SCHLESWIG-HOLSTEINISCHER LANDTAG
12. Wahlperiode

Drucksache 12/823
07. 05. 90

Bericht

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

Zwölfter Tätigkeitsbericht

In der Anlage übersende ich gemäß § 19 Abs. 3 Satz 2 des Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 1. Juni 1978 den zwölften Tätigkeitsbericht des Landesbeauftragten für den Datenschutz bei der Präsidentin des Schleswig-Holsteinischen Landtages.

Becker

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

ZWÖLFTER TÄTIGKEITSBERICHT

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

nach § 19 Absatz 3 des Gesetzes zum Schutz
vor Mißbrauch personenbezogener Daten
bei der Datenverarbeitung
vom 1. Juni 1978

(Berichtszeitraum: März 1989 bis Februar 1990)

Inhaltsverzeichnis

1. Datenschutz auf dem Weg in die 90er Jahre

Wir befinden uns weiter auf dem Weg in die Informationsgesellschaft. Die automatisierte Datenverarbeitung hat fast alle Lebensbereiche ergriffen, ohne daß ein Ende der Entwicklung absehbar wäre. Es vergeht kein Jahr, ja fast kein Monat, in dem nicht in wichtigen Bereichen die elektronische Datenverarbeitung eingeführt oder stets weiter ausgebaut wird. Die Zeit der überschaubaren Insellösungen geht vorbei. Die zunehmende Vernetzung und Verknüpfung setzt einen Kontrapunkt zu datenschutzrechtlichen Denkansätzen wie dem Zweckbindungsprinzip. Der einzelne sieht sich mehr und mehr einem für ihn unüberschaubaren Geflecht der Informationsverarbeitung gegenüber, das das tägliche Leben dominiert und Teil dessen auch seine eigenen personenbezogenen Daten sind.

Der Schutz der Persönlichkeitsrechte in einer unpersönlicher, anonymer und technokratischer werdenden Welt bleibt ein zentrales Thema. Deshalb wird der Datenschutz auch und gerade in den 90er Jahren an Bedeutung gewinnen. Immer mehr Abhängigkeit von der Informationstechnik wird den Ruf nach Korrektiven und Schutz für das Individuum lauter werden lassen. Der Weg in die Informationsgesellschaft ist auf Dauer nicht gangbar, wenn nicht effektiver Datenschutz ein ständiger Wegbegleiter ist. Die Aufgaben für den Datenschutz werden umfangreicher und komplizierter. Wo vermeintlich „abschließende" Regelungen erreicht sind, zwingt der Fortschritt der Technik stets zu weiterführenden Überlegungen. Die treibende Kraft ist der ungebremste Ausbau der elektronischen Datenverarbeitung, auf die der Datenschutz im wesentlichen nur reagieren kann. Auch der Gesetzgeber reagiert in der Regel nur auf die Entwicklungen, die sich auf dem Informationsmarkt ergeben. Häufig reagiert er zu langsam oder zu spät. Die „Hausaufgaben", die sich aus dem Volkszählungsurteil des Jahres 1983 zwingend ergeben, sind weitgehend noch nicht gemacht. Das ständige Herumschleppen der Gesetzgebungshypotheken von gestern behindert den Blick nach vorn und die Entwicklung von Lösungsansätzen für die Probleme von morgen. Auch hier gilt, was in abgewandelter Form derzeit in der Politik so häufig zitiert wird: „Wer mit seinen Gesetzen zu spät kommt, den überholt die Informationstechnik." Denn diese nimmt unbeirrt von Gesetzentwürfen und -diskussionen ihren Weg, und es ist nichts in Sicht, was ihre Verbreitung aufhalten könnte.

Der Bund hat inzwischen modifizierte Entwürfe zum Bundesdatenschutzgesetz und zum Bundesverfassungsschutzgesetz vorgelegt. Einige grobe Mängel der Vorentwürfe scheinen allem Anschein nach ausgemerzt, ohne daß man sagen könnte, es handle sich nunmehr um Gesetzentwürfe mit Vorbildwirkung auch für die Länder. Allenthalben spürbar ist der politische Kompromiß, die Suche nach dem gemeinsamen Nenner, der an vielen Stellen – wie so oft – der kleinste ist.

In zentralen Bereichen wie z. B. bei der Strafprozeßordnung oder bei den Justizmitteilungen kommt der Gesetzgebungsprozeß nicht voran. Dies hat die mißliche Folge, daß in den Ländern zunehmend Polizeigesetze verabschiedet werden, denen im Bereich der Strafverfolgung das Fundament fehlt. Denn die Polizei kann bei der Aufklärung von und Vorbeugung vor Straftaten ihre Befugnisse nur aus der Strafprozeßordnung herleiten.

Da die Gerichte zunehmend auch den sogenannten Übergangsbonus nicht mehr als Grundlage der Datenverarbeitung gelten lassen wollen, entsteht allmählich eine Situation, in der weder Polizei noch Bürger wissen, welche Eingriffe in das Recht auf informationelle Selbstbestimmung bei der Strafverfolgung nun eigentlich zulässig sind. Dies ist für beide Seiten nicht akzeptabel. Erfahrungsgemäß geht es aber eher zu Lasten der Bürger.

In Schleswig-Holstein ist die Situation etwas günstiger, soweit der Landesgesetzgeber Kompetenzen hat. Das inzwischen verabschiedete Schulgesetz und die bislang bekanntgewordenen Entwürfe zum Landesdatenschutzgesetz und zum Landesverfassungsschutzgesetz berücksichtigen viele Vorschläge des Datenschutzbeauftragten. Nach den Erfahrungen mit der „Pfeiffer-Liste" legt der Landesbeauftragte vor allem großen Wert auf klare Regelungen, unter welchen Voraussetzungen Daten des Verfassungsschutzes an die Landesregierung oder an einzelne ihrer Mitglieder übermittelt werden dürfen. Sichergestellt muß auch sein, daß die Daten nur zweckgerecht verwendet und nicht im politischen Tageskampf mißbraucht werden. Werden die vorgelegten Entwürfe noch weiter verbessert statt verwässert, könnten in den genannten Bereichen Gesetze entstehen, die zur deutlichen Stärkung der Rechte der Bürger führen.

Ungünstiger sieht die Situation im Bereich des Archivwesens aus, wo dem Landesbeauftragten noch immer kein Gesetzentwurf der Landesregierung bekannt ist. Es mehren sich die Fälle, in denen es zum Konflikt zwischen den Interessen des Datenschutzes und einer effektiven, insbesondere historischen Forschung kommt. Wichtige Forschungsvorhaben werden verhindert oder verzögert, weil der Landesgesetzgeber die hierfür notwendigen gesetzlichen Grundlagen nicht rechtzeitig schafft. Der Landesbeauftragte ist es leid, sich eine „Bremserrolle" gegenüber der Forschung vorwerfen zu lassen. Aber er ist der Wahrer des Rechts auf informationelle Selbstbestimmung der Bürger und nicht befugt, hierüber zu verfügen. Nur der Gesetzgeber kann regeln, in welchem Umfang die Forschung personenbezogene Daten Dritter einbeziehen darf. Gleiches gilt für den Umgang mit medizinischen Daten im Bereich der Universitäten und der Krankenhäuser. Rechtsgrundlage für die Zugriffe der Forscher auf personenbezogene Patientendaten in Krankengeschichten und Krankenregistern ist bislang ausschließlich die Einwilligung der Betroffenen, die oft genug in der Praxis nicht eingeholt werden kann.

Die besten Gesetze reichen aber nicht aus, wenn sich die Datenverarbeitungspraxis hierdurch nicht entscheidend verbessert. Die Bürger erwarten zu Recht, daß sich nicht nur die Vorschriften ändern, sondern daß dies auch reale Auswirkungen hat. Deshalb legt der Landesbeauftragte großen Wert auf die Kontrolltätigkeit. Die Überprüfung der Datenverarbeitung bei der Polizei des Landes Schleswig-Holstein, die im Berichtszeitraum den Schwerpunkt bildete, zeigt, daß es dort in der Praxis noch viele Mängel bei der Datenverarbeitung gibt. Der Datenschutzbeauftragte mußte eine Reihe von Beanstandungen aussprechen. Er hat sie mit konkreten Vorschlägen verbunden, bei deren Beachtung sich die reale Situation des Datenschutzes in den Polizeibehörden erheblich verbessern würde. Auch in anderen Bereichen der Datenverarbeitung zeigt sich der Unterschied zwischen Theorie und Praxis. Ohne die Kontrollen der Datenschutzbeauftragten wären die Vollzugsdefizite im Datenschutzrecht vermutlich erheblich größer.

Thema Nummer eins sind fast überall die Veränderungen in Mittel- und Osteuropa, die ein noch größeres Tempo als der Ausbau der Datenverarbeitungstechnik angeschlagen haben. Sie haben Folgen auch für die Datenverarbeitung und verlangen datenschutzrechtliche Konsequenzen. Der Abbau der Grenzkontrollen und das Zusammenwachsen der beiden deutschen Staaten werden zu einem vermehrten Datenaustausch auf allen Lebensgebieten führen. Der Datenschutz darf dabei im Eifer des Gefechts nicht auf der Strecke bleiben. Zu den Absprachen und Regelungen, die jetzt mit der DDR getroffen werden, müssen auch datenschutzrechtliche Vorkehrungen gehören. Sie müssen getroffen sein, bevor Daten in größerem Umfang mit der DDR ausgetauscht werden.

Auch in der DDR selbst gibt es Interesse an datenschutzrechtlichen Fragestellungen. Staatliche Stellen aus dem Bezirk Rostock sind an den Landesbeauftragten mit der Bitte um Rat und Unterstützung herangetreten. Man beabsichtigt dort, datenschutzrechtliche Vorschriften zu erarbeiten. Der Landesbeauftragte hat seine Bereitschaft erklärt, seine Erfahrungen einzubringen. Da nun einmal die DDR im Datenschutzrecht vor einem Neuanfang steht und auf anderen Grundlagen aufbauen muß, wäre es allerdings nicht richtig, unsere Datenschutzgesetze einfach auf die DDR zu übertragen. Denkbar ist, daß dort eigene, neue Ansätze gefunden werden, die durch eine bloße Aufoktroyierung unserer Datenschutzgesetze nicht verschüttet werden sollten. Der Landesbeauftragte wird deshalb im Rahmen seiner Kontakte mit den entsprechenden Stellen in der DDR nicht nur reden, sondern auch zuhören.

Datenschutzrechtliche Folgen müssen die Veränderungen in der DDR und im Ostblock aber auch bei uns selbst haben. Hier bieten sich neue Chancen für mehr Datenschutz. Was im Zeichen des kalten Krieges entstanden ist, darf nicht unverändert fortgeführt werden. Insbesondere bei den Geheim-

diensten müssen Datenverarbeitungspraktiken kritisch überprüft werden, deren Notwendigkeit man unter anderen politischen Gegebenheiten bejahen konnte.

Die Abschaffung der „Adressendatei Ost" (ADOS), in der die Daten von Aus- und Übersiedlern gespeichert wurden, kann nur ein Anfang sein. Es ist erfreulich, daß der schleswig-holsteinische Innenminister dem Drängen des Landesdatenschutzbeauftragten nachgekommen ist und als erster den Ausstieg aus ADOS verkündet hat. Aber hier geht es weniger um die Beendigung eines etablierten Datenverarbeitungsverfahrens als vielmehr um die rechtzeitige Entscheidung, mit dem System gar nicht erst richtig zu beginnen. ADOS war nämlich eine Neuentwicklung, die unter anderen politischen und nachrichtendienstlichen Rahmenbedingungen konzipiert worden war. Die Datenerfassung hatte bei Beginn der Veränderungen in der DDR gerade erst angefangen, so daß der Abschied von ADOS keine allzu bitteren Tränen gekostet haben wird.

Wichtiger sind die notwendigen Folgerungen auf anderen Gebieten. Seit Jahrzehnten sammelt z. B. der Bundesgrenzschutz (BGS) an den Grenzen nach von den Geheimdiensten vorgegebenen Rastern Daten über reisende Bundesbürger. Nach entsprechenden „Enthüllungen" Anfang der 80er Jahre wurde das Verfahren ein wenig modifiziert und umbenannt, im Kern aber unverändert fortgeführt. Die politischen Veränderungen der vergangenen Monate bieten die Chance, diese Praktiken zu beenden. Freies Reisen sollte immer auch das Recht auf unbeobachtetes und nicht registriertes Reisen sein. Der Landesbeauftragte ist deshalb dafür eingetreten, daß der BGS an der Grenze nur noch terrorismus- und spionagebezogene Daten sammelt, da es insoweit auch um polizeirelevante Daten geht. Kurz vor Fertigstellung des Berichts traf die Mitteilung ein, daß der Innenminister auch die Amtshilfe des BGS für den schleswig-holsteinischen Verfassungsschutz weitgehend einstellen möchte. Dies hat der Landesbeauftragte mit Befriedigung zur Kenntnis genommen.

Zieht man Bilanz, so hinterläßt der Ausblick auf die 90er Jahre gemischte Gefühle. Gesicherten Freiheitsräumen für den einzelnen stehen neue Bedrohungen gegenüber. Wir brauchen nicht weniger, sondern mehr Datenschutz, weil wir auch immer mehr automatisierte Datenverarbeitung bekommen. Das Persönlichkeitsrecht ist nicht statisch, sondern muß stets dynamisch gegen neue Gefährdungen geschützt und erkämpft werden. Daß der Datenschutzbeauftragte dies mit vollem Engagement tut, darauf können sich die Bürgerinnen und Bürger von Schleswig-Holstein verlassen.

2. Das Parlament und „sein" Datenschutzbeauftragter

Auch der 11. Tätigkeitsbericht wurde auf breiter parlamentarischer Basis beraten. Der Landesbeauftragte erhielt Gelegenheit, den federführenden Innen- und Rechtsausschuß sowie den Ausschuß für Kultur, Jugend und Sport und den

Sozialausschuß über das Spektrum der datenschutzrechtlichen Sachverhalte und Forderungen des vergangenen Jahres zu informieren und Fragen zu beantworten. Dabei konnte er die zunehmende Bereitschaft der Ministerien hervorheben, ihn als Berater schon bei der Vorbereitung von Gesetzentwürfen zu beteiligen. Seine Mitarbeiterinnen und Mitarbeiter und er selbst haben dies besonders gern getan, weil ihre Hinweise und Empfehlungen häufig aufgegriffen und in Gesetzentwürfen berücksichtigt wurden. Hierzu ist insbesondere auf die Novellierung des Landesschulgesetzes zu verweisen, die vom ersten Vorentwurf über die Regierungsvorlage bis zur parlamentarischen Beratung datenschutzrechtlich begleitet wurde. Auch an den laufenden Vorarbeiten zu einem Verfassungsschutz- und Polizeigesetz sowie zur Novellierung des Landesdatenschutzgesetzes beteiligte der Innenminister den Datenschutzbeauftragten und zeigte Offenheit für manche „bessere" datenschutzgerechtere Lösung.

Ebenso positiv beurteilt der Landesbeauftragte die Tatsache, daß das Landesparlament selbst zunehmend die Dienste „seines" Datenschutzbeauftragten in Anspruch nimmt. Dies zeigte sich nicht nur bei den Beratungen zu Gesetzentwürfen der Regierung, sondern auch, als es um die Absicht des Parlaments ging, aus der „Kieler Affäre" die Konsequenzen für das Landesverfassungsrecht zu ziehen. Der Landesbeauftragte erhielt Gelegenheit, Empfehlungen zur datenschutzrechtlichen Absicherung des parlamentarischen Akteneinsichts- und Aktenvorlagerechts zu machen, die in den Beratungen allseits aktzeptiert wurden.

Aber das Parlament „nahm" nicht nur, es „gab" auch. Dank seiner Unterstützung und der Bemühungen der Landtagsverwaltung konnte die Dienststelle des Landesbeauftragten eine „behördenferne" und gleichzeitig „parlamentsnahe" Unterkunft im „Regierungsviertel" beziehen. Die Beendigung der provisorischen Unterbringung 14 Monate nachdem die Dienststelle des Landesbeauftragten aus dem Innenministerium herausgelöst und an das Parlament angegliedert worden war, beginnt allerdings wieder mit einem Provisorium: Die neuen Diensträume müssen in den nächsten beiden Jahren erst noch umgebaut werden.

3. Parlamentsreform und Reform des kommunalen Verfassungsrechts: Transparenz und Datenschutz

Offenheit, das war in den letzten Monaten zu erleben, ist unverzichtbare Grundlage eines demokratischen Miteinander. Nur wenn Entscheidungsabläufe transparent sind, sind die Bürger, sind ihre Repräsentanten in den Vertretungskörperschaften des Staates und der kommunalen Verwaltung in der Lage, die Entwicklung im Gemeinwesen zu gestalten. Offenheit und Transparenz sind die Basis demokratischer Lebensformen und haben ihre Bezüge zum Recht auf informationelle Selbstbestimmung. Abstriche davon bedürfen besonderer Rechtfertigung.

Andererseits sind die Achtung der Menschenwürde und die Möglichkeit für den einzelnen, sich frei zu entfalten, Grundbedingungen für den Bestand und die Fortentwicklung der Demokratie. Diese Persönlichkeitsrechte konkretisieren sich u. a. in einem Anspruch auf Privatheit und dem Recht, selbst zu bestimmen, welche Informationen über die eigene Persönlichkeit offenbart werden sollen. Einschränkungen dieses Rechts können nur durch normenklare gesetzliche Vorschriften gerechtfertigt werden.

Beide Grundsätze, das Recht der Öffentlichkeit auf Information über Entscheidungsvorgänge und das Recht der Bürger auf Vertraulichkeit ihrer persönlichen Verhältnisse haben gemeinsame Wurzeln, geraten aber im Einzelfall immer wieder einmal in Konflikt. Dieser ist deshalb nicht einfach zu lösen, weil beide Rechtspositionen einander im Grundsatz gleichrangig gegenüberstehen.

In welche Richtung Konfliktlösungen gehen müssen, zeigt das „Flick-Urteil" des Bundesverfassungsgerichts. Dort wird ausgeführt, daß sich „Beweiserhebungsrechte des parlamentarischen Untersuchungsausschusses und grundrechtlicher Datenschutz ... auf der Ebene des Verfassungsrechts gegenüber(stehen) und ... im konkreten Fall einander so zugeordnet werden (müssen), daß beide soweit wie möglich ihre Wirksamkeit entfalten" (BVerfGE 67, 143 f.). Dieser Grundsatz dürfte nicht nur auf die politische Kontrolle durch das Parlament anwendbar sein, sondern auch für die aus dem Verfassungsgrundsatz kommunaler Selbstverwaltung abgeleiteten Kontrollrechte kommunaler Vertretungskörperschaften seine Bedeutung haben.

Davon ist der Landesbeauftragte ausgegangen, als er den Landtag bei den Erörterungen einer Verfassungsreform in Schleswig-Holstein und einer Novelle zum Kommunalverfassungsrecht beraten hat. Das gesetzgeberische Ziel war, durch mehr demokratische Offenheit die Rechte der Vertretungskörperschaften und ihrer Mitglieder auf Information gegenüber der Verwaltung zu stärken. Mittel dazu sollten u. a. das Recht auf Akteneinsicht und die Öffentlichkeit der Sitzungen von Fachausschüssen sein. Wie war unter diesen Vorgaben das Persönlichkeitsrecht betroffener Bürger zu wahren?

Wie die Exekutive muß auch die Legislative Umfang und Intensität von Eingriffen in das informationelle Selbstbestimmungsrecht gegen das Recht auf Information der Allgemeinheit abwägen. Überdies muß das in einem Gesetz geschehen, das die Grundsätze der Normenklarheit und der Verhältnismäßigkeit berücksichtigt. Der Landesbeauftragte empfahl deshalb, das für die neue Verfassung des Landes vorgesehene erweiterte Informationsrecht des Landtages in seinem Wortlaut zu ergänzen. Daraufhin wurde der Begriff der „überwiegenden schutzwürdigen Belange einzelner" in den Entwurf eingefügt, bei deren Gefährdung die Landesregierung gehalten ist, Auskünfte an das Parlament zu verweigern oder die

Vorlage von Akten abzulehnen. Mit dem Rechtsbegriff der „schutzwürdigen Belange" ist der wesentliche Ausgangspunkt für das notwendige weitere Verfahren verankert. Es folgt daraus nämlich, daß

- jedes Informationsersuchen der Vertretungskörperschaft oder ihrer Mitglieder zu einer Einzelentscheidung der informationsverwaltenden Stelle führen muß,
- diese Entscheidung eine konkrete Abwägung zwischen Individualrecht der Betroffenen und Aufgabenerfüllung der Vertretungskörperschaft im Einzelfall voraussetzt und
- eine nachprüfbare Rechtsentscheidung zu treffen ist, die nicht von politischer Zweckmäßigkeit oder zufälligen Abstimmungsmehrheiten bestimmt werden darf.

Da vorgesehen ist, zu der neuen Verfassungsbestimmung ein ausführendes Gesetz zu erlassen, sollten dort die notwendigen eingehenderen Regelungen getroffen werden. Hierzu könnten Kriterien für die Entscheidung gehören, wann dem Individualrecht der Vorrang vor dem Informationsanspruch der Vertretung gebührt. Maßnahmen und Verfahren sind anzuordnen, die den Schutz und die Sicherheit besonders vertraulicher Informationen und Akten im Parlament gewährleisten. Schließlich bedarf es als Korrelat zu einem erweiterten Informationsrecht eines Schutzes der Informationen gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote und einer Verpflichtung der Abgeordneten, die erlangten Kenntnisse vertraulich zu behandeln.

Da die Forderung nach Offenheit und Transparenz auch den Rechtskreis der einzelnen Abgeordneten berührt - denn auch sie sind als Personen gegenüber „ihrem" Parlament Träger des eigenen informationellen Selbstbestimmungsrechts – sah sich der Landesbeauftragte veranlaßt, in diesem Zusammenhang auch eine klare gesetzliche Grundlegung für die schon heute praktizierten Mitteilungspflichten der Abgeordneten in den „Verhaltenregeln für die Mitglieder des Schleswig-Holsteinischen Landtages" anzuregen. Der Zweck der Angaben zur Person, die Befugnis der Präsidentin des Landtages, diese Informationen zu verwenden, und die Notwendigkeit, sie zu schützen, sollten nach Auffassung des Landesbeauftragten im Abgeordnetengesetz festgelegt werden.

In diesen Anregungen sieht der Landesbeauftragte eine tragfähige Grundlage für Entscheidungen zwischen Offenbarungspflicht und Recht auf Vertraulichkeit. Die Einzelfallabwägung und die nach Rechtsgrundsätzen und nicht allein nach Mehrheiten zu treffende Entscheidung sind darüber hinaus der methodische Ansatz, auch die Informationsersuchen kommunaler Vertretungskörperschaften gegenüber den Kommunalverwaltungen zu beurteilen.

4. Sorgen der Bürgerinnen und Bürger, Ergebnisse von Kontrollen, Beratung der Behörden

4.1 Allgemeine und innere Verwaltung

4.1.1 Personalwesen

4.1.1.1 Das neue Mitbestimmungsgesetz – Mitbestimmung auch für den Betroffenen?

Der Entwurf eines neuen Mitbestimmungsgesetzes für die Beschäftigten im öffentlichen Dienst enthält von dem Grundsatz, daß eigentlich alle Beschäftigten unter die Mitbestimmung des Personalrates fallen sollen, eine Reihe von Ausnahmen. Für Beamte der Besoldungsgruppe B und vergleichbare Angestellte ist beabsichtigt, die Mitbestimmung durch den Personalrat generell auszuschließen, für andere Mitarbeiter soll der Personalrat nur auf Antrag tätig werden. Soweit im Einzelfall besonders schutzwürdige persönliche Interessen von Beschäftigten berührt werden, soll die Beteiligung des Personalrats von der Zustimmung der Betroffenen abhängig gemacht werden.

Der Personalrat hat als Interessenvertreter der Mitarbeiter die Aufgabe, an den sie betreffenden Entscheidungen der Dienststelle mitzuwirken. Mit der Einschaltung des Personalrates ist aber in aller Regel auch eine Offenbarung besonders schützenswerter Daten des Betroffenen verbunden.

Aus datenschutzrechtlicher Sicht wäre es deshalb zu begrüßen, wenn jeder für sich selbst die Entscheidung treffen könnte, ob er eine Mitbestimmung durch den Personalrat in seinem Fall wünscht.

Nach dem Gesetzentwurf ist weiter vorgesehen, dem Personalrat schriftliche Unterlagen und in Dateien gespeicherte Daten uneingeschränkt zugänglich zu machen. Nur für Personalakten und für dienstliche Beurteilungen ist eine Sonderregelung geplant. Über deren Inhalt bzw. Ergebnis soll der Personalrat lediglich insoweit informiert werden, wie es für die Erfüllung seiner Aufgaben erforderlich ist.

Für den Landesbeauftragten stellt sich die Frage, weshalb diese Einschränkungen nicht auch bei der Bereitstellung schriftlicher Unterlagen und in Dateien gespeicherter Daten gelten sollen. Auch solche Daten dürfen dem Personalrat nur zu seiner rechtmäßigen und erforderlichen Aufgabenerfüllung zugänglich gemacht werden.

Wie wichtig eindeutige gesetzliche Regelungen für die Datenflüsse an den Personalrat sind, zeigt nachfolgender Fall: Versetzungsanträge von Lehrkräften sollten in Kopie an einen Personalrat weitergegeben werden. Für den Landesbeauftragten war die Rechtslage eindeutig. Nach dem derzeit gültigen Personalvertretungsgesetz dürfen Personalakten nur mit Zustimmung der Mitarbeiter und nur von den von ihnen bestimmten Mitgliedern des Personalrates eingesehen werden. Versetzungsanträge sind rechtlich mit ihrem Eingang beim Dienstherrn als Bestandteil der Personalakte anzusehen.

Soweit Kopien quasi als Auszug aus der Personalakte ohne Zustimmung der Betroffenen an den Personalrat weitergegeben werden, liegt darin ein Verstoß gegen geltendes Recht, den der Landesbeauftragte im konkreten Fall gegenüber der Ministerin für Bildung, Wissenschaft, Jugend und Kultur beanstandet hat. Wohlgemerkt, es ging in diesem Fall nicht darum, dem Personalrat den Zugang zu Daten zu verwehren, die er im Einzelfall objektiv benötigt. Der Dienstherr ist aber verpflichtet, eben nur diese Daten und nicht weitere „überflüssige" Informationen bereitzustellen.

Die Ministerin für Bildung, Wissenschaft, Jugend und Kultur hat aufgrund der Bedenken des Landesbeauftragten den für das Beamtenrecht zuständigen Innenminister um Stellungnahme gebeten. Dieser hat sich der Meinung des Landesbeauftragten angeschlossen.

4.1.1.2 Auch Gleichstellungsbeauftragte achten das Persönlichkeitsrecht

Die „Richtlinien zur Gleichstellung der Frauen im schleswig-holsteinischen Landesdienst" (Gleichstellungsrichtlinien) berühren auch Probleme des Datenschutzes. Richtlinien und Verwaltungsanweisungen können nämlich das Verfahren nur im Rahmen bestehender Gesetze gestalten. Sie können insbesondere nicht ohne gesetzliche Grundlage das informationelle Selbstbestimmungsrecht Betroffener einschränken.

Soweit die behördeninternen Gleichstellungsbeauftragten Angaben über einzelne Mitarbeiterinnen und Mitarbeiter erhalten, ist das datenschutzrechtlich unbedenklich, solange diese Angaben den Bereich der personalverwaltenden Dienststelle nicht verlassen, also „Dritten" nicht zugänglich werden. Die Gleichstellungsbeauftragten werden nach den Richtlinien nur innerhalb der Dienststelle tätig, sind der Dienststellenleitung unterstellt und haben keine Entscheidungsrechte. In diesem Rahmen kann das organisatorische Verfahren für eine interne Personalentscheidung auch ohne Gesetz geregelt werden. So wie sich die Dienststelle spezieller Personalreferenten und ihrer Mitarbeiter bedienen kann, bleibt ihr auch eine Beratung durch eine interne Gleichstellungsbeauftragte unbenommen.

Allerdings folgt daraus nicht das generelle Recht der Gleichstellungsbeauftragten, in die vollständigen Personalakten Einsicht zu nehmen. Das Informationsrecht ist vielmehr auf solche Unterlagen begrenzt, die zur Aufgabenerfüllung erforderlich sind. Eine Verfahrensvereinfachung oder eine Erleichterung der Entscheidung allein rechtfertigen noch nicht die Akteneinsicht. Verantwortlich für den Umfang der vorgelegten Informationen bleibt die Dienststellenleitung. Sie wird im Konfliktfall begründen müssen, weshalb eine bloße Auskunft oder eine Teileinsicht nicht ausgereicht hätte und deshalb die Entscheidung schriftlich dokumentieren müssen. Wird in Mitarbeiterrechte eingegriffen, so ist eine vorherige Unterrichtung geboten.

Unverzichtbar ist eine gesetzliche Regelung jedoch, wenn im Rahmen ressortübergreifender Abstimmungen im Einzelfall „im Benehmen" mit der Frauenministerin personenbezogene Informationen etwa über Vergleichsfälle und Konkurrentinnen und Konkurrenten den Zuständigkeitsbereich der personalverwaltenden Dienststellen verlassen sollen.

4.1.1.3 Die Telefondatenerfassung erhält durch ISDN eine neue Qualität

Der Landesbeauftragte hat das Problem der Telefondatenerfassung wiederholt aufgegriffen (zuletzt im 11. TB, S. 12). Er muß nun auf die neueste Entwicklung in der Fernmeldetechnik der Deutschen Bundespost hinweisen und abermals warnen, denn die Deutsche Bundespost bietet als besonderen Postdienst auf Antrag einen Einzelgebührennachweis für solche Teilnehmer an, die an das digitale Fernmeldenetz (ISDN) angeschlossen sind. Dieser Postdienst listet Datum, Uhrzeit, Zielnummer und Gebühreneinheiten aller Einzelgespräche auf, die von einem bestimmten Anschluß geführt wurden. Der Anschlußinhaber kann so jedes ausgehende Gespräch nach Zeitpunkt und Zielnummer feststellen. Durch einen Vergleich des Einzelgebührennachweises mit internen Aufzeichnungen dienstlicher Gespräche können damit die Zielnummern privater Telefongespräche von dienstlichen Anschlüssen auch dann ermittelt werden, wenn sie in der Nebenstellenanlage selbst nicht registriert wurden.

Ob dieser neue Service der Deutschen Bundespost mit dem Recht auf informationelle Selbstbestimmung vereinbar ist, wird vom Bundesbeauftragten für den Datenschutz untersucht. Die Vorkehrungen, die öffentliche Stellen des Landes Schleswig-Holstein in diesem Zusammenhang zu treffen haben, hat der Landesbeauftragte zu beurteilen. Soll den einvernehmlich erarbeiteten Grundsätzen für die Gebührendatenerfassung in Schleswig-Holstein entsprochen werden, bleibt nur die Möglichkeit, daß öffentliche Stellen, die sich mit automatisch aufzeichnenden Nebenstellenanlagen an das ISDN-Netz anschließen und Privatgespräche über diese Anschlüsse zulassen, keinen Einzelgebührennachweis in Anspruch nehmen. Der Innenminister beabsichtigt, für die Inanspruchnahme zusätzlicher Datenaufzeichnungen der Bundespost durch die Dienststellen eine besondere Genehmigung der jeweiligen obersten Dienstbehörde vorzusehen. Sie müßte für solche Dienststellen versagt werden, in denen automatisch aufzeichnende Nebenstellenanlagen verwendet werden.

4.1.2 Verfassungsschutz

4.1.2.1 Zweckbindung innerhalb des Verfassungsschutzes

Im 11. Tätigkeitsbericht (S. 21) hatte der Landesbeauftragte über Schwachstellen in den neuen Sicherheitsrichtlinien berichtet. Er machte dabei Verfahrensvorschläge, mit deren

Hilfe das Freiwilligkeitsprinzip bei der Überprüfung von Angehörigen der Mitarbeiter gewährleistet werden sollte. Wie berichtet, hat der Innenminister diese Vorschläge abgelehnt.

In einer anderen wichtigen Frage hat der Datenschutzbeauftragte eine wesentliche Verbesserung erreicht. Auf seinen Vorschlag hat der Innenminister zugesichert, daß Daten, die im Rahmen einer Sicherheitsüberprüfung erhoben worden sind, künftig darüber hinaus nur noch für Zwecke der Spionageabwehr genutzt werden. Auf eine Nutzung für sonstige Zwecke des Verfassungsschutzes wird völlig verzichtet. Damit ist Schleswig-Holstein nach Kenntnis des Landesbeauftragten das erste Land, das den Zweckbindungsgrundsatz im Rahmen der Sicherheitsüberprüfung in dieser umfassenden Weise anerkannt hat. Erstmalig ist damit auch bestätigt worden, daß hinsichtlich der Datennutzung zwischen den verschiedenen Aufgaben der Verfassungsschutzbehörde zu unterscheiden ist.

Der Landesbeauftragte wertet dies auch im Hinblick auf zu erwartende bundesgesetzliche Regelungen zur Sicherheitsüberprüfung als einen wichtigen Durchbruch. Er verspricht sich daraus eine Verbesserung der Position der betroffenen Mitarbeiter und deren Angehöriger.

Ungelöst ist weiterhin das Problem der fehlenden Rechtsgrundlage für die Sicherheitsüberprüfung. Hierfür ist ein spezielles, normenklares Gesetz notwendig. Bis zu seinem Erlaß dürfen Sicherheitsüberprüfungen nur im unbedingt erforderlichen Umfang durchgeführt werden. Dabei muß auch berücksichtigt werden, daß infolge der Veränderungen in der DDR und Osteuropa nicht mehr so häufig und nicht mehr so intensiv überprüft werden muß.

Die jetzt zugesagte Zweckbindung der Daten ist ein wichtiger Schritt, um die Folgen aus der fehlenden Rechtsgrundlage für das Recht auf informationelle Selbstbestimmung abzumildern.

4.1.2.2 Neue Wege im Landesverfassungsschutzgesetz

Kurz vor Fertigstellung dieses Berichts hat das Kabinett den Entwurf für ein neues Landesverfassungsschutzgesetz verabschiedet. Der Landesbeauftragte war frühzeitig beteiligt und hat sich schriftlich und in Besprechungen hierzu geäußert. Seine Vorstellungen sind weitgehend berücksichtigt worden. Von einigen Einzelpunkten abgesehen, ist der Landesbeauftragte insgesamt mit dem vorgelegten Entwurf zufrieden. Er dürfte im Ergebnis zu mehr Rechtssicherheit und zu mehr Datenschutz beim Verfassungsschutz führen. Zu den wesentlichen Veränderungen gegenüber dem bisherigen Gesetz gehören:

- Die Aufgaben des Verfassungsschutzes, insbesondere bei der Beobachtung verfassungswidriger Bestrebungen, werden präziser umschrieben.

- Bei den Befugnissen wird stärker differenziert; sie werden den einzelnen Aufgaben zugeordnet.
- Die nachrichtendienstlichen Mittel werden im Gesetz beispielhaft aufgezählt. Ihre verbindliche Festlegung in einer Dienstanweisung wird vorgeschrieben. Die Verwendung der mit nachrichtendienstlichen Mitteln erhobenen Daten wird speziell geregelt. Greifen nachrichtendienstliche Mittel besonders intensiv in die Rechte der Bürger ein, so ist ihre Anordnung dem Minister vorbehalten. Die Bürger müssen im nachhinein unterrichtet werden.
- Erstmals wird das Zweckbindungsprinzip innerhalb des Verfassungsschutzes geregelt.
- Das Auskunftsrecht der Bürger auch gegenüber dem Verfassungsschutz wird grundsätzlich anerkannt. Wird dem Auskunftsanspruch ausnahmsweise nicht Genüge getan, so ist der Betroffene ausdrücklich darauf hinzuweisen, daß er den Landesbeauftragten für den Datenschutz anrufen kann.
- Die Verarbeitung personenbezogener Daten, insbesondere die Speicherung in Dateien, wird im Vergleich zum bisherigen Recht restriktiv geregelt.
- Der Datenaustausch zwischen Polizei und Verfassungsschutz wird eingeschränkt.
- Eine allgemeine Berichtspflicht der Behörden des Landes gegenüber dem Verfassungsschutz besteht nur, sofern ein Terrorismus- oder Spionageverdacht besteht.

Der Landesbeauftragte sieht in diesem Gesetzentwurf viele seiner seit Jahren erhobenen Forderungen bestätigt. Er hofft, daß er möglichst bald vom Gesetzgeber verabschiedet wird, damit Bürgerinnen und Bürger in Schleswig-Holstein dem Gesetz entnehmen können, mit welchen Eingriffen in ihr informationelles Selbstbestimmungsrecht durch die Verfassungsschutzbehörde sie rechnen müssen.

4.1.2.3 Der Bundesgrenzschutz beobachtet an der Grenze nicht mehr für den Verfassungsschutz

Zum freien Reisen gehört auch die Gewißheit, daß Grenzübertritte nicht beobachtet und gespeichert und den Bürgern später einmal entgegengehalten werden, wenn sie in das „falsche" Land gereist sind. Diese Freiheit galt für die Bundesbürger in der Vergangenheit nur mit gewissen Einschränkungen. Der Bundesgrenzschutz (BGS) leistete nämlich seit Jahrzehnten Amtshilfe in der Form, daß er Daten über Bürger nach von den Geheimdiensten vorgegebenen Rastern erhob und an diese weiterleitete. Man unterscheidet zwischen der „benannten" und der „unbenannten Amtshilfe". Bei der benannten Amtshilfe werden von den Geheimdiensten Namen an den BGS übermittelt, die dort in die Grenzfahndungsdatei eingespeichert werden. Werden die betreffenden Personen beim Grenzübertritt kontrolliert, so sind ihr Name und der

ihrer Begleiter unauffällig zu notieren und an die ausschreibende Geheimdienstbehörde zu übermitteln. Bei der „unbenannten Amtshilfe" werden Daten über Bürger erhoben, bei denen Umstände vorliegen, die auf ein von den Geheimdiensten vorgegebenes Raster „passen". Derartige Daten wurden in den vergangenen Jahren vornehmlich – aber nicht ausschließlich – an den Ostgrenzen erhoben.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich stets gegen diese Form der Amtshilfe gewandt. Sie konnten sich dabei auch auf Rechtsgutachten stützen, die im Auftrag des Bundesinnenministers erarbeitet worden waren und in denen nachgewiesen war, daß derartige Datenerhebungen nicht zu den Aufgaben des BGS zählen. Sie wären also nur auf der Basis einer eigenständigen Rechtsgrundlage zulässig gewesen. Gleichwohl ist die Praxis in den vergangenen Jahren auf der Grundlage einer vom Bundesinnenminister herausgegebenen Dienstanweisung fortgeführt worden.

Die Veränderungen im Osten haben den Landesbeauftragten erneut veranlaßt, die schleswig-holsteinische Verfassungsschutzbehörde aufzufordern, zu überprüfen, ob sie an dieser Form der Amtshilfe des BGS weiter festhält und ob und in welcher Form die vom BGS bislang übermittelten Daten gespeichert werden. Sie hat daraufhin mitgeteilt, daß ab sofort auf „unbenannte" Amtshilfersuchen an den BGS verzichtet werden kann. Dieser Teil der Amtshilfe des BGS wird folglich für die schleswig-holsteinische Verfassungsschutzbehörde in Zukunft nicht mehr praktiziert. Was die Speicherung der bislang vom BGS übermittelten Daten angeht, so hat die Verfassungsschutzbehörde mitgeteilt, daß sie weitgehend bereits gelöscht sind. Man werde im Zuge der weiteren Bereinigungsarbeiten Hinweise auf derartige vom BGS gemeldete Reisen tilgen.

Zu lösen bleibt nach Auffassung des Landesbeauftragten noch das Problem der „benannten Amtshilfe". Auch sie ist nur auf der Grundlage einer ausdrücklichen gesetzlichen Ermächtigung zulässig. Es stellt sich sogar die Frage, unter welchen Voraussetzungen diese Form der Amtshilfe mit dem verfassungskräftigen Trennungsgebot zwischen Polizei und Nachrichtendiensten vereinbar ist. Hier geht es nämlich darum, daß die Verfassungsschutzbehörden den BGS um die Vornahme einer den Polizeibehörden vorbehaltenen Datenverarbeitungsmaßnahme ersuchen, nämlich um die Einspeicherung von Daten in die polizeiliche Fahndungsdatei. Ohne ein Ersuchen von Verfassungsschutzbehörden würden die betreffenden Daten dort nicht gespeichert und dementsprechend auch beim Grenzübertritt nicht abgerufen. Der Landesbeauftragte hat deshalb erhebliche Zweifel, ob diese Form der Amtshilfe unter verfassungsrechtlichen Gesichtspunkten zulässig sein kann. Derzeit hat allerdings die schleswig-holsteinische Verfassungsschutzbehörde keine Amtshilfeersuchen an den BGS im Rahmen der „benannten Amtshilfe" gestellt.

4.1.2.4 Abschied von ADOS

Vor einem Jahr wurde von den Verfassungsschutzbehörden des Bundes und der Länder die „Adressendatei Ost" (ADOS) eröffnet. In ihr wurden Daten über frühere Wohnsitze und Arbeitsstätten von Aus- und Übersiedlern aus dem Ostblock gespeichert. Wäre ADOS so wie geplant aufgebaut und betrieben worden, so wären darin Millionen von Datensätzen gespeichert worden. Zweck der Speicherung war es, im Falle von Spionageverdachtsfällen mit Hilfe der gespeicherten Adressen früherer Wohn- und Arbeitsorte in der DDR nunmehr in der Bundesrepublik lebende Zeugen ausfindig zu machen. Es handelte sich also gewissermaßen um die vorbeugende Speicherung möglicher Zeugen möglicher künftiger Spionageverdachtsfälle.

Eine derart weit im Vorfeld angelegte Speicherung war dem Landesbeauftragten aus dem gesamten Sicherheitsbereich bislang noch nicht bekannt. Er hat deshalb erhebliche rechtliche Bedenken gegen ADOS geltend gemacht und den Innenminister darauf hingewiesen, daß das geltende Recht hierfür keine Grundlage enthält. Er hat darüber hinaus Zweifel angemeldet, ob eine verfassungsmäßige Grundlage für ADOS überhaupt möglich wäre. Eine so weit ins Vorfeld verlagerte Datenspeicherung stößt an grundsätzliche verfassungsrechtliche Grenzen. Den Innenminister des Landes Schleswig-Holstein hat er aufgefordert, die von der schleswig-holsteinischen Verfassungsschutzbehörde eingegebenen Daten in ADOS zu löschen.

Dem hat der Innenminister nunmehr mit der Mitteilung „Adios ADOS" zugestimmt. Zwischenzeitlich haben auch der Bund und die anderen Länder reagiert und mitgeteilt, daß die in ADOS gespeicherten Datensätze vernichtet wurden. Der Landesbeauftragte begrüßt dies und ist darüber hinaus der Auffassung, daß auch für künftige Fälle ausgeschlossen sein muß, daß Sicherheitsbehörden mögliche spätere Zeugen noch nicht einmal begangener Straftaten auf Vorrat speichern.

4.1.3 Öffentliche Sicherheit und Ordnung

4.1.3.1 Datenschutzkontrolle bei der Polizei: Noch manches liegt im argen

Im Berichtszeitraum konnte eine umfassende Querschnittsprüfung der Datenverarbeitung bei der Polizei des Landes abgeschlossen werden. Die Kontrolle erstreckte sich über einen Zeitraum von mehr als einem Jahr. In ihrem Verlauf wurden sowohl das Kriminalpolizeiamt mit mehreren Hauptsachgebieten als auch eine Kriminalpolizeidirektion und eine Kriminalpolizeistelle geprüft. In den verschiedenen polizeilichen Datensammlungen wurden stichprobenweise Erhebungen vorgenommen. Einbezogen waren sowohl Kriminalakten als auch Vorgangsablagen, Rauschgifttäterakten, Hinweisakten, Personenakten und andere kriminalpolizeiliche perso-

nenbezogene Sammlungen. Im Mittelpunkt standen dabei die Personenerkenntnisdatei „PED", die Arbeitsdateien „PIOS-Rauschgift", „PIOS-Organisierte Kriminalität" und „PIOS-Innere Sicherheit". Bei den manuellen Dateien standen die Lichtbildvorzeigekarteien im Vordergrund.

Das Ergebnis der Kontrolle kann dahin gehend zusammengefaßt werden, daß eine Vielzahl von Mängeln in der Datenverarbeitung der Polizei festgestellt wurde. Der Landesbeauftragte hat deshalb eine Reihe von Beanstandungen ausgesprochen. Zugleich hat er konkrete Empfehlungen zur Veränderung der polizeilichen Datenverarbeitung und zur Überarbeitung der ihr zugrunde liegenden Vorschriften gegeben. Schwerpunkte seiner Feststellungen waren:

Polizeiliche Kriminalakten

Kern der polizeilichen personenbezogenen Datenverarbeitung ist die Kriminalakte. Zum Zeitpunkt der Prüfung waren noch 240 000 Kriminalakten im Land Schleswig-Holstein vorhanden. Noch vor zehn Jahren lag die Zahl bei ca. 600 000 bis 650 000. Ohne daß die zugrunde liegenden Gesetze oder Erlasse geändert worden sind, wurde die Zahl der Kriminalakten in diesem Zeitraum um 400 000 verringert (vgl. dazu auch 11. TB, S. 57). Dem Landesbeauftragtenn stellt sich die Frage, welcher Bestand an Kriminalakten zur rechtmäßigen Aufgabenerfüllung nun tatsächlich erforderlich ist. Er hat deshalb darauf gedrängt, die Zweckbestimmung der Kriminalakten konkret zu definieren, damit ein Maßstab für die Beurteilung der Erforderlichkeit der noch vorhandenen Kriminalakten gegeben ist. Nach seiner Einschätzung könnte der derzeitige Bestand erneut um 30 bis 40 % verringert werden, ohne daß die polizeiliche Aufgabenerfüllung ernsthaft gefährdet würde.

Für polizeiliche Kriminalakten über abgeschlossene Ermittlungsverfahren, die für Zwecke der künftigen Strafverfolgung vorgehalten werden, gibt es nach Auffassung des Landesbeauftragten wie auch der Rechtsprechung derzeit keine Rechtsgrundlage. Kriminalakten können deshalb nach den von der Rechtsprechung zum Übergangsbonus entwickelten Grundsätzen bis zum Inkrafttreten entsprechender Vorschriften nur aufbewahrt werden, sofern es für die Fortführung einer geordneten polizeilichen Tätigkeit unumgänglich ist. Hieraus ergibt sich ein engerer Maßstab als das im Datenschutzrecht sonst geltende Erforderlichkeitsprinzip. Daraus leitet sich die Forderung ab, daß Kriminalakten nicht schematisch angelegt werden dürfen, sondern daß im Einzelfall die Erforderlichkeit zu prüfen und insbesondere eine Prognoseentscheidung zu treffen ist, ob Rückfallgefahr besteht und ob das Vorhalten einer Kriminalakte für die Aufklärung einer zu erwartenden weiteren Straftat erforderlich ist.

Die Kontrolle hat gezeigt, daß derzeit im Bereich der Landespolizei weitgehend nicht nach dieser Maxime verfahren wird, sondern daß Kriminalakten häufig routinemäßig ange-

legt werden. Der Landesbeauftragte hat eine Reihe von Einzelfällen herausgegriffen und beanstandet.

- So war beispielsweise eine Kriminalakte vorhanden, weil ein neunjähriges Mädchen einen Ladendiebstahl mit einer Beute im Wert von 3,75 DM begangen hatte.
- In einem anderen Fall war ein Schnapsfläschchen im Wert von 1,39 DM gestohlen worden.
- Eine Kriminalakte wurde angelegt, weil der Betroffene einem anderen eine Tüte Pommes frites ins Gesicht geworfen hatte; der Geschädigte hatte keinen Strafantrag gestellt.
- Auch der Ladendiebstahl einer Schachtel Zigaretten im Wert von 3,85 DM führte zur Anlegung einer Kriminalakte.
- In einem weiteren Fall hatte der Betroffene andere Asylanten bei der Essensausgabe „behindert".
- Anlaß für eine andere Kriminalakte war, daß eine 74jährige Frau eine Flasche Nagellackentferner gestohlen hatte.
- Wegen fahrlässiger Brandstiftung wurde eine Kriminalakte angelegt, weil jemand bei Schweißarbeiten in einer Garage einen Pkw in Brand gesetzt hatte.
- In einem anderen Fall hatte ein Fahrzeugführer einen Dritten als Fahrer angegeben, als im Zusammenhang mit einer Geschwindigkeitsüberschreitung gegen ihn ermittelt wurde.

Der Landesbeauftragte hat das Verfahren bei der Anlegung von Kriminalakten beanstandet und Vorschläge zur künftigen Vermeidung dieser Mängel unterbreitet. Sie zielen darauf ab, bei Bagatellfällen nicht stets Kriminalakten anzulegen, sondern eine auf den Einzelfall bezogene Entscheidung zu treffen. Insgesamt müssen die Vorschriften für die Anlegung der Kriminalakten präziser gefaßt werden. Es ist sogar zu überlegen, ob nicht ein begrenzter Zugriff der Polizei auf im staatsanwaltlichen Informationssystem (GAST) gespeicherte Daten über strafrechtliche Ermittlungsverfahren es ermöglichen könnte, bei der Polizei auf die Erfassung von Ersttätern weitgehend zu verzichten. Derzeit besteht in der Regel eine doppelte Speicherung im GAST-Verfahren und in der PED.

Der Landesbeauftragte hat erneut Bedenken dagegen geäußert, daß **Suizidversuche** in Schleswig-Holstein zur Anlegung einer Kriminalakte mit zweijähriger Speicherfrist führen. Er hat in diesem Zusammenhang auf frühere Forderungen verwiesen, die bislang eine Änderung der Praxis noch immer nicht bewirkt haben. Der Landesbeauftragte sieht bei einem Suizidversuch, sofern die Durchführung nicht mit einer strafbaren Handlung (Sachbeschädigung, Brandstiftung) verbunden ist oder Anhaltspunkte für ein Drittverschulden vorliegen, keinen Grund für das Anlegen einer Kriminalakte.

Ebenso sind Kriminalakten über Personen zu kritisieren, die von Angehörigen vorübergehend als vermißt gemeldet worden, inzwischen aber wieder zurückgekehrt waren.

- In einem Fall war z. B. eine Tochter vom nächtlichen Discobesuch erst am Nachmittag des folgenden Tages nach Hause gekommen. Es wurde eine Kriminalakte angelegt.

- In einem anderen Fall bestand noch eine Kriminalakte aus dem Jahr 1973, weil der Betroffene damals als Jugendlicher aus einem Erziehungsheim „abgängig" war.

Einen Strukturmangel besonderen Gewichts stellt es nach Auffassung des Landesbeauftragten dar, daß in den polizeilichen Kriminalakten häufig nur das Entstehen eines Verdachts und die Einleitung eines Ermittlungsverfahrens vermerkt ist, nichts aber über den Ausgang des staatsanwaltschaftlichen oder gerichtlichen Verfahrens. Obwohl das Dateisystem GAST der Staatsanwaltschaft automatisch einen Aufkleber erstellt, mit dessen Hilfe an die Polizei zumindest das staatsanwaltschaftliche Aktenzeichen zurückgemeldet wird, hat der Landesbeauftragte in einer ganzen Reihe von Kriminalakten noch nicht einmal diesen, geschweige denn eine inhaltliche Information über die staatsanwaltschaftliche Beurteilung des Falles vorgefunden. Es ist deshalb davon auszugehen, daß sich im Kriminalaktenbestand Fälle befinden, in denen Personen gerichtlich vom Straftatvorwurf freigesprochen worden sind, ohne daß dies in den Kriminalakten zumindest vermerkt ist.

- So war beispielsweise in einem Fall eine Kriminalakte wegen des Verdachts einer versuchten Vergewaltigung angelegt worden. Der Betroffene bestritt die Tat. Obwohl die Akte bereits fünf Jahre alt war, war in ihr keine Information enthalten, ob dieser immerhin schwerwiegende Vorwurf zutraf oder nicht. Darüber hinaus war das Lichtbild des Verdächtigen noch in der Lichtbildvorzeigekartei vorhanden.

Der Landesbeauftragte hat verlangt, daß die Polizei auch selbst aktiv werden muß, um sich über den Fort- und Ausgang des gerichtlichen Verfahrens zu erkundigen. Dies gilt um so mehr, als die Speicherung personenbezogener Daten in Kriminalakten, wie dargelegt, derzeit ohnehin nur auf den „Übergangsbonus" gestützt werden kann. Er hat deshalb konkret vorgeschlagen, nach Abschluß der kriminalpolizeilichen Ermittlungen eine relativ kurze Wiedervorlagefrist zu vermerken, nach deren Ablauf bei der Justiz nachgefragt werden muß, wie der Straftatverdacht dort beurteilt worden ist. Das endgültige Aussonderungsprüfdatum sollte erst dann gespeichert werden können, wenn der Verfahrensausgang aktenkundig ist. Bei Freisprüchen und Verfahrenseinstellungen sind besondere Regelungen erforderlich, unter welchen Voraussetzungen gleichwohl eine Speicherung für wie lange noch fortbestehen darf.

Beim Kriminalpolizeiamt hat der Landesbeauftragte eine Reihe von Kriminalakten vorgefunden und beanstandet, deren Aussonderungsprüfdatum längst überschritten war.

- So war z. B. noch eine Akte über eine Frau vorhanden, die im Jahre 1963 als damals bereits 70jährige erkennungsdienstlich behandelt worden war.
- In anderen Fällen war das Aussonderungsprüfdatum 1985 bzw. 1987 bereits abgelaufen, ohne daß die Kriminalakte vernichtet worden wäre.
- Es wurden auch Kriminalakten aus den Jahren 1950, 1958 und 1975 gefunden, die zwar nicht mehr in der Datei PED registriert, bislang aber noch nicht vernichtet waren.

Polizeiliche Erkenntnisdatei (PED)

Alle Personen, zu denen eine Kriminalakte geführt wird, werden in der landesweit betriebenen elektronischen polizeilichen Erkenntnisdatei PED gespeichert. Fehler bei der Anlegung einer Kriminalakte setzen sich deshalb bei der Speicherung dort mit nicht auszuschließenden weitreichenden Konsequenzen für die Betroffenen fort. Der Landesbeauftragte hat festgestellt, daß die für die Speicherung in der PED maßgeblichen Dienstvorschriften lückenhaft sind. Aus datenschutzrechtlicher Sicht sind wesentliche Fragen dort nicht geregelt.

Ein Mangel des PED-Datenbestandes liegt darin, daß nicht eindeutig erkennbar ist, in welcher Eigenschaft eine Person dort erfaßt ist. Neben Verurteilten, Verdächtigen und Beschuldigten enthält die PED zumindest auch Datensätze über Suizidenten und Vermißte. In welchem Umfang auch Datensätze über Opfer, gefährdete Personen, Anzeigeerstatter, Hinweisgeber, Zeugen, Geschädigte, Querulanten oder „andere Personen" in der PED angelegt worden sind, konnte im Rahmen der Prüfung mangels entsprechender Kennzeichnung der Datensätze nicht eindeutig geklärt werden. Das PED-Handbuch schließt derartige Speicherungen zumindest nicht ausdrücklich aus.

Insgesamt waren in der PED 4 850 Personen registriert, die älter als siebzig Jahre sind. Der Landesbeauftragte hat verlangt, daß hierzu eine spezielle Überprüfung stattfindet. Das gleiche gilt für die ca. 2 000 Personen, die mit dem personengebundenen Hinweis „krank", „geisteskrank" oder „Freitodgefahr" gespeichert sind. Wegen der besonderen Sensibilität derartiger Vermerke ist eine kontinuierliche Überwachung und Aktualisierung derartiger Datensätze erforderlich. Es ist auch notwendig, den Zweck der Speicherung personengebundener Hinweise präzise und eng begrenzt festzulegen. Unzulässig wäre es beispielsweise, mit Hilfe solcher Zusätze eine Person von vornherein negativ abzustempeln. Etwas anderes gilt hingegen für eine Speicherung von personengebundenen Hinweisen zum Zwecke der Eigensicherung von Polizeibeamten oder der betreffenden Person.

Der Landesbeauftragte hat auch verlangt, daß festgelegt wird, unter welchen Voraussetzungen in der PED Zusatzeintragungen über Mittäter, Angehörige, Vormünder, Pfleger, Bewährungshelfer usw. vorgenommen werden dürfen.

Er hat eine Reihe von Vorschlägen unterbreitet, mit deren Hilfe die datenschutzrechtlichen Mängel der PED beseitigt werden könnten.

Erkennungsdienstliche Unterlagen und Lichtbildvorzeigekarteien

Im Laufe der Prüfung wurde festgestellt, daß die Gründe für erkennungsdienstliche Behandlungen in den Kriminalakten in der Regel nicht dokumentiert sind. Zumeist wird nur pauschal auf § 81 b der Strafprozeßordnung verwiesen, der seinerseits nur eine Generalklausel enthält.

- So war beispielsweise aus einer Akte nicht erkennbar, warum eine Person erkennungsdienstlich behandelt wurde, obwohl es sich nur um einen Ladendiebstahl handelte und die Person eine Ersttäterin war.
- In ähnlicher Weise war in einem anderen Fall ein Jugendlicher erkennungsdienstlich behandelt worden, ohne daß die Gründe für einen derartigen schwerwiegenden Eingriff dokumentiert gewesen wären.

Von besonderer Sensibilität sind sog. Lichtbildvorzeigekarteien. Es handelt sich dabei um Fotosammlungen, die die Polizei in Ermittlungsfällen Tatopfern oder Zeugen vorlegt, damit diese den möglichen Täter daraus erkennen. Auch wenn die Personalien bei dieser Gelegenheit nicht unmittelbar offenbart werden, so kann doch nicht ausgeschlossen werden, daß beispielsweise ein Zeuge eine Person erkennt, die zwar nicht als Täter der aufzuklärenden Straftat in Betracht kommt, von der aber anzunehmen ist, daß die Polizei sie zu den potentiellen Tätern derartiger Straftaten rechnet. Schon bei früherer Gelegenheit bestand Veranlassung, die Handhabung von Lichtbildvorzeigekarteien zu beanstanden (vgl. 4. TB, S. 18).

Der Landesbeauftragte hat nunmehr festgestellt, daß teilweise der Ausgang des Ermittlungsverfahrens, sofern er der Polizei überhaupt bekannt wird, keinen Einfluß auf den Verbleib des Fotos etwa eines Freigesprochenen in der Lichtbildvorzeigekartei hat. Da Fotos dort generell fünf Jahre verbleiben, ist es möglich, daß eine Person auch lange Zeit nach einem Freispruch noch in einer derartigen Datensammlung verzeichnet ist und ihr Foto Zeugen und Opfern von Straftaten als potentieller Tatverdächtiger vorgelegt wird. Der Landesbeauftragte hat verlangt, daß durch entsprechende präzise Vorschriften künftig sichergestellt wird, daß der Ausgang des Verfahrens vor Gericht bei der weiteren Aufbewahrung von Fotos in der Lichtbildvorzeigekartei sowie ganz allgemein von erkennungsdienstlichen Unterlagen berücksichtigt wird.

Datensammlungen im Bereich der Rauschgift- und Wirtschaftskriminalität

Der Landesbeauftragte hat auch für diesen Bereich eine Reihe von datenschutzrechtlichen Verbesserungsvorschlägen unterbreitet. Sie zielen vor allem darauf ab, die Vielfalt der dort betriebenen Dateien aufeinander abzustimmen und zu vermeiden, daß schutzwürdige Belange der Betroffenen durch das Nebeneinander mehrerer Dateien auf Bundes- wie auch auf Landesebene beeinträchtigt werden.

Sammlung „organisierte Kriminalität"

Auch hier bestehen besondere Datensammlungen. Der Landesbeauftragte hat insbesondere kritisiert, daß in diesen Dateien auch Informationen über „andere Personen" erfaßt sind, die weder Verdächtige noch Beschuldigte sind, ohne daß hierfür hinreichende rechtliche Grundlagen bestehen. Er hat deshalb verlangt, daß diese Datenbestände auf das unumgängliche Maß beschränkt werden. Hierzu müssen restriktive und präzise Regelungen erlassen werden.

Sammlungen und Karteien im Bereich „Staatsschutz"

Im Bereich des polizeilichen Staatsschutzes mußte der Landesbeauftragte mehrere Beanstandungen aussprechen. Sie bezogen sich insbesondere auf die Speicherung von Sachverhalten, die keinen Straftatbestand betrafen. Der Landesbeauftragte hat den Eindruck gewonnen, daß im Staatsschutzbereich systematisch „Vorfelddaten", d. h. Informationen, die nicht strafbares Verhalten betreffen und damit allenfalls in die Zuständigkeit des Verfassungsschutzes fallen, gesammelt werden. Insbesondere im Rahmen der Spionageabwehr hat der Landesbeauftragte einzelne Datensätze über Vorgänge und Vorfälle vorgefunden, die mehrere Jahrzehnte zurücklagen und die offenbar mangels Relevanz nie zu strafrechtlichen Konsequenzen geführt haben. In der Kartei „Innere Sicherheit" hat der Landesbeauftragte eine Fülle von Datensätzen festgestellt, die allenfalls extremistisches Verhalten und extremistische Äußerungen, nicht aber Straftatbestände betrafen. Er hat diese Datenspeicherungen beanstandet.

In die Kontrolle einbezogen war auch die bundesweite „Arbeitsdatei PIOS-Innere Sicherheit" (APIS). Es mußten Beanstandungen ausgesprochen werden, weil Fälle gespeichert waren, die nach Auffassung des Landesbeauftragten keine Relevanz für die Erfassung in einem bundesweiten Dateisystem dieses Typs besaßen. Es handelte sich dabei vornehmlich um Beleidigungen und Farbschmierereien. Der Landesbeauftragte geht davon aus, daß die für die Erfassung von Daten in APIS maßgeblichen Vorschriften nicht präzise genug sind. So wurden beispielsweise nach öffentlicher Kritik an der Speicherung von Volkszählungsgegnern sämtliche diesbezüglichen Datensätze unterschiedslos gelöscht,

auch wenn tatsächlich Straftaten mit bundesweitem Bezug betroffen waren. Man kann schätzen, daß ca. 90 % der gespeicherten Datensätze gelöscht werden müßten, wenn man den gleichen Maßstab auch im übrigen anlegen würde. Es müssen deshalb präzise und gegenüber der bestehenden APIS-Errichtungsanordnung engere Vorschriften für die Erfassung von Daten durch schleswig-holsteinische Polizeibehörden in APIS geschaffen werden.

Die Reaktion des Innenministers

Der Innenminister hat in einer ersten Stellungnahme betont, daß mit der auch von ihm für notwendig gehaltenen Überarbeitung von Regelungen für die Datenverarbeitung bei der Polizei bewußt gewartet worden sei, bis der Landesbeauftragte seinen Prüfbericht fertiggestellt habe. Der nunmehr vorgelegte Bericht verlange gravierende Einschnitte in die derzeitige Praxis bei der Kriminalpolizei. Es bedürfe deshalb einer gründlichen Auswertung und Prüfung im einzelnen, welche Konsequenzen letztlich aus ihm für die polizeiliche Datenverarbeitung in Schleswig-Holstein zu ziehen seien. Dabei müsse auch die derzeitige Entwicklung des Strafverfahrens- bzw. Gefahrenabwehrrechts im Auge behalten werden. Ansatzpunkt für Verbesserungen müßten die der Datenverarbeitung zugrunde liegenden Regelungen sein.

Der Innenminister hat das Kriminalpolizeiamt beauftragt, den Bericht auszuwerten und die Konsequenzen für die polizeiliche Datenverarbeitung darzustellen sowie Vorschläge für eine entsprechende Umsetzung insbesondere im Hinblick auf ein Polizeigesetz zu erarbeiten. In Einzelfällen seien bereits beanstandete Datensätze gelöscht worden. Die Bereinigungsarbeiten würden fortgesetzt. Eine abschließende Stellungnahme des Kriminalpolizeiamtes erwartet der Innenminister noch im Frühjahr.

4.1.3.2 Der Schutz des Fernmeldegeheimnisses bei der Polizei

Das Hamburger Verfassungsgericht (NJW 1989, S. 1081) hatte die Frage zu entscheiden, ob der Senat Unterlagen aus einer Telefonabhörmaßnahme in der Hafenstraße einem parlamentarischen Untersuchungsausschuß vorzulegen hatte. Es hat die Frage verneint, da auch die Übermittlung der Daten aus der Telefonüberwachung an den Untersuchungsausschuß und die dortige Verwendung ein eigenständiger Eingriff in das Fernmeldegeheimnis sei. Außerdem stehe die in der Strafprozeßordnung angelegte strenge Zweckbindung einer Weitergabe oder sonstigen Verwertung der durch Telefonabhörmaßnahmen gewonnenen Daten entgegen. Nur wenn es um eine Straftat gehe, zu deren Aufklärung ebenfalls eine Telefonabhörmaßnahme zulässig wäre, dürften die Daten verwendet werden. Ihre Speicherung müsse im übrigen auch zeitlich strikt begrenzt werden.

Aus dieser Entscheidung sind weitergehende Folgerungen für die Verwendung von Daten, die im Wege von strafprozessualen Telefonabhörmaßnahmen gewonnen worden sind, durch die Polizei zu ziehen. Zumindest dürften sich folgende Konsequenzen ergeben:

- Die durch Telefonabhörmaßnahmen gewonnenen Daten sind in den jeweiligen Datensammlungen besonders zu kennzeichnen, damit es überhaupt erst möglich ist, sie nur zweckgerecht und zeitlich begrenzt zu verwenden.
- Eine Weitergabe dieser Daten an andere Polizeibehörden kommt nur im Rahmen der Verfolgung von Straftaten in Betracht, bei denen ebenfalls eine Telefonabhörmaßnahme zulässig wäre.
- Die Daten sind zu löschen, sobald sie für diesen Zweck nicht mehr erforderlich sind. Dies gilt auch dann, wenn die Speicherfrist nach anderen Vorschriften noch nicht abgelaufen ist.
- Eine Weitergabe derartiger Daten an andere als Polizeibehörden, etwa Nachrichtendienste, scheidet grundsätzlich aus.
- Die vorgenannten Grundsätze gelten auch dann, wenn die auf diesem Wege gewonnenen Daten zwischenzeitlich in Form von Vermerken, zusammenfassenden Berichten oder sonstwie verarbeitet und in einen neuen Zusammenhang gebracht worden sind.

Der Landesbeauftragte wird sich bei seinen Kontrollen ein Bild darüber verschaffen, ob diese Grundsätze bei den schleswig-holsteinischen Polizeibehörden beachtet werden.

4.1.3.3 „Schengen" und die Folgen für den Datenschutz

1985 unterzeichneten die Regierungen Frankreichs, der Bundesrepublik Deutschland und der Beneluxstaaten in Schengen/Luxemburg ein Abkommen über den schrittweisen Abbau der Grenzen zwischen ihren Ländern. In einem Zusatzübereinkommen hierzu sollen Maßnahmen zum Ausgleich der befürchteten Sicherheitsdefizite vereinbart werden. Kernstück dieser Ausgleichsmaßnahmen ist die Schaffung eines gemeinsamen automatisierten Informationssystems für den Bereich der Fahndung („Schengener Informationssystem" – SIS). Daneben sieht der Entwurf des Zusatzübereinkommens einen intensiven Informationsaustausch zum Zwecke der Bekämpfung bestimmter Formen der Kriminalität vor. Ausländer- und asylrechtliche Entscheidungen sollen vereinheitlicht und zu diesem Zweck ebenfalls Daten ausgetauscht werden. Für die Kontrollen an den gemeinsamen Außengrenzen sollen Verfahren festgelegt werden, Polizei und andere Sicherheitsbehörden sollen europaweit eng zusammenarbeiten.

Der Entwurf enthält auch umfangreiche datenschutzrechtliche Regelungen. Beispielsweise wollen sich die Vertragsstaa-

ten verpflichten, Datenschutzvorschriften für das Schengener Informationssystem, entsprechend den Grundsätzen der Datenschutzkonvention des Europarates und insbesondere der Empfehlung des Ministerkomitees des Europarates an die Mitgliedsstaaten über die Nutzung personenbezogener Daten im Polizeibereich, als Mindeststandard zu erlassen. Weiter sieht der Entwurf Auskunfts-, Berichtigungs- und Klagerechte für die Betroffenen, Kontrollorgane auf nationaler und internationaler Ebene sowie die Zweckbindung der übermittelten Daten vor.

Die für Ende 1989 vorgesehene Unterzeichnung des Zusatzabkommens wurde im Hinblick auf die aktuellen Vorgänge in Osteuropa verschoben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat über die bereits erreichten datenschutzrechtlichen Vorschriften hinaus weitere Verbesserungen verlangt. Sie hat insbesondere vorgeschlagen, daß

- die Voraussetzungen, nach denen Informationen aus den nationalen in den internationalen Fahndungsbestand übernommen werden sollen, unter Berücksichtigung der Verhältnismäßigkeit (z. B. nach der Schwere der Straftaten) festgelegt werden (bei Verdacht auf kleinere Straftaten muß nicht gleich europaweit gefahndet werden),
- die Voraussetzungen, unter denen die verschiedenen Inlandsbehörden auf die Daten des Schengener Informationssystems zugreifen können, definiert werden,
- die Voraussetzungen, unter denen verdeckte Registrierungen, d. h. die heimliche Beobachtung, erlaubt werden, konkret beschrieben werden,
- die Kriterien, nach denen Zweckdurchbrechungen „zur Verhütung einer Straftat mit erheblicher Bedeutung" sowie aus schwerwiegenden „Gründen der Staatssicherheit" erlaubt sein sollen, präziser beschrieben werden,
- eine Verpflichtung, Zweckänderungen zu Kontrollzwecken zu dokumentieren, aufgenommen wird.

Die Datenschutzgarantien sollten auch für den konventionellen Datenaustausch gelten, der heute schon in beträchtlichem Umfang betrieben wird und kaum minder risikoreich für das Recht auf informationelle Selbstbestimmung der Betroffenen ist. Es muß sichergestellt sein, daß Daten nicht übermittelt werden dürfen, bevor nicht die einzelnen Vertragsstaaten ihre im Entwurf des Zusatzübereinkommens vorgesehene Verpflichtung, spezielle nationale Regelungen für das Erheben und Nutzen von Daten zu erlassen, erfüllt haben. Derzeit hat Belgien überhaupt kein Datenschutzgesetz, in den Niederlanden fehlt es an Regelungen für den Polizeibereich.

Die in dem Vertragsentwurf ebenfalls enthaltene pauschale Verpflichtung der Vertragsparteien, daß ihre nationalen Sicherheitsdienste sich untereinander unter Berücksichtigung des nationalen Rechts und nach Maßgabe ihrer jeweiligen Zuständigkeit bei der Abwehr von Nachteilen für die Staats-

sicherheit unterstützen, stellt nach deutschem Verfassungsrecht keine tragfähige Grundlage für einen umfassenden Datenaustausch der Geheimdienste dar. Das Zusatzübereinkommen enthebt den deutschen Gesetzgeber auch nicht der dringenden Notwendigkeit, vor dessen Inkrafttreten für die polizeiliche Datenverarbeitung verfassungsrechtlich einwandfreie nationale Rechtsgrundlagen zu schaffen.

Der Landesbeauftragte hält es in besonderem Maße für problematisch, daß mit Hilfe des Schengener Informationssystems Instrumentarien wie z. B. die verdeckte polizeiliche Beobachtung, die derzeit weder in der Strafprozeßordnung noch im Polizeirecht hinreichend gesetzlich geregelt sind, „europäisiert" werden, bevor der Gesetzgeber entschieden hat, ob und in welchem Umfang sie auf nationaler Ebene weiterbetrieben werden sollen.

Besonders bedenklich ist auch, daß die Speicherung zum Zwecke der verdeckten Registrierung (polizeiliche Beobachtung) im Rahmen des Schengener Informationssystems „auf Veranlassung der für die Staatssicherheit zuständigen Stellen" zulässig sein soll, was bedeuten kann, daß auch Geheimdienste derartige Anträge zur Ausschreibung stellen. Zwar ist im entsprechenden Artikel des Entwurfs für ein Zusatzabkommen vorgesehen, daß dies nur zulässig ist, „soweit das nationale Recht es erlaubt". Da der Übergangsbonus aber allenthalben großzügig interpretiert wird, ist nicht auszuschließen, daß auch an eine polizeiliche Beobachtung zugunsten der Nachrichtendienste auf seiner Basis gedacht wird. Der Gesetzgeber könnte auch insoweit durch die faktischen Möglichkeiten des Schengener Informationssystems präjudiziert werden.

Der Landesbeauftragte hat den Innenminister aufgefordert, diese Gesichtspunkte bei den Beratungen in den Bund-Länder-Gremien der Polizei und im Bundesrat zu berücksichtigen.

4.1.3.4 Vorstellungen zur Novellierung des Landespolizeirechts

Nachdem der Landesbeauftragte dem Innenminister im vergangenen Jahr Vorschläge für die Novellierung des Landesdatenschutzgesetzes unterbreitet hat, hat er nunmehr auch zur anstehenden Novellierung des Landespolizeirechts erste Anregungen gegeben. Er hat dabei insbesondere auf folgende Punkte abgestellt:

- Es darf nicht nur darum gehen, die bestehende Praxis der polizeilichen Datenverarbeitung im Gesetz etwas genauer zu beschreiben, als es bislang der Fall ist. Zuvor ist vielmehr eine **kritische Analyse der Datenverarbeitungspraxis geboten.** Vom Grundsatz, Eingriffsmaßnahmen nur gegen Störer und Straftatverdächtige zuzulassen, sollte nur in begründeten Ausnahmefällen abgewichen werden.
- Zurückhaltung ist insbesondere im Bereich der sogenannten **vorbeugenden Verbrechensbekämpfung** geboten,

soweit hierfür überhaupt eine Gesetzgebungskompetenz des Landes besteht (vgl. dazu auch Tz. 4.3.1). Problematisch wäre insbesondere die Einführung einer Befugnis zur Erhebung und Speicherung von Daten über Kontakt- und Begleitpersonen, Zeugen, Hinweisgeber und Opfer von Straftaten zum Zwecke der vorbeugenden Straftatenbekämpfung.

- Im Bereich der **Gefahrenabwehr** sollten gestufte Gefahrbegriffe verwendet werden, um bei den daran anknüpfenden Eingriffsmaßnahmen dem Verhältnismäßigkeitsprinzip Genüge zu tun. Datenerhebungsbefugnisse im Vorfeld von Gefahren sind abzulehnen. Eine Datenerhebung ist in diesem Stadium grundsätzlich nur auf freiwilliger Basis möglich. Es sollte auch im Bereich der Datenverarbeitung an dem Grundsatz festgehalten werden, daß nur Eingriffe gegenüber Störern zulässig sind. Ausnahmen müssen eng begrenzt und tatbestandlich präzise gefaßt werden.
- **Daten** sind grundsätzlich **beim Betroffenen** selbst und **in offener Form zu erheben**. Eine Datenerhebung bei Dritten oder in heimlicher Form muß die normenklar geregelte Ausnahme sein. Die heimliche Datenerhebung ist nämlich schon vom Ansatz her auf Kollision mit dem Recht auf informationelle Selbstbestimmung angelegt.
- Falls dem Landesgesetzgeber überhaupt eine Kompetenz für die Regelung der **Datenverarbeitung im Zusammenhang mit öffentlichen Versammlungen** zukommt, ist die besondere grundrechtliche Sensibilität der Versammlungsfreiheit zu beachten. Eine Datenerhebung mit Hilfe von Bild- und Tonaufzeichnungen kann nur bei unmittelbar drohenden Straftaten in Betracht kommen und nur solche Personen erfassen, die diese Straftaten begehen wollen oder in deren unmittelbarer Nähe sie begangen werden sollen. Die Aufzeichnungen dürfen nur zur Strafverfolgung verwendet werden, wenn die Begehung der Straftaten nicht verhindert werden konnte.
- Auch die Verarbeitung von im Vorfeld einer Veranstaltung erhobenen Daten, z. B. **über Veranstalter und Anmelder**, muß geregelt werden. Von Bedeutung ist auch insoweit, ob und für welche Zwecke diese Daten an andere Behörden, etwa die Geheimdienste, übermittelt werden dürfen.
- Sofern im Landespolizeirecht überhaupt ein Erfordernis für Regelungen über besondere Formen der Datenerhebung wie **Observation, polizeiliche Beobachtung, Einsatz technischer Mittel, Rasterfahndung** besteht, dürfen derartige Befugnisse jedenfalls nicht weiter gehen als die in der Strafprozeßordnung zugelassenen.
- Es ist zu prüfen, ob **Observationen** im Rahmen der Gefahrenabwehr ein geeignetes und erforderliches Mittel sein können. Trifft dies zu, so sind die Voraussetzungen präzise zu regeln. Es ist eine besondere Anordnungskompetenz vorzusehen. Besonderer Regelung bedarf die zweckgerechte Verarbeitung der im Rahmen einer Observation er-

hobenen Daten, insbesondere die Verwendung von Daten über Dritte, gegen die die Observation nicht gerichtet war, sowie dieFrage, wann und in welchem Umfang die Betroffenen nach Abschluß der Observation zu unterrichten sind.

- Auch bei der **polizeilichen Beobachtung** ist zunächst die Eignung und die Erforderlichkeit für Zwecke der Gefahrenabwehr zu prüfen. Dabei ist in Rechnung zu stellen, daß die polizeiliche Beobachtung in erheblichem Umfang unbewertete Daten über Nichtstörer, nämlich Kontakt- und Begleitpersonen, erbringt. Falls die polizeiliche Beobachtung für Zwecke der Gefahrenabwehr überhaupt in Betracht kommt, bedarf es einer Regelung über die zweckgerechte Verarbeitung dieser Daten und über besonders kurze Speicherfristen.
- **Der Einsatz verdeckter Ermittler** dürfte im Bereich der Gefahrenabwehr kaum erforderlich werden. Wegen der Langfristigkeit, auf die ihr Einsatz angelegt ist, scheiden sie zur Bekämpfung konkreter, unmittelbar bevorstehender Gefahren regelmäßig aus. Inwieweit verdeckte Ermittler zur Bekämpfung der organisierten Kriminalität eingesetzt werden dürfen, muß der Gesetzgeber im Rahmen des Strafverfahrensänderungsgesetzes entscheiden.
- Die Vorschriften zur **Identitätsfeststellung** sind eng und mit konkreten Tatbeständen zu fassen. Identitätsfeststellungen an Orten, die „erfahrungsgemäß" Ziel- oder Verabredungspunkt von Straftaten sind, sind ohne nähere Eingrenzung abzulehnen. Hierbei ist zu berücksichtigen, daß sich in den modernen Polizeigesetzen anderer Bundesländer an die Befugnis zur Identitätsfeststellung weitere einschneidende Folgebefugnisse, nämlich zum Festhalten und Durchsuchen, aber auch zum Verbringen bzw. zur Vorladung in die Dienststelle zum Zwecke der erkennungsdienstlichen Behandlung, knüpfen.
- Der Gesetzgeber sollte auch vergleichbare Regelungen für Daten treffen, die aufgrund der modernen Möglichkeiten der elektronischen Datenverarbeitung zur **Identifizierung** führen, ohne daß der Bürger dies bemerken kann. Zu denken ist in diesem Zusammenhang vor allem an die durch das zentrale Verkehrsinformationssystem ZEVIS eröffnete Möglichkeit, im Straßenverkehr durch Online-Anfragen die Halter von Kfz heimlich zu identifizieren. Da die Voraussetzungen für ZEVIS-Anfragen im Straßenverkehrsgesetz denkbar weit gefaßt sind, sollte der Landesgesetzgeber die Verwendung der so gewonnenen Daten restriktiv regeln.
- Speichert die Polizei unvollständige Daten (z. B. Verdachtsdaten, Daten über eingeleitete Ermittlungsverfahren), so muß sie sich selbst in angemessenen Abständen **nach dem Ausgang von Gerichtsverfahren erkundigen**, solange sie von der Justiz nicht ohnehin unterrichtet wird. Auf jeden Fall ist sicherzustellen, daß derartige unvollständige Daten nicht ohne vorherige Erkundigung an Dritte weitergegeben werden.

- Das Gesetz selbst sollte **Fristen** für die regelmäßige Überprüfung und die Höchstdauer von Datenspeicherungen vorsehen. Hierbei sind die Vorgaben des Bundeszentralregistergesetzes als äußerster Rahmen zu beachten, soweit es um die Speicherung strafrelevanter Sachverhalte geht. Erforderlich ist auch eine Regelung der Fristen für die Speicherung von Daten in Akten und anderen polizeilichen Sammlungen, die nicht den Dateibegriff erfüllen.
- Bei der Übermittlung von Daten an den Verfassungsschutz ist das **Trennungsgebot** zu beachten. Daten, die mit besonderen polizeilichen Befugnissen erhoben worden sind, die dem Verfassungsschutz nicht zustehen, dürfen allenfalls im Rahmen der Spionageabwehr oder Terrorismusbekämpfung übermittelt werden.

4.1.4 Statistik

4.1.4.1 Wann sind Statistikstellen ausreichend vom Verwaltungsvollzug getrennt?

Zur Wahrung des Statistikgeheimnisses mußten bei der Volkszählung 1987 erstmals die örtlichen Stellen, bei denen die personenbezogenen Zählungsergebnisse zusammenliefen, räumlich, organisatorisch und personell von anderen Verwaltungsstellen getrennt werden. Das Volkszählungsgesetz zog damit die Konsequenz aus der Rechtsprechung des Bundesverfassungsgerichts. In der Praxis stellten sich sehr schnell Probleme insbesondere bei der personellen Abschottung heraus. Die Diskussion und die gerichtlichen Auseinandersetzungen um den Einsatz solcher Mitarbeiter, die in der Schlußphase der Volkszählung regelmäßig zwischen der Erhebungsstelle und ihrer sonstigen Tätigkeit gewechselt haben (sog. Springer), mögen noch in Erinnerung sein.

Die Vorgaben des Bundesverfassungsgerichts zum Statistikgeheimnis gelten aber über die Volkszählung hinaus generell auch für alle folgenden statistischen Erhebungen. Schon bei dem Landesgesetz über die Nutzung von Volkszählungsdaten durch kommunale Stellen hat der Landesbeauftragte darauf hingewirkt, daß neben einer praktikablen Organisation kommunaler Statistikstellen durch personelle Trennungen vom Verwaltungsvollzug Interessenkonflikte und Durchbrechungen des Statistikgeheimnisses vermieden werden.

Das gleiche Problem stellte sich sodann bei der Durchführung des Agrarstatistikgesetzes. Nach der ursprünglichen Vorstellung des Innenministers sollte die Erhebungsstelle von der Verwaltung so abgeschottet werden, daß Mitarbeiter der Erhebungsstelle während der Bearbeitung personenbezogener Erhebungsunterlagen nicht mit Aufgaben des Verwaltungsvollzugs betraut werden. Das sollte dadurch sichergestellt werden, daß ein mehrfacher Wechsel zwischen der Tätigkeit in der Erhebungsstelle und im Verwaltungsvollzug **am selben Tag** nicht zulässig und die Zeiten der Bearbeitung in der Erhebungsstelle vorher festzulegen waren.

Das reichte nach Auffassung des Landesbeauftragten nicht aus. Ein Interessenkonflikt kann nicht allein dadurch vermieden werden, daß Mitarbeiter nicht am selben Tag zu ihrer sonstigen Tätigkeit zurückkehren oder daß die Bearbeitungszeit in der Erhebungsstelle vorher festgelegt wird. Eine wirksame personelle Abschottung ist nur gegeben, wenn in der Erhebungsstelle keine Mitarbeiter eingesetzt werden, deren sonstige Tätigkeit sie in Verbindung mit den zu erhebenden Statistikdaten bringt.

Der Innenminister hat auf Empfehlung des Landesbeauftragten in der betreffenden Rechtsverordnung nun folgende Regelung vorgesehen: „Für eine Tätigkeit in der Erhebungsstelle dürfen nur Mitarbeiterinnen und Mitarbeiter ausgewählt werden, die die Einzelangaben nicht für ihre sonstige Tätigkeit im Verwaltungsvollzug nutzen können." Trotz dieser eindeutigen Aussage mochte beim Landesbeauftragten gleichwohl keine rechte Freude aufkommen. Denn es war eine Ausnahmeregelung angefügt, die bei organisatorischen oder personellen Problemen wieder die zunächst vorgesehene „Springerlösung" zuläßt. Der Bürger muß also im – hoffentlich wohlbegründeten – Einzelfall aus organisatorischen Gründen Abstriche an der Qualität der Abschottung hinnehmen. In erster Linie dürfte das kleinere Gemeinden betreffen, wo es von jeher schwierig ist, eine wirksame Geheimhaltung innerhalb der Verwaltung überzeugend sicherzustellen.

Die optimale Trennung des Verwaltungsvollzuges von statistischen Einzelangaben wird für den Landesbeauftragten in den Erörterungen künftiger statistischer Vorschriften eine bedeutsame Rolle spielen. Für ihn sind nur solche Alternativen konsensfähig, die nicht ein „Weniger" an Abschottung enthalten als die Grundsatzregelung in der genannten Verordnung. Lösungen müssen ggf. unter Beachtung der örtlichen Verhältnisse auf den Einzelfall zugeschnitten werden. Die Gewährleistung des Datenschutzes sollte durch einen Genehmigungsvorbehalt der Aufsichtsbehörde sichergestellt werden.

4.1.4.2 Wie groß ist die Wohnungsnot? Eine Stichprobe soll Antwort geben

In Pressemeldungen wurde bezweifelt, ob es denn tatsächlich erforderlich und datenschutzrechtlich unbedenklich sei, kurze Zeit nach der Volkszählung mit ihrer Gebäude- und Wohnungszählung schon wieder eine große Zahl von Bürgern zur Auskunft über ihre Wohnsituation zu verpflichten. Der Landesbeauftragte hat dem Innenminister zu den Beratungen eines „Gebäude- und Wohnungsstichprobengesetzes" im Bundesrat seine datenschutzrechtlichen Überlegungen vorgetragen. Wie so oft bei statistischen Erhebungen wird dem betroffenen Bürger auch hier kaum verständlich gemacht, „ob das denn alles sein muß". Eine häufige Frage Betroffener, warum gerade sie in den Kreis der Auskunftspflichtigen gehören, wird mit dem lapidaren Hinweis auf ein „mathema-

tisches Zufallsverfahren" beschieden. Auch zu der Frage, ob anstelle einer Auskunftspflicht nicht eine freiwillige Erhebung ausreichen würde, äußern sich weder das Gesetz noch die Begründung. Dabei hat das Bundesverfassungsgericht im Volkszählungsurteil gefordert, der Gesetzgeber müsse sich vor künftigen Entscheidungen über statistische Erhebungen mit dem jeweiligen Stand der Methodendiskussion auseinandersetzen, um festzustellen, ob und in welchem Umfang die herkömmlichen Methoden der Informationserhebung und -verarbeitung beibehalten werden können.

Zweifel blieben auch, ob alle im Gesetz vorgesehenen Fragen erforderlich sind, um für den Wohnungsbau Planungsgrundlagen zu erhalten. Sind tatsächlich die Wohnungswechsel der letzten zehn Jahre von Bedeutung, oder hätte nicht auch ein kürzerer Zeitraum ausgereicht? Könnte nicht auf so sensible Fragen wie nach der „sozialen Stellung" oder der „Art des Zusammenlebens" verzichtet werden? Muß nicht der Begriff des Nettoeinkommens exakt im Gesetz geregelt werden, um unterschiedliche Interpretationen der einzelnen Statistikämter vor Ort zu vermeiden? In welchem Verhältnis stehen die Fragen der Statistik zu besonderen Geheimhaltungsvorschriften in anderen Gesetzen wie dem Sozialgesetzbuch und der Abgabenordnung?

Die Stellungnahme des Innenministers offenbarte ein bekanntes Dilemma, denn einigen Anregungen würde man gern folgen, müßte aber entsprechend dem Bundesgesetz verfahren. Zu anderen Fragen hat man statistisch-wissenschaftliche Argumente vorgetragen, die allerdings die Zweifel des Landesbeauftragten nicht ausgeräumt haben.

Nicht zuletzt aufgrund der auch anderweitig erhobenen datenschutzrechtlichen Bedenken sind die Beratungen zu dem Gesetzentwurf noch nicht abgeschlossen worden.

4.1.4.3 Europa wächst zusammen – ohne Datenschutz?

Die Bürger vertrauen darauf, daß ihre Angaben zur Statistik vertraulich bleiben. Kein Sterbenswörtchen, das ihre persönlichen Verhältnisse offenbar werden ließe, darf die statistischen Ämter verlassen. Der Bundesgesetzgeber hat das strenge Statistikgeheimnis als Grundlage für diesen Vertrauensschutz im Gesetz verankert. Auf Landesebene laufen seit geraumer Zeit Vorarbeiten, entsprechende Regelungen auch für statistische Erhebungen des Landes und der Kommunalverwaltungen zu entwickeln. Nun besteht die akute Gefahr, daß die Daten der Bürger sogar europaweit bekannt werden, denn ein neuer „Partner" kommt hinzu.

Die Kommission der Europäischen Gemeinschaft hat den Entwurf einer Ratsverordnung zur Übermittlung statistischer Daten dem Statistischen Amt der EG vorgelegt. Es ist zu befürchten, daß aufgrund der sehr allgemein gehaltenen Vorschrift deutsche Stellen personenbezogene Daten übermitteln müssen, ohne daß auf der Ebene der Europäischen Gemein-

schaft ein angemessener Datenschutz besteht und das Statistikgeheimnis sichergestellt ist. Insbesondere ist eine unabhängige Datenschutzkontrolle auf Gemeinschaftsebene nicht gewährleistet und sind für Fälle der zweckwidrigen Verwendung von Statistikdaten im Gemeinschaftsrecht keine Sanktionen vorgesehen.

Inzwischen hat neben der Konferenz der Datenschutzbeauftragten auch der Innenausschuß des Deutschen Bundestages eine Verbesserung der Datenschutzregelungen für die Verordnung gefordert. Die endgültige Reaktion aus Brüssel steht noch aus.

4.2 Datenschutz im Kommunalbereich

4.2.1 Kommunalverfassungsrecht – die datenschutzrechtliche Botschaft wurde empfangen

Das neue Kommunalverfassungsrecht ist verabschiedet. Die beabsichtigte Öffnung der Kommunalpolitik wurde von Schlagwörtern, wie „lebendiger", „bürgernäher" und „leistungsfähiger", begleitet. Für den Landesbeauftragten war dagegen von besonderem Interesse, ob auch Begriffe wie „informationelles Selbstbestimmungsrecht" und „Wahrung schutzwürdiger Belange der Betroffenen" in den Entwurf eingeflossen sind. Aus diesen Begriffen leitete sich dann auch seine Kritik an dem Referentenentwurf ab.

Öffentlichkeit von Sitzungen

Um ihre demokratischen Rechte wirksam wahrnehmen zu können, müssen die Bürger die Möglichkeit haben, unmittelbare, nicht durch Berichte gefilterte Informationen über die Tätigkeit der Vertretung und ihrer Ausschüsse zu erhalten. Dem dient die Öffentlichkeit von Sitzungen. Datenschutzrechtliche Bedenken müssen allerdings geltend gemacht werden, wenn die Sitzungsöffentlichkeit dazu führt, daß der Anspruch des einzelnen auf angemessenen Schutz seiner persönlichen Daten gefährdet wird.

Der Referentenentwurf sah vor, daß die abschließende Entscheidung über den Ausschluß der Öffentlichkeit selbst dann in das Ermessen des jeweiligen Gremiums gestellt werden sollte, wenn berechtigte Interessen einzelner am Schutz ihrer personenbezogenen Daten überwiegen. Eine solche Beeinträchtigung des Persönlichkeitsrechts konnte nicht unwidersprochen bleiben. Auf Anregung des Landesbeauftragten wurde für diesen Fall eine Rechtspflicht zum Ausschluß der Öffentlichkeit in das Gesetz aufgenommen.

Auskunfts- und Akteneinsichtsrechte der Mandatsträger

Zur Verbesserung ihrer Informationsrechte war zunächst beabsichtigt, kommunalen Mandatsträgern ein nahezu unbe-

grenztes Auskunfts- und Akteneinsichtsrecht gegenüber der Verwaltung einzuräumen. Ein solcher Anspruch sollte ursprünglich schon dann gegeben sein, wenn die Auskunft oder Akteneinsicht der Aufgabenerfüllung der Mandatsträger nur „dienlich ist".

Der Landesbeauftragte hat erreicht, daß im Gesetz vorgesehen ist, daß

- Auskunft oder Akteneinsicht nur gewährt werden dürfe, soweit dies für die Vorbereitung oder Kontrolle der Ausführung von einzelnen Beschlüssen der Vertretung oder ihrer Ausschüsse **erforderlich** ist,
- Auskunft und Akteneinsicht nicht gewährt werden dürfen, wenn Vorgänge nach einem Gesetz geheimzuhalten sind oder das Bekanntwerden des Inhalts die berechtigten Interessen einzelner oder Dritter beeinträchtigen kann,
- die abschließende Entscheidung über die Auskunftsgewährung bzw. Akteneinsicht nicht die Vertretungskörperschaft trifft, sondern der Bürgermeister bzw. der Magistrat oder der Kreisausschuß.

Bei dieser Ausgestaltung der Informationsrechte dürfte es auch in Zukunft eigentlich nicht zu der befürchteten Ausweitung der Datenflüsse an kommunale Mandatsträger kommen. Aus datenschutzrechtlicher Sicht sind die Neuregelungen zu begrüßen, zumal Entscheidungen über eine Auskunftsgewährung oder Akteneinsicht in dem gebotenen Maße rechtlich nachprüfbar sein werden.

4.2.2 Ein Mensch in Gefahr – die Telefonvermittlung speichert seine Worte

Wenn ein Mensch in höchster Not Polizei, Feuerwehr oder eine Rettungsleitstelle anruft, wird er voraussichtlich mit jeder Maßnahme einverstanden sein, die ihm hilft. Mit dieser einleuchtenden Überlegung rechtfertigten schleswig-holsteinische Kreise Verfahren, die in Rettungsleitstellen alle eingehenden Telefongespräche aufzeichneten. Es wurden jedoch nicht nur die Telefongespräche aufgenommen, die in echten Notfällen geführt werden mußten, vielmehr auch andere, wie z. B. bei Unterbringung psychisch Kranker, Ausländerangelegenheiten, der Sozialarbeit des Kreisjugendamtes. Neben den eigentlichen Notrufanschlüssen waren deshalb weitere Anschlüsse über die Rettungsleitstelle geschaltet.

Der Landesbeauftragte hat hiergegen Bedenken angemeldet, denn die unbefugte Aufnahme des nichtöffentlich gesprochenen Wortes eines anderen verletzt dessen Persönlichkeitsrecht und steht unter Strafe. Bei den eigentlichen Notrufen sind allerdings durchweg rechtfertigende Situationen denkbar. Die mutmaßliche Einwilligung der Anrufer in rettende und sichernde Maßnahmen, zu denen auch die Gesprächsaufzeichnung gehört, kann unterstellt werden. Für die Aufzeichnung der übrigen Gespräche ist keine Rechtferti-

gung zu erkennen. Sie wären nur mit ausdrücklicher Einwilligung der Anrufenden zulässig. Der Innenminister hat sich in einem Erlaß an die Kreise dieser Auffassung angeschlossen.

4.2.3 Meldewesen

4.2.3.1 Ein kleiner Programmfehler gefährdet Menschenleben

Einen von seinen Auswirkungen her besonders schwerwiegenden datenschutzrechtlichen Verstoß hatte der Landesbeauftragte im Bereich des Melderechts zu beanstanden. In mehreren Städten und Gemeinden war es zu einer Neuauflage des örtlichen Adreßbuches gekommen. Die hierfür erforderlichen Daten waren von den Meldebehörden an die jeweiligen Verlage übermittelt worden. Die Abwicklung dieser Melderegisterauskünfte erfolgte wie üblich über die Datenzentrale Schleswig-Holstein als Auftragnehmerin.

Von einer Übermittlung mußten selbstverständlich die mit einer Auskunftssperre versehenen Anschriften ausgeschlossen werden, bei denen die Veröffentlichung eine Gefährdung für Leben, Gesundheit, persönliche Freiheit und ähnlich schutzwürdige Belange der Betroffenen bedeutet hätte. Die Aufträge an die Datenzentrale zur Herstellung der Registerauszüge waren in diesem Punkt eindeutig. Gleichwohl ist es durch verschiedene Ursachen, auf die unter Tz. 6.3 näher eingegangen wird, zu einer Weitergabe gesperrter Daten gekommen, so daß die Anschriften besonders gefährdeter Personen nun beim Kauf eines Adreßbuches jedem zugänglich waren.

Zwar hat man versucht, den Verkauf der fehlerhaften Exemplare soweit wie möglich zu stoppen; ein umfassender Erfolg konnte wegen des Vertriebs über den Buchhandel naturgemäß nicht erzielt werden. Ein Umzug war für mehrere Familien aus Sicherheitsgründen unumgänglich.

Dieses Beispiel zeigt, welche schwerwiegenden Folgen bereits ein kleiner Fehler bei der automatisierten Datenverarbeitung haben kann und in welchem Maße Auftraggeber die einwandfreie Durchführung ihrer Aufträge kontrollieren und sicherstellen müssen.

Der Verantwortung für die Rechtmäßigkeit ihres Handelns können sich die Verwaltungen nicht dadurch entziehen, daß sie die technische Durchführung bei anderen Stellen im Auftrage erledigen lassen. Sie können diese Verantwortung allerdings nur tragen, wenn sie sich über die Richtigkeit und die Aktualität der eingesetzten Programme hinreichend Sicherheit verschafft haben. Das ist auch im vorliegenden Fall wieder einmal nicht geschehen, da noch immer „in vielen Verwaltungsbereichen automatisierte Verfahren vor ihrem erstmaligen Einsatz und nach Programmänderungen nicht ausreichend von denen getestet werden, die für die Rechtmäßigkeit und Richtigkeit der Verwaltungsakte die Verantwortung tragen" (vgl. 8. TB, S. 65). An dieser Situation, die der

Landesbeauftragte schon 1986 gerügt hat, hat sich offensichtlich bis heute nichts geändert. Bei den Auftraggebern scheint es weitgehend am Bewußtsein für das Problem und die damit verbundenen Risiken zu fehlen. Jedenfalls ist den seit langem erhobenen Forderungen des Landesbeauftragten (6. TB, S. 61; 8. TB, S. 65; 10. TB, S. 58) bis heute nicht entsprochen worden. Weder haben die Anwender darauf gedrängt, die unzureichende Testorganisation für kommunale Programme zu verbessern, noch haben die kommunalen Landesverbände sich in der Lage gesehen, ihre betroffenen Mitglieder hier wirksam zu unterstützen, noch hat die Datenzentrale als eine der größten Partnerinnen für kommunale Datenverarbeitungsaufträge im Lande diese Risiken ausgeräumt. Weitere Schäden für die Belange der Bürger sind deshalb nicht auszuschließen.

4.2.3.2 Keine regelmäßigen Meldedatenübermittlungen zur Suche nach Schwarzhörern

Verzieht der Schuldner einer Sparkasse mit unbekanntem Ziel, so muß sie von sich aus Anstrengungen unternehmen und erforderlichenfalls rechtliche Schritte veranlassen, wenn sie verhindern will, daß er sich seinen Verpflichtungen entzieht. Es käme wohl niemand auf den Gedanken, zu ihren Gunsten ein Verfahren einzuführen, das es gestattete, von Amts wegen mit Hilfe öffentlicher Stellen nach säumigen Schuldnern zu „fahnden". Genau das beabsichtigten aber die öffentlich-rechtlichen Rundfunkanstalten und ihre Gebühreneinzugszentrale (GEZ). Durch Datenträgeraustausch sollten die Meldebehörden der GEZ alle Zu- und Fortzüge aus ihrem Bereich mitteilen, damit die Rundfunkanstalten ihre Gebührenschuldner nach einem Wohnortwechsel leichter zur Zahlung heranziehen konnten.

Der Landesbeauftragte mußte darauf hinweisen, daß für eine solche regelmäßige Übermittlung von Meldedaten die Rechtsgrundlage fehlt. Eine Erweiterung der in der Meldedatenübermittlungsverordnung zugelassenen regelmäßigen Datenübermittlungen in der gewünschten Weise würde darüber hinaus erheblichen datenschutzrechtlichen Bedenken begegnen. Ein so umfassender Eingriff in die Persönlichkeitsrechte auch Unbeteiligter steht nicht im angemessenen Verhältnis zu dem erstrebten Erfolg. Denn bei vollständiger Mitteilung aller Zu- und Fortzüge gelangte eine Vielzahl personenbezogener Daten auch solcher Einwohner in den Verfügungsbereich der GEZ, die ihrer Gebührenpflicht nachkommen oder für die eine Gebührenpflicht gar nicht besteht. Demgegenüber können die Anschriften „unbekannt" verzogener Gebührenschuldner durch eine einfache Melderegisterauskunft festgestellt werden.

Die Argumente des Landesbeauftragten für den Datenschutz haben offenbar bewirkt, daß die Angelegenheit nicht weiter verfolgt wurde.

4.2.3.3 Das gefährdete Adoptionsgeheimnis – was lange währt, wird gut

Das Adoptionsgeheimnis ist gefährdet, wenn der zuständige Standesbeamte die Geburt eines Kindes der Meldebehörde mitteilt, die für den Hauptwohnsitz der Mutter zuständig ist, obwohl eine Adoption des Kindes vorgesehen ist und ein Adoptionspflegeverhältnis eingegangen wird. Das Kind wird in diesem Fall voraussichtlich nie den Wohnsitz der leiblichen Mutter teilen. Durch den Datenaustausch einer Meldebehörde mit den Religionsgesellschaften war dieser Sachverhalt im konkreten Fall kirchlichen Stellen bekanntgeworden, und die Mutter sah sich zu einer Rechtfertigung ihrer Adoptionspläne genötigt. Eine Änderung der Dienstanweisung für Standesbeamte, die dieses Risiko vermeiden sollte, war von den beteiligten Stellen durchweg positiv aufgenommen worden. Sie drohte auf dem langen Weg durch die Institutionen jedoch unterzugehen. Der Landesbeauftragte befürchtete, „daß auch in diesem Fall die Bürokratie über den gesunden Menschenverstand siegt" (11. TB, S. 12).

In Schleswig-Holstein ist dieser Vorschlag inzwischen umgesetzt worden. Die Mitteilung an die Meldebehörde des Hauptwohnsitzes der Mutter unterbleibt künftig, wenn dem zuständigen Standesbeamten eine Mitteilung über ein bestehendes oder beabsichtigtes Pflegeverhältnis vorliegt. Die Adoptionsvermittlungsstellen teilen dies dem Standesbeamten mit. Der Landesbeauftragte stellt mit Befriedigung fest, daß er mit seiner Befürchtung nicht recht behalten hat.

4.2.4 Kurschatten anderer Art

Viele Fremdenverkehrsgemeinden halten eine strenge Kontrolle der Kurabgabe aus finanziellen Gründen für unverzichtbar. Dafür werden immer umfangreichere Überwachungsverfahren eingeführt. Ein solches Verfahren veranlaßte den Landesbeauftragten, die Rechtmäßigkeit der Datenverarbeitung bei einem Kurbetrieb zu überprüfen. Was war geschehen? Das Haus eines Petenten war mehrfach durch Außendienstmitarbeiter der Kurverwaltung kontrolliert worden. In zwei Fällen wurden Pkw ermittelt, deren Kennzeichen nicht mit den Angaben in der gespeicherten Gästeliste der Kurverwaltung übereinstimmten. Daraufhin wurden bei den zuständigen Kraftfahrzeug-Zulassungsstellen die Halter erfragt. Die hierfür angegebenen Begründungen waren nicht mehr zu ermitteln. Ohne weitere Sachverhaltsaufklärung bzw. Anhörung der Betroffenen wurden die Fahrzeughalter nachträglich zur Kurabgabe herangezogen. Der dafür zugrunde gelegte Zeitraum wurde geschätzt. Man vertraute darauf, daß sich die Betroffenen bei fehlerhafter Festsetzung schon melden würden.

Die Kurverwaltung hat die Kraftfahrzeughalter ermittelt, ohne daß eine Abgabepflicht der Betroffenen hinreichend nachgewiesen war. Die bloße Tatsache, daß sich das Kenn-

zeichen eines parkenden Pkw nicht mit den gespeicherten Gästedaten deckte, war für sich allein keinesfalls geeignet, daraus bereits den Schluß zu ziehen, daß sich der Halter des Pkw seiner Zahlungspflicht entzogen habe. Es hätte sich auch um den Besuch auswärtiger Kinder des Vermieters handeln können. Fahrzeughalter und Gast mußten nicht identisch sein. Der Gast konnte unmittelbar nach Ankunft seine Kurabgabe entrichtet haben, ohne dabei den Vermieter anzugeben. Würde er dann die Kurkarte direkt dem Vermieter vorlegen, wäre eine Meldung nach der Satzung nicht erforderlich. Oder anderweitig untergebrachte Gäste könnten Gäste des Vermieters besucht haben.

Außerdem war die Halteranfrage in diesem Zusammenhang unzulässig. Das Straßenverkehrsgesetz läßt Auskünfte grundsätzlich nur zu, wenn sie Bezug zum Straßenverkehr haben. Für den Landesbeauftragten wurde aber auch erkennbar, auf welch ein perfektes Kontrollverfahren er hier gestoßen war. Mit Hilfe eines Computers war es der Kurverwaltung möglich, sämtliche Übernachtungen innerhalb des Ortes festzuhalten und je nach Bedarf auszuwerten. Jeder Vermieter war nämlich grundsätzlich verpflichtet, die von ihm aufgenommenen Personen beim Kurbetrieb unter Angabe des An- und Abreisetages anzumelden. Ausgenommen waren nur solche Kurgäste, die bereits bei ihrer Ankunft oder innerhalb von 24 Stunden danach Kurkarten vorweisen konnten, deren Gültigkeit sich auf die Dauer der Beherbergung erstrecken mußte. In diesen Fällen wurden die Namen der Vermieter beim Kauf der Kurkarte auf freiwilliger Basis erfragt, ohne jedoch den Gast über die Verwendung dieser Daten aufzuklären.

Die Kurverwaltung war so in der Lage, nahezu lückenlos die Gästedaten den Vermietern zuzuordnen und in ihrer Datenverarbeitungsanlage zu speichern. Die EDV-mäßige Auswertung dieser Angaben ermöglichte es dann, bei den einzelnen Vermietern eine unterdurchschnittliche Gästeauslastung festzustellen, verbunden mit dem Verdacht, daß Gäste nicht zur Zahlung der Kurabgabe angemeldet wurden. Die Einleitung der genannten, umfangreichen Kontrollmaßnahmen unter Verletzung des informationellen Selbstbestimmungsrechts war die Folge.

Ob ein solches Verfahren angemessen ist, um die vollständige Erhebung der Kurabgaben zu sichern, ist zu bezweifeln. Zumindest bedarf es präziser Regelungen in einer kommunalen Satzung. Sie sollte insbesondere

- zunächst den Zweck der Verarbeitung von Gäste- und Vermieterdaten bestimmen (z. B. Überwachung der Kurabgabeerhebung),
- sodann den Katalog der erforderlichen Daten abschließend festlegen,
- schließlich regeln, in welcher Weise konkret eine Nutzung der gespeicherten Daten erfolgen darf (z. B. Feststellung der Auslastung von Beherbergungsbetrieben) und

– eine Datenübermittlung an andere Stellen ausdrücklich ausschließen, soweit nicht die Einwilligung der Betroffenen vorliegt.

Die Kurabgabensatzung der betreffenden Gemeinde erfüllte nicht die an sie zu stellenden Anforderungen in bezug auf das Überwachungsverfahren. Die notwendige Ergänzung ist inzwischen in Abstimmung mit dem Landesbeauftragten eingeleitet worden.

4.2.5 Fremdenverkehrsgemeinde verunsichert Wohnmobilfahrer

Verwundert zeigte sich ein Wohnmobilfahrer, als er nach einer kurzen Rast in einem Ostseebad zu seinem Fahrzeug zurückkehrte und hinter seinem Scheibenwischer ein „Merkblatt für Inhaber von Wohnmobilen" vorfand. Darin wurde er von der Gemeinde darauf hingewiesen, man halte das Übernachten in Wohnmobilen auf öffentlichen Verkehrsflächen grundsätzlich für unzulässig und werde es als Ordnungswidrigkeit verfolgen. Außerdem komme es in diesem Zusammenhang immer wieder zur Einleitung von Fäkalien in die Oberflächenentwässerung und zu Verkehrsbehinderungen, was regelmäßig zu „unerfreulichen Begegnungen" zwischen Wohnmobilinhabern einerseits und Polizeibeamten und Mitarbeitern der Ordnungsämter andererseits führe. Folgender Nachsatz war besonders bemerkenswert: „NS: Denken Sie bitte daran, Ihr Fahrzeug ist bereits mit Standort, Datum und Nummer registriert!"

Der Betroffene hatte verständlicherweise den Eindruck, daß er nun bereits als potentieller Umweltsünder und Falschparker gespeichert sei, obwohl er nur ganz korrekt eine kleine Pause während der Heimfahrt eingelegt hatte.

Aufgrund dieses doch recht bedenklichen Sachverhaltes waren weitere Nachforschungen für den Landesbeauftragten eine Selbstverständlichkeit. Erstaunt mußte er feststellen, daß das Merkblatt offensichtlich nur leere Drohungen enthielt. Der Ordnungsamtsleiter hatte zwar das Merkblatt entworfen, dann aber die Sache an die Kurverwaltung abgegeben, damit der eigentliche, nach außen hin nicht erkennbare Zweck der Maßnahme, nämlich die Überwachung der Kurabgabeerhebung, von dort in eigener Zuständigkeit verfolgt werden konnte. Auf Befragen bestätigte er ausdrücklich, daß es eine Speicherung von Wohnmobildaten im Ordnungsamt nicht gebe.

Die Kurverwaltung wiederum erklärte, daß auch dort keine Datenspeicherungen vorgenommen würden, sondern das Merkblatt nur vorsorglich und auf Wunsch des Ordnungsamtes verteilt würde. Ordnungswidrigkeitenverfahren seien noch in keinem Fall eingeleitet worden.

Nachdem sich die Befürchtungen des Landesbeauftragten nicht bestätigt hatten, blieb nur noch darauf hinzuweisen, daß aus rechtsstaatlicher Sicht die Bürger auch einen Anspruch

darauf haben, von der Behörde wahrheitsgemäß darüber unterrichtet zu werden, wann und zu welchen Zwecken personenbezogene Daten über sie gespeichert werden. Eine Überarbeitung des Merkblattes wurde zugesagt.

4.2.6 Prüfung einer Stadtverwaltung

Auch 1989 wurde wieder die Einhaltung des Datenschutzes im kommunalen Verwaltungsbereich geprüft. Der Schwerpunkt der Prüfung lag diesmal bei Einzelfragen zur Rechtmäßigkeit der Datenverarbeitung. Das Verwaltungshandeln der Stadt war erwartungsgemäß bestimmt von der Maxime, mit möglichst wenig Aufwand die gestellten Aufgaben rationell zu erfüllen. Der Datenschutz kann in diesem Zusammenhang oftmals eine zusätzliche Arbeitserschwernis darstellen. Gleichwohl hat man sich konstruktiv mit den widerstreitenden Interessen auseinandergesetzt. Die Ergebnisse fanden nicht immer die uneingeschränkte Zustimmung des Landesbeauftragten. Die vorgefundenen Mängel konnten aber durchweg in einer datenschutzgerechten Weise behoben werden. Folgende Ergebnisse der Prüfung sind wegen ihrer allgemeinen Bedeutung besonders hervorzuheben:

Vernichtung von Daten durch eine private Entsorgungsfirma

Für die Vernichtung ihrer Abfälle mit personenbezogenen Daten wurde von der Stadt eine private Entsorgungsfirma eingesetzt. Das gesamte anfallende Papier sowie der Inhalt der Papierkörbe wurde in verschließbaren Containern gesammelt und nach Bedarf von der Firma abgeholt. Es wurde jeweils bestätigt, daß die überlassenen Unterlagen unter Beachtung der gesetzlichen Bestimmungen restlos vernichtet werden. Darüber hinausgehende Vorkehrungen, das Risiko einer rechtswidrigen Verwertung von Unterlagen auszuschalten, waren von der Stadt allerdings nicht getroffen worden.

Ein wirksamer schriftlicher Verwertungsvertrag konnte im Prüfungszeitpunkt nicht vorgelegt werden. Die Vernichtung des Datenabfalls bedarf aber einer sachgerechten Organisation. Neben internen Dienstanweisungen ist ein wirkungsvoller Verwertungsvertrag unabdingbar. Die hierzu vom Landesbeauftragten in seinem 9. Tätigkeitsbericht (S. 18) gegebenen Empfehlungen besitzen nach wie vor Gültigkeit. Über die vertragliche Bindung hinaus sollte nicht vergessen werden, daß jede auftraggebende Stelle selbst verpflichtet ist, die Zuverlässigkeit der beauftragten Firma sowie die Sicherheit und die Ordnungsmäßigkeit der Datenvernichtung zu überprüfen. Auf unangemeldete stichprobenartige Kontrollen sollte auf keinen Fall verzichtet werden. Entsprechende Befugnisse müssen vertraglich abgesichert werden.

Hausreinigung

Die Reinigung der Büroräume war von der Stadt ebenfalls an einen privaten Auftragnehmer vergeben worden. Ein wirksamer schriftlicher Gebäudereinigungsvertrag lag nicht vor. Als Auftraggeberin obliegt es der Stadt, durch geeignete Maßnahmen sicherzustellen, daß es im Rahmen der Reinigungstätigkeit nicht zu einem Mißbrauch personenbezogener Daten kommt. Dazu gehört in erster Linie, daß Unterlagen mit personenbezogenen Daten nach Verlassen der Büroräume nicht unverschlossen zurückbleiben dürfen. Da gleichwohl nicht auszuschließen ist, daß Reinigungskräfte in den Büros Zugang zu personenbezogenen Daten erhalten, muß vor allem auf eine hinreichende vertragliche Bindung des Reinigungsunternehmens geachtet werden. Hierzu gehört, daß eine Unterrichtung darüber erfolgt, welche Kraft wann und in welchen Räumen tätig wird, daß die Reinigungskräfte auf das Datengeheimnis verpflichtet werden und daß Auftraggeber das Recht haben, unzuverlässige Kräfte abzulehnen.

Die Stadt hat zugesagt, das Vertragsverhältnis entsprechend zu gestalten und die Einhaltung der Vertragsbedingungen zu überwachen.

Versendung der Protokolle von Magistratssitzungen

Die Niederschriften über Sitzungen des Magistrats wurden regelmäßig an alle Stadtvertreter versandt. Nur soweit Personalangelegenheiten behandelt worden waren, wurden diese Beschlüsse in eine besondere Anlage zum Protokoll nur für die Mitglieder des Magistrats und den Bürgervorsteher aufgenommen. Gleichwohl enthielten die Protokolle auch eine Reihe anderer schutzwürdiger personenbezogener Daten. Der Landesbeauftragte hat deshalb auf eine Entscheidung des Oberverwaltungsgerichts Lüneburg vom 29.01.1985 – 5 A 91/84 – hingewiesen, wonach die Weiterleitung der vollständigen Sitzungsprotokolle von Magistratssitzungen an alle Stadtvertreter gegen die Gemeindeordnung verstößt. Von den Sitzungen des Magistrats darf folglich der Stadtvertretung nur das Beratungsergebnis mitgeteilt werden.

Belege in Beihilfeakten

Die im Zusammenhang mit Beihilfeanträgen eingereichten Belege über entstandene Kosten wurden im Regelfall zusammen mit der Entscheidung an den Antragsteller zurückgereicht. In der Akte verblieb nur der eigentliche Beihilfeantrag sowie die Bearbeitungsunterlagen. In besonders umfangreichen oder kostenintensiven Fällen (Sanatoriumsaufenthalte u. ä.) wurden zusätzlich Kopien der Belege zur Beihilfeakte genommen, um so ggf. die Entscheidung gegenüber dem Rechnungsprüfungsamt besser begründen zu können. Nach den Beihilfevorschriften sind die bei der Bearbeitung der Beihilfen bekanntgewordenen Angelegenheiten geheimzu-

halten. Sie dürfen nur für den Zweck verwandt werden, für den sie vom Betroffenen offenbart worden sind. Um einer möglichen Zweckentfremdung entgegenzuwirken, ist in den Beihilfevorschriften ausdrücklich vorgesehen, **alle** Belege an den Beihilfeberechtigten zurückzugeben. Für die Fertigung von Kopien bestand keine Notwendigkeit. Sie widersprach vielmehr den datenschutzrechtlichen Zielen der Beihilfevorschriften. Die vorhandenen Akten waren entsprechend zu bereinigen.

Behandlung von Lohn- und Gehaltspfändungen

Im Rahmen privatrechtlicher Zwangsvollstreckungsverfahren ist die Stadt als Drittschuldnerin nach der Zivilprozeßordnung verpflichtet, Auskünfte an Gläubiger zu erteilen. Allerdings wurden Anfragen von Gläubigern auch dann beantwortet, wenn noch gar kein Pfändungs- und Überweisungsbeschluß zugestellt worden war. Begründet wurde dies damit, daß man als Dienstherr im Rahmen der Fürsorgepflicht auf diese Weise kostenpflichtige Zwangsvollstreckungsmaßnahmen gegenüber den Mitarbeitern habe verhindern können. Die Zustimmung der Mitarbeiter zu den erteilten Auskünften war jedoch nicht eingeholt worden. Auch gingen die Auskünfte, die im Rahmen von Drittschuldnererklärungen erteilt wurden, zum Teil erheblich über das gesetzlich vorgeschriebene Maß hinaus. In einem Fall betrafen sie nicht einmal das laufende Beschäftigungsverhältnis (Offenbarung einer viermonatigen Entziehungskur). Bei einer derart gravierenden Verletzung des geltenden Datenschutzrechts war eine Beanstandung unvermeidbar.

Einrichtung von Auskunftssperren nach dem Landesmeldegesetz

Im Melderegister der Stadt waren zum Prüfungszeitpunkt eine Reihe von Auskunftssperren eingerichtet, weil die Betroffenen der Meldebehörde das Vorliegen von Tatsachen glaubhaft gemacht hatten, die die Annahme rechtfertigten, daß ihnen oder anderen Personen bei einer eventuellen Datenübermittlung eine Gefahr für Leben, Gesundheit, persönliche Freiheit und ähnliche schutzwürdige Belange erwachsen konnte.

Schwierigkeiten bei der Bearbeitung der Anträge waren vor allem dann aufgetreten, wenn das Vorliegen von Tatsachen von Betroffenen nicht durch Belege nachgewiesen werden konnte. In einem Fall wurde z. B. eine Gefahr für Leben und Gesundheit anerkannt, weil ein Vater seiner Familie nach der Trennung Gewalt angedroht hatte. Da ein Nachweis der Gefahr durch Belege nicht möglich war, wurde die Auskunftssperre „vorsorglich" auf ein Jahr befristet. In einem ähnlichen Fall, in dem eine Person gegen einen Sexualstraftäter ausgesagt hatte, begrenzte man die Auskunftssperre auf zwei Jahre. Eine erneute Überprüfung der Fälle vor Fristablauf fand nicht statt.

In Anbetracht des besonderen Gefährdungspotentials für die Betroffenen muß auch bei einem unklaren Sachverhalt auf eine eigenmächtige Befristung der Auskunftssperre verzichtet werden. Allenfalls kann ein Wiedervorlagetermin vorgesehen werden, an dem die Voraussetzungen nachzuprüfen sind. Außerdem muß die Aufhebung der Auskunftssperre den Betroffenen auf jeden Fall vorher schriftlich mitgeteilt werden. Die Stadt will in Zukunft entsprechend verfahren.

Datei über Einziehungsersuchen

Zur Überwachung des jeweiligen Verfahrensstandes hatte die Stadtkasse eingehende Einziehungsersuchen in einer besonderen Datei gespeichert. Diese „Schuldnerkartei" wurde manuell bereits seit mehreren Jahren geführt. Sie war alphabetisch nach den Namen der Zahlungspflichtigen geordnet. Jährlich wurden etwa 1 200 bis1 300 Einziehungsersuchen neu eingespeichert. Der überwiegende Teil der Fälle war inzwischen erledigt und damit zur rechtmäßigen Aufgabenerfüllung der Kasse nicht mehr erforderlich, gleichwohl aber nicht gelöscht worden.

Zumindest für die Mitarbeiter der Kasse war jederzeit nachvollziehbar, wann und weshalb in der Vergangenheit gegen einen Bürger der Stadt ein Einziehungsersuchen gelaufen war und wie es abgewickelt wurde. Der Landesbeauftragte hat veranlaßt, daß der, wegen seiner subjektiven Aussagekraft hochsensible Datenbestand in der Weise reorganisiert wird, daß auf ein „Personenkonto" für den Betroffenen ganz verzichtet wird und eine karteimäßige Speicherung von Daten nur noch bezogen auf den jeweiligen Einzelfall erfolgt.

4.3 Justizverwaltung

4.3.1 Die Strafprozeßordnung ist ein Kernbereich des Rechtsstaates

Zu den wichtigsten Gesetzen, die nach dem Volkszählungsurteil des Bundesverfassungsgerichts dringend der Überarbeitung bedürfen, gehört die Strafprozeßordnung. In dem besonders sensiblen Bereich strafrechtlicher Ermittlungen kommt es darauf an, daß der Gesetzgeber für alle Beteiligten, nämlich die Staatsanwaltschaft, die Polizei, den Verdächtigten und Beschuldigten, aber auch für jeden unverdächtigen Bürger klar und präzise regelt, welche Datenzugriffe zum Zwecke der Strafverfolgung zulässig sind. Zu Recht wird die Strafprozeßordnung von vielen als das kleine Einmaleins des Rechtsstaats betrachtet. Besonders hier kommt es deshalb darauf an, daß ein ausgewogener Kompromiß zwischen dem Strafverfolgungsinteresse und den Grundrechten der Betroffenen gefunden wird.

Die konkurrierende Gesetzgebungszuständigkeit für die Strafprozeßordnung liegt beim Bund. Der Bundesminister der Justiz arbeitet seit Jahren an einer Novellierung der Strafprozeßordnung. Die dem Landesbeauftragten bislang bekanntgewordenen Entwürfe lassen die Tendenz erkennen, daß die ursprünglich vorgesehene, zumindest in Teilbereichen eher datenschutzfreundliche Konzeption mehr und mehr zugunsten der Strafverfolgungsinteressen aufgeweicht wurde. Zum letzten bekanntgewordenen Entwurf vom Juni 1989 hat der Landesbeauftragte in seiner Stellungnahme davon abgesehen, auf alle einzelnen Vorschriften einzugehen, sondern sich auf einige aus seiner Sicht wesentliche Punkte konzentriert.

Dem Sinn des Volkszählungsurteils wird es nicht gerecht, die bestehende Datenverarbeitung der Strafverfolgungsbehörden lediglich gesetzlich abzusichern. Statt dessen ist die Chance wahrzunehmen, die bislang entwickelten Verfahren auf ihre Erforderlichkeit kritisch zu überprüfen. Als Beispiel können die Vorschriften über die Überwachung des Telefonverkehrs gelten. Im Hinblick auf die rasche Fortentwicklung und Erweiterung der Telekommunikation kommt der Überwachung des Fernmeldeverkehrs heute eine andere Bedeutung zu als zur Zeit der Formulierung des derzeit maßgeblichen § 100a StPO. Die modernen Möglichkeiten der Auswertung aufgezeichneter Telefongespräche und die Tatsache, daß der Polizei leistungsfähige Dateien zur Verfügung stehen, die früher nicht gekannte Möglichkeiten der Speicherung und Auswertung von Telefonüberwachungsdaten ermöglichen, sollten Veranlassung geben, zu prüfen, ob die überkommenen Eingriffsnormen nicht restriktiver gefaßt werden müssen.

Auch auf dem Gebiet des Erkennungsdienstes und der Kriminaltechnik sind die technischen Möglichkeiten enorm verbessert. Warum noch förmlich erkennungsdienstlich behandeln, wenn ohnehin aus dem Paß- und Personalausweisregister ein Foto zu erhalten ist? Handschriftproben können digitalisiert gespeichert und abgeglichen werden, so daß es auf die „Handschrift" der Fingerabdrücke gar nicht mehr unbedingt ankommt. Unter welchen Voraussetzungen die Polizei wessen Handschriften wie lange speichern darf, ist bislang nicht gesetzlich geregelt. Daneben laufen aber die „klassischen" erkennungsdienstlichen Behandlungen nach den „Ed-Richtlinien" weiter. Ein anderes Beispiel ist die Genomanalyse, zu der inzwischen immerhin ein eigener Gesetzentwurf vorliegt (vgl. dazu Tz. 4.3.2).

Der Landesbeauftragte hat sich dafür ausgesprochen, den Bereich der Datenverarbeitung für Zwecke künftiger Strafverfolgung abschließend in der Strafprozeßordnung zu regeln. Diese Form der Datenverarbeitung ist im Kern nicht Gefahrenabwehr, sondern die Vorbereitung auf künftige Strafverfolgung. Deshalb ist die größere Sachnähe zum Strafverfolgungsrecht gegeben. Es ist darüber hinaus auch zweckmäßig, die Befugnisse im Rahmen der Strafverfolgung

bundeseinheitlich und nicht von Land zu Land unterschiedlich zu regeln.

Der Zweckbindungsgrundsatz muß im Gesetzentwurf stärker zur Geltung gebracht werden. Dies gilt sowohl für die Verwendung der Daten durch Strafverfolgungsbehörden als auch für ihre Weitergabe an andere Behörden. Bei der polizeiinternen Verwendung ist zu beachten, daß Daten, die mit besonderen Erhebungsmethoden gewonnen wurden, wie z. B. im Wege der Observation oder der polizeilichen Beobachtung, nur für die Verhinderung und Verfolgung solcher Straftaten verwendet werden dürfen, zu deren Aufklärung sie ebenfalls hätten eingesetzt werden dürfen. Die Weitergabe von Daten an die Geheimdienste sollte in der Strafprozeßordnung selbst abschließend und restriktiv geregelt werden und nicht der Regelung der Geheimdienstgesetze überlassen werden. Daten, die unter Inanspruchnahme von Befugnissen erhoben worden sind, die nur den Strafverfolgungsbehörden, nicht aber den Geheimdiensten zustehen, sollten letzteren nur in besonderen Fällen übermittelt werden dürfen.

Eine andere Schwäche der im Gesetzentwurf vorgesehenen Zweckbindungsregelungen ist, daß sie häufig lediglich die Verwendung von Daten „zu Beweiszwecken" ausschließen, nicht aber die sonstige Nutzung für andere Zwecke. Da Datenverarbeitung nur in seltenen Fällen unmittelbar gerichtsverwertbare Beweise erbringt, sondern in erster Linie der Gewinnung neuer Ermittlungsansätze dient, dürften derartige Zweckbindungsregeln ihre Wirkung weitgehend verfehlen.

Der Entwurf sieht an verschiedenen Stellen Datenverarbeitungsmaßnahmen bezüglich „anderer Personen" vor, d. h. Personen, gegen die weder ein Verdacht noch eine Beschuldigung vorliegen. Er ermöglicht die Speicherung von Daten über diesen Personenkreis, sieht ihre Weiterübermittlung an die Geheimdienste ohne nähere Einschränkung vor und läßt es zu, daß „andere Personen" Ziel besonderer Fahndungsmethoden werden. Der Landesbeauftragte hat verlangt, den Entwurf dahin gehend zu überarbeiten, daß die Verarbeitung von Daten über „andere Personen" auf das sachlich und zeitlich vertretbare Mindestmaß beschränkt wird.

Des weiteren sollen neue Rechtsgrundlagen für die Anwendung besonderer Datenerhebungsmethoden geschaffen werden. Dies gilt für die Rasterfahndung, die polizeiliche Beobachtung und den Einsatz verdeckter Ermittler. Der Landesbeauftragte tritt dafür ein, daß die Notwendigkeit von Rasterfahndungsmaßnahmen noch einmal kritisch überprüft wird, zumal nach seiner Kenntnis in den vergangenen Jahren von dieser Methode – vermutlich mangels Effektivität – kaum mehr Gebrauch gemacht worden ist. Er fragt deshalb, ob eine zwingende Notwendigkeit besteht, eine derartige Vorschrift in das Gesetz aufzunehmen, von der eine Vielzahl unverdächtiger Personen betroffen sein könnte. „Besondere Datenerhebungsmethoden", wie etwa verdeckte Ermittler, Observation, polizeiliche Beobachtung, sollten möglichst nur für

die Bekämpfung der organisierten Kriminalität verwendet werden dürfen, zumal von seiten der Strafverfolgungsbehörden ihre Erforderlichkeit in der Regel stets mit dem Anwachsen der organisierten Kriminalität begründet wird. Der Gesetzentwurf gewährleistet dies bislang nicht.

Besondere Kritik ist an den vorgesehenen Dateiregelungen zu üben. Sie begrenzen die Datenverarbeitung bei Polizei und Staatsanwaltschaften nicht wirklich, sondern bieten statt dessen erhebliche Spielräume für die Erweiterung der bestehenden Verfahren. Dies gilt insbesondere für die pauschal erteilte Befugnis für Polizei, Staatsanwaltschaft, Gerichte und Vollstreckungsbehörden, Dateien gemeinsam zu betreiben. Eine derartige gemeinsame Datei dieser Behörden ist dem Landesbeauftragten bislang nicht bekannt. Würde der Entwurf in dieser Form verabschiedet und würden seine Spielräume von den angesprochenen Behörden konsequent genutzt, so könnte eine Datenverarbeitung bislang nicht gekannten Ausmaßes entstehen.

Ein weiterer Schwachpunkt ist die Bestimmung über die Speicherung von Daten zum Zwecke der „Vorgangsverwaltung". Da im Entwurf nirgendwo auch nur ansatzweise geregelt ist, was unter „Vorgangsverwaltung" zu verstehen ist, handelt es sich um eine Blankettnorm, auf deren Grundlage gespeichert wird, ohne daß klar wäre, was mit den mit Hilfe der Datei „Vorgangsverwaltung" gewonnenen Daten geschehen darf. Statt dessen kommt es darauf an, daß exakt festgelegt wird, für welche Zwecke die „Vorgänge" genutzt werden dürfen. Erst danach können die datenschutzrechtlichen Risiken eingeschätzt werden, die in derartigen Dateien liegen.

Der Gesetzentwurf sieht weitgehende Möglichkeiten zur Einführung von Online-Verbindungen zwischen den Dateien der Strafverfolgungsbehörden vor. Darüber hinaus soll der Staatsanwaltschaft ermöglicht werden, ein zentrales bundesweites Verfahrensregister einzurichten, in dem alle Ermittlungsverfahren gespeichert werden. Die Erforderlichkeit ist in Frage zu stellen, da vergleichbare Systeme bei der Polizei längst bestehen und kein überzeugender Grund für eine doppelte Speicherung gegeben ist.

Der Landesbeauftragte hat die Auffassung vertreten, daß parallel zum Ausbau der elektronischen Datenverarbeitung die Rechtsschutzmöglichkeiten in der Strafprozeßordnung fortentwickelt werden müssen. Es muß möglich sein, Datenerhebungs- und Speicherungsmaßnahmen gerichtlich auch unabhängig vom jeweiligen Strafverfahren und dessen Stand überprüfen zu lassen.

Der Justizminister des Landes Schleswig-Holstein hat dem Landesbeauftragten bislang noch nicht mitgeteilt, ob und welche Positionen er übernimmt und im Gesetzgebungsverfahren des Bundes geltend macht.

4.3.2 Genomanalyse im Strafverfahren

Die Genomanalyse bietet die Möglichkeit, Personen anhand von Blutproben, Körpersekreten oder Haarteilen mit einer bislang nicht erreichten, wenn auch nicht 100%igen Eindeutigkeit zu unterscheiden bzw. zu identifizieren. Mit ihrer Hilfe können aber auch Informationen aus dem Kernbereich der Privatsphäre der Betroffenen, etwa über Persönlichkeitsstrukturen und Krankheiten, die diesen selbst möglicherweise nicht bekannt sind, ans Tageslicht gebracht werden. Auch die Strafverfolgungsbehörden interessieren sich für die Genomanalyse. Presseberichten zufolge haben das Bundeskriminalamt sowie einzelne Landeskriminalämter technische Einrichtungen zur Durchführung von Genomanalysen geschaffen. Soweit dem Landesbeauftragten für den Datenschutz bekannt, gibt es bei der schleswig-holsteinischen Polizei bisher keine eigenen Untersuchungseinrichtungen.

Mit der Zulässigkeit der Genomanalyse im Strafverfahren haben sich schon mehrere Gerichte beschäftigt. Das Landgericht Berlin (NJW 1989, S. 787) kam in seinem Beschluß zur Zulässigkeit der Durchführung einer DNS-Analyse im Strafverfahren zu einem differenzierten Ergebnis. Es geht davon aus, daß die DNS-Analyse derzeit nur die sogenannten nichtkodierenden Bereiche entschlüsselt, die nach dem bisherigen Stand der Wissenschaft keine Aufschlüsse über genetisch bedingte Persönlichkeitsmerkmale und Krankheitsveranlagungen zulassen. Ein über den völlig persönlichkeitsneutralen Spurenvergleich hinausgehender Informationsüberschuß sei nach dem gegenwärtigen Stand der Wissenschaft nicht möglich. Auf dieser Grundlage hält die Kammer die Durchführung der DNS-Vergleichsanalyse für vereinbar mit § 81 a Strafprozeßordnung. Wegen der Gefahren für das allgemeine Persönlichkeitsrecht sei aber bei der Anordnung von DNS-Vergleichsanalysen der Verhältnismäßigkeitsgrundsatz zu beachten. Sie komme nur als Ultima ratio in Betracht. Mit dieser Erwägung verneinte die Kammer im von ihr zu entscheidenden Fall die Erforderlichkeit einer DNS-Analyse.

Das Landgericht Darmstadt (Az. 10 Js 21 985/82) kommt ebenfalls zur Vereinbarkeit der DNS-Analyse mit § 81 a Strafprozeßordnung. Maßgeblich ist für die Kammer, daß die Analyse aus dem nichtkodierenden Teil der DNS stammt, so daß mit ihrer Hilfe keine Informationen über die Persönlichkeit des Betroffenen gewonnen werden könnten. Im vom Landgericht Darmstadt entschiedenen Fall führte die Verwendung der DNS-Analyse im übrigen zum Freispruch des Angeklagten. Auch das Landgericht Heilbronn (NJW 90, S. 794) sieht in § 81 a Strafprozeßordnung eine ausreichende Rechtsgrundlage für die Verwendung eines genetischen Fingerabdrucks als Beweismittel.

Der Landesbeauftragte für den Datenschutz hat Bedenken, ob § 81 a Strafprozeßordnung als Rechtsgrundlage für die Durchführung von DNS-Analysen tatsächlich ausreichend ist. Es ist nicht ausgeschlossen, daß angesichts der rasanten

Fortentwicklung der Möglichkeiten der Genomanalyse schon in kurzer Zeit bei den Testverfahren ein persönlichkeitsrelevanter Informationsüberschuß erzeugt werden kann, der Rückschlüsse auf Persönlichkeitsstrukturen der Betroffenen zuläßt. Deshalb ist es notwendig, daß diese Möglichkeit für das Strafverfahren gesetzlich ausgeschlossen und durch enge Zweckbindungsregeln sichergestellt wird, daß die DNS-Analyse ausschließlich zu Identifizierungszwecken benutzt wird. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu entsprechende Beschlüsse gefaßt. Der Landesbeauftragte hat den Innenminister und den Justizminister des Landes gebeten, diesen Beschlüssen im Rahmen der Novellierung der Strafprozeßordnung Rechnung zu tragen (vgl. Tz. 4.3.1).

4.3.3 Geschäftsstellenautomation der Staatsanwaltschaften (GAST) ohne Rechtsgrundlage?

Das Oberlandesgericht Frankfurt (NJW 1989, S. 47) ist zu dem Ergebnis gekommen, daß die zentralen Namenskarteien der Staatsanwaltschaften auf keiner gesicherten Rechtsgrundlage beruhen. Der Gesetzgeber habe nur noch bis zum Ende der laufenden Legislaturperiode des Deutschen Bundestages eine Schonfrist zur Schaffung entsprechender Vorschriften. Diesem Urteil kommt für Schleswig-Holstein insofern besondere Bedeutung zu, als hier die zentralen Namenskarteien der Staatsanwaltschaften im Gegensatz zu anderen Ländern auf Landesebene automatisiert im sog. System GAST geführt werden.

Der Justizminister hat deshalb eine Zeitlang die Einbringung eines eigenen Gesetzentwurfs des Landes Schleswig-Holstein zur Änderung der Strafprozeßordnung mit dem Ziel der rechtlichen Absicherung des GAST-Verfahrens in Erwägung gezogen. Der Landesbeauftragte war frühzeitig in diese Überlegungen einbezogen und hat mehrfach hierzu Stellung genommen. Er hat von einer derartigen Vorgehensweise aus grundsätzlichen Erwägungen abgeraten und darüber hinaus an den vorgesehenen Vorschriften Einzelkritik geübt. Zwischenzeitlich ist die Absicht offenbar fallengelassen worden, durch eine schleswig-holsteinische Initiative die Strafprozeßordnung punktuell zu novellieren.

Falls, wie anzunehmen, der Deutsche Bundestag in dieser Legislaturperiode die Novellierung der Strafprozeßordnung nicht mehr beschließt, stellt sich die Frage, wie das GAST-Verfahren rechtlich zu beurteilen ist. Der Landesbeauftragte steht auf dem Standpunkt, daß unabhängig von der Grundsatzfrage, ob und wie lange für das GAST-Verfahren der sog. Übergangsbonus in Anspruch genommen werden kann, an weiteren datenschutzrechtlichen Verbesserungen des Verfahrens gearbeitet werden muß. Er beabsichtigt, GAST einer datenschutzrechtlichen Prüfung zu unterziehen und dem Justizminister Vorschläge für eine möglichst datenschutzfreundliche, restriktive Handhabung des Systems zu machen.

4.3.4 Die Mitteilungen in Strafsachen auf dem Prüfstand des Bundesverfassungssgerichts

Ein Bürger aus Schleswig-Holstein hat Verfassungsbeschwerde beim Bundesverfassungsgericht erhoben, der folgender Sachverhalt zugrundeliegt. Gegen ihn liefen staatsanwaltschaftliche Ermittlungen wegen eines Sexualdelikts (Exhibitionismus). Er unterrichtete seinen Arbeitgeber, eine Behörde, darüber. Diese erhielt in der Folge auf Anfrage von der Staatsanwaltschaft eine Kopie der Anklageschrift und vom Amtsgericht die gesamte Strafakte zur Einsichtnahme übersandt. Daraufhin wurde das Arbeitsverhältnis des Petenten fristlos und fristgerecht gekündigt. Das Strafverfahren gegen ihn wurde nach § 3 Strafprozeßordnung gegen eine geringe Geldbuße eingestellt, da nur eine „geringe Schuld" des Betroffenen vorlag und das öffentliche Strafverfolgungsinteresse nach Erledigung der gerichtlichen Auflagen weggefallen war.

Das Bundesverfassungsgericht hat den Landesbeauftragten für den Datenschutz um Stellungnahme gebeten. Er ist dieser Bitte nachgekommen und hat dabei ausgeführt, daß die derzeitige Regelung der Mitteilungen in Strafsachen (MiStra) als reine Verwaltungsvorschrift nicht ausreicht, um einen Eingriff in das Recht auf informationelle Selbstbestimmung zu rechtfertigen. Ein solcher liegt bei der Mitteilung über laufende Strafermittlungsverfahren an Dritte zweifellos vor. Auch inhaltlich ist die MiStra in der gegenwärtig geltenden Fassung zu kritisieren. So ist dort nicht festgelegt, zu welchem Zweck Mitteilungen über Strafsachen gemacht werden dürfen und wie die zweckgerechte Verwendung dieser Informationen bei Empfängern sichergestellt werden kann. Die Datenübermittlung im Rahmen der MiStra ist der Regelfall, der Verzicht auf eine Mitteilung die Ausnahme. In vielen Bereichen ist auch nicht geregelt, in welchem Umfang die Betroffenen über die beabsichtigte Übermittlung zu unterrichten sind. Auch in anderer Hinsicht sind die gültigen MiStra-Regelungen inhaltlich nicht befriedigend.

Weiter hat der Landesbeauftrage ausgeführt, bis zur Schaffung einer einwandfreien gesetzlichen Grundlage dürfe die MiStra nur noch in einem engen Rahmen angewandt werden, wenn dies nötig sei, um einen noch verfassungswidrigeren Zustand zu vermeiden.

Ob diese engen Grenzen im betreffenden Fall eingehalten worden sind, konnte anhand der vorliegenden Informationen nicht abschließend beurteilt werden. So ist ein wichtiges Kriterium, ob der Petent Publikumsverkehr gehabt hat oder nicht. Darauf kommt es u. a. an, wenn entschieden werden muß, ob aufgrund des gegen ihn eingeleiteten Strafverfahrens sofortige Maßnahmen unabdingbar notwendig waren oder nicht. Gerade weil es inzwischen zu einer Einstellung des Verfahrens nach § 153 a Strafprozeßordnung gekommen ist, stellt sich die Frage, ob man mit der Übermittlung der den Petenten belastenden Daten nicht bis zum Abschluß des Verfahrens hätte warten müssen.

Der Landesbeauftragte ist der Meinung, daß dieser Fall plastisch vor Augen führt, welch schwerwiegenden Eingriff eine Mitteilung über Strafsachen für den Betroffenen bedeuten kann. Das eigentliche Strafverfahren brachte durch die im Rahmen der Verfahrenseinstellung zu zahlende Geldbuße eine erheblich geringere Belastung als der Verlust des Arbeitsplatzes. Derart schwerwiegende Folgen können nicht auf der Basis einer Verwaltungsanordnung herbeigeführt werden.

In einem anderen Fall, der den Landesbeauftragten in dieser Einschätzung bestärkt, waren ebenfalls Mitteilungen über die Einleitung eines Ermittlungsverfahrens an den vermeintlichen Dienstherrn des Betroffenen, eine Kirchenverwaltung, gerichtet worden. Dabei war der Betroffene zum Zeitpunkt der Mitteilung gar nicht mehr bei dieser Kirchenverwaltung beschäftigt. Während das zuständige Gericht und die Staatsanwaltschaft auf dem Standpunkt stehen, der Betroffene selbst habe in der Hauptverhandlung seinen Arbeitgeber entsprechend angegeben, wird dies von ihm bestritten.

Der Landesbeauftragte kann nicht nachprüfen, welche der beiden Sachverhaltsdarstellungen richtig ist. Klar ist aber, daß, wenn man seiner Empfehlung entsprechend den Betroffenen vor der Mitteilung unterrichtet hätte, dieser die Chance gehabt hätte, klarzustellen, ob er noch bei der betreffenden Stelle beschäftigt ist oder nicht.

Der Landesbeauftragte hat deshalb den Justizminister aufgefordert, bei der Anwendung der MiStra wesentlich restriktiver als bisher zu verfahren, solange keine gesetzliche Grundlage für die dort vorgesehenen Übermittlungen geschaffen ist. Dies gilt vor allem für die Zeit nach dem Ablauf der Legislaturperiode des Deutschen Bundestages, falls – wovon auszugehen ist – bis dahin keine einwandfreie Rechtsgrundlage geschaffen worden ist. Dann dürfte auch der Übergangsbonus abgelaufen sein. Die bisherige Übermittlungspraxis kann dann nicht mehr unverändert fortgeführt werden.

4.3.5 Novellierung des Bundeszentralregistergesetzes: Nägel mit Köpfen machen

Der Landesbeauftragte hat zum Arbeitsentwurf eines dritten Gesetzes zur Änderung des Bundeszentralregistergesetzes Stellung genommen und begrüßt, daß darin weitere Präzisierungen und datenschutzrechtliche Verbesserungen vorgesehen sind. Er hat aber darauf hingewiesen, daß es notwendig ist, eine einheitliche Konzeption von Regelungen für die Speicherung und Nutzung von Daten aus dem gesamten Strafverfolgungsbereich vorzulegen. Im Bundeszentralregister werden nämlich im wesentlichen nur Informationen über erfolgte Verurteilungen gespeichert.

Daneben speichert die Polizei Daten über eingeleitete Ermittlungsverfahren. Diese Daten sind insofern sensibler als die im Bundeszentralregister erfaßten, da es sich lediglich um Verdachtsdaten handelt, die durch die Justiz noch nicht ab-

schließend überprüft sind. Häufig erfährt die Polizei noch nicht einmal, wie die Justiz das von ihr vorgelegte Verdachtsmaterial beurteilt hat und ob es zu einer Verurteilung gekommen ist (siehe Tz. 4.1.3.1). Deshalb sind bei der Polizei wesentlich mehr Daten als im Bundeszentralregister erfaßt. Die polizeilichen Übermittlungsvorschriften in den entsprechenden internen Richtlinien sind teilweise weiter gefaßt als die Auskunftsbestimmungen des Bundeszentralregistergesetzes. Verwertungsbeschränkungen, wie sie etwa im Bundeszentralregistergesetz für tilgungsreife Informationen vorgesehen sind, werden häufig als für die Polizei nicht bindend angesehen.

Der Landesbeauftragte hat deshalb die Beobachtung gemacht, daß Behörden nicht selten versuchen, neben der Auskunft aus dem Bundeszentralregister auch Informationen aus polizeilichen Datenbeständen zu erhalten. Letztere sind in der Praxis in der Regel „ergiebiger" als die Bundeszentralregisterauskunft. Bürger schildern immer wieder, daß sie feststellen mußten, daß sie bei der Polizei mit Daten über frühere Verdachtsfälle gespeichert sind. Diese tauchen paradoxerweise in einem „polizeilichen Führungszeugnis" nicht auf, da dieses nur auf der Grundlage der Speicherungen im Bundeszentralregister erstellt wird. Die Polizei gibt sie aber an andere Behörden weiter.

Der Landesbeauftragte hat in seiner Stellungnahme vor allem auf die Notwendigkeit abgestellt, eine übergreifende Regelung zu treffen, die sowohl die Datenspeicherung im Bundeszentralregister als auch bei der Polizei und anderen Behörden einbezieht. Dabei muß zwischen dem Interesse der Allgemeinheit an der Kenntnis und der Verwendung von Daten über Straftaten und dem Resozialisierungsanspruch der Betroffenen eine ausgewogene Lösung gefunden werden. Dies müßte nicht unbedingt im Bundeszentralregistergesetz geschehen. Es liegt aber nahe, dies dort zu tun, da gerade dieses Gesetz den Anspruch hat, diesem Interessensausgleich zu dienen. Der Landesbeauftragte hat deshalb empfohlen, bei Gelegenheit des dritten Gesetzes zur Änderung des Bundeszentralregisters Nägel mit Köpfen zu machen und umfassend für alle staatlichen Sammlungen zu regeln, wie lange Informationen über Straftaten aufbewahrt und unter welchen Voraussetzungen und für welche Zwecke sie verwendet werden dürfen.

Daneben sind noch einzelne Vorschriften des Arbeitsentwurfs verbesserungsbedürftig. Es ist insbesondere notwendig, den Kreis derjenigen Behörden, die eine unbeschränkte Auskunft aus dem Bundeszentralregister erhalten können, einzuschränken, und die Zwecke, zu denen dies erfolgen darf, präziser und restriktiver zu regeln.

Der Landesbeauftragte hat den Justizminister aufgefordert, die von ihm vorgetragenen Gesichtspunkte im weiteren Gesetzgebungsverfahren geltend zu machen. Welche Argumente der Justizminister übernimmt und in das Verfahren einbringt, ist dem Landesbeauftragten noch nicht mitgeteilt worden.

4.3.6 Kein Datenschutz fürs Grundbuch?

Ein Petent hat dem Landesbeauftragten mitgeteilt, ihm sei anonym vorgeworfen worden, er habe öffentliche Gelder veruntreut. Die Staatsanwaltschaft habe in Kenntnis der Vorwürfe keine Veranlassung gesehen, Ermittlungen gegen ihn aufzunehmen. Die gleichen Vorwürfe seien aber auch der Presse zugespielt worden. Ein Journalist habe daraufhin unter Verweis auf seine journalistische Aufgabe, das öffentliche Interesse an dem „Fall" und den erhobenen Vorwürfen, Einsicht in die Grundakte des Loseblattgrundbuchs des Grundstücks des Petenten erbeten. Nach Ablehnung durch die Geschäftsstelle habe der Grundbuchrichter Grundakteneinsicht (Handblatt der Grundakte) gewährt und über seine Entscheidung einen Vermerk zu den Grundakten genommen, aus dem auch die gegen den Petenten gerichteten Vorwürfe ersichtlich waren.

Das zuständige Amtsgericht hat die sogleich eingelegte Dienstaufsichtsbeschwerde mit der Begründung zurückgewiesen, der Grundbuchrichter habe im Rahmen richterlicher Unabhängigkeit die kritisierte Entscheidung getroffen, so daß eine Überprüfung im Wege der Dienstaufsicht nicht möglich sei. Datenschutzrechtliche Belange seien auch deshalb nicht berührt, da die Grundbuchordnung den Datenschutzgesetzen des Bundes und der Länder vorgehe und da im übrigen Grundbuch und Grundakte keine Datei darstellten. Dem Petenten wurde allerdings mitgeteilt, daß der vom Grundbuchrichter angefertigte Vermerk über die Grundbucheinsicht, aus dem auch die Vorwürfe gegen ihn ersichtlich waren, aus den Grundakten entfernt und zu den Generalakten genommen wurde.

Der vom Landesbeauftragten eingeschaltete Justizminister hat die Rechtsauffassung des Amtsgerichts, wonach es sich bei der Entscheidung über Grundbucheinsicht um eine Tätigkeit im Rahmen der richterlichen Unabhängigkeit handelt, bestätigt. Er hat darüber hinaus darauf hingewiesen, daß nach einer Entscheidung des Oberlandesgerichts Hamm (MDR 10/1988) auch das Rechercheinteresse eines Journalisten im Einzelfall ein berechtigtes Interesse im Sinne der Grundbuchordnung sei.

Der Landesbeauftragte rechnet die Entscheidung des Richters über die Gewährung von Einsicht in Grundakten nicht der rechtsprechenden Tätigkeit zu. Der Richter entscheidet in diesem Zusammenhang keinen Rechtsstreit, sondern er genehmigt die Grundbucheinsicht anstelle des Grundbuchrechtspflegers, wenn besondere rechtliche Schwierigkeiten bei der Interpretation der Grundbuchordnung auftreten. Es handelt sich also im Kern um eine Verwaltungsentscheidung, die dem Richter übertragen worden ist. Derartige Tätigkeiten sind der Kontrolle durch den Landesbeauftragten für den Datenschutz nicht entzogen.

Im vorliegenden Fall war zwar zu berücksichtigen, daß die Grundakten, in die hier Einsicht gewährt worden war, den

Dateibegriff nicht erfüllen. Das Recht auf informationelle Selbstbestimmung gilt aber unabhängig vom verwendeten Datenverarbeitungsverfahren. Der Landesbeauftragte hat deshalb anläßlich des vorliegenden Falles erneut darauf hingewiesen, daß auch im Rahmen der Entscheidung über die Gewährung von Grundbucheinsicht eine Abwägung zwischen dem Interesse des Einsichtbegehrenden und dem Recht auf informationelle Selbstbestimmung des Betroffenen vorzunehmen ist. Die zitierte Gerichtsentscheidung ist für ihn „nicht ohne weiteres nachvollziehbar". Er kann aber nicht beanstanden, daß in Schleswig-Holstein entsprechend dieser Rechtsauslegung verfahren wird.

Die bereits früher erhobene Forderung, die Gewährung von Grundbucheinsicht zu dokumentieren (vgl. 11. TB, S. 32), war im vorliegenden Fall erfüllt. Wegen der Besonderheit des Falles, wonach aus dem Antrag auf Gewährung der Grundbucheinsicht die unberechtigten Vorwürfe gegen den Petenten ersichtlich waren, war es auch sachgerecht, daß der Antrag nicht bei den Grundakten aufbewahrt, sondern zu den Generalakten genommen wurde.

Ganz unabhängig davon ist aber nach wie vor klärungsbedürftig, wie weit die der Kontrolle des Landesbeauftragten entzogene richterliche Tätigkeit geht und wo die Verwaltungstätigkeit der Gerichte beginnt, die in vollem Umfang der Datenschutzkontrolle unterliegt. Darüber hinaus zeigt der vorliegende Fall auch, wie wichtig es ist, daß die Voraussetzungen für die Grundbucheinsicht in der Grundbuchordnung präzisiert werden und daß in diesem Zusammenhang auch die Frage der Dokumentationspflicht abschließend geregelt wird.

4.3.7 Wenn zwei sich streiten, erfährt es manchmal der Dritte

Ein Bürger wandte sich an den Landesbeauftragten mit folgendem Anliegen: In einem Verwaltungsstreitverfahren, das er angestrengt hatte, weil er sich gegen die Heranziehung zur Auskunftserteilung im Rahmen der Volkszählung 1987 wandte, wurde ihm der Name und der Wohnort eines Verfahrensbeteiligten bekannt, der offenbar ebenfalls gegen die Heranziehung zur Volkszählung geklagt hatte. Der Petent vermutete, daß auch dem anderen Verfahrensbeteiligten seine Daten auf die gleiche Weise bekanntgegeben wurden.

Er hat damit ein allgemeines Problem angeschnitten, das immer dann entstehen kann, wenn ein Gerichtsverfahren einen Gegenstand, aber mehrere Beteiligte hat. Im Bereich der Verwaltungsgerichtsbarkeit können derartige Fallgestaltungen beispielsweise auftauchen, wenn sich mehrere Kläger gegen ein Planungsprojekt wenden. Nicht selten sind dabei, etwa bei Klagen gegen Flughafenplanungen, gesundheitliche Daten, wie z. B. besondere Lärmempfindlichkeit, Gegenstand des Vorbringens.

Weder die Verwaltungsgerichtsordnung noch die Zivilprozeßordnung enthalten Vorschriften, wie in derartigen Fällen

das Recht auf informationelle Selbstbestimmung der Verfahrensbeteiligten gewahrt wird. Statt dessen sehen beide Verfahrensordnungen ein pauschales Akteneinsichtsrecht der Verfahrensbeteiligten vor.

Der Justizminister stimmte der Auffassung des Landesbeauftragten zu, wonach auch bei der Gewährung von Akteneinsicht sowie bei sonstigen prozeßleitenden Verfügungen das Recht auf informationelle Selbstbestimmung zu beachten ist. Er vermochte allerdings im vorliegenden Fall kein Fehlverhalten des Richters zu erkennen, da der Name des Petenten sowie des anderen Verfahrensbeteiligten auf einem Schriftstück gemeinschaftlich genannt war, welches von der Gegenseite im Verfahren vorgelegt worden war. Eine Schwärzung eines der Namen wäre nach Auffassung des Justizministers auf eine Manipulation in einem fremden Schriftstück hinausgelaufen. Darüber hinaus verwies er darauf, daß es einen zu großen Arbeitsaufwand bedeutet hätte, alle Schriftsätze bei mehreren tausend anhängigen Sachen nach dem Volkszählungsgesetz daraufhin durchzusehen, ob dort die Namen anderer Verfahrensbeteiligter enthalten waren. Zudem handele es sich im vorliegenden Fall nicht um besonders sensible Daten. Verwaltungsgerichtliche Verfahren seien grundsätzlich öffentlich, so daß jedermann die Namen der Verfahrensbeteiligten hätte in Erfahrung bringen können.

Der Landesbeauftragte ist der Meinung, daß es einen Unterschied macht, ob sich jedermann aktiv in öffentlichen Gerichtsverhandlungen über die Prozeßbeteiligten informieren kann oder ob durch prozeßleitende Handlungen des Gerichts derartige Informationen „ frei Haus" geliefert werden. Notwendig ist nach seiner Auffassung aber vor allem, daß der Gesetzgeber im Rahmen der Novellierung der Zivilprozeßordnung und der Verwaltungsgerichtsordnung Vorschriften schafft, die auch im Bereich der Akteneinsicht sowie sonstiger prozeßleitender Verfügungen das Recht auf informationelle Selbstbestimmung angemessen berücksichtigen. Bis dies realisiert ist, sind die Gerichte aufgerufen, im Rahmen der Auslegung und Anwendung des Prozeßrechts das Recht auf informationelle Selbstbestimmung zu beachten.

4.3.8 Gefahr für den Sozialdatenschutz in Gerichtsakten

Der Landesbeauftragte berichtete im 9. Tätigkeitsbericht (S. 30) über einen Fall, in dem ein Jurastudent für seine Dissertation die in den Gerichtsakten enthaltenen Jugendgerichtshilfeberichte ausgewertet hatte. Das hielt der Landesbeauftragte für unzulässig, denn das Sozialgesetzbuch (SGB X) verpflichtet nicht nur die abgebende, sondern auch die empfangende Stelle zum Schutz und zur Geheimhaltung der Sozialdaten. Das soll nun für Strafakten teilweise aufgehoben werden.

Die neue Regelung soll dem Sozialdatenschutz unterliegende Daten von den Einschränkungen des Sozialgesetzbuches ausnehmen, wenn sie Teile von Akten eines Strafverfahrens oder

einer entsprechenden Datei geworden sind. Die Nutzung soll für die wissenschaftliche Forschung ermöglicht werden. Der Landesbeauftragte hat gegenüber dem Justizminister erhebliche Bedenken gegen diese geplante „Ergänzung" des § 78 SGB X geltend gemacht und darauf hingewiesen, daß der Gesetzgeber mit der Nichtöffentlichkeit von Jugendgerichtsverfahren gerade hier ein besonderes Schutzbedürfnis anerkannt hat. Die Informationen aus der Jugendgerichtshilfe in Strafakten sind in der Regel besonders sensibel. Ob und welche personenbezogenen Daten für wissenschaftliche Zwecke offenbart werden dürfen, muß sich nach Auffassung des Landesbeauftragten aus der Sensibilität der Daten und nicht aus dem Aufbewahrungsort beantworten.

Der Landesbeauftragte hat den Justizminister gebeten, seine Bedenken im Bundesrat vorzubringen.

4.4 Sozial- und Gesundheitswesen

4.4.1 Soziales

4.4.1.1 Die neue Zentraldatei der Rentenversicherung

Die Totalerfassung aller Arbeitnehmer, vor der der Landesbeauftragte bereits im letzten Tätigkeitsbericht (vgl. 11. TB, S. 42) gewarnt hat, ist mit Inkrafttreten des Sozialversicherungsausweisgesetzes des Bundes Realität geworden. Die ablehnende Haltung Schleswig-Holsteins im Bundesrat, die sich neben anderen auch auf datenschutzrechtliche Gründe stützte, konnte die Verabschiedung des Gesetzes nicht verhindern. Die vorgesehenen lückenlosen und perfekt anmutenden Überwachungsmaßnahmen greifen tief in das informationelle Selbstbestimmungsrecht der Betroffenen ein und treffen in weitem Umfang Personen, die eigentlich nicht gemeint sind, weil sie keiner illegalen Beschäftigung oder Schwarzarbeit nachgehen.

Unverändert sollen nämlich auch alle geringfügig Beschäftigten für die ganze Bundesrepublik zentral bei der Datenstelle des Verbandes Deutscher Rentenversicherer (VDR) mit monatlichem Verdienst und Arbeitszeit gespeichert werden. Da sie, Schüler, Werkstudenten und Hausfrauen mit Nebenbeschäftigung, im Regelfall nicht sozialversicherungspflichtig sind, hält der Landesbeauftragte die Einrichtung dieser zentralen Datei für unvereinbar mit dem Grundsatz der Verhältnismäßigkeit. Die Zentraldatei wird von den Krankenkassen gespeist, die schon bisher in ihrem Zuständigkeitsbereich nachprüfen konnten, ob die gleichen Personen bei mehreren Arbeitgebern einer geringfügigen Beschäftigung nachgehen. Die nunmehr vorgesehene Zentraldatei soll darüber hinaus die Prüfung ermöglichen, ob gleiche Personen auch in den Zuständigkeitsbereichen verschiedener Krankenkassen gemeldet sind. Das bedeutet, „mit Kanonen auf Spatzen zu schießen", nur um diese wenigen Fälle herauszufinden. Denn der Kontrollzweck kann nach Auffassung des Landesbeauf-

tragten im wesentlichen bereits durch interne Kontrollen der Krankenkassen erfüllt werden.

Er stellt fest, daß hier wieder einmal dem Wunsch nach möglichst perfekten Kontrollregelungen der Vorrang vor dem informationellen Selbstbestimmungsrecht gegeben wurde.

4.4.1.2 Rentenreformgesetz – künftig online von Lübeck nach Palermo?

Das Rentenreformgesetz als ein umfangreiches gesetzgeberisches Vorhaben dieser Legislaturperiode des Bundestages gab Anlaß, neben der Konsolidierung der Rentenversicherung auch bereichsspezifische Datenschutzregelungen zu entwickeln. Datenschutzrechtliche Verbesserungen konnten dabei erreicht werden.

In der letzten Phase des Gesetzgebungsverfahrens wurde allerdings eine Vorschrift eingefügt, die erhebliche datenschutzrechtliche Bedenken erregt. Sie gestattet nämlich nicht nur den Rentenversicherungsträgern, sondern sämtlichen Krankenkassen, Berufsgenossenschaften und Arbeitsämtern über einen Online-Anschluß den Zugriff auf Versichertendaten. Es wird auch der Direktabruf durch ausländische Stellen zugelassen, ohne daß dafür ein dem deutschen Recht vergleichbarer Datenschutz bei den Empfängern Voraussetzung ist.

Eine so umfassende Erlaubnis zum Direktabruf ist nicht erforderlich und birgt unüberschaubare und unkontrollierbare Risiken für die Versicherten. Das Gesetz hätte den Kreis der Abrufberechtigten sowie Art und Umfang der abrufbaren Daten einschränken müssen. Denn es ist davon auszugehen, daß die Rentenversicherung sehr sensible Daten über das Einkommen sowie über familiäre und gesundheitliche Verhältnisse eines großen Teils der Bevölkerung erfaßt und die Betroffenen nur einen sehr begrenzten Einfluß auf die Erhebung und Verarbeitung ihrer Daten haben. Direktabrufe durch ausländische Stellen hätten deshalb in dieser Form nicht zugelassen werden dürfen.

Leider ist es nicht mehr gelungen, diese höchst problematische Regelung des Direktabrufs zu ändern. Der Landesbeauftragte wird weiter dafür eintreten, daß sie nachgebessert wird.

4.4.1.3 Erst Beratung, dann Entziehung des elterlichen Sorgerechts

Der Entwurf eines Gesetzes zur Neuordnung des Kinder- und Jugendhilferechts soll das aus dem Jahre 1922 stammende Jugendwohlfahrtsgesetz ablösen. Er enthält eine Reihe von Regelungslücken und bedeutet aus datenschutzrechtlicher Sicht keine Verbesserung.

Nach wie vor sollen Mitarbeiter der Kinder- und Jugendhilfe sowohl Aufgaben der Leistungsverwaltung (z. B. Beratungs-

tätigkeit) als auch Aufgaben der Eingriffsverwaltung (beispielsweise die vorläufige Unterbringung in einer Einrichtung) wahrnehmen können. Eine klare Abgrenzung dieser Tätigkeiten gegeneinander sieht der Gesetzentwurf nicht vor. Angemessener Datenschutz fordert aber, daß Erkenntnisse aus der Beratungstätigkeit nur zweckgebunden genutzt werden. Eltern, die freiwillig das Angebot zur Erziehungsberatung annehmen, dürfen nicht Gefahr laufen, daß die dabei gewonnenen Erkenntnisse z. B. für die Entziehung des Sorgerechts verwandt werden. Daß dies nicht bloße Theorie ist, hat sich in der Praxis bei Prüfungen des Landesbeauftragten in den vergangenen Jahren gezeigt (9. TB, S. 52). Er fordert daher ein gesetzliches Nutzungsverbot der Daten aus der Beratungstätigkeit für Aufgaben der Eingriffsverwaltung. Einen entsprechenden Formulierungsvorschlag hat er dem Sozialminister für die Bundesratsberatungen zugeleitet.

Darüber hinaus fehlen klare Regelungen zur Erhebung, Speicherung, Löschung, Auswertung und Weitergabe personenbezogener Daten. Hier ist ein eigener Abschnitt zum Datenschutz wie z. B. im Gesundheitsreformgesetz (Sozialgesetzbuch V) notwendig.

Auch sollte keine Unklarheit darüber bleiben, welche verfahrensrechtlichen Regelungen für Amtspfleger bzw. Amtsvormünder, private Vormünder und Pfleger gelten. Der Landesbeauftragte hat vorgeschlagen, einheitlich die Vorschriften des Verfahrensrechts aus dem Sozialgesetzbuch anzuwenden, damit alle Vormünder und Pfleger gleich effektiv und datenschutzgerecht arbeiten können.

Die Aktivitäten der Jugendgerichtshilfe müssen schließlich dem Sozialdatenschutz unterliegen, denn gerade die Daten der Jugendgerichtshilfe sind besonders sensibel und schützenswert. Der Landesbeauftragte hat hierfür eine Klarstellung gefordert.

Inzwischen liegt ein Bericht des Ausschusses für Jugend, Familie, Frauen und Gesundheit des Deutschen Bundestages zum Gesetzentwurf vor, der vorschlägt, den Datenschutz in einem eigenen Abschnitt des Gesetzes zu regeln. Dies könnte zu einer wesentlichen Verbesserung des Gesetzes führen. Insbesondere ist eine klarere Regelung der Zweckbindung vorgesehen. Dennoch entspricht auch dieser Vorschlag noch nicht allen datenschutzrechtlichen Anforderungen. Der Landesbeauftragte wird daher weiter auf eine Verbesserung des Jugendhilferechts hinwirken.

4.4.1.4 Dürfen Kommunalpolitiker Akten des Jugendamtes einsehen?

Die Ministerin für Bildung, Wissenschaft, Jugend und Kultur hat angefragt, wann Mitglieder kommunaler Vertretungskörperschaften in Akten des Jugendamtes Einsicht nehmen dürfen. Zuständig für Leistungen der Jugendhilfe sind in Schleswig-Holstein die Jugendämter bei den Kreisen und

kreisfreien Städten. Es sind Aufgaben der kommunalen Selbstverwaltung. Akten des Jugendamtes dürfen ausschließlich unter Beachtung der Vorschriften des Sozialgesetzbuches eingesehen werden. Dieses Gesetz bestimmt, daß personenbezogene Sozialdaten – und die Aufzeichnungen des Jugendamtes gehören dazu – offenbart werden dürfen, soweit dies für die Erfüllung der Aufgaben und damit auch für die gesetzlich vorgesehene Kontrolle durch die zuständigen Vertretungskörperschaften (Stadtvertretung oder Kreistag) erforderlich ist. Der Umfang der Kontrolle richtet sich nach der Gemeinde- und der Kreisordnung.

Der Landesbeauftragte hat darauf hingewiesen, daß Gemeinde- und Kreisordnung auch die Einsicht in Steuer- und Personalakten nicht für alle Mitglieder der Vertretungskörperschaften vorsehen, sondern auf die Mitglieder der zuständigen Ausschüsse beschränken. Er hat gegenüber dem Innenminister nachdrücklich angeregt, eine entsprechende Einschränkung auch für Informationen vorzusehen, die wie die Jugendamtsakten dem Sozialgeheimnis unterliegen. Dieser hat den Vorschlag aufgegriffen. Nach der Novellierung des Kommunalverfassungsrechts ist die Akteneinsicht nunmehr auf die Mitglieder des zuständigen Sozial- bzw. Jugendwohlfahrtsausschusses beschränkt.

4.4.1.5 Private Kleiderkammern auf dem Weg zur „Fürsorge" alter Zeiten?

Es widerspricht dem Geist des Sozialhilferechts und verstößt gegen den Sozialdatenschutz, wenn Bedürftige, bevor sie Sozialhilfe erhalten, zunächst unter Vorlage eines Berechtigungsscheins des Sozialamtes Hilfsangebote privater Organisationen in Anspruch nehmen müssen. Ein Schreiben eines Sozialamtes an einen Bedürftigen macht den Sachverhalt deutlich: „Bevor ich über Ihren Antrag entscheiden kann, fordere ich Sie hiermit auf, mit dem anliegenden Berechtigungsschein die Kleiderkammer des Deutschen Roten Kreuzes aufzusuchen und Ihren Bedarf, soweit möglich, dort abzudecken. Sollten wider Erwarten einige Kleidungsstücke dort nicht vorhanden sein, bitte ich Sie, unter Vorlage der Bestätigung des Deutschen Roten Kreuzes dieses nachzuweisen und erneut einzureichen."

Aus dieser Aufforderung ergibt sich, daß das Sozialamt Bekleidungsbeihilfe nur leistet, wenn ein freier Träger bescheinigt, die entsprechenden Kleidungsstücke könnten nicht aus einer Kleiderkammer zur Verfügung gestellt werden. Das erscheint bedenklich. Bürger, die eine Sozialleistung beantragen, müssen damit nämlich Bedürftigkeit und die Tatsache, daß sie Sozialhilfeempfänger sind, einer privaten Stelle gegenüber offenbaren.

Die Nachrangigkeit der Sozialhilfe darf aber nicht zu Lasten des Sozialdatenschutzes gehen. Die Sozialämter unterliegen nämlich einer strengen Geheimhaltungspflicht, soweit es um personenbezogene Sozialdaten der Antragsteller geht. Dazu

gehört auch die Information, daß Bürger Sozialleistungen erhalten oder beantragt haben. Die Bedürftigkeit und der Gang zum Sozialamt gelten vielfach noch immer als Makel. Eine Offenbarung von Sozialdaten ist daher mit wenigen Ausnahmen ohne Einwilligung der Betroffenen unzulässig, wenn sie nicht zur Aufgabenerfüllung der Sozialhilfestelle erforderlich ist. Dieses Verbot darf nun nicht dadurch unterlaufen werden, daß die Antragsteller selbst zur Auskunft gegenüber Dritten gezwungen werden.

Der Landesbeauftragte hält die Ausgabe von Berechtigungsscheinen, die zugleich der Rückmeldung an das Sozialamt dienen, nicht für erforderlich. Andere Hilfeformen und eine andere Organisationsform wären vorstellbar. Denkbar wäre z. B. eine Inanspruchnahme der Kleiderkammer, die einen Bezug zum Sozialamt nicht erkennen ließe. Unter Umständen könnte auf eine Kontrolle ganz verzichtet werden, wenn den Bedürftigen die Inanspruchnahme der Kleiderkammer als sinnvolle Alternative zur Bekleidungsbeihilfe überzeugend nahegebracht würde. Auch zeigt die Praxis in zahlreichen Sozialämtern, daß die angemessene Ausstattung mit Kleidung sehr wohl auf andere Weise sichergestellt werden kann. Eine Reihe von Bundesländern kennt solche privaten Kleiderkammern überhaupt nicht. In vielen Fällen erhalten die Antragsteller regelmäßig eine zweckgebundene, einmalige Barleistung oder ausnahmsweise einen Gutschein für die Anschaffung eines Kleidungsstückes.

In Schleswig-Holstein hingegen scheint das eingangs beschriebene Beispiel häufige Praxis zu sein. Das ist alarmierend, denn der gesetzliche Sozialhilfeanspruch würde so wieder zur „Fürsorge" früherer Zeiten. Der Landesbeauftragte hat dies kritisiert und erwartet, daß die Sozialhilfeträger ihre Praxis ändern.

4.4.1.6 Erhebung von Sozialdaten hinter dem Rücken der Betroffenen ist unzulässig

Ein Bürger hat sich darüber beschwert, daß das Sozialamt hinter seinem Rücken den Arbeitgeber nach seinem Einkommen gefragt hat. Seine volljährige Tochter bezieht Sozialhilfe. Als Unterhaltsberechtigter sollte er dem Sozialamt gegenüber Angaben über seine wirtschaftliche Situation machen. Der Vater übersandte daraufhin eine Gehaltsabrechnung. Seine Angaben genügten dem Sozialamt offensichtlich nicht. Es wandte sich, ohne den Bürger selbst um weitere Angaben zu bitten, direkt an den Arbeitgeber und erbat detaillierte Angaben.

Das Bundessozialhilfegesetz verpflichtet den Arbeitgeber, dem Sozialamt über die Art und Dauer der Beschäftigung, die Arbeitsstätte und den Arbeitsverdienst des Unterhaltspflichtigen Auskunft zu geben, soweit die Durchführung des Gesetzes dies erfordert. Der Landesbeauftragte hat gegenüber dem Sozialamt deutlich gemacht, daß er in dem konkreten Fall die Einschaltung des Arbeitgebers nicht für erforder-

lich hielt. Das Sozialamt hätte vielmehr den Betroffenen, der ja durchaus auskunftswillig war, um ergänzende Angaben bitten müssen. Erst wenn der Unterhaltspflichtige selbst die erforderlichen Angaben nicht gemacht hätte oder sich konkrete Anhaltspunkte für falsche Angaben ergeben hätten, hätte es erforderlich sein können, den Arbeitgeber unmittelbar zu befragen.

Das Sozialamt hat sich für sein Verhalten ausdrücklich bei dem betroffenen Bürger entschuldigt.

4.4.2 Gesundheit

4.4.2.1 Prüfung im Klinikum der Christian-Albrechts-Universität zu Kiel

Der Landesbeauftragte hat seine Prüfung in weiteren Abteilungen des Klinikums der Christian-Albrechts-Universität fortgesetzt. Er fand auch hier die „gewohnten" Schwachstellen (vgl. 11. TB, S. 60). Beispielsweise existierten keine schriftlichen Hinweise zum Datenschutz in Dienstanweisungen, Aktenordnungen oder anderen Organisationsregelungen. Die nach dem Landesdatenschutzgesetz vorgeschriebene Datenübersicht wurde nicht geführt und erst im Rahmen einer Gesamtübersicht für das Klinikum erstellt. Erst auf Intervention des Landesbeauftragten wurden die Mitarbeiter angewiesen, für die Verarbeitung personenbezogener Patientendaten künftig private Personal-Computer nicht mehr zu benutzen. Der Landesbeauftragte empfahl auch anläßlich dieser Prüfung, die Einwilligung der Patienten einzuholen, wenn Arztbriefe oder Abschlußberichte den Hausärzten oder nachbehandelnden Ärzten übersandt werden sollen, und in der Praxis kritisch zu überprüfen, wann Auskünfte an Angehörige erteilt werden dürfen.

Daneben gab es aber auch neue Probleme und Regelungen, die in anderen Bereichen nicht angetroffen wurden.

Datenweitergaben an das Tumorzentrum

Daten über Tumorpatienten werden dem zum Klinikum der Christian-Albrechts-Universität gehörenden Tumorzentrum zugänglich gemacht. Auf den Formularen „Ersterhebung für die Nachsorge" und „Nachuntersuchung" werden umfangreiche Daten zur Person einschließlich Beruf und Staatsangehörigkeit sowie detaillierte medizinische Daten weitergegeben. Eine Einwilligung der Patienten hierzu wird nicht eingeholt. Diese Offenbarung von Patientendaten wird auf den Behandlungsvertrag gestützt und die Tätigkeit des Tumorzentrums als Mitbehandlung gewertet.

Die Datenweitergaben an das Tumorzentrum sind nur zulässig, soweit sie tatsächlich der Mit- und Nachbehandlung der Patienten dienen. Allerdings hat der Landesbeauftragte festgestellt, daß den Mitarbeiterinnen des Tumorzentrums von

der Archivleiterin jeweils die gesamte Krankengeschichte zum Heraussuchen der erforderlichen Patientendaten und zum Ausfüllen der Meldungen zur Verfügung gestellt wird. Damit erhalten diese mehr Daten als erforderlich. Der Landesbeauftragte hat das als Verstoß gegen die ärztliche Schweigepflicht beanstandet.

Weitergabe von Daten an Doktoranden

Auch in den geprüften Bereichen hatten Doktoranden mit Genehmigung des zuständigen Oberarztes Zugriff auf Patientendaten. Eine Rechtsgrundlage hierfür besteht nicht. Jede Weitergabe von Patientendaten an Doktoranden bedarf daher der ausdrücklichen Einwilligung der Patienten (vgl. 11. TB, S. 63). Der Landesbeauftragte hat die leitenden Ärzte über die Rechtslage unterrichtet. Die Abteilung hat daraufhin einen Zusatz in das Formular „Einverständniserklärung (Einwilligung in diverse Eingriffe)" aufgenommen, in welchem sich die Patienten damit einverstanden erklären können, daß ihre Krankenunterlagen durch Doktoranden für Forschung und Lehre personenbezogen ausgewertet werden dürfen.

Der Landesbeauftragte begrüßt, daß hier ohne Zögern nach einer datenschutzgerechten Lösung gesucht wurde. Der vorgelegte Erklärungstext genügt jedoch datenschutzrechtlichen Anforderungen noch nicht. Eine wirksame Einwilligung setzt nämlich voraus, daß die Patienten den zugrundeliegenden Sachverhalt kennen. Deshalb müssen sie über die vorgesehene Datennutzung jedenfalls soweit informiert werden, daß sie den Umfang des Zugriffes auf ihre Krankheitsdaten absehen und sich ein Bild von der Art ihrer Verwendung machen können. Ideal wäre es, würde jeweils die Einwilligung der Patienten für ein konkret bezeichnetes Forschungsvorhaben eingeholt. Will sich die Klinik jedoch die Möglichkeit offenhalten, Patientendaten auch künftig für wissenschaftliche Zwecke zu nutzen, so muß sie den Patienten darlegen, mit welchen Informationsflüssen sie in diesem Fall zu rechnen haben.

Der Landesbeauftragte hat erneut darauf hingewiesen, daß im Bereich der medizinischen Forschung und Lehre geprüft werden sollte, ob die Möglichkeiten, Datenbestände zu anonymisieren, tatsächlich ausgeschöpft worden sind. Da ein Personenbezug für das jeweilige Forschungsthema in der Regel nicht erforderlich ist, dürfte die Anonymisierung in den meisten Fällen die datenschutzgerechte Lösung darstellen. Daten ohne Personenbezug stehen der Wissenschaft selbstverständlich zur freien Verfügung.

„Vier-Augen-Prinzip" – für den Computer am Krankenbett

Im Klinikum werden oft sehr umfangreiche Rechnersysteme zur dateimäßigen Verarbeitung von Patientendaten einge-

setzt. Der Landesbeauftragte hat bei seiner Prüfung festgestellt, daß in den geprüften Bereichen weitgehend Experten mit „ihren" Systemen arbeiten, teilweise auch Programme selbst schreiben und verändern, ohne daß Vorgesetzte oder andere Mitarbeiter in der Lage sind, dies wirksam zu kontrollieren. Die einzige „Kontrolle" besteht in der Annahme und dem Vertrauen darauf, daß der zuständige Kollege schon sorgfältig und gewissenhaft damit umgehen wird. Das genügt aus datenschutzrechtlicher Sicht nicht. Gerade bei derartig sensiblen Daten ist das Vier-Augen-Prinzip unverzichtbar. Zumindest ein weiterer Mitarbeiter muß in der Lage sein, die Verfahren einzusetzen und damit auch Kontrollfunktionen wahrzunehmen.

Therapievergleiche

Ziel sog. multizentrischer Therapiestudien (Randomisation), die jeweils von mehreren Universitäten gemeinsam betrieben werden, ist es, im Versuch herauszufinden, welche von verschiedenen als gleichwertig angesehenen Therapien in der Praxis erfolgreicher ist. Hierzu werden Einzelfälle an die jeweils federführende Universität gemeldet. Dem Landesbeauftragten wurde erläutert, daß die erste Meldung an die federführende Universität telefonisch und ohne Personenbezug erfolgt. Der gemeldete Fall erhält eine Code-Nummer, und spätere Meldungen erfolgen dann jeweils nur noch unter dieser Nummer. Die Übermittlung ausreichend anonymisierter Patientendaten zur Auswertung im Rahmen multizentrischer Studien ist datenschutzrechtlich nicht zu beanstanden. Dem Landesbeauftragten ist allerdings bekannt, daß nicht in allen Bereichen stets so sorgfältig verfahren wird.

Auskünfte aus dem Archiv

Auskünfte aus dem Krankenarchiv auch des zuletzt geprüften Bereichs dürfen nicht ohne Entscheidung eines Arztes von den dafür nicht autorisierten Archivkräften routinemäßig erteilt werden. Während bei den Prüfungen der ersten beiden Klinikabteilungen festgestellt wurde, daß dies ohne Wissen der zuständigen Ärzte doch geschah, gab es hierfür in dem nunmehr geprüften Archiv keinerlei Anhaltspunkte.

Allerdings mußte auch hier darauf hingewiesen werden, daß – abgesehen von gesetzlichen Verpflichtungen – Grundlage für Mitteilungen aus dem Archiv die Einwilligung der Patienten ist. Vor solchen Auskünften muß daher den Mitarbeitern grundsätzlich eine Einwilligungserklärung der Patienten vorgelegt werden. Dies geschah auch in dem zuletzt untersuchten Bereich nicht immer. Der Landesbeauftragte hat insoweit eine Änderung des Verfahrens gefordert.

4.4.2.2 Mit der Praxisaufgabe wechselt auch die Patientendatei

Spektakulären Presseberichten konnte der Landesbeauftragte entnehmen, daß Ärzte mit Patientendateien einen „lukrativen

Handel" betreiben. Auch die Datenschutzaufsichtsbehörde hat ihn darüber unterrichtet, daß Zahnärzte bei Praxisaufgaben ihre Patientendateien Kollegen ohne Einwilligung und auch ohne Information der betroffenen Patienten zur Verfügung stellten. Patientenunterlagen einer Petentin waren nicht etwa dem unmittelbaren Praxisnachfolger übergeben worden, sondern einem ihr völlig fremden Zahnarzt, dessen Praxis in großer räumlicher Entfernung lag. Sie fühlte sich in ihren schutzwürdigen Belangen beeinträchtigt, obwohl ihr Zahnarzt sie in einem Rundbrief von der Übergabe der ärztlichen Unterlagen unterrichtet hatte.

Diese Beschwerden bestärken den Landesbeauftragten in seiner bereits früher erhobenen Forderung (vgl. 8. TB, S. 52), diesen Fragenkreis detailliert in der Ärzlichen Berufsordnung zu regeln. Patientendaten unterliegen als hochsensible Gesundheitsdaten der ärztlichen Schweigepflicht. Für ihre Weitergabe bedarf es einer konkreten Befugnis des behandelnden Arztes, üblicherweise der Einwilligung der Patienten. Dies gilt auch dann, wenn der behandelnde Arzt die Informationen an einen Kollegen weitergibt.

Die Zahnärztekammer hat dem Landesbeauftragten mitgeteilt, sie werde bei der Überprüfung von Praxisübernahmeverträgen, die ihr stets vorgelegt werden, künftig darauf hinweisen, daß den Patienten eine Widerspruchsmöglichkeit gegen die Übergabe ihrer Karteikarten eingeräumt werden muß. Die Ärztekammer erwägt, die Berufsordnung dahin gehend zu ändern, daß die Patienten bei Praxisaufgabe durch eine Anzeige über die beabsichtigte Übergabe der Patientenunterlagen informiert und auf eine Widerspruchsmöglichkeit hingewiesen werden.

Der Landesbeauftragte sieht hierin erste Ansätze zu einer Verbesserung des Patientendatenschutzes. Damit kann es jedoch nicht sein Bewenden haben. Er hält es nach wie vor für erforderlich, daß die Regelung der genannten Fälle in den Berufsordnungen beider Kammern erfolgt und daß auf das Einverständnis der Patienten abgestellt wird.

4.4.2.3 „Freiwillig oder mit Gewalt?" – Offenbarung medizinischer Daten

Wenn Behörden die Bürger nach personenbezogenen Daten befragen, dann müssen sie klar und deutlich sagen, ob eine gesetzliche Auskunftspflicht besteht oder ob die Offenbarung persönlicher Daten in das Belieben der Bürger gestellt ist. In seinem 11. Tätigkeitsbericht (S. 48) hat der Landesbeauftragte einer Staatsanwaltschaft insoweit den „Spiegel vorgehalten" und kritisiert, daß sie einen Arzt nicht ausführlich genug über die Rechtslage informiert hatte, als sie ihn um die Herausgabe medizinischer Daten über den verstorbenen Ministerpräsidenten Dr. Barschel für Zwecke des Todesermittlungsverfahrens „bat".

Das gleiche Problem, wobei allerdings die agierenden Behörden und die betroffenen Personen andere waren, ist aufgetre-

ten, als Asylsuchende auf Aids getestet wurden. Unter der Überschrift „Aids-Tests bei Asylsuchenden – nur ein bißchen freiwillig?" hatte der Landesbeauftragte im 11. Tätigkeitsbericht (S. 47) das als „freiwillig routinemäßig" bezeichnete Verfahren kritisiert. Anlaß hierfür war der Fall einer unter dieser flotten aber unklaren Devise untersuchten Asylbewerberin. Man hatte sie nämlich nicht darüber aufgeklärt, ob sie sich dem mit weitreichenden Konsequenzen verbundenen Test freiwillig stellte oder ob sie ihm aufgrund einer gesetzlichen Vorschrift zwangsweise unterzogen wurde. Sie konnte zu dieser Frage auch nicht mehr Stellung nehmen. Sie war nämlich untergetaucht, nachdem ihr ein positives Testergebnis bekanntgegeben worden war. Später stellte sich allerdings heraus, daß sie dazu gar keinen Anlaß hatte, denn ein Kontrolltest ergab, daß sie gar nicht infiziert war.

Während sich der Generalstaatsanwalt immer noch schwer tut, Konsequenzen aus dem vom Landesbeauftragten kritisierten Vorgehen der Staatsanwaltschaft in der Todesermittlungssache zu ziehen, hat inzwischen der Minister für Soziales, Gesundheit und Energie für seinen Bereich Änderungen veranlaßt. Ein in der Frage der Rechtsgrundlagen nur Verwirrung stiftender Erlaß wurde zurückgezogen. Den Asylbewerbern wird künftig anläßlich der allgemeinen ärztlichen Untersuchung im Aufnahmelager nach vorheriger Information über alle denkbaren Konsequenzen auch ein HIV-Test auf freiwilliger Grundlage angeboten. Die Betroffenen werden ausdrücklich um eine schriftliche Einverständniserklärung gebeten. Daneben sollen die Asylbewerber auch auf die Möglichkeit hingewiesen werden, daß sie sich bei den Aids-Beratungsstellen anonym testen lassen können.

Der Landesbeauftragte begrüßt diese Entwicklung.

4.4.2.4 Mikroverfilmung im Auftrag verletzt das Patientengeheimnis

Viele Krankenhäuser leiden an akuter Raumnot. Ihre Archive quellen über. Was liegt näher, als die alten Krankengeschichten auf Mikrofilm festzuhalten. Häufig wendet man sich an eine Privatfirma. Hierin liegt nach Auffassung des schleswig-holsteinischen Landesbeauftragten eine unzulässige Durchbrechung des Patientengeheimnisses, wenn die betroffenen Patienten nicht zugestimmt haben (vgl. 8. TB, S. 54).

Andere Länder regeln dies ausdrücklich so in ihren Krankenhausgesetzen und lassen nur eine Mikroverfilmung im Krankenhaus selbst zu. Der Bayerische Verfassungsgerichtshof hat mit einem Beschluß vom 06.04.1989 in der entsprechenden Regelung des Bayerischen Krankenhausgesetzes eine sachgerechte Erwägung des Gesetzgebers gesehen, den Kreis der mit medizinischen Daten befaßten Personen möglichst begrenzt zu halten und das Patientengeheimnis zu schützen. Er vermochte darin keinen unzulässigen Eingriff in die Freiheit der wirtschaftlichen Betätigung des Mikrofilmunternehmens zu erblicken. Die wirtschaftliche Handlungsfreiheit und

die Berufswahl seien nicht betroffen. Die Regelung im Einzelfall müsse mit Rücksicht auf die besondere Schutzbedürftigkeit von Krankendaten hingenommen werden.

Der Landesbeauftragte sieht sich durch diese Entscheidung in seiner Rechtsauffassung bestätigt. Er hat die Krankenhäuser im Lande darauf hingewiesen.

4.4.3 Genetische Informationen sind hochsensible Daten

„Kunst und Wissenschaft, Forschung und Lehre sind frei". Nach vierzig Jahren Grundgesetz ist diese lapidare Aussage des Art. 5 Abs. 3 als eine Selbstverständlichkeit anzusehen. Aber auch dieses Grundrecht hat Grenzen. Sie liegen dort, wo andere Grundrechte zu achten sind, so das allgemeine Persönlichkeitsrecht, das informationelle Selbstbestimmungsrecht der Mitbürger. In die Persönlichkeitsphäre anderer dürfen auch Wissenschaftler nur mit deren Einwilligung eindringen, und Forschungsergebnisse dürfen nicht schrankenlos verwendet werden.

Biologische Forschung an menschlichen Erbanlagen berührt den innersten Kern der Persönlichkeit. Deshalb darf nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder eine Entschlüsselung der Erbinformationen des einzelnen (Genomanalyse) nicht ohne Einschränkungen erfolgen. Sie darf

- grundsätzlich nur vorgenommen und ihre Ergebnisse weiterverwandt werden, soweit die Betroffenen eingewilligt haben;
- auch dann nur zu ganz bestimmten vorher festgelegten Zwecken erfolgen. Zusätzliche Erkenntnisse über die Persönlichkeit der Betroffenen sind zu vermeiden;
- ohne Einwilligung der Betroffenen nur im überwiegenden Interesse der Allgemeinheit durchgeführt werden; dazu sind normenklare gesetzliche Regelungen, etwa für Straf- und Abstammungsverfahren, Voraussetzung (vgl. hierzu Tz. 4.3.2);
- im Arbeitsverhältnis grundsätzlich nicht angewandt werden; Ausnahmen müssen gesetzlich geregelt sein; wegen der Zwangssituation der Arbeiter reicht ihre Einwilligung nicht;
- im Versicherungswesen nicht eingeführt werden; das Versicherungsvertragsgesetz sollte ausdrücklich klarstellen, daß Genomanalysen mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschliessen, unvereinbar und deshalb nicht erforderlich sind;
- das Recht auf informationelle Selbstbestimmung Dritter, zu dem auch das Recht auf Nichtwissen gehört, nicht verletzen.

Die Konferenz betrachtet ihre Entschließung als Beitrag für den Dialog mit den Vertretern der Wissenschaft. Wegen der

Aktualität der Fragen und der auch von anderer Seite angeregten gesetzgeberischen Maßnahmen hat der Landesbeauftragte die Vorsitzenden der Fraktionen des Schleswig-Holsteinischen Landtages und die zuständigen Ministerinnen und Minister gebeten, die Überlegungen der Datenschutzbeauftragten im Rahmen ihrer Aktivitäten zu berücksichtigen und ihre Forderungen aufzunehmen.

4.5 Kultusbereich

4.5.1 Hochschulen
Keine „Fahndung" nach BAföG-Empfängern

Der Landesbeauftragte hat erreicht, daß die Christian-Albrechts-Universität künftig darauf verzichtet, jeden mit einer wissenschaftlichen Hilfskraft abgeschlossenen Anstellungsvertrag in Kopie dem Amt für Ausbildungsförderung zuzuleiten, unabhängig von der Frage, ob die betroffene Person Empfänger von Leistungen nach dem Bundesausbildungsförderungsgesetz (BAföG) ist oder nicht. Dem war die Beschwerde eines Betroffenen vorausgegangen, der auf diese Praxis aufmerksam machte. Das Gesetz sieht zwar eine Auskunftsverpflichtung des Arbeitgebers gegenüber dem Amt für Ausbildungsförderung vor. Das bedeutet jedoch nicht, daß die Universität aus Vereinfachungsgründen in jedem Falle auf Verdacht die entsprechenden Daten übermittelt. Zunächst ist der Antragsteller selbst um die erforderlichen Angaben und Nachweise zu bitten.

Der Landesbeauftragte begrüßt, daß die Ministerin für Bildung, Wissenschaft, Jugend und Kultur diese Auffassung teilt und veranlaßt hat, daß die bisherige Verfahrensweise eingestellt wird.

4.5.2 Schulen

4.5.2.1 Schulgesetznovelle

Der Landesbeauftragte hatte bereits in einem frühen Stadium Gelegenheit, seine Vorstellungen in das Gesetzgebungsverfahren einzubringen, so daß für ihn die Möglichkeit bestand, einen Beitrag zur Verbesserung der Datenschutzbestimmungen im Schulgesetz zu leisten. Er hat vor allem erreicht, daß

- das Schulgesetz nunmehr einen abschließenden Katalog der zulässigen Schülerdaten enthält,
- die Übermittlung von Schülerdaten an Private nur mit Einwilligung der Betroffenen zulässig ist,
- auch die Weitergabe von Daten der Bildungsberatungsstellen vom Willen der Betroffenen bzw. der Erziehungsberechtigten abhängt,
- die Benutzung privater Datenverarbeitungsgeräte für die Verarbeitung personenbezogener schulischer Daten für unzulässig erklärt wurde.

Weitere Verbesserungen wären möglich gewesen. Die Verarbeitung von medizinischen Daten im schulärztlichen und schulpsychologischen Dienst sowie die Abgrenzung der Zuständigkeiten zwischen der Schule und den Gesundheitsämtern ist z. Z. nicht eindeutig geregelt. Eine konkretere Regelung für die Verarbeitung dieser Daten erscheint deshalb notwendig, weil sie im Hinblick auf die ärztliche Schweigepflicht einen höheren Schutz genießen als „normale" Schülerdaten.

Nicht voll erfüllt wurde die Forderung nach detaillierteren Regelungen zur automatisierten Datenverarbeitung von Schüler-, Eltern- und Lehrerdaten im Gesetz. Es enthält lediglich eine Ermächtigung, die vorsieht, daß der Einsatz der automatisierten Datenverarbeitung durch Verordnung geregelt wird, soweit er zur Erfüllung des Unterrichts- und Erziehungsauftrages der Schule erforderlich ist.

Es ist begrüßenswert, daß eine ursprünglich vorgesehene Vorschrift entfallen ist, die es ermöglicht hätte, Mitschüler und Lehrkräfte über Erkrankungen von Schülern zu unterrichten. Der Landesbeauftragte betrachtete diese Vorschrift als „Aids-Vorschrift" und wies darauf hin, daß die gesetzlichen Möglichkeiten schon heute ausreichen, in Fällen einer Gesundheitsgefährdung durch eine HIV-Infektion von ärztlicher bzw. amtsärztlicher Seite die notwendigen Maßnahmen zu veranlassen. Dazu könnte im Ausnahmefall auch einmal die Unterrichtung der Mitschüler durch den Arzt gehören. Es wäre deshalb höchst problematisch gewesen, eine spezielle gesetzliche Regelung für HIV-Infektionen zu schaffen, zumal es doch in der Vergangenheit bereits – im Gegensatz zur HIV-Infektion – Fälle hochinfektiöser Erkrankungen wie Hepatitis B gegeben hat, die offensichtlich keine unüberwindbaren Probleme beim Schutz der Mitschüler aufwarfen.

4.5.2.2 Runderlaß „Datenschutz in Schulen"

Als Übergangsregelung und zur Einübung in die nach dem Schulgesetz vorgesehenen Datenschutzregelungen hat die Ministerin für Bildung, Wissenschaft, Jugend und Kultur zunächst einen an alle Schulen gerichteten Runderlaß herausgegeben, an dessen Konzeption der Landesbeauftragte mitgearbeitet hat. Er enthält konkrete Handlungsanweisungen für die Schulleiter und Lehrkräfte, z. B. präzise Regelungen zum Einsatz von Datenverarbeitungsgeräten. Er sieht vor, daß zur Verarbeitung von Schulverwaltungsdaten nur schuleigene, in den Schulen stehende Datenverarbeitungsgeräte eingesetzt werden dürfen und daß die Verwendung derselben Geräte im Unterricht ausgeschlossen sein muß. Damit wird der Forderung nach der Abschottung zwischen Schulverwaltungs- und Unterrichtsbereich Rechnung getragen. Der Erlaß sieht weiter vor, die Programmentwicklung, Freigabe, Organisation und Verantwortlichkeit der automatisierten Datenverarbeitung sowie deren Kontrolle durch Dienstanweisung zu regeln, wie es der Landesbeauftragte empfohlen hatte.

Nach dem Runderlaß müssen die Schulen beim Einsatz von Datenverarbeitungsgeräten folgende Sicherungsmaßnahmen beachten:

- Der Zugang zu den Datenverarbeitungsgeräten ist mechanisch zu sichern.
- Das Betriebssystem ist vor mißbräuchlicher und unberechtigter Benutzung zu schützen.
- Datenträger und Ausdrucke sind verschlossen aufzubewahren.
- Alle Datenträger sind in Übersichten nachzuweisen und regelmäßig zu kontrollieren.
- Daten und Programme sind regelmäßig zu sichern und an anderer Stelle gesichert auszulagern.
- Kopien auf einer Festplatte sind nach Gebrauch zu löschen.
- Zugriff und Benutzung von Programmen und Daten sind durch Identifizierungs- und Authentifizierungsprozeduren abzusichern.
- Über alle Zugriffe auf personenbezogene Daten ist eine lückenlose Dokumentation zu führen (Log-Journal) und regelmäßig zu kontrollieren.
- Es sollten mindestens zwei Personen mit den Datenverarbeitungsgeräten vertraut sein (4-Augen-Prinzip).

4.5.2.3 Eltern sollen sich zu einer Gesamtschule äußern

Eine Stadt schrieb Bürger in der Nachbargemeinde an und forderte sie auf, auf Fragebögen mitzuteilen, ob sie ihr Kind in einer künftigen Gesamtschule anmelden würden. Die Nachbargemeinde hatte der Stadt Namen und Anschriften der vom Alter ihrer Kinder her in Frage kommenden Eltern übermittelt. Datenquelle war die örtliche Grund- und Hauptschule. Die Eltern erblickten in dem Verfahren einen Datenschutzverstoß. Sie hatten Recht.

Zwar ist es nach dem Schulgesetz Aufgabe des Schulträgers, Schulgebäude und -anlagen zu planen und zu bauen. Eine Rechtsgrundlage für personenbezogene Datenerhebungen und Datenübermittlungen liegt in dieser Aufgabenzuweisung jedoch nicht. Der Landesbeauftragte hat daher die Auskunft der Grund- und Hauptschule, die Datenerhebung durch die Gemeinde sowie die Datenübermittlung an die Stadt beanstandet. Er hat außerdem den ihm zugeleiteten Fragebogen geprüft. Dort fehlte ein ausdrücklicher Hinweis darauf, daß die betroffenen Eltern die freie Wahl hätten, die Fragen zu beantworten. Damit war die Möglichkeit nicht von der Hand zu weisen, daß die Bürger den Eindruck hatten, zur Antwort verpflichtet zu sein. Auch die Gestaltung des Fragebogens mußte daher gerügt werden. Zugleich hat der Landesbeauftragte die Stadt aufgefordert, die unzulässigerweise erhaltenen Elterndaten zu löschen.

Die Stadt hat dem Landesbeauftragten die Löschung gemeldet. Darüber hinaus hat die Ministerin für Bildung, Wissenschaft, Jugend und Kultur inzwischen empfohlen, in vergleichbaren Fällen künftig den Bedarf und den Elternwunsch nach einer Gesamtschule auf andere Weise zu ermitteln. So könnten etwa die Schulen des künftigen Einzugsbereiches entsprechende Fragebögen an die Eltern zur freiwilligen Beantwortung weiterleiten, oder interessierte Eltern könnten über Anzeigen in der Lokalpresse um Meldung gebeten werden. Der Landesbeauftragte hält Befragungen, die von vornherein auf der Grundlage der Freiwilligkeit durchgeführt werden, für datenschutzgerecht und geht davon aus, daß künftig landesweit so verfahren wird.

4.5.2.4 Probleme mit gemeinsamer Kindergarten- und Schülerdatei

Auch im Berichtsjahr erreichten den Landesbeauftragten wieder Beschwerden wegen der umfangreichen Datenerhebungen bei schulärztlichen Untersuchungen. Er mußte dabei immer wieder feststellen, daß die Schulärzte unverändert alte Fragebögen mit einem zu umfangreichen Datenkatalog verwenden. Nunmehr wurde bekannt, daß ein Kreisgesundheitsamt freiwillige Vorsorgeuntersuchungen im Kindergarten anbietet, dann aber die gewonnenen Erkenntnisse mit den später anfallenden Daten aus schulärztlichen Untersuchungen verknüpft. Dieses Vorgehen ist von den betroffenen Eltern zu Recht kritisiert worden.

Die Vorsorgeuntersuchungen im Kindergarten sind in Schleswig-Holstein nur mit dem vorherigen Einverständnis der Eltern zulässig. Aber auch wenn sie das Einverständnis gegeben haben, erlaubt das nicht, die Ergebnisse der Vorsorgeuntersuchungen im Kindergarten mit denen der schulärztlichen Untersuchungen zu verknüpfen.

Der Landesbeauftragte hat dem Gesundheitsamt seine Rechtsauffassung mitgeteilt und geht davon aus, daß künftig entsprechend verfahren wird.

4.5.3 Die Forschung und ihre datenschutzrechtlichen Schranken

Auch im Berichtsjahr wurde der Landesbeauftagte häufig um datenschutzrechtliche Beurteilungen gebeten, wenn wissenschaftliche Institutionen oder einzelne Forscher personenbezogene Daten einer öffentlichen Stelle nutzen wollten, die ursprünglich für andere Zwecke erhoben wurden. Die Nutzung solcher Daten ist in Schleswig-Holstein – von wenigen Spezialregelungen abgesehen – nur mit Einwilligung der Betroffenen oder in ausreichend anonymisierter Form zulässig.

So erschien es unzulässig, daß Prüfungsämter des Landes frühere Anschriften von Absolventen pädagogischer Prüfungen für Zwecke einer bundesweiten Untersuchung herausga-

ben, die sich mit dem weiteren beruflichen Werdegang von Pädagogen beschäftigte.

Die alten Anschriften durften für wissenschaftliche Zwecke allenfalls herausgegeben werden, wenn es unerläßlich gewesen wäre. Davon konnte man hier nicht ausgehen, denn den Prüfungsämtern war zuzumuten, von sich aus Kontakt mit den ehemaligen Prüflingen aufzunehmen und auf eine Beteiligung an dem geplanten Forschungsvorhaben hinzuwirken. Die bloße bürotechnische Vereinfachung, in der von den Forschern ins Auge gefaßten Art, rechtfertigte die Datenübermittlung jedenfalls nicht.

Noch restriktiver sind die personenbezogenen Daten zu behandeln, die nicht nur gesperrt sind, sondern darüber hinaus noch besonderen Geheimhaltungsvorschriften unterliegen. Das ist durchweg bei medizinischen Daten der Fall. So mußte der Landesbeauftragte, bei allem Verständnis für das Anliegen der Forschung, vor einer unzulässigen Datennutzung warnen, als Wissenschaftler Einsicht in die Krankenakten ehemaliger jüdischer Patienten eines Landeskrankenhauses erbaten, um deren Behandlung und Schicksal während des „Dritten Reiches" zu untersuchen.

Diese Unterlagen unterfallen der ärztlichen Schweigepflicht. Es bedarf schon einer konkreten Befugnisnorm, wenn diese Akten der Wissenschaft zugänglich gemacht werden sollen. Eine gesetzliche Befugnis zur Offenbarung der Patientendaten war in diesem Fall nicht zu erkennen. Da andererseits die Einwilligung der Betroffenen nicht mehr eingeholt werden kann, die ärztliche Schweigepflicht aber über den Tod hinaus wirkt, gab es keine Möglichkeit, den Forschern entgegenzukommen. Die ärztliche Schweigepflicht hat Gesetzesrang. Sie verpflichtet den Arzt, Daten für Forschungszwecke ohne Einwilligung der Patienten nur in anonymisierter Form Dritten zugänglich zu machen.

Das sollte bei einem weiteren Vorhaben geschehen, bei dem eine Hochschule des Landes in Zusammenarbeit mit einem Institut für Humangenetik ein Forschungsprojekt zur Gen-Diagnose an Ungeborenen in Familien mit Erbkrankheiten durchführt. Von der beteiligten Klinik erfuhr der Landesbeauftragte, daß man dort die Beteiligung an dem Forschungsprojekt als Weitergabe anonymisierter Patientendaten betrachtete. Er hat daraufhin die Erhebungsbögen für das Forschungsprojekt überprüft und stellte fest, daß die Angaben nicht ausreichend anonymisiert waren, obwohl Name und Anschrift der betroffenen Patienten fehlten. Der Fragebogen enthielt nämlich u. a. das vollständige Geburtsdatum sowie die Angabe des Berufs in einem durch die Postleitzahl eingegrenzten kleinräumigen Erhebungsbereich. Dies kann in Einzelfällen durchaus zur Wiederherstellung des Personenbezuges führen. Die Hochschule hat auf Verlangen des Landesbeauftragten auf die Angabe des Berufs verzichtet und gibt nur noch das Geburtsjahr an.

5. Medien

Das Landesrundfunkgesetz verbessert den Datenschutz

Heftige Diskussionen löste die Änderung des Landesrundfunkgesetzes aus, die im Juli 1989 dem Landtag zur ersten Lesung vorlag. Sie berührten den Landesbeauftragten allerdings nicht, denn der Datenschutz wurde verbessert. Das Gesetz ergänzt die bestehenden datenschutzrechtlichen Vorschriften, die auf frühere Anregungen des Landesbeauftragten zurückgehen, und schafft darüber hinaus zusätzliche Sicherheiten für den Umgang mit personenbezogenen Daten. Nach wie vor dürfen also personenbezogene Daten nur für die Vermittlung von Programmen und zur Abrechnung erhoben und gespeichert werden. Anschließend sind sie zu löschen. Ihre Weitergabe ist grundsätzlich unzulässig. Nutzungsgewohnheiten oder gar ein „Benutzerprofil" dürfen aus den Teilnehmerdaten nicht erschließbar sein.

Zusätzlich sind Regelungen eingeführt worden, die den Rundfunkveranstalter eindeutig als Verantwortlichen für die Sicherung der publizistischen Daten bestimmen und die datenverarbeitungstechnische Behandlung medienrechtlicher Gegendarstellungen, Unterlassungserklärungen und Widerrufe festlegen. Aufgenommen wurde auch die Verpflichtung, durch technische und organisatorische Maßnahmen sicherzustellen, daß nicht mehr benötigte Daten rechtzeitig gelöscht werden. Verschlüsselungen zur Datensicherung müssen auf dem neuesten Stand der Technik gehalten werden, und es muß gewährleistet sein, daß unbeabsichtigte Datenübermittlungen vermieden werden. Aus datenschutzrechtlicher Sicht sind diese Ergänzungen zu begrüßen. Sie waren aufgrund der technischen Entwicklung und vergleichbarer Regelungen im Staatsvertrag zum Bildschirmtext allerdings auch notwendig geworden.

6. Ordnungsmäßigkeit der Datenverarbeitung

6.1 Endlich eine TÜV-Plakette für Computer-Software?

Praktisch alle Wirtschaftsgüter des täglichen Bedarfs, deren Gebrauch für den Benutzer mit Risiken verbunden sein kann, werden von unabhängigen Prüfinstitutionen daraufhin getestet, ob der Produzent seiner Pflicht zur sorgfältigen Konstruktion und zur Warnung vor unsachgemäßer Handhabung nachgekommen ist. In einigen Bereichen sind daneben auch die Benutzer gehalten, in regelmäßigen Abständen die Zuverlässigkeit und Sicherheit ihrer Geräte kontrollieren zu lassen. Geprüfte und für gut befundene Produkte erhalten ein Testat, das sich in einem entsprechenden Aufkleber dokumentiert. Allgemein bekannt ist die TÜV-Plakette auf den Kraftfahrzeugkennzeichen, auf Druckbehältern, auf Heizungsanlagen, Kindersitzen usw. Bei Elektrogeräten, Haushaltsgeräten, Kosmetikartikeln und vielen anderen Dingen gibt es spezielle Zertifikate. Es gilt der Grundsatz, daß das Vertrauen in die

Werbung und die Produktbeschreibung des Herstellers zwar gut, die Kontrolle seiner Versprechungen aber besser ist.

Der große Bereich der Computertechnologie und insbesondere der Computer-Software bildete bis jetzt eine Ausnahme, obwohl die Risiken und das Sicherheitsbedürfnis der Benutzer hier als ebenso groß einzuschätzen sind, wie z. B. bei Haushaltsgeräten oder Ölheizungen. Aus nicht recht nachvollziehbaren Gründen meinte man jedoch, den wortreichen Produktbeschreibungen im EDV-Bereich Glauben schenken zu können. Wenn die großen Computerhersteller erklärten: „Unser Betriebssystem arbeitet fehlerfrei" oder „Dieses Datennetz ist gegen unbefugte Zugriffe geschützt", dann wurde das nicht nur als eine Behauptung, sondern als eine unumstößliche Tatsache gewertet.

Diese auch für viele Anwender so bequeme Fiktion haben einige junge Computer-Freaks in den letzten Jahren gehörig ins Wanken, teilweise gar zum Einstürzen gebracht. In „schamloser", nicht immer legaler Weise haben sie dem EDV-Establishment deutlich gemacht, auf welch tönernen Füßen viele Sicherheitssysteme stehen. Es würde den Rahmen dieses Berichtes sprengen, wollte man auch nur die gravierensten Fälle der letzten Jahre darstellen. Die Tageszeitungen berichten ohnehin in immer kürzeren Abständen über die Erfolge der Hacker, Spione und Betrüger. Faktum ist, daß nach Angaben des Bundeskriminalamtes die Zahl der Computerbetrügereien innerhalb eines Jahres von 2787 auf 3875 anstieg. 1988 wurden nahezu 300 Delikte registriert, bei denen Daten ausgespäht, Dateien verfälscht oder Sabotage an Computersystemen begangen wurden. Dabei sind diese Zahlen nur die Spitze eines Eisbergs. Das Bundeskriminalamt gibt zu: „Die Dunkelziffer ist gewaltig."

Mit einer gewissen Befriedigung stellt der Landesbeauftragte fest, daß Wirtschaft, Verwaltung und Wissenschaft vor diesem Hintergrund – endlich – einen Gedanken aufgreifen, den er bereits vor zehn Jahren (vgl. 3. TB, S. 47) zur Diskussion gestellt hat: Das Sicherheitstestat für Computer-Hard- und -Software.

Ein erster Schritt in diese Richtung sind die vom Bundesinnenminister in Zusammenarbeit mit dem Bundeswirtschaftsminister herausgegebenen „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik". Als einheitliche „Meßlatte" zur Beurteilung von EDV-Systemen wurden sie unter Beteiligung von Wirtschaft und Wissenschaft erarbeitet. Sie sind eine Fortentwicklung des in Fachkreisen bekannten „Orange Book" des amerikanischen Verteidigungsministeriums (Trusted Computer System Evaluation Criteria) und stehen allen Stellen, die sich mit Fragen der Sicherheit informationstechnischer Anwendungen befassen, zur Verfügung. Verantwortlich für diese Kriterien und ihre Fortschreibung zeichnet die beim Bundesinnenminister neu eingerichtete „Zentralstelle für Sicherheit in der Informationstechnik – ZSI –", die zudem beauftragt ist, selbst derartige

Systeme auf Sicherheit zu prüfen und zu bewerten. Sie kann aber auch andere Stellen autorisieren, bestimmte Prüfungen durchzuführen. Produkte, die die Prüfungen erfolgreich durchlaufen haben, sollen ein Sicherheitszertifikat erhalten. Es ist sogar geplant, der Zentralstelle eine gesetzliche Grundlage zu geben und sie zu einem eigenständigen Bundesamt auszubauen. Mehrere hundert Spezialisten sollen sich dort ganz gezielt mit dem Problem der Verschlüsselungstechniken und den Möglichkeiten der Entschlüsselung durch Unbefugte sowie mit Fragen der allgemeinen Datensicherheit befassen. Es scheint jedoch nicht ganz einfach, die Interessenlage der Sicherheitsbehörden und die der sonstigen Datenverarbeiter „unter einen Hut zu bringen".

Der Landesbeauftragte begrüßt und unterstützt diese Entwicklung im Grundsatz nachdrücklich. Seinen Prüfungsbeamten hat er Weisung erteilt, in die Checklisten für künftige Sicherheitsüberprüfungen folgende Frage aufzunehmen: „Setzen Sie Betriebssysteme und Programme ein, die ein Sicherheitstestat haben? Wenn nein, warum nicht?". Auf diese Weise soll erreicht werden, daß bei den Behörden im Lande der Einsatz geprüfter EDV-Produkte zur Regel wird und nicht die Ausnahme bleibt.

6.2 Auch die Anwender erkennen PC-Risiken

Bisher waren es eigentlich nur die Datenschutzbeauftragten (vgl. 11. TB, S. 67) und die Verkäufer von Sicherheits-Software, die vor den Risiken beim Einsatz von Personal-Computern gewarnt haben. Die Computerhersteller und -verkäufer hielten sich ebenso „bedeckt" wie die vielen Anwender. Statt Sicherheitskonzepte zu entwickeln und öffentlich zu diskutieren, wurden immer neue Geräte angeschafft. Man kann davon ausgehen, daß derzeit bei den Behörden im Lande bereits mehr als 2 000 Kleincomputer im Einsatz sind.

Positiv ist deshalb zu bewerten, daß nunmehr auch die Datenzentrale Schleswig-Holstein die Initiative ergriffen hat und ihren Kunden eine Orientierungshilfe zum Thema „Datenschutz und Datensicherung beim Einsatz von Arbeitsplatzrechnern" an die Hand gibt (die Datenzentrale hat nach eigenen Angaben bei ihren Kunden über 600 PC installiert). In der Broschüre wird deutlich, daß sich endlich auch die Datenverarbeitungspraktiker mit dieser spezifischen Problematik auseinandersetzen müssen. Folgenden Ausführungen der Datenzentrale kommt nach Auffassung des Landesbeauftragten eine besondere Bedeutung zu:

- Aufgrund der weiten Verbreitung der Arbeitsplatzrechner kann sich heute jedermann anhand von allgemein zugänglicher Literatur detaillierte Kenntnisse über das Betriebssystem und seine Arbeitsweise aneignen. Daten auf der Magnetplatte eines ungeschützten Arbeitsplatzrechners können daher von Unbefugten auch ohne Kenntnisse über

das Anwendungsprogramm, das die Daten geschrieben hat, sichtbar gemacht, kopiert oder gelöscht werden.

- Darüber hinaus gibt es sogenannte Dienstprogramme zu kaufen, mit denen jedes Zeichen auf der Platte/Diskette gelesen und verändert werden kann. Derartige Programme sind sogar in der Lage, gelöschte Daten wieder lesbar zu machen, weil in der Regel beim Löschen die betroffenen Plattenbereiche nicht überschrieben, sondern nur als frei gekennzeichnet werden.
- Wichtiger als das Vorhandensein derartiger Programme zu kontrollieren, ist es, die Verarbeitungsergebnisse stichprobenartig zu überprüfen. Der Vorgesetzte muß – wie bei konventioneller Vorgangsbearbeitung auch – die Verarbeitungsschritte nachvollziehen. Es reicht nicht, das Anwendungsprogramm zu überprüfen, freizugeben und gelegentlich mit dem Original zu vergleichen. Wenn jemand Verarbeitungsergebnisse verfälschen möchte, wird er nicht das Anwenderprogramm manipulieren, sondern die von dem Programm geschriebenen Dateien, weil dies viel leichter zu bewerkstelligen ist.
- Wegen der geringen Abmessungen von Gerät und Datenträger sind diese für Diebstähle besonders anfällig. Sogar Festplatten können in wenigen Minuten ausgebaut werden.
- Daneben besteht auch die Gefahr, daß PC-Benutzer selbst sensible Daten entwenden. Werden Daten auf wechselbaren Datenträgern gesichert, kann man diese in fremde Systeme wieder einspielen. Will man dieser Gefahr begegnen, muß man das Diskettenlaufwerk des Arbeitsplatzrechners für die Benutzer außer Betrieb setzen.
- Computerviren gelangen in der Regel über Anwenderprogramme in die Systeme. Es sollten daher grundsätzlich nur Anwenderprogramme renommierter Software-Häuser und Distributoren (sie erstellen die für den Verkauf bestimmten Kopien) zum Einsatz kommen. Insbesondere sollten Computerspiele nicht auf dienstlich genutzten PC installiert werden. Da von Computerspielen eine besondere Faszination ausgeht und sie die menschliche Neugier wecken, reicht es nicht, ein schriftliches Verbot auszusprechen. Die Mitarbeiter müssen vielmehr über die Virengefahr aufgeklärt werden.

Wohlgemerkt, die vorstehenden Warnungen und Ratschläge entspringen nicht dem vermeintlich überzogenen Sicherheitsdenken eines Datenschutzbeauftragten, sondern sind das Ergebnis der Erfahrungen und Gefährdungsanalysen des größten EDV-Anwenders der öffentlichen Verwaltung im Lande. Der Landesbeauftragte fühlt sich durch sie in seiner Ansicht bestärkt, daß Verwaltungsverfahren und hier insbesondere solche, in denen Daten verarbeitet werden, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (Steuer-, Sozial-, Gesundheitsdaten, Daten der Sicherheitsbehörden), nur unter ganz besonders wirksamen Schutzvorkehrungen auf Personal-Computern ablaufen dürfen.

Auch der Innenminister hat sich im Rahmen des von ihm erarbeiteten Landeskonzeptes „Informations- und Kommunikationstechniken – IKOTECH –" mit der datenschutzrechtlichen Problematik der dort eingesetzten Arbeitsplatzrechner befaßt. Er glaubt, daß das erforderliche Maß an Datensicherheit u. a. durch folgende Maßnahmen zu erreichen ist:

- Der Zugriff auf die Rechner ist nur nach Eingabe individueller Paßworte möglich.
- Die Benutzer haben keine Zugriffe auf das Betriebssystem.
- Der Zugriff auf Programme wird durch ein „Menü" gesteuert. Ein Abweichen vom „Pfad" der zugelassenen Anwendungen soll damit unterbunden werden.
- Die Arbeitsplatzrechner haben keine Diskettenstationen. Die Kopie und die Entnahme von Dateien und Programmen soll dadurch unmöglich gemacht werden.
- Zugriffe aus öffentlichen Netzen auf IKOTECH-Komponenten sind nicht möglich.
- Sicherungskopien der Dateien werden programmgesteuert vom Zentralrechner erstellt und dort verschlüsselt gespeichert.
- Neue bzw. fortgeschriebene Verarbeitungsprogramme werden direkt vom Zentralrechner auf die Terminals überspielt.
- Jedes Ressort verwaltet seine Dateien selbst. Auf die jeweiligen Datenbestände kann von anderen Ressorts nur zugegriffen werden, wenn und soweit dies ausdrücklich vereinbart ist.

Der Landesbeauftragte wird sich von der Wirksamkeit dieser Konzeption nach Abschluß des Pilotprojektes und Aufnahme des „Echtbetriebes" mit umfangreicheren personenbezogenen Datenbeständen im Rahmen einer Prüfung überzeugen.

6.3 Überprüfung der Datenzentrale beginnt mit einer Beanstandung

Es ist ungewöhnlich, daß die datenschutzrechtliche Überprüfung eines Rechenzentrums mit einer förmlichen Beanstandung beginnt, normalerweise wird ein solches Verdikt – wenn überhaupt – erst nach Abschluß einer Prüfung ausgesprochen. Im Falle der Datenzentrale Schleswig-Holstein erforderte es die unter Tz. 4.2.3.1 beschriebene unzulässige Übermittlung von gesperrten Einwohnermeldedaten an Adreßbuchverlage jedoch, diesen exemplarischen Sachverhalt vorab zu untersuchen und datenschutzrechtlich zu bewerten.

Folgendes war geschehen: Im Jahre 1978 erhielt die Datenzentrale von einer Gemeinde den Auftrag, aus deren Einwohnermeldedatenbestand bestimmte Datensätze auszuwählen.

Die Gemeinde gab das erstellte Magnetband an ein Unternehmen weiter, das anhand der Daten ein Adreßbuch erstellte. Da es sich damals um eine einmalige Sonderauswertung handelte, wurde zur Prüfung der Richtigkeit der Auswahl kein Testdatenbestand generiert, ein Programmierer der Datenzentrale begnügte sich mit einem visuellen Vergleich mit den Echtdaten. Da später auch weitere Gemeinden derartige Auswertungen bestellten, wurde das Programm im Verlaufe von fünf Jahren siebenundzwanzigmal genutzt. Auch die Änderungen durch das neue Melderecht wurden zwischenzeitlich eingearbeitet. Stets meinte man, auf systematische Tests verzichten zu können, da sich bisher keine Gemeinde über eine fehlerhafte Verarbeitung beschwert hatte.

Als ein vorsichtiger Kunde eine Kontrolliste über die nicht in den Auswahlbestand zu übernehmenden gesperrten Daten verlangte, beging man sogar eine „Sünde", die jedem EDV-Chef Alpträume bereitet. Es wurde nicht das bestehende Programm durch den Einbau einer „Entweder-oder-Schaltung" (entweder Kontrolliste oder Adreßbuchbestand) ergänzt, sondern es wurde der Einfachheit halber die Kontrolliste mit einem zweiten Programm, das ursprünglich für ganz andere Zwecke entwickelt worden war, erzeugt. Auf diese Weise blieb auch jetzt noch ein kapitaler Programmfehler unentdeckt, der vom Beginn an dazu geführt hat, daß auch Datensätze, die wegen einer Gefahr für Leib und Leben des betreffenden Bürgers von einer Übermittlung ausdrücklich ausgeschlossen waren, an die Adreßbuchverlage weitergegeben wurden. Das Auswahlprogramm war falsch, das vermeintliche Kontrollprogramm arbeitete richtig, verschleierte aber gerade deshalb den Fehler. Der Kunde der Datenzentrale wurde getäuscht und Bürger massiv in ihren schutzwürdigen Belangen beeinträchtigt.

Passierte dieser „Unfall", weil Programmierer schlampig gearbeitet haben? Dies mag auf den ersten Blick naheliegen. Die wirkliche Ursache liegt jedoch tiefer und ist darin zu sehen, daß niemand ihre Arbeit wirklich systematisch kontrolliert hat. Die Gemeinden als Auftraggeber der Datenzentrale sahen sich dazu nicht in der Lage. Ein Bürgermeister formulierte dies dem Landesbeauftragten gegenüber wie folgt: „Im übrigen teile ich Ihnen mit, daß die Gemeinde als Auftraggeberin keine Möglichkeit besitzt, ähnliche Vorfälle zu verhindern. Sie hat keinen Einfluß auf die Programme und den Arbeitsablauf. Maßnahmen zur Verhinderung ähnlicher Fehler können daher nur von der Datenzentrale vorgenommen werden." Die Datenzentrale berief sich dagegen unter Hinweis auf die Verträge mit den Gemeinden und ihre Benutzungsordnung darauf, daß die Kunden die rechtliche Verantwortung für die Datenübermittlung durch die nicht beanstandete Abnahme des Magnetbandes übernommen hätten. Im übrigen habe die Automationskommission der kommunalen Landesverbände die Freigabe für das Programm erteilt (getestet hat sie die Programme allerdings nicht, das war allen Beteiligten bekannt).

Der Landesbeauftragte hat sich dieser Argumentation, die eindeutig zu Lasten der betroffenen Bürger geht, nicht anschließen können. Ihm stellen sich folgende Fragen:

- Sollen die Bürger Folgen fehlerhafter Computerprogramme etwa als Schicksalsschläge klaglos hinnehmen?
- Ist das der Preis den wir dafür zahlen, daß die Verwaltung mit Computern wirtschaftlicher arbeitet?
- Kann man den Bürgern Nachteile zumuten, nur weil Behörden aus Kostengründen Teile ihrer Aufgaben durch Dienstleistungsrechenzentren erledigen lassen?

Die Antwort hierauf muß ein klares „Nein" sein und deshalb hat er sowohl das Verhalten der Kommunen als auch das der Datenzentrale beanstandet. Bezüglich der Beanstandung gegenüber den Kommunen wird auf Tz. 4.2.3.1 verwiesen. Der Datenzentrale hat der Landesbeauftragte vorgehalten, daß sie entgegen ihrer Verpflichtungen aus dem Landesdatenschutzgesetz

- nicht ausschließlich nach den Weisungen der Auftraggeber gearbeitet,
- keine hinreichend wirksamen technischen und organisatorischen Maßnahmen zur Auftragskontrolle ergriffen und
- die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme nicht genau genug überwacht hat.

Wegen der Tragweite und der grundsätzlichen Bedeutung der erkennbar gewordenen datenschutzrechtlichen Probleme hat er zudem den Innenminister als Fachaufsichtsbehörde für das Meldewesen von dieser Beanstandung in Kenntnis gesetzt.

Die Datenzentrale hat daraufhin entsprechend den Vorschlägen des Landesbeauftragten folgende Sofortmaßnahmen ergriffen:

- Alle Programme (nicht nur diejenigen aus dem Bereich Einwohnerwesen), mit deren Hilfe personenbezogene Daten an Behörden oder Unternehmen übermittelt werden, sind dahin gehend untersucht worden, ob die Vorgaben der Auftraggeber bezüglich der Auswahlkriterien und des Umfanges der zu übermittelnden Daten hinreichend konkret sind und exakt eingehalten werden.
- Das DZ-interne Verfahren zum Test der Richtigkeit der Programme ist entscheidend verbessert worden.
- Es werden künftig spezielle Testdatenbestände benutzt.
- Die Testverfahren werden dokumentiert.
- Die Programmierung und die Tests der Programme werden nicht mehr von dem gleichen Mitarbeiter durchgeführt.
- Die Leistungsbeschreibungen der Datenzentrale sind den tatsächlichen Gegebenheiten angepaßt worden.
- Bei Aufträgen über Einzelauswertungen werden die Auftraggeber darauf hingewiesen, daß sie die Richtigkeit des

Produktionsergebnisses mit besonderer Aufmerksamkeit selbst zu überprüfen haben.

- Das Verfahren zur Erstellung von Adreßbuchdatenbeständen selbst ist grundlegend geändert worden.

Mit diesen Maßnahmen ist allerdings das Grundproblem des wirksamen Tests und der Freigabe von automatisierten Verfahren im kommunalen Bereich durch Fachleute der Auftraggeber (nicht durch Programmierer der Datenzentrale), auf das der Landesbeauftragte bereits seit Jahren nachdrücklich hinweist (vgl. zuletzt 10. TB, S. 58), nicht gelöst. Weder die Datenzentrale, noch der Innenminister als oberste Kommunalaufsichtsbehörde, noch die Arbeitsgemeinschaft der kommunalen Landesverbände sahen sich aufgrund der durch diesen Vorgang deutlich zutage getretenen Unzulänglichkeiten veranlaßt, die Forderung des Landesbeauftragten nach einer unabhängigen und kompetenten Test- und Freigabeinstitution aufzugreifen.

Im weiteren Verlauf der Prüfung der Datenzentrale wird sich der Landesbeauftragte deshalb insbesondere mit der Frage befassen, wie genau sie es mit der Regelung in ihrer eigenen Satzung nimmt, nach der die automatisierten Verfahren „von der zuständigen Fachverwaltung des Landes oder von der durch die kommunalen Landesverbände für zuständig erklärten Stelle freigegeben werden". Über die wirksame Umsetzung dieser Verpflichtung in die Praxis hofft er in seinem nächsten Tätigkeitsbericht berichten zu können. Ein Vorfall der vorstehend geschilderten Art darf sich jedenfalls nicht wiederholen!

7. Datenschutz auf internationaler Ebene

Der europäische Einigungsprozeß und die auch in anderen Bereichen zunehmende internationale Verflechtung verstärken den Datenfluß über die Grenzen. In diesem Bericht finden sich Ausführungen zu zwei Beispielen dieser Art, nämlich dem Schengener Informationssystem (Tz. 4.1.3.3.) und der Europäischen Statistik (Tz. 4.1.4.3).

Die internationale Konferenz der Datenschutzbeauftragten im August 1989 in Berlin, an der der Landesbeauftragte teilgenommen hat, hatte sich den grenzüberschreitenden Datenverkehr zum Schwerpunkt gemacht. Die Ergebnisse der Konferenz wurden in einer „Berliner Resolution" zusammengefaßt, in der ein wirksamer internationaler Datenschutz gefordert wird. Dem Datenschutz müsse, so heißt es darin, die gleiche Priorität wie der Förderung der Datenverarbeitung und der Telekommunikation zukommen. Den Regierungen wird deshalb u.a. empfohlen, einzeln und im Rahmen internationaler Organisationen gleichwertige gesetzliche Sicherungen zu schaffen. Die Betroffenen müssen Gelegenheit haben, ihre Rechte auch gegenüber international operierenden Datenverarbeitungssystemen wahrzunehmen.

Die Datenschutzbeauftragten der EG-Länder haben in einer Zusatzerklärung auf die besonderen Probleme im Zusammenhang mit der Verwirklichung des EG-Binnenmarktes 1992 hingewiesen. Die Europäische Gemeinschaft und ihre Mitgliedstaaten wurden aufgefordert, in ihre Planungen für „Europa 92" die Notwendigkeit eines umfassenden und konsistenten Datenschutzes einzubeziehen. Die Europaratskonvention 108 solle für die Institutionen der EG wie auch für alle Mitgliedstaaten verbindlich gemacht werden. Außerdem müsse eine unabhängige Datenschutzkontrollinstanz auf EG-Ebene eingerichtet werden.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Kiel hat sich mit den Fragen des internationalen Datenschutzes befaßt und einen eigenen Arbeitskreis zu dieser Thematik eingerichtet. Der Landesbeauftragte beabsichtigt darüber hinaus, seine Kontakte zur benachbarten dänischen Datenschutzkontrollinstitution zu verstärken.