hat er nicht gefragt.

Die **Mitarbeiter** der Amtsverwaltung, an deren Arbeitsplätzen die Anlagen verdeckt installiert wurden, waren **informiert.** Allerdings herrschte in den überwachten Räumen Publikumsverkehr. Die Überwachungsmaßnahme lief ca. vier Wochen. In dieser Zeit wurden insgesamt vier Video-Bänder beschrieben. Eine Tonaufzeichnung erfolgte nicht.

Der behördliche Datenschutzbeauftragte hat auf einem privaten Spielgerät die Bänder eingesehen. Er übergab sie nach dem Ende der Überwachungsmaßnahme dem Leiter des Ordnungsamtes. Dieser verwahrte sie vorübergehend in seiner **Privatwohnung.**

Nach **Aufdeckung** durch einen **Mitarbeiter,** der einen als Tarnung verwendeten Leitz-Ordner benutzen wollte, wurde in einer außerordentlichen Amtsausschußsitzung beschlossen, die **Kriminalpolizei** einzuschalten und **Anzeige** gegen Unbekannt zu erstatten. Die Video-Bänder mit den Aufzeichnungen wurden der Polizei übergeben. Sie verbleiben dort als Beweismittel bis zum Ende des strafrechtlichen Ermittlungsverfah-

rens. Die Presse und der Datenschutzbeauftragte wurden ebenfalls informiert.

Aufgrund der von uns durchgeführten Nachschau wurde „die Aufzeichnung des Verhaltens von Personen in zwei Räumen der Amtsverwaltung auf optisch-elektronischen Bildträgern (Video-Aufzeichnung) gem. § 25 Abs. 2 i. V. m. § 32 LDSG **beanstandet,** da die Tatsache der Aufzeichnung für die Betroffenen (Mitarbeiter und Besucher der Amtsverwaltung) nicht erkennbar gemacht worden ist (§ 32 Abs. 1 Satz 2 LDSG)."

Soweit die **Fakten,** die **eigentlichen Ursachen** für diese rechtlich unzulässige Verfahrensweise lagen nach unseren Erkenntnissen nicht in der Absicht begründet, schutzwürdige Belange von Betroffenen zu beeinträchtigen, sondern in einer **dreifachen Unkenntnis.** Dem ehrenamtlich tätigen Amtsvorsteher und den ihn beratenden Mitarbeitern der Verwaltung und des Unternehmens war offenbar nicht bekannt,

- daß diese Art der Video-Überwachung ein höchst **unwirksames Mittel** zur Aufdeckung von Manipulationen an Datenverarbeitungsgeräten darstellt, da dabei der eigentliche Vorgang der Manipulation nicht protokolliert wird,
- daß Videoaufzeichnungen durch öffentliche Stellen an die **datenschutzrechtliche Bedingung** geknüpft sind, daß „die Tatsache der Aufzeichnung für die Betroffenen durch geeignete Maßnahmen erkennbar gemacht wird", und
- daß es auf dem Markt **bewährte Software-Produkte** gibt, die derartige Manipulationen unmöglich machen und bereits entsprechende Versuche protokollieren.

Bereits durch einen Blick in das Landesdatenschutzgesetz sowie in die von uns im Amtsblatt (1992, S. 753) veröffentlichten Hinweise hätte der Wissensstand der handelnden Personen so weit angehoben werden können, daß dieser „Skandal" zu vermeiden gewesen wäre. Für uns ist dieser Fall ein **Lehrstück** dafür, daß neben der Fahrlässigkeit die **Unwissenheit** als häufigster **auslösender Faktor** für Datenschutzverletzungen anzusehen ist. Hierauf weisen wir in den Informationsveranstaltungen der DATENSCHUTZAKADEMIE seit Jahren immer wieder hin.

7. Neue Medien und Technologien

7.1 Mobilkommunikation

Die neuen mobilen Sprach- und Datenübertragungsdienste bringen neben Mobilität, Erreichbarkeit an fast jedem Ort und Bequemlichkeit auch neue Risiken für den Datenschutz. Die Verantwortung für die Vertraulichkeit liegt beim Dienstbetreiber und beim Anrufer.

Die Verbreitung mobiler **Sprach- und Datenübertragungsdienste** hat in jüngster Vergangenheit stark zugenommen. So

gibt es bereits jetzt in Deutschland mehr als eine halbe Million Teilnehmer der Funktelefonnetze C und D. Seit Juni diesen Jahres ist auch ein öffentlicher mobiler Datenübertragungsdienst der Telekom in Deutschland verfügbar. Es ist zu erwarten, daß sich die Teilnehmerzahl mobiler Kommunikationsdienste in Zukunft weiter vergrößern wird.

Die „Szene" auf der Angebotsseite stellt sich z.Z. wie folgt dar (Anmerkung: Die nachfolgenden Darstellungen basieren weitgehend auf einer Erhebung der Datenschutzbeauftragten der Länder Berlin, Bremen und Hamburg):

a) Die beiden **Mobiltelefonnetze „B" und „C"** gelten als technisch überholt. Neuanschlüsse sind beim B-Netz nicht mehr und beim C-Netz nur noch für einen absehbaren Zeitraum möglich. Die Übermittlung der Inhaltsdaten und der für den Verbindungsauf- und -abbau erforderlichen Daten erfolgt analog.

   Beim **B-Netz** ist es für den Verbindungsaufbau erforderlich, den gegenwärtigen Ort des Mobilteiles zu kennen, da nicht permanent gespeichert wird, wo sich dieses z.Z. aufhält. Neben der Rufnummer des Mobilteiles muß dem Anrufer also die Kennzahl des Funkvermittlungsbereiches, in dem sich das Mobilteil befindet, bekannt sein. Beim **C-Netz** gibt es eine bundeseinheitliche Rufnummer, unter der das Mobilteil unabhängig von seinem jeweiligen Standort erreicht werden kann. Hierzu muß der momentane Standort des Mobilteiles im C-Netz gespeichert sein.

   Bei Gesprächen von Mobiltelefonen werden die **Verbindungsdaten** inklusive der **Standortkennung** von der Telekom **gespeichert** und langfristig aufbewahrt. Die Übermittlung der über Funktelefone des B- bzw. C-Netzes geführten Gespräche erfolgt analog. Daher ist ein Abhören solcher Gespräche auf der Funkstrecke mit inzwischen frei käuflichen Scannern relativ leicht möglich.

b) Bei den D-Netzen (**D 1- und D 2-Netz**) werden die **Sprachsignale digitalisiert** übermittelt. Dies gilt sowohl für die Funkstrecke als auch im Festnetz. Hierzu sind die D-Netze an das ISDN der Telekom angeschlossen. So können die Vorteile der Digitalisierung auch auf der Verbindung im Festnetz genutzt werden. Jedes der beiden D-Netze besitzt eine eigene Infrastruktur.

   Um eine Verbindung zu einem **Mobilteil** aufbauen zu können, ist es notwendig, seinen **momentanen Standort** zu kennen. Hierzu wird eine für jeden Mobilanschluß eindeutige Kennung verwendet, die auf einer Chipkarte gespeichert ist. Beim Einschalten des Gerätes meldet es sich mit seiner Kennung bei der nächsten Basisstation an. Diese schickt die Information über den Aufenthaltsort an die Funkvermittlungsstelle, bei der dieses Mobilteil registriert ist. Dort wird in einem Register neben den Grunddaten auch die jeweilige Basisstation gespeichert, in deren Bereich das

Mobilteil sich gerade befindet sowie festgehalten, ob das Mobilteil ein- oder ausgeschaltet ist.

Daneben werden in der Funkvermittlungsstelle auch **alle anderen Mobiltelefone,** die sich in ihrem Bereich aufhalten, registriert. Wird von einem Mobiltelefon aus eine Verbindung aufgebaut, muß es sich zuerst gegenüber dem Netz authentifizieren.

Verbindungsdaten fallen bei den Netzbetreibern an. Erfaßt werden: Art der Verbindung (abgehender oder ankommender Anruf, Notruf), Kennung des rufenden und des gerufenen Anschlusses, Kennung des Ursprungs- und Zielstandortes, Verbindungsbeginn und -ende, Dienstkennung, aktivierte Zusatzdienste, Datenaufkommen.

c) Die Unterschiede zwischen den D-Netzen und dem **E-Netz** liegen lediglich in unterschiedlichen Trägerfrequenzen.

d) Das **Modacom-System** besteht aus einem terrestrischem Festsender-Kleinzellennetz mit Basisstationen zur Bereitstellung der Funkstreke. Sie sind über Festverbindungen mit einer Funkvermittlungseinrichtung verbunden. Die Funkmodems buchen sich nach dem Anschalten im Netz ein, d.h. sie senden ein Signal aus, das von der nächsten Basisstation empfangen und an die Vermittlungseinrichtung weitergeleitet wird. Dadurch wird der **Standort** der mobilen Terminals dem Netz **bekanntgegeben.** Die Terminals werden in einer Art Standby-Modus versetzt und können die für sie bestimmten Nachrichten empfangen. Die Funkmodems fischen sich die für sie bestimmten Informationen aus dem übertragenen Datenstrom heraus. Dabei wird das Modem jeweils nur dann aktiviert, wenn eine Nachricht mit der jeweiligen Modem-Id übertragen wird.

Sowohl der genaue **Authentifikationsmechanismus** als auch das für die Datenübertragung verwendete Protokoll werden von den Betreibern und von den Herstellern **geheim gehalten.**

e) Gegenwärtig umkreisen ca. 500 **Kommunikationssatelliten** die Erde. Geostationäre Kommunikationssatelliten strahlen die von einer festen Erdfunkstelle oder einer mobilen Sendeanlage gesendeten Signale nach der Umsetzung in einen anderen Frequenzbereich verstärkt zu anderen ortsfesten Erdfunkstellen oder mobilen Empfangsanlagen zurück. Bei bereits in der Planung befindlichen **Satellitennetzen** werden die empfangenen Daten u.U. vor der Zurückstrahlung zur Erde noch an andere Satelliten übermittelt. Weiterhin existieren Satelliten, deren regelmäßige Bewegung um den Erdball zum Transport von Daten genutzt wird. In diesem Fall werden die Daten in den Satelliten während des Transportes im Orbit zwischengespeichert.

Satelliten werden für **alle** denkbaren **Telekommunikationsdienste** genutzt. Nutzer sind dabei zunächst öffentliche Einrichtungen für Post und Telekommunikation wie z.B. die Telekom. Daneben benutzen aber auch private Unter-

nehmen z.B. für die Verbindung von Konzernzentralen mit den verschiedenen Zweigstellen zunehmend die Satellitentechnik für Kommunikationszwecke.

f) Das **„Global Positioning System" (GPS)** erlaubt die satellitengestützte Bestimmung der eigenen Position an einem beliebigen Ort auf der Erde bis auf wenige Meter genau. Es besteht aus 21 Satelliten, die die Erde in einer Höhe von 20.200 Kilometer umkreisen. Mit einem GPS-Empfangsgerät werden die vier dem Standort am nächsten befindlichen Satelliten angepeilt. Auf der Grundlage der Signallaufzeiten wird der Standort berechnet. GPS-Empfänger sind auf dem freien Markt erhältlich und werden gegenwärtig vor allem im Bereich der Schiffahrt aber gelegentlich auch bereits die Positionsbestimmung im Autoverkehr genutzt.

   GPS selbst ist ein **„passives" System.** Die Positionsdaten werden nur an das abfragende Empfangsgerät gesandt. Dies geschieht nicht ständig, sondern nur auf Anforderung durch das Empfangsgerät.

g) **Euteltracs** ist ein Satellitendienst für die **Standortbestimmung** und den **Nachrichtenaustausch.** Das System wird überwiegend von Speditionen im Bereich des Flottenmanagements eingesetzt. Für Euteltracs werden zwei geostationäre Satelliten genutzt. Die Positionsbestimmung einer Mobileinheit erfolgt, indem durch eine zentrale Station ein Signal über die beiden Satelliten an die Mobileinheit gesandt wird. Die Mobileinheit berechnet aus den unterschiedlichen Signallaufzeiten den Standort und sendet diesen zurück an die Station. Die Positionsermittlung erfolgt automatisch in frei einstellbaren Intervallen. Dadurch kann der Weg des Mobilteiles in der Zentrale kontinuierlich mitverfolgt werden. Auch das Abrufen von technischen Fahrzeug- und Frachtdaten wie Öldruck oder Frachttemperatur ist möglich. Zusätzlich können mit dem zum Mobilteil gehörigen Terminal auch Nachrichten ausgetauscht werden.

h) Im Bereich der **Fernortung** haben satellitengestützte Systeme zur Lokalisierung **gestohlener Fahrzeuge** in letzter Zeit eine zunehmende Publizität erlangt. Solche Systeme werden sowohl von politischer Seite propagiert als auch in der Privatwirtschaft erprobt. Von einem deutschen Automobilhersteller ist bekannt, daß dort z.Z. diesbezügliche Versuche durchgeführt werden.

i) Zwar werden **Satellitenverbindungen** schon lange für die Herstellung von **Telefonverbindungen** über große Entfernungen (z.B. im Transatlantikverkehr) genutzt. Aber auch für vergleichsweise geringe Entfernungen setzt die Telekom bei Bedarf Satellitenanlagen ein. Dies betrifft z.B. die Verbindung mit der Deutschen Botschaft in Moskau, Telefon-, Telex- und Datex-P-Verbindungen in verschiedene Länder Osteuropas, aber auch zahlreiche Verbindungen in die „fünf neuen Länder", in denen bis zur Instandsetzung der terristrischen Netze Satellitenkapazität zum Betrieb eines zu-

sätzlichen Fernsprechnetzes genutzt wird. Für den Benutzer von Telekommunikationseinrichtungen bleibt der Einsatz der Satelliten meist verborgen.

k) Die bestehenden Dienste werden in absehbarer Zeit um **weitere satellitengestützte Telekommunikationsanwendungen** ergänzt werden. Derzeit planen verschiedene Hersteller die Einführung satellitengestützter Telefonnetze, deren Endgeräte nicht wesentlich größer als die momentan im Handel befindlichen „D-Netz-Handys" sein sollen. Diese Systeme sollen ab 1994 erprobt werden und bis Ende des Jahrzehnts weltweit flächendeckend zur Verfügung stehen.

Da die **übertragenen Informationen** in der Regel in den Computeranlagen der Dienstanbieter und der Systembetreiber zumindest **temporär gespeichert** werden, stellen sich hier Fragen nach der Datensicherheit bei der Verarbeitung in diesen Anlagen bzw. bei der Übertragung zwischen diesen.

Grundsätzlich kann jeder, der über ein entsprechendes Empfangsgerät verfügt, die von einem Satelliten abgestrahlten Nachrichten empfangen. Nach Untersuchungen des Bundesamtes für die Sicherheit in der Informationstechnik ist es zwar derzeit nur professionellen Anwendern möglich, Nachrichteninhalte von Satellitenverbindungen tatsächlich zu verstehen. Die momentan im freien Handel erhältlichen Scanner erlauben dies nur für wenige Verbindungen. Durch das reine Abhören der Verbindung können die Kommunikationsinhalte in der Regel nicht in Erfahrung gebracht werden, da im allgemeinen **Multiplex-** und **Datenkompressionsverfahren** bei der Übertragung eingesetzt werden. Da die entsprechenden Protokolle und Verfahren jedoch mindestens fachöffentlich bekannt sind, kann hier nicht von einem wirksamen Schutz ausgegangen werden.

Mit dem steigenden Umfang der Datenübertragung via Satellit dürfte das Interesse am Abhören der Inhalte und den dazu notwendigen Geräten in der Zukunft jedoch zunehmen. Es wird dann nur noch eine Frage der Zeit sein, bis solche Geräte am Markt für jedermann erhältlich sind.

Die mit der Nutzung von Mobilfunkdiensten verbundenen Vorteile gehen also mit **Gefährdungen für den Datenschutz** der Benutzer einher. Neben den auch bei anderen Telekommunikationsdiensten gespeicherten Angaben, wer wann mit wem in Verbindung war, wird bei der Mobilkommunikation auch erhoben, wo sich der mobile Teilnehmer jeweils aufhält. Die Speicherung dieser Daten ermöglicht die Bildung von höchst **problematischen Bewegungsprofilen.**

Darüber hinaus ist vielfach auch die **Vertraulichkeit** der Kommunikationsinhalte **gefährdet,** insbesondere dann, wenn **Daten unverschlüsselt** per Funk **übertragen** werden. Dies gilt sowohl für die analogen Telefon-Netze B und C als auch für den von der Telekom betriebenen mobilen Datenübertra-

gungsdienst Modacom. Bei satellitengestützten Diensten ist es sogar möglich, die übertragenen Daten im gesamten, teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich des Satelliten unbemerkt abzuhören und aufzuzeichnen.

Von den Herstellern und Betreibern mobiler Dienste ist deshalb zu fordern, daß sie diesen Gefahren für das Fernmeldegeheimnis und für den Datenschutz durch technische Vorkehrungen entgegenwirken.

Die **Teilnehmer** von mobilen Diensten und hier in erster Linie die „Anrufer" **müssen** über die mit der Nutzung verbundenen **Risiken** und den erreichten Sicherheitsstandard **aufgeklärt sein.** Sofern bei bestimmten Diensten **Sicherheitsmerkmale** eingebaut sind, muß deren Effektivität für die Aufsichts- und Kontrollorgane auch **nachprüfbar** sein. Dies setzt eine **Veröffentlichung** der getroffenen Sicherheitsmaßnahmen, z.B. der verwendeten Verschlüsselungsalgorithmen, voraus.

Falls durch den Dienstbetreiber nicht das aus der Sicht des Teilnehmers erforderliche Sicherheitsniveau gewährleistet werden kann, muß eine Übertragung personenbezogener oder sonstiger sensibler Daten mit dem jeweiligen Dienst unterbleiben oder der Teilnehmer selbst muß zusätzliche Sicherheitsvorkehrungen treffen.

Die Mobilkommunikation ist dadurch gekennzeichnet, daß bei verschiedenen Dienst- und Netzbetreibern, aber auch bei sog. Service-Providern (Unternehmen, die lediglich Dienste vermarkten) personenbezogene Daten gespeichert werden. Im Zuge der anstehenden **Überarbeitung des Telekommunikationsrechts** muß gesetzlich dafür Sorge getragen werden, daß die personenbezogene Datenverarbeitung bei diesen Stellen auf das wirklich erforderliche Maß beschränkt wird und daß die Nutzer darüber aufgeklärt worden sind, bei welcher Stelle welche personenbezogenen Daten verarbeitet werden.

Besonders problematisch ist es, wenn bei der **internationalen Mobilkommunikation** auch in solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen das Fernmeldegeheimnis nicht sichergestellt wird. Deshalb ist es erforderlich, auch auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei mobilen Kommunikationsdiensten gewährleisten.

Es reicht jedoch nicht, an die Verantwortung der Betreiber und Anbieter zu appellieren sowie nationale und internationale Regelungen zu fordern. Der wirksamste Schutz für die Rechte der Betroffenen (d.h. alle Personen, deren Daten Gegenstand der Kommunikation sind) ist durch die Initiatoren eines Kommunikationsvorganges zu erreichen. Gerade **Behörden** und **sonstige öffentliche Stellen** (das gilt besonders für Sicherheitsbehörden, Rettungsdienste usw.) sollten sich immer wieder vergegenwärtigen, daß auch im Bereich der Kommunikation „viele Wege nach Rom führen".

Es ist nicht zwingend, den „modernsten" oder kostengünstigsten, sondern den **sichersten Weg** zu **wählen.** Wie auch beim Einsatz anderer (neuer) technischer Systeme sind die spezifischen Fragen der Rechtmäßigkeit und Sicherheit der Verarbeitung zu entscheiden, bevor man sich der Technik bedient. Die **Verantwortung für** negative **„Technikfolgen"** kann nicht auf Dienstleister abgewälzt werden, da sie zum Betroffenen nicht in einer Rechtsbeziehung stehen.

7.2 „Rasterfahndung" durch die Gebühreneinzugszentrale der Rundfunkanstalten (GEZ)?

Die öffentlich-rechtlichen Rundfunkanstalten wollen den Rundfunkgebühreneinzug durch automatische Auswertung der Melderegister wirkungsvoller gestalten. Aus datenschutzrechtlichen Gründen sollte von einer pauschalen Übermittlung von Melderegisterdaten abgesehen werden.

Schon seit langem wird von den öffentlich-rechtlichen Rundfunkanstalten gefordert, regelmäßig aus den Melderegistern über **alle Sterbefälle** und **Wohnortwechsel** informiert zu werden. Hessen und Nordrhein-Westfalen verfügen über entsprechende Bestimmungen in ihren Meldedatenübermittlungsverordnungen. Das Problem dabei ist, daß von der GEZ die Daten aller Wohnsitzveränderungen Volljähriger in der Bundesrepublik ausgewertet werden könnten. Darunter fielen auch eine große Anzahl von Angaben, die nicht für die Erhebung von Rundfunkgebühren benötigt werden. So würden Informationen über Wohnungswechsel beispielsweise auch dann bekannt gegeben, wenn Rundfunkgebühren von Teilnehmern weitergezahlt werden oder von Einwohnern, die gar nicht zahlungspflichtig sind.

Seit Jahren haben wir uns deshalb gegen regelmäßige und pauschale Datenübermittlungen an die GEZ gewandt und stattdessen ein Verfahren vorgeschlagen, mit dem die GEZ **ungeklärte Einzelfälle** mit den Melderegistern abgleichen könnte, das aber zugleich die Datenübermittlung auf das erforderliche Maß beschränken würde (vgl. 9. TB, S. 11).

Unter Hinweis auf die Höhe der entgehenden Rundfunkgebühren, die Bemerkungen der Rechnungshöfe und vorliegende Rechtsgutachten drängen die Rundfunkanstalten in der letzten Zeit erneut auf ungehinderten Datenzugang, offenbar mit Aussicht auf Erfolg. Ein Arbeitskreis der Innenministerkonferenz hat bereits einen Formulierungsvorschlag für eine entsprechende **Änderung der Meldedatenübermittlungsverordnungen** gemacht, nach dem eine regelmäßige Übermittlung von Daten für den Fall der An-, Abmeldung und des Todes von den Meldebehörden an die Rundfunkanstalten bzw. die GEZ zugelassen würde. Die Innenministerkonferenz schlägt – gegen die Stimme Schleswig-Holsteins – eine Verankerung einer solchen Vorschrift im Melderechtsrahmengesetz vor.

Die **Konferenz der Datenschutzbeauftragten** hat hingegen mit Mehrheit in einer Entschließung Bedenken geäußert und entsprechende Regelungen abgelehnt. Sie hat dabei betont, daß

- die Regelung im Ergebnis zu einem **bundesweiten Melderegister** über Volljährige bei der GEZ führen könnte,

- gegen das Verfassungsrechtlich garantierte **Verhältnismäßigkeitsprinzip** verstoßen würde; den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat,

- dabei der Grundsatz unbeachtet bliebe, daß nur zur rechtmäßigen Aufgabenerfüllung erforderliche Daten verarbeitet werden dürfen; das vorgesehene Verfahren würde nicht zwischen erforderlichen und nichterforderlichen Daten unterscheiden, sondern diese Unterscheidung dem **Datenempfänger,** nämlich der GEZ, **überlassen,** über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft.

Damit soll ein Bedürfnis der GEZ an besserer Information über die Gebührenpflichtigen nicht in Abrede gestellt werden. Es kommt jedoch darauf an, **verfassungskonforme,** insbesondere am Verhältnismäßigkeitsgrundsatz orientierte **Lösungen** zu finden und nicht die Möglichkeiten der elektronischen Datenverarbeitung zur Übermittlung und Verarbeitung von Millionen von Datensätzen an die GEZ zu nutzen, obwohl bei weitem nicht alle davon gebraucht werden.

8. Was es sonst noch zu berichten gibt

– Neues Landesbeamtengesetz

Aufgrund vieler Einzeleingaben und einer Reihe von Prüfungen haben wir von Mängeln bei der Personalaktenführung öffentlicher Stellen berichtet. Durch die am 01.01.1993 in Kraft getretene Novelle zum Beamtenrechtsrahmengesetz des Bundes wird nun für die **Personalaktenführung** eine **grundlegende Neuordnung** und Klärung herbeigeführt. Der Landesgesetzgeber muß die Vorgaben des Rahmenrechts umsetzen. An den Vorbereitungen des Regierungsentwurfs sind wir beteiligt worden und konnten eine weitgehende Übereinstimmung in den Grundsatzfragen feststellen. Ein zügiger Fortgang des Gesetzgebungsverfahrens ist zu wünschen.

– **Auskünfte aus Gewerbeanmeldungen an Private**

Immer wieder erbitten Privatleute **Auskünfte aus** den Datenbeständen kommunaler Ordnungsämter über **Gewerbeanmeldungen.** Überwiegend stellen Gläubiger Fragen nach den Privatanschriften der Inhaber bzw. der Geschäftsführer von Betrieben. Eine spezielle Rechtsgrundlage für solche Auskünfte besteht z.Z. nicht. Sie soll mit einer im Entwurf vorliegenden Ergänzung der Gewerbeordnung geschaffen werden. Dem Minister für Wirtschaft, Technik und Verkehr haben wir für eine Übergangszeit bis zur Verabschiedung der vorliegenden Gesetzesnovelle empfohlen, Auskünfte auf der Grundlage der allgemeinen Datenübermittlungsvorschriften des LDSG zuzulassen. Dabei kann zu der dort vorgesehenen Abwägung des rechtlichen Interesses Auskunftsbegehrender mit schutzwürdigen Belangen Betroffener der Wortlaut des Novellierungsentwurfs herangezogen werden. Der Minister für Wirtschaft, Technik und Verkehr ist dieser Anregung gefolgt und hat die zuständigen Stellen durch einen Erlaß unterrichtet.

– **Denkmalschutzgesetz wird um Datenschutzregelungen ergänzt**

Das geltende Denkmalschutzgesetz enthält keine ausreichende **Rechtsgrundlage** für die **Verarbeitung personenbezogener Daten** durch die **Denkmalschutzbehörde** (vgl. 9. TB, S. 47). Wir wurden an Vorüberlegungen zu einer Gesetzesnovelle beteiligt und haben normenklare Regelungen vorgeschlagen. Es sollen die Zwecke der Datenverarbeitung festgelegt und hierfür Name und Anschrift von Grundstückseigentümern aus den Grundbüchern entnommen und auch Daten der Besitzer, der Belegenheit des Kulturdenkmals sowie Informationen über seinen Charakter und Zustand verarbeitet werden dürfen. Die Strukturen des Denkmalbuchs werden in einer Verordnung geregelt und die Gemeinden und unteren Bauaufsichtsbehörden als mögliche Datenempfänger festgelegt. Die Vorarbeiten zur Novellierung des Gesetzes sollten konsequent und zügig abgeschlossen und das Gesetzgebungsverfahren eingeleitet werden.

– **Kennzeichnungspflicht für kleine Wasserfahrzeuge**

Eine Verordnung über die Kennzeichnung und Registrierung von Kleinfahrzeugen auf den Binnenschiffahrtsstraßen plant das Bundesministerium für Verkehr. Alle **Wasserfahrzeuge** mit einer Höchstlänge bis zu 20 Metern einschließlich Segelsurfbretter sollen danach einer **Kennzeichnungspflicht** unterliegen. In **Kleinfahrzeugverzeichnissen** sollen neben den zu vergebenden Kennzeichen auch die Eigentümerdaten gespeichert werden. Diese Daten sollen dann in einem zentralen Register bei der Wasserschutzpolizei Nordrhein-Westfalen gespeichert werden. Ob

eine derartige zentrale Erfassung sinnvoll und notwendig ist, wird noch zu diskutieren sein.

Der Verordnungsentwurf zeichnet sich im übrigen durch klare Vorschriften über das Erheben, Speichern, Übermitteln und Löschen von Daten aus. Wir hatten deshalb in unserer Stellungnahme gegenüber dem Minister für Wirtschaft, Technik und Verkehr nur wenige Änderungswünsche vorzutragen, die in der Hauptsache auf die Konkretisierung von Formulierungen einzelner Vorschriften abzielten.

– **Grundwasserentnahmeabgabengesetz**

Zunächst wiederholte der uns zugeleitete Entwurf eines **Grundwasserentnahmeabgabengesetzes** in seinem Datenschutzteil lediglich die Generalklausel des LDSG, daß die „erforderlichen personenbezogenen Daten" verarbeitet werden dürften.

Die Erhebung personenbezogener Daten ist erforderlich, um die Grundlagen einer Abwasserabgabe zu ermitteln, eine solche Abgabe festzusetzen und sie vom Abgabepflichtigen zu erheben. Dazu werden Daten benötigt, die die Abgabepflichtigen identifizieren und die es ermöglichen, eine Abgabepflicht nach Grund und Höhe festzustellen. Soweit solche Daten bereits nach bestimmten anderen Gesetzen erhoben wurden, muß ihre Verwendung für die Grundwasserabgabe bereichsspezifisch geregelt werden. Wir haben dem zuständigen Landtagsausschuß entsprechende Formulierungsvorschläge zugeleitet, die bei der Verabschiedung des Gesetzes berücksichtigt wurden.

– **Medizinische Untersuchung von Ausländern weggefallen**

Während in der Vergangenheit Ausländer routinemäßig ärztlich untersucht wurden, fallen nach dem Ausländerrecht, das ab 1991 gilt, alle Pflichtuntersuchungen fort. Auf unseren Hinweis haben die beteiligten Ressorts von routinemäßigen Untersuchungen Abstand genommen und den Runderlaß, der dies noch vorsah, ersatzlos aufgehoben. **Pflichtuntersuchungen von Ausländern** gibt es **künftig nicht mehr.** Eine Ausnahme bilden lediglich die Gesundheitsuntersuchungen von Asylbewerberinnen und Asylbewerbern nach dem Asylverfahrensgesetz.

– **Offenbarung der Einkommensverhältnisse der Mieter**

Nach den Plänen der Bundesregierung ist vorgesehen, durch Gesetz eine besondere Form der **Förderung für sozialgebundene Wohnungsbauvorhaben** einzuführen. Die Höhe der Förderung soll im Einzelfall von den **Einkommensverhältnissen der Mieter** abhängig gemacht werden, die laufende Auszahlung jedoch an die Vermieter erfolgen. Damit wäre zwangsläufig eine Information der Vermieter über Einkommensverhältnisse der Mieter ver-

bunden. Weiter müßte das Einkommen der Mieter ständig kontrolliert und das Ergebnis in umfangreichen Datenverarbeitungsvorgängen festgehalten werden. Die damit verbundenen Eingriffe in ihr Persönlichkeitsrecht könnten die Mieter nicht durch Verzicht auf entsprechende Mietverträge umgehen, da sie auf den in Betracht kommenden Wohnraum angewiesen sind. Es bestehen daher erhebliche Zweifel, ob das in Aussicht genommene Verfahren einen angemessenen Ausgleich zwischen dem Allgemeininteresse an effektiver Förderung des sozialen Wohnungsbaus und dem **Persönlichkeitsschutz der Mieter** schafft. Wir haben den Innenminister auf die grundsätzlichen Bedenken hingewiesen und eine eingehendere Stellungnahme in Aussicht gestellt, sobald für die ohnehin erforderlichen Rechtsgrundlagen konkrete Formulierungsentwürfe vorliegen.

- **Wahl zur Landwirtschaftskammer**

  Öffentlich ausgelegte **Wählerlisten** anläßlich der Wahlen zur **Landwirtschaftskammer** haben wegen ihres Detaillierungsgrades Kritik hervorgerufen. Leider konnten wir keine Änderung erreichen, da Art und Inhalt der Wählerlisten in der entsprechenden Wahlordnung bindend vorgeschrieben sind. Vor der nächsten Wahl zur Landwirtschaftskammer erscheint eine Überarbeitung der Regelung angezeigt.

- **Automatisierte Verfahren**

  Richtlinie über die **Dokumentation automatisierter Verfahren** hat die IT-Kommission des Landes beschlossen. Sie befindet sich zur Zeit in dem Abstimmungsverfahren nach dem Mitbestimmungsgesetz. Sobald dies abgeschlossen ist, verfügt die Landesverwaltung erstmals über eine einheitliche „Norm" auf diesem Gebiet. Wenn diese Richtlinie zudem mit den künftigen Regelungen in der Verordnung zu § 7 Abs. 4 LDSG korrespondiert und konsequent beachtet wird, dürfte ein großer Schritt in Richtung auf eine **revisionsfähige automatisierte Datenverarbeitung** getan sein. Eine ausführliche Darstellung erfolgt im nächsten Tätigkeitsbericht.

- **Verarbeitung von Dateibeschreibungen arbeitsintensiv**

  Qualität und Menge der eingehenden **Dateibeschreibungen** nach § 8 Abs. 1 LDSG lassen sehr zu wünschen übrig, so daß in der Dienststelle des Datenschutzbeauftragten ein **erheblicher Personal- und Zeitaufwand** erforderlich ist, um aus ihnen die Grundlagen für die Dateienübersicht nach § 24 LDSG zu extrahieren. Nunmehr wird versucht, die Probleme dadurch in den Griff zu bekommen, daß sich ein Mitarbeiter über ca. ein bis zwei Jahre ausschließlich mit der Aufbereitung befaßt. Im Augenblick ist noch nicht abzuschätzen, ob dies ausreicht, die im Landesdatenschutzgesetz vorgegebenen Termine zu halten.

– **PC-Labor eingerichtet**

Vielfältig sind die von den Behörden eingesetzten PC-Systeme und die entsprechenden Software-Produkte. Das hat uns zur Einrichtung eines **„PC-Labors"** veranlaßt. Auf der Basis eines kleinen PC-Netzes können die zuständigen Mitarbeiter in der Dienststelle die marktgängige **Hard- und Software** (einschließlich Viren) **testen,** Stärken und Schwächen feststellen und Vorschläge für datenschutzrechtlich relevante Sicherheitsmaßnahmen erarbeiten. Dies ist eine Voraussetzung dafür, daß bei Prüfungen und Beratungsgesprächen „vor Ort" die notwendige Sachkompetenz vorhanden ist.

9. Rückblick

– **Sicherheitsüberprüfungsverfahren datenschutzrechtlich verbessert (14. TB, S. 17)**

Unsere Querschnittskontrolle bei den Geheimschutzbeauftragten hat gezeigt, daß die in den Sicherheitsrichtlinien des Landes vorgeschriebene **Trennung der Funktionen** von **Geheimschutzbeauftragtem** und **personalverwaltenden Stellen** in der Praxis nicht hinreichend gewährleistet ist.

Im Juni 1993 hat uns der Innenminister mitgeteilt, es werde nunmehr zugelassen, daß die **Sicherheitserklärung** vom Betroffenen **verschlossen** beim Geheimschutzbeauftragten abgegeben wird, so daß dieser keine Kenntnis von ihrem Inhalt erhält.

Durch diese Neuregelung werden die datenschutzrechtlichen Risiken, die bei einer Vermischung von Personalverwaltung und Geheimschutzbeauftragtem bestehen, weitgehend abgebaut.

– **Verfassungsschutz hat seine Datenbestände noch einmal umfassend bereinigt (15. TB, S. 27)**

Die aufgrund des neuen Verfassungsschutzgesetzes notwendige Datenbereinigungsaktion hat die Verfassungsschutzbehörde zum Ende des 1. Quartals 1993 beendet. Im Vergleich zum Datenbestand vom Dezember 1991 sind die Datensätze dabei um ca. 58 % reduziert worden. Die Entwicklung im rechtsextremistischen Bereich hat allerdings dazu geführt, daß sich bis Jahresende die Anzahl der Datensätze wieder auf ca. 50 % des Ausgangsdatenbestandes (Dezember 1991) erhöht hat.

– **Führung von Personalakten über Referendare (15. TB, S. 24)**

Wir hatten über die Prüfung der **Personalaktenführung über Referendare** beim Schleswig-Holsteinischen Ober-

landesgericht in Schleswig berichtet, eine Reihe praktischer datenschutzrechtlicher Hinweise gegeben und Änderungen in den Rechtsgrundlagen (**Kapazitätsverordnung**) vorgeschlagen. Erfreulicherweise hat sich der Justizminister unserer Auffassung in **allen Punkten** angeschlossen. Auch eine entsprechende Änderung der Kapazitätsverordnung ist auf dem Weg und soll unsere Vorschläge vollständig berücksichtigen.

– **Studentendatenverordnung in Kraft (15. TB, S. 72)**

Die Studentendatenverordnung an deren Erarbeitung wir beteiligt waren, ist am 13.10.1993 erlassen worden (Nachrichtenblatt des Wissenschaftsministeriums 1993, S. 414). Sie regelt, welche **personenbezogenen Daten der** in Schleswig-Holstein **Studierenden** für welche Zwecke von den Hochschulverwaltungen verarbeitet werden dürfen und konkretisiert insoweit die allgemeinen Vorgaben des Hochschulgesetzes. Dabei wurden die von uns gegebenen datenschutzrechtlichen Anregungen berücksichtigt.

– **Aus- und Fortbildung von Führungskräften auf dem Gebiet der Informationstechnik (15. TB, S. 101)**

Die Vermittlung des Themenbereichs „Rechtsvorschriften zur Datenverarbeitung und zum Datenschutz" ist in der DATENSCHUTZAKADEMIE erfolgreich angelaufen (vgl. Tz. 1.4). Leider haben sich bisher noch keine Träger für vergleichbare Seminare auch für die Gebiete „Informatik/Informationstechnik" und „Revision/Kosten-Nutzen-Analysen" gefunden. Falls öffentliche Aus- und Fortbildungseinrichtungen kein Interesse an der Realisierung derartiger Angebote zeigen, werden wir 1994 erste Gespräche mit gewerblichen Einrichtungen führen.

– **Automation in der Landwirtschaftsverwaltung (15. TB, S. 82)**

Das **Regelwerk** für den Einsatz der automatisierten Verfahren in den Ämtern für Land- und Wasserwirtschaft hat der Minister für Ernährung, Landwirtschaft, Forsten und Fischerei zwischenzeitlich **vervollständigt.** Außerdem hat er von dem Fortbildungsangebot der DATENSCHUTZAKADEMIE für Systembetreuer und Datenschutzbeauftragte Gebrauch gemacht. Welche Auswirkungen sich hieraus für die Handhabung der informationstechnischen Systeme in der Praxis ergeben haben, werden künftige Prüfungen „vor Ort" zeigen.

– **In Schleswig-Holstein gibt es bisher keine Fernüberwachung per Satellit (15. TB, S. 76)**

Von der Möglichkeit, die Richtigkeit von Angaben der Landwirte in Förderanträgen nach dem EU-Recht durch

Satellitenfernerkundung zu überprüfen, wird in Schleswig-Holstein bisher **kein Gebrauch** gemacht. Es ist zu hoffen, daß hierauf auf Dauer verzichtet wird.

– **Test- und Freigabe von landesweit eingesetzten automatisierten Verfahren (13. TB, S. 71)**

Nach einem Machtwort des Innenministers werden die landesweit eingesetzten automatisierten Verfahren nunmehr zwar einem **Test** durch einen Beauftragten der künftigen Anwender (Kommunen) unterzogen. Bedenken gegen die Effektivität der Verfahrensweise kommen aber auf, wenn man sich die Zahlen vergegenwärtigt. Das **Einwohnerinformationssystem** als ein Verfahren unter vielen z.B. umfaßt nach einer Veröffentlichung der Datenzentrale zur Zeit **1.572 Programme.** Der neu eingeführte Test erfolgt durch **einen Mitarbeiter** einer Meldebehörde.

– **Protokollierung von Einsichtnahmen in das Grundbuch (15. TB, S. 58)**

Wir hatten über unsere Bemühungen berichtet, eine **Protokollierung** von **Einsichtnahmen in das Grundbuch** zu erreichen. Auch der Justizminister hatte diese Notwendigkeit Anfang vergangenen Jahres ausdrücklich bejaht und angekündigt, mit den Gerichten praktische Fragen zu klären. Derzeit bereitet er einen Erlaß vor, nach dem künftig in einer gesonderten Liste der Name des Einsichtnehmenden sowie das Datum und der Grund für die Einsicht festgehalten werden. Mit einer solchen, aufgrund des Landesdatenschutzgesetzes erforderlichen Regelung werde Schleswig-Holstein den anderen Bundesländern beispielhaft vorangehen. Diese hatten sich wegen des befürchteten Mehraufwandes für die Justizverwaltung gegen eine solche Regelung ausgesprochen. Deshalb ist auch in der im Dezember 1993 vom Bundestag verabschiedeten Änderung der Grundbuchordnung bundesweit noch keine Protokollierungspflicht bei konventioneller Einsichtnahme enthalten. Nach den neu in das Gesetz aufgenommenen Vorschriften über das „maschinell" (per EDV) geführte Grundbuch allerdings dürfen automatisierte Abrufverfahren nur eingerichtet werden, wenn die Zulässigkeit der Abrufe auf der Grundlage einer Protokollierung kontrolliert werden kann.

Beim **Landesbeauftragten für den Datenschutz**
derzeit erhältliche Publikationen

Datenschutz in Schleswig-Holstein
Text des Landesdatenschutzgesetzes und
des Bundesdatenschutzgesetzes
mit einer erläuternden Einführung

Schleswig-Holsteinischer Datenschutztag '92
Landtagsforum 2. Juni 1992
Dokumentation

Faltblätter „Hat der Bürger Rechte!?"
- Die Rechte des Bürgers im Datenschutz
- Was Sie über den Datenschutz wissen sollten
- Die Arbeit des Datenschutzbeauftragten
- Die Pflichten der datenverarbeitenden Stellen

Tätigkeitsberichte
der letzten drei Jahre als Landtagsdrucksache

Tätigkeitsberichte
als Sammlung

Diverse Aufkleber

DATENSCHUTZAKADEMIE SCHLEWIG-HOLSTEIN
- Broschüre
- Jahresprogramm 1993/94

BfD–INFO 1: Bundesdatenschutzgesetz
– Text und Erläuterung
BfD–INFO 2: Der Bürger und seine Daten
herausgegeben vom Bundesbeauftragten für den Datenschutz