13. Wahlperiode

Drucksache **13/1756**

HESSISCHER LANDTAG

04. 03. 92

Zwanzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 1991
nach § 30 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 4. März 1992 · Ausgegeben am 5. Mai 1992

Herstellung: Johannes Weisbecker, 6000 Frankfurt am Main · Auslieferung: Kanzlei des Hessischen Landtags · Postf. 3240 · 6200 Wiesbaden 1

INHALTSVERZEICHNIS

KKD 13/1756

56

KERNPUNKTE DES 20. TÄTIGKEITSBERICHTS

1. Nach dem Gemeinsamen Erlaß von Innen- und Justizministerium vom 18./20. Juni 1991 darf die Polizei Abhörprotokolle grundsätzlich nur noch mit Zustimmung der ermittelnden Staatsanwaltschaft weitergeben. Der Datenaustausch zwischen diesen Behörden in Strafverfahren muß aber über diesen Fall hinaus generell präziser geregelt werden (Ziff. 2).
2. Betrifft eine Landtagsanfrage personenbezogene Sachverhalte, muß die Landesregierung bei ihrer Antwort mangels gesetzlicher Regelung im Einzelfall zwischen dem Informationsanspruch des Parlaments und dem Persönlichkeitsrecht des Betroffenen abwägen. Eine pauschale Auskunftsverweigerung unter Berufung auf das Recht auf informationelle Selbstbestimmung ist nicht gerechtfertigt (Ziff. 3).
3. Das Frankfurter Ordnungsamt registrierte rechtswidrig Personen, die bei Kontrollen im Sperrgebiet über die Sperrgebietsordnung "belehrt" worden waren (Ziff. 4).
4. Das am 1. Januar 1991 in Kraft getretene Gesetz zur Neuregelung des Ausländerrechts hat gravierende datenschutzrechtliche Mängel. Der vom Bundesinnenministerium vorgelegte Entwurf für konkretisierende Verwaltungsvorschriften bringt zwar Verbesserungen, ist aber noch keineswegs zufriedenstellend (Ziff. 5.1).
5. Eine Ausländerbehörde wollte unzulässigerweise bei allen psychiatrischen Krankenhäusern ihres Zuständigkeitsbereichs Daten über sämtliche ausländischen Patienten erheben (Ziff. 5.2).
6. Für die mit mehr als 10 Mio. Datensätzen größte Datensammlung über Ausländer, das Ausländerzentralregister beim Bundesverwaltungsamt in Köln, gibt es noch immer keine ausreichende Rechtsgrundlage. Das Arbeitspapier des Bundesinnenministeriums vom 15. Juli 1991 zu einem Entwurf für ein Ausländerzentralregistergesetz muß aus der Sicht des Datenschutzes in vielen Punkten überarbeitet werden (Ziff. 5.3).
7. Das neue Kinder- und Jugendhilferecht hat vielfältige datenschutzrechtliche Konsequenzen auch für kommunale Erziehungsberatungsstellen (Ziff. 6.3).
8. Eine Prüfung des in der Stadt- und Universitätsbibliothek Frankfurt/Main installierten Hessischen Bibliotheksinformationssystems HEBIS-Leih hat ergeben, daß sich mit dem dortigen automatisierten Ausleihverfahren keine Leserprofile erstellen lassen (Ziff. 8.2).
9. Der Einsatz von Telefaxgeräten zur Übermittlung von Patientendaten an ein Krankenhaus ist nur akzeptabel, wenn durch eine Reihe organisatorischer und technischer Maßnahmen sichergestellt wird, daß Unbefugte keinen Zugang zu den Daten haben (Ziff. 9.1).
10. Bei der Patientenaufnahme in Krankenhäusern wird oft in mehrfacher Hinsicht gegen das Datenschutzrecht verstoßen. Überprüfungen in mehreren Krankenhäusern haben gezeigt, daß zum Teil Daten erhoben werden, die für die Durchführung des Behandlungsvertrags nicht erforderlich sind, die Patienten nicht darüber informiert werden, welche Angaben freiwillig sind, und auch die übrigen gesetzlichen Informationspflichten nicht eingehalten werden (Ziff. 9.2).
11. Für die Datenverarbeitung der Finanzverwaltung fehlen nach wie vor die notwendigen bereichsspezifischen gesetzlichen Regelungen. Der Entwurf zur Novellierung der Abgabenordnung, den das Bundesfinanzministerium am 25. November 1991 vorgelegt hat, enthält trotz der im Vergleich zu früheren Entwürfen deutlichen Verbesserungen immer noch einige Mängel (Ziff. 10).
12. Angesichts der mit der Fernwartung verbundenen besonderen Gefahren für die Datensicherheit muß in jedem Einzelfall geprüft werden, ob es problemlosere adäquate Maßnahmen gibt (Ziff. 15.1).
13. Bei der ersten Prüfung eines Kommunalen Gebietsrechenzentrums wurden deutliche Datensicherheitsmängel festgestellt (Ziff. 15.2).
14. Der neue Rundfunkstaatsvertrag hat den Datenschutz der Rundfunkteilnehmer erheblich verbessert. Zu den wichtigsten Regelungen zählt das Verbot, aus Abrechnungsdaten privater Veranstalter Teilnehmerprofile zu erstellen (Ziff. 13).

KKD 13/1756

S. 8

1. Vorwort

Am 22. Oktober 1991 hat Spiros Simitis seine langjährige Tätigkeit als der Hessische Datenschutzbeauftragte beendet, und der Hessische Landtag hat mich zu seinem Nachfolger gewählt. Der Präsident des Hessischen Landtags, Karl Starzacher, hat die Amtsführung von Spiros Simitis vor dem Landtag gewürdigt.

Dieser Tätigkeitsbericht druckt die Reden ab, die zu diesem Anlaß gehalten worden sind (17.3 bis 17.5). Ich brauche ihnen nichts hinzuzufügen: Der Landtagspräsident faßt die großen Verdienste zusammen, die der scheidende Datenschutzbeauftragte sich erworben hat; Simitis zieht Bilanz, und ich benenne Absichten und Schwerpunkte.

Der Wechsel im Amt wird, so hoffe ich fest, das hohe Niveau des Datenschutzes in Hessen nicht mindern. Ich werde die Arbeit von Spiros Simitis in derselben Richtung fortsetzen. Dies belegt, so denke ich, schon dieser Tätigkeitsbericht, der die Kontinuität der Amtsführung erkennen läßt.

W.H.

2. Verwendung von Abhörprotokollen

2.1
Ausgangspunkt

Im 19. Tätigkeitsbericht sind zwei Berichte an den Hessischen Landtag abgedruckt, in denen ich auf datenschutzrechtliche Fragen im Zusammenhang mit der Weitergabe personenbezogener Daten aus einer Telefonüberwachung nach §§ 100a, 100b StPO von der Polizei über das Innenministerium an den früheren Minister Milde persönlich sowie die Offenlegung dieser Informationen im Landtag eingegangen bin. (19. Tätigkeitsbericht, Ziff. 1.6, 17.2.1 und 17.2.3).

Aufgrund der Berichte setzte der Landtag einen Untersuchungsausschuß ein (UNA 12/4), der sich sowohl mit dem konkreten Ablauf der Datenweitergaben als auch mit einer rechtlichen Bewertung befassen sollte. Im Mittelpunkt der Tätigkeit dieses Ausschusses standen die Fragen, wer im einzelnen von den Erkenntnissen aus der Telefonüberwachung erfahren hatte und auf welchen Wegen diese Informationen weitergeleitet worden waren. Der Ausschuß schloß nach zehn Sitzungen am 21. März 1991 ohne schriftlichen Bericht seine Tätigkeit ab.

2.2
Konsequenzen

Zwei unmittelbare Konsequenzen ergaben sich aus der Tätigkeit des Hauptausschusses und des Untersuchungsausschusses des Hessischen Landtags.

2.2.1
Gemeinsamer Erlaß: Zustimmungsvorbehalt der Staatsanwaltschaft

Zum einen einigten sich das Justizministerium und das Ministerium des Innern und für Europaangelegenheiten auf einen Gemeinsamen Erlaß, der die Verwendung von Daten regelt, die zur Durchführung eines Ermittlungsverfahrens aufgrund von Eingriffen in das Fernmeldegeheimnis (Art. 10 GG, §§ 100a, 100b StPO) erlangt werden. Demnach dürfen die Polizeibehörden solche Daten grundsätzlich nur mit Zustimmung der ermittelnden Staatsanwaltschaft weitergeben. Bei Weigerung der Staatsanwaltschaft entscheidet der Generalstaatsanwalt nach Anhörung des Direktors des Landeskriminalamtes über die Weitergabe. Sollte die ermittelnde Staatsanwaltschaft nicht erreichbar sein, dürfen die Polizeibehörden in Fällen, "in denen die unverzügliche Datenweitergabe zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit für erforderlich gehalten wird, bei Gefahr im Verzug Daten auch ohne Zustimmung übermitteln. Die Genehmigung der Staatsanwaltschaft ist unverzüglich einzuholen" (Staatsanzeiger 28/1991 S. 1662).

2.2.2
Interministerielle Arbeitsgruppe

2.2.2.1
Zwischenstand

Auf Anregung des früheren Justizministers Koch wurde eine Arbeitsgruppe gebildet, die sich aus Vertretern der beiden erwähnten Ministerien und meiner Dienststelle zusammensetzt und die erforderlichen Konsequenzen für die Bereiche Polizei, Staatsanwaltschaft und Ministerialverwaltung beraten soll.

Das Justizministerium hat im November einen ersten Bericht dieser Arbeitsgruppe "Datenweitergabe aus Strafverfahren" vorgelegt und dem Innenministerium sowie mir übersandt. In einem Gutachten, das diesem Bericht beigefügt ist, werden neben einer Reihe weiterer Fallkonstellationen auch die Einschaltung der Polizei durch die Staatsanwaltschaft zu Ermittlungszwecken und die dazu notwendigen Datenflüsse behandelt.

Zu diesem zentralen Fragenkomplex erzielte die Arbeitsgruppe allerdings keinen Konsens. Während ich die rechtlichen Bewertungen des Gutachtens in allen wesentlichen Punkten teile, hat das Innenministerium grundlegende Bedenken geäußert. Dies gilt insbesondere für die von mir unterstützte Absicht der Justizministerin, die Fälle, in denen zu Ermittlungszwecken personenbezogene Daten weitergegeben werden dürfen, durch einen förmlichen Erlaß zu präzisieren.

Generell neigt das Innenministerium der Ansicht zu, man könne es bei dem o.a. "Gemeinsamen Erlaß" im wesentlichen bewenden lassen. Demgegenüber ist das Ministerium der Justiz der Auffassung, der in Ermittlungsverfahren stattfindende Austausch personenbezogener Daten zwischen den beteiligten Polizeidienststellen und der Staatsanwaltschaft sowie die Mitteilungen bei der Strafverfolgung erlangter Kenntnisse an dritte öffentliche oder private Stellen müsse umfassend analysiert werden.

2.2.2.2
Umfassender Arbeitsauftrag

Ich teile die Auffassung des Ministeriums der Justiz. Nur ein umfassender Arbeitsansatz wird dem Auftrag gerecht, wie ihn der damalige Justizminister Koch gegenüber Medien und Öffentlichkeit formuliert hat, nämlich "den verfassungsrechtlich zulässigen Umfang von in Ermittlungsverfahren gewonnenen Daten abzugrenzen und Vorschläge für die normative Absicherung vorzulegen" (Presseerklärung des Justizministeriums vom 4. Februar 1991).

Hinzu kommt ein weiterer Gesichtspunkt: Derzeit behandelt der Deutsche Bundestag den Gesetzentwurf des Bundesrates zur Bekämpfung der Organisierten Kriminalität (Bundestags-Drucks. 12/989 vom 25. Juli 1991). Es muß befürchtet werden, daß mit diesem speziellen Gesetz lediglich eine Teilnovellierung der Strafprozeßordnung und damit des "Grundgesetzes" für die Ermittlungstätigkeit von Staatsanwaltschaft und Polizei zustande kommt. Die allgemeine Neufassung der Strafprozeßordnung mit dem Ziel einer umfassenden Festlegung der datenschutzrechtlichen Verarbeitungsbefugnisse könnte dadurch ins Hintertreffen geraten.

Offene Fragen gibt es auch weiterhin vor allem zur Zulässigkeit von Mitteilungen im Rahmen der Dienst- und Fachaufsicht. Der oft zitierte § 13 Abs. 4 HDSG ("Personenbezogene Daten, die für andere Zwecke erhoben worden sind, dürfen auch zur Ausübung von Aufsichts- und Kontrollbefugnissen ... in dem dafür erforderlichen Umfang verwendet werden.") löst die bisher aufgetretenen Probleme nicht eindeutig. Insbesondere die Verwendung von Daten, die einem besonderen Amts- oder Berufsgeheimnis unterliegen oder aus anderen Gründen als besonders sensibel einzustufen sind, bedarf der Klärung. Schon ein Vergleich der Häufigkeit von Berichten nachgeordneter Dienststellen an das Ministerium der Justiz einerseits und an das Ministerium des Innern andererseits weist deutliche Unterschiede auf. Während im Justizbereich lediglich in Ausnahmefällen "nach oben" berichtet wird, beanspruchen die aufsichtsführenden Dienststellen der Polizei eine möglichst umfassende Kenntnis der Informationen, die nachgeordnete Dienststellen erhoben oder ermittelt haben.

Ich erwarte daher, daß die Arbeitsgruppe intensiv und zügig ihre Beratungen weiterführt und das Innenministerium seine Mitarbeit fortsetzt. Auch sollte den zuständigen Ausschüssen des Landtags so bald wie möglich ein Zwischenbericht einschließlich einer Präsentation der weiteren Arbeitsschritte vorgelegt werden.

3. Auskunftsrecht des Parlaments bei personenbezogenen Sachverhalten

3.1
Informationsverweigerung der Landesregierung bei parlamentarischen Anfragen

In der Vergangenheit hat es wiederholt Probleme gegeben, wenn die Landesregierung bei der Beantwortung von Kleinen Anfragen der Abgeordneten Einzelangaben über bestimmte Personen mitteilen sollte. Für diesen Konflikt zwischen dem Informationsanspruch des Parlaments und dem Persönlichkeitsrecht der Betroffenen gab es im Berichtsjahr erneut mehrere Beispiele.

Exemplarisch war die Antwort der Landesregierung auf zwei Anfragen, in denen es um die Einbürgerung einer Landtagskandidatin kurz vor der Wahl ging (Drucks. 12/7608 und 12/7856). Das Hessische Innenministerium teilte den Abgeordneten mit:

"Einbürgerungsbewerber haben – wie die Beteiligten an allen Verwaltungsverfahren – einen Anspruch auf Geheimhaltung ihrer personenbezogenen Daten. Die Landesregierung hält es daher nicht für zulässig, Einzelheiten aus einem Einbürgerungsverfahren ohne das Einverständnis der Betroffenen zu veröffentlichen. Das Grundrecht auf informationelle Selbstbestimmung geht dem geschäftsordnungsmäßigen Auskunftsrecht eines einzelnen Abgeordneten zumindest dann vor, wenn die Frage auf eine öffentliche Beantwortung zielt."

Mit Schreiben vom 25. Februar 1991 habe ich daraufhin den Hessischen Innenminister gebeten, mir seine Rechtsauffassung näher zu erläutern und insbesondere darzulegen, aus welchen Gründen und unter welchen Voraussetzungen das Recht auf informationelle Selbstbestimmung der Beantwortung einer parlamentarischen Anfrage entgegenstehen soll.

In seiner Antwort vom 21. März 1991 beruft sich der Innenminister auf die Entscheidung des Bundesverfassungsgerichts zum Beweiserhebungsrecht von Untersuchungsausschüssen (BVerfGE 67, 100) und leitet aus ihr darüber hinausgehende Einschränkungen für Antworten auf parlamentarische Anfragen ab, die personenbezogene Daten enthalten und als Landtagsdrucksachen veröffentlicht werden.

3.2
Güterabwägung im Einzelfall statt pauschaler Informationssperre

Zutreffend ist der Hinweis auf das Urteil des Bundesverfassungsgerichts insoweit, als sich das Persönlichkeitsrecht des einzelnen und das in Art. 91 der Landesverfassung statuierte, in der Geschäftsordnung des Landtags konkretisierte Auskunftsrecht der Legislative gegenüber der Exekutive auf verfassungsrechtlicher Ebene gegenüberstehen (vgl. BVerfGE 67, 101, Leitsatz 5a und S. 143). Zu weit geht dagegen die Schlußfolgerung, bei parlamentarischen Dokumenten, die der Öffentlichkeit zugänglich sind, habe der Datenschutz automatisch Vorrang vor dem Auskunftsrecht des oder der Abgeordneten.

Weder die Hessische Landesverfassung noch die Geschäftsordnung des Landtags äußern sich zu der speziellen Frage des Personenbezugs bei von der Landesregierung erbetenen Auskünften. Auch das Hessische Datenschutzgesetz enthält dazu keine explizite Regelung.

Da es um die Weitergabe durch Landesministerien, also öffentliche Stellen, geht, die dem HDSG unterliegen, wäre an eine Anwendung von § 14 zu denken, der die Datenübermittlung innerhalb des öffentlichen Bereichs zuläßt, wenn diese "zur rechtmäßigen Erfüllung von Aufgaben des Empfängers erforderlich ist". Allerdings zielt diese Vorschrift mit ihrer Bezugnahme auf eine klare Aufgabendefinition beim Datenadressaten eher auf Behörden und sonstige administrative Stellen ab.

Auch § 16 HDSG, der die Übermittlung an Empfänger außerhalb des öffentlichen Bereichs normiert und dafür die Wahrung der schutzwürdigen Belange des Betroffenen zur Voraussetzung macht, erscheint nicht unmittelbar einschlägig. Es ist jedoch zu bedenken, daß die Antworten der Landesregierung nicht nur dem Parlament bzw. dem Fragesteller zugestellt, sondern durch die Publikation als Drucksache der Öffentlichkeit und damit privaten Dritten zugänglich gemacht werden.

In anderen Bundesländern hat der Gesetzgeber das Problem bereit s aufgegriffen. So sieht § 14 i.V.m. § 13 Abs. 2 S. 1 Nr. 8 des neuen Hamburgischen Datenschutzgesetzes vom 5. Juli 1990 vor, daß eine Offenbarung "von Daten durch die Landesregierung zulässig ist, wenn sie der Bearbeitung von Eingaben sowie Kleinen und Großen Anfragen dient und überwiegende schutzwürdige Interessen eines Betroffenen nicht entgegenstehen". Nach Art. 23 der schleswig-holsteinischen Landessatzung kann die Landesregierung "die Beantwortung von Fragen (und) die Erteilung von Auskünften ... ablehnen, wenn dem Bekanntwerden des Inhalts gesetzliche Vorschriften oder Staatsgeheimnisse oder schutzwürdige Interessen einzelner, insbesondere des Datenschutzes, entgegenstehen ...". Die Ablehnung ist auf Verlangen des Fragestellers vor dem Parlamentarischen Einigungsausschuß zu begründen.

Vergleicht man diese bereits vorhandenen Regelungen mit den in §§ 14 und 16 HDSG enthaltenen Kriterien der Erforderlichkeit für die Kontrollfunktion des Parlaments einerseits und den schutzwürdigen Belangen der Personen, deren persönliche Verhältnisse offenbart werden, andererseits, so ergibt sich ein übereinstimmendes Bild: In Zweifelsfällen hat eine Güterabwägung stattzufinden. Diese muß Aspekte berücksichtigen wie die Sensitivität der mitzuteilenden Angaben, die Bedeutung gerade der personenbezogenen Daten für die Klärung einer politischen Frage, die mögliche Einstufung des Betroffenen als Person öffentlichen Interesses usw. Auch die Form der Erörterung im Parlament (öffentlich, nicht-öffentlich) und gegebenenfalls die Anordnung von Geheimschutzmaßnahmen können im Abwägungsprozeß eine Rolle spielen; darauf hat ja auch das BVerfG in seiner Entscheidung zum Beweiserhebungsrecht von Untersuchungsausschüssen (a.a.O, S. 144) hingewiesen.

Steht jedenfalls die Bearbeitung eines Vorgangs in einem Verwaltungsverfahren im Vordergrund einer Anfrage und nicht die Ausforschung biographischer Details, muß der Informationsanspruch des Landtags grundsätzlich Vorrang haben. Dies hätte auch für die beiden oben genannten Anfragen gegolten.

3.3
Diskussion der zuständigen Landtagsgremien

In einem Brief an den Landtagspräsidenten hatte ich auf diese Streitfrage aufmerksam gemacht und ihn gebeten, das Problem in den zuständigen Gremien des Hessischen Landtags und gegenüber der Landesregierung anzusprechen. Dabei sollte in die Überlegungen auch die Möglichkeit einbezogen werden, bei einer eventuellen Novellierung des HDSG die Datenübermittlung an den Landtag mitzuregeln.

Auf Anfrage des Landtagspräsidenten hat der Hessische Ministerpräsident mit Schreiben vom 21. August 1991 mitgeteilt, er könne "nach derzeitiger Rechtslage" nicht der Position zustimmen, daß über die Offenbarung personenbezogener Daten in Antworten auf parlamentarische Anfragen jeweils im Einzelfall aufgrund einer Güterabwägung zu entscheiden sei.

Aus § 38 Abs. 1 Satz 2 des Hessischen Datenschutzgesetzes ergebe sich nämlich die Wertung des Gesetzgebers, daß die (als verfassungsrechtlich bedeutsam anerkannten) Informationsrechte des Landtags eine Offenbarung personenbezogener Daten nicht rechtfertigten – ein Standpunkt, den ich nicht teile. Diese Wertung stehe – so der Ministerpräsident – in Übereinstimmung mit der Verfassungsrechtsprechung zum Verhältnis zwischen parlamentarischen Informationsrechten und dem Persönlichkeitsrecht des einzelnen. Für eine ausdrückliche Regelung der Datenübermittlung an den Landtag im Rahmen einer Novellierung des Hessischen Datenschutzgesetzes bestehe daher kein Anlaß.

Die kontroversen Standpunkte wurden in der Sitzung des Ältestenrats vom 10. September 1991 eingehend diskutiert, und zwar im Beisein des damaligen Datenschutzbeauftragten, Prof. Dr. Simitis. Der Ältestenrat hat den Unterausschuß für Informationsverarbeitung und Datenschutz (UID) gebeten, sich mit der Problematik zu befassen, zu klären, ob ein Regelungsbedarf besteht, und dem Ältestenrat einen Lösungsvorschlag zu machen. Der UID wiederum hat am 21. Oktober 1991 mich beauftragt, einen ausformulierten Regelungsvorschlag als Grundlage für die weiteren Beratungen vorzulegen. Diesen Text werde ich im Frühjahr 1992 vorlegen.

4. Registrierung von "Belehrungen" über die Sperrgebietsverordnung

4.1
Folgen eines Spaziergangs im Sperrgebiet

Bei einem Spaziergang durch den Grüneburgpark in Frankfurt geriet ein Bürger in eine Kontrolle durch Mitarbeiter der Gesundheitsaufsicht des Frankfurter Ordnungsamtes. Nachdem seine Personalien festgestellt worden waren, wurde er zusammen mit anderen Anwesenden darüber "belehrt", daß der Park im Geltungsbereich der Sperrgebietsverordnung liege und die Prostitution dort verboten sei. Die Mitarbeiter des Ordnungsamtes ließen ihn außerdem eine Bestätigung unterschreiben, daß er von der Sperrgebietsverordnung Kenntnis genommen habe. Nach vergeblichen Bemühungen um Löschung seiner Daten im Frankfurter Ordnungsamt bat mich der Betroffene um Unterstützung.

Wie sich bei der von meinen Mitarbeitern durchgeführten Überprüfung im Frankfurter Ordnungsamt herausstellte, wurden Personen kontrolliert, die z.B. wegen ihres Geschlechts, Alters, der Kleidung und bestimmter Verhaltensweisen den Verdacht erweckten, der Prostitution nachzugehen. Die "Belehrung" enthielt eine Beschreibung der Sperrgebiete und Toleranzzonen sowie den Hinweis, daß ein Verstoß gegen die Sperrgebietsverordnung nach § 120 Abs. 1 Nr. 1 Gesetz über Ordnungswidrigkeiten (verbotene Ausübung der Prostitution) als Ordnungswidrigkeit geahndet werden könne bzw. eine "beharrliche Zuwiderhandlung" gegen die Verordnung ein Vergehen nach § 184a Strafgesetzbuch sei.

Die Originale der Belehrungsbogen gab die Abteilung "Gesundheitsaufsicht" an die Abteilung für die Bearbeitung der Ordnungswidrigkeiten weiter, die sie jahrgangsweise alphabetisch sortiert in Ordnern aufbewahrte.

Zusätzlich speicherte die Ordnungswidrigkeitenbehörde der Stadt Frankfurt die Daten aller Personen, die "belehrt" worden waren, in der automatisierten Datei "ROSI". Zum Zeitpunkt der Überprüfung enthielt diese Datei ca. 1.500 Datensätze. Bei etwa 400 der Betroffenen waren zusätzlich Daten zu einem oder mehreren Ordnungswidrigkeitenverfahren gespeichert.

In diesen Fällen wurden die Daten der Betroffenen in einem weiteren automatisierten Datenverarbeitungssystem, einem Ordnungswidrigkeitenindex, gespeichert, in dem außer Straßenverkehrsangelegenheiten alle Ordnungswidrigkeitenvorgänge der Stadt Frankfurt registriert sind. Zur Zeit der Überprüfung enthielt der Index Daten über ca. 20.000 Ordnungswidrigkeitenverfahren.

Keine der drei Dateien hatte der Magistrat, wie gesetzlich vorgeschrieben, an das Dateienregister des Hessischen Datenschutzbeauftragten gemeldet. Löschungsfristen waren ebenfalls nicht festgelegt.

4.2
Rechtswidrige Datenspeicherung

Für die Verfolgung von Ordnungswidrigkeiten war die Registrierung der "Belehrungen" nicht erforderlich und daher gemäß § 11 Abs. 1 Hessisches Datenschutzgesetz unzulässig. Denn ob eine Person die Sperrgebietsverordnung kennt oder nicht, ist für die Verwirklichung der Tatbestandsmerkmale des § 120 Abs. 1 OWiG ohne Bedeutung, und für die Durchführung eines konkreten Bußgeldverfahrens ist die "Belehrung" gleichfalls unerheblich.

Auch zur Gefahrenabwehr, d.h. zur Verhinderung künftiger Verstöße gegen die Sperrgebietsverordnung, war die Datenspeicherung nicht zulässig, da sie in diesem Fall gegen den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit verstieß. Danach muß eine Datenverarbeitungsmaßnahme zur Erreichung des angestrebten Zwecks geeignet und erforderlich sein, außerdem darf der mit ihr verbundene Zweck nicht außer Verhältnis zur Bedeutung der Sache und den vom Bürger hinzunehmenden Einbußen stehen (BVerfGE 65,1,54). Soweit die Betroffenen die Prostitution nicht zugaben, erfolgte die "Belehrung" und anschließende Registrierung einzig

aufgrund der subjektiven Einschätzung der Außendienstbeamten des Gesundheitsdienstes. Sicherlich können die Beamten des Gesundheitsdienstes aufgrund ihrer Erfahrung meistens zuverlässig beurteilen, ob jemand der verbotenen Prostitution nachgeht, Irrtümer sind jedoch leicht möglich. Die Registrierung einer Person wegen Verdachts der verbotenen Prostitution ist ein derart schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung, daß für den Verdacht objektiv richtige Informationen vorliegen müssen.

Entsprechend meiner Forderung hat der Magistrat der Stadt Frankfurt die Belehrungsbögen vernichtet und die Datei "ROSI" gelöscht. Der automatisierte Ordnungswidrigkeitenindex war und ist dagegen sowohl als Aktennachweissystem als auch als Mittel, sich schnell über den Stand eines Ordnungswidrigkeitenverfahrens zu informieren, erforderlich und daher zulässig. Eine vorläufige Dateibeschreibung liegt mir mittlerweile vor, nach Mitteilung des Magistrats soll mir die endgültige in Kürze zugehen.

5. Ausländerverwaltung

5.1
Das Gesetz zur Neuregelung des Ausländerrechts

Am 1. Januar 1991 ist das Gesetz zur Neuregelung des Ausländerrechts (BGBl. I 1990 S. 1354) in Kraft getreten. Das Artikelgesetz sieht neben der vollständigen Novellierung des Ausländergesetzes (AuslG) die Änderung einer Reihe anderer Gesetze, wie beispielsweise des Asylverfahrensgesetzes und des X. Buches des Sozialgesetzbuches, vor. Diese Gesetze enthalten jetzt erstmals Regelungen für die Verarbeitung personenbezogener Daten durch die Ausländerbehörden und anderer mit der Ausführung ausländerrechtlicher Vorschriften betrauter Behörden. Das gleiche Ziel verfolgen die aufgrund von Ermächtigungsnormen im Ausländergesetz erlassenen Rechtsverordnungen des Bundes wie die Ausländerdatenübermittlungsverordnung (BGBl. I S. 2997), die Ausländerdateienverordnung (BGBl. I S. 2999) und die Verordnung zur Durchführung des Ausländergesetzes (BGBl. I S. 2983), alle vom 18. Dezember 1990.

Mit diesem Regelungswerk haben Bundestag und Bundesregierung endlich auf die bereits im Volkszählungsurteil des Bundesverfassungsgerichts vom Jahr 1983 formulierten Vorgaben reagiert und für diesen wichtigen Verwaltungsbereich spezifische Datenverarbeitungsregelungen erlassen. Die Bestimmungen weisen allerdings in weiten Teilen gravierende datenschutzrechtliche Mängel auf. Eine abschließende Beurteilung soll jedoch erst erfolgen, wenn feststeht, in welcher Weise die bestehenden Spielräume bei der Auslegung und Anwendung des Ausländergesetzes genutzt werden. So bedürfen das gesamte Ausländergesetz und mithin auch die Datenverarbeitungsregelungen der Konkretisierung durch Verwaltungsvorschriften. Für einen Teil der Datenverarbeitungsvorschriften hat das Bundesinnenministerium einen Richtlinienentwurf vorgelegt (Stand: 25. Februar 1991). Diese "vorläufigen Anwendungshinweise zu § 76 und § 77 Ausländergesetz" bringen zwar deutliche Verbesserungen für den Datenschutz, sind aber noch keineswegs zufriedenstellend. Einige exemplarische rechtliche Mängel der derzeitigen Rechtslage zeigt der folgende Überblick.

5.1.1
Erhebung personenbezogener Daten

§ 75 Ausländergesetz regelt die Erhebung personenbezogener Daten durch die Ausländerbehörden und andere mit der Ausführung des Gesetzes betraute Behörden wie beispielsweise die Einbürgerungsbehörden, den Bundesgrenzschutz und den Zoll oder die Polizeibehörden bei der Abschiebung und Festnahme. Das Gesetz schreibt vor, daß Informationen vorrangig beim Ausländer selbst zu erheben sind. Damit soll sichergestellt werden, daß der einzelne stets weiß, welche Behörde was und aus welchem Grund über ihn erfahren hat. Allerdings sind die Voraussetzungen, unter denen die Informationen bei anderen öffentlichen und privaten, inländischen wie ausländischen Stellen ohne Kenntnis des Betroffenen eingeholt werden dürfen, weit gefaßt. So reicht es beispielsweise aus, daß die Mitwirkung des Ausländers "einen unverhältnismäßigen Aufwand erfordern würde" oder "die zu erfüllende Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht" und in beiden Fällen "keine überwiegenden schutzwürdigen Interessen des Betroffenen beeinträchtigt werden". Voraussichtlich wird deshalb die Erhebung bei Dritten große Bedeutung erlangen. Das ist nicht nur bedenklich wegen der geringeren Transparenz für den einzelnen, sondern auch deshalb, weil damit Daten für Zwecke verwendet werden, für die sie ursprünglich nicht erhoben und gespeichert worden sind. Eine solche Kontextänderung bringt zwangsläufig die Gefahr von Verfälschungen und Fehlinterpretationen mit sich, weshalb die allgemeinen Datenschutzgesetze eine Zweckänderung mit Recht nur ausnahmsweise zulassen.

Statt sich detailliert damit auseinanderzusetzen, wer welche Daten zu welchen Zwecken erheben darf, hat sich der Gesetzgeber mit einer Generalklausel begnügt: Die Datenerhebung ist rechtmäßig, wenn die gewünschte Information für die Aufgabenerfüllung der jeweiligen Behörde erforderlich ist. Dies ist keine den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts gerecht werdende bereichsspezifische gesetzliche Grundlage für die Datenerhebung. Angesichts dieser Zurückhaltung des Gesetzgebers kommt nunmehr den Verwaltungsvorschriften zur Ausfüllung des Ausländergesetzes maßgebliche Bedeutung zu. Zu § 75 Ausländergesetz liegt bisher noch kein Entwurf vor. Es bleibt daher abzuwarten, inwieweit die künftige Verwaltungsvorschrift präzise festlegt, wer welche Daten bei wem zu welchem Zweck erheben darf.

5.1.2
Datenübermittlungen an die Ausländerbehörden

Kernstück der Datenverarbeitungsregelungen sind die in § 76 Ausländergesetz allen öffentlichen Stellen auferlegten Informationspflichten gegenüber den Ausländerbehörden. Die öffentlichen Stellen haben danach nicht nur deren Anfragen zu beantworten, sondern in bestimmten Situationen, etwa wenn sie von einem Ausweisungsgrund erfahren, von sich aus die Ausländerbehörden zu informieren. Vor allem Beratungsstellen für Ausländer, aber auch beispielsweise Jugendbetreuer und Sozialarbeiter haben die Befürchtung geäußert, daß das für jede fürsorgerische und pädagogische Arbeit erforderliche Vertrauensverhältnis durch die Unterrichtungspflichten gestört werde. Die Kritik gipfelte in der Bezeichnung "Spitzelparagraph" und in Charakterisierungen wie "Pflicht zur Denunziation" oder "totalitärer Überwachungswahn". Diese Reaktion kam nicht von ungefähr, denn der schwer verständliche Gesetzestext mit seinen zahlreichen Verweisungen und vage formulierten Generalklauseln macht die Interpretation schwierig. Das Bundesinnenministerium ist in den "vorläufigen Anwendungshinweisen" teilweise auf die Kritik eingegangen und hat eine Reihe von Klarstellungen getroffen, die allerdings nicht ausreichen.

Das gilt z.B. für den Hinweis, daß ausschließlich öffentliche und nicht etwa auch privatrechtlich organisierte Stellen, welche Aufgaben der öffentlichen Verwaltung wahrnehmen, Kirchen und Einrichtungen in privater Trägerschaft von der Übermittlungspflicht betroffen sind. Damit ist keine ausreichende Präzisierung erreicht. Statt beispielhaft aufzuzählen, welche Stellen nicht übermittlungspflichtig sind, müßten in der Verwaltungsvorschrift die Einrichtungen, die den Ausländerbehörden Daten zu übermitteln haben, abschließend benannt werden.

5.1.2.1
Datenübermittlungen auf Ersuchen

§ 76 Abs. 1 Ausländergesetz verpflichtet öffentliche Stellen, "ihnen bekannt gewordene Umstände" auf Ersuchen den mit der Ausführung des Gesetzes betrauten Behörden mitzuteilen. Gänzlich offen bliebe der Umfang der Angaben, würde nicht der Verweis auf § 75 AuslG den Schluß zulassen, daß nur zur Aufgabenerfüllung der ersuchenden Behörde erforderliche Daten gemeint sind. Auch in den "vorläufigen Anwendungshinweisen" fehlt eine Festlegung, welche Daten bei welcher Behörde erfragt werden dürfen.

Das Gesetz zur Neuregelung des Ausländerrechts hat lediglich die Weitergabe von Daten, die dem Sozialgeheimnis (§ 35 Sozialgesetzbuch I) unterliegen, etwas präziser geregelt. Die Offenbarung von Sozialdaten an Ausländerbehörden ist nicht mehr allein dem Ermessen der Sozialbehörden überlassen, sondern der durch Artikel 8 novellierte § 71 Abs. 2 Sozialgesetzbuch X enthält jetzt einen Katalog der zulässigen Übermittlungszwecke, was zweifellos eine Verbesserung des Sozialdatenschutzes ist. Andererseits läßt der Gesetzgeber beispielsweise die Übermittlung von subjektiven Einschätzungen und Prognosen zu. So können Jugendämter den Ausländerbehörden Angaben "über das zu erwartende soziale Verhalten" mitteilen. Derart unsichere Informationen als Entscheidungsgrundlage in Ausländerverfahren zu verwenden, ist jedenfalls aus der Sicht des Datenschutzes nicht akzeptabel.

5.1.2.2
Eigenständige Übermittlungspflichten

Nach § 76 Abs. 2 Ausländergesetz haben alle öffentlichen Stellen die Ausländerbehörde zu informieren, wenn sie Kenntnis erlangen vom unrechtmäßigen Aufenthalt eines Ausländers, dem Verstoß gegen eine räumliche Beschränkung sowie sonstigen Ausweisungsgründen. Sieht man sich die Ausweisungsgründe in den §§ 46 und 47 AuslG im einzelnen an, wird deutlich, daß eine Vielzahl von Mitteilungspflichten begründet wird. Zum einen geht es um so vage formulierte Angaben wie jene, daß der Ausländer die "freiheitlich demokratische Grundordnung oder die Sicherheit der Bundesrepublik Deutschland gefährdet" oder einen "nicht nur geringfügigen Verstoß" gegen Rechtsvorschriften begangen hat. Ausdrücklich genannt werden ein Verstoß gegen eine die Gewerbsunzucht regelnde Rechtsvorschrift und der Verbrauch von gefährlichen Betäubungsmitteln, wenn der Betroffene nicht zur erforderlichen Rehabilitation bereit ist. Mitzuteilen ist darüber hinaus die Kenntnis, daß ein Ausländer durch sein Verhalten die öffentliche Gesundheit gefährdet oder längerfristig obdachlos ist, aber auch der Bezug von Sozialhilfe, der Tatbestand der Sozialhilfebedürftigkeit und bestimmte Arten der Hilfe zur Erziehung.

Diese Flut von Übermittlungstatbeständen wird in den "vorläufigen Anwendungshinweisen" zwar eingeschränkt dadurch, daß ansatzweise für jede Behörde im einzelnen festgelegt wird, welche Daten übermittelt werden dürfen. Im Ergebnis werden damit sowohl der Kreis der übermittlungspflichtigen Stellen als auch die Menge der jeweils zu übermittelnden Informationen erheblich reduziert. Dennoch bleibt eine Reihe von Mängeln: Die Übermittlung eines Ausweisungsgrundes muß, anders als im Entwurf, auf die Fälle beschränkt werden, in denen durch die Unterrichtung unmittelbar eine Maßnahme der Ausländerbehörde veranlaßt werden kann. Soweit ein Ausweisungsgrund gar nicht zu einer Ausweisung führen kann, weil der Ausländer beispielsweise einen erhöhten Ausweisungsschutz nach § 48 Ausländergesetz genießt, muß die Übermittlung unterbleiben, denn sie wäre eine – unzulässige – Datenverarbeitung auf Vorrat.

5.1.2.3
Weitere Übermittlungspflichten

Polizei, Staatsanwaltschaften, Gerichte und Bußgeldbehörden haben nach § 76 Abs. 4 Ausländergesetz die Ausländerbehörden über die Einleitung und die Erledigung eines anhängigen Verfahrens zu unterrichten. Hier sind Einschränkungen unbedingt notwendig: Die Polizei darf Strafsachen nicht bereits bei einem vagen oder gar nur vorläufigen Anfangsverdacht mitteilen, sondern erst dann, wenn die Verdachtslage eine Konkretisierung erreicht hat, die es der Kriminalpolizei angezeigt erscheinen läßt, die Staatsanwaltschaft zu beteiligen. Die aufgrund des § 76 Abs. 5 erlassene Ausländerdatenübermittlungsverordnung enthält weitere Mitteilungspflichten für im einzelnen genannte Behörden wie die Meldebehörden, die Staatsangehörigkeitsbehörden, die Justiz-, Polizei- und Ordnungsbehörden, die Arbeitsämter und die Gewerbebehörden. Inhaltlich beschränkt sich die Rechtsverordnung im wesentlichen auf die Auflistung der bei den einzelnen Behörden anfallenden Bearbeitungsdaten.

5.1.3
Schutzrechte der Betroffenen

Die Pflicht zur Löschung personenbezogener Angaben sieht das Gesetz nur für wenige Sachverhalte vor. Das betrifft zum einen die Vernichtung von Unterlagen, die aufgrund erkennungsdienstlicher Maßnahmen gewonnen wurden (§ 78 Abs. 4), und zum anderen gem. § 80 Abs. 2 und 3 Dokumente über die Ausweisung und Abschiebung und Mitteilungen nach § 76 Abs. 1. Für alle anderen Fälle bestehen – anders als noch im Regierungsentwurf vorgesehen – keine bereichsspezifischen Pflichten zur Löschung oder Sperrung von Informationen. Da aber gerade die Ausländerbehörde nicht zuletzt aufgrund der vielfältigen Übermittlungspflichten anderer Behörden über eine breite Informationssammlung verfügt, hätte es hier konkreter, auf den Einzelfall abstellender Regelungen bedurft.

Der Gesetzgeber verzichtet ebenfalls auf das noch im Gesetzentwurf der Bundesregierung enthaltene Auskunftsrecht für den Betroffenen. Damit bleibt er hinter den meisten in den letzten Jahren erlassenen bereichsspezifischen Datenschutzregelungen zurück. Der Betroffene bleibt auf die Geltendmachung des Auskunftsanspruchs nach den allgemeinen Datenschutzgesetzen angewiesen.

5.2
Unsicherheit beim Umgang mit dem neuen Ausländergesetz

Wie dringend die Ausländerbehörden präzise Verwaltungsvorschriften zum Ausländergesetz benötigen, zeigt folgender Fall, auf den mich ein psychiatrisches Krankenhaus aufmerksam machte: Eine Ausländerbehörde hatte an alle psychiatrischen Krankenhäuser ihres Zuständigkeitsbereichs ein Schreiben verschickt, in dem sie Informationen über sämtliche ausländische Patienten forderte. Verlangt wurde der Name des Patienten, der Grund und die (voraussichtliche) Dauer des Aufenthalts sowie die Auskunft, ob eine polizeiliche Anmeldung erfolgt sei. Das war in mehrfacher Hinsicht unzulässig:

§ 76 Abs. 1 Ausländergesetz (AuslG) verpflichtet öffentliche Stellen, ihnen bekannt gewordene Umstände den Ausländerbehörden aufgrund eines konkreten Ersuchens im Einzelfall mitzuteilen. Für "Gruppenauskünfte" dagegen bietet die Bestimmung keine ausreichende Rechtsgrundlage.

Außerdem muß die Ausländerbehörde grundsätzlich die benötigten Daten beim Betroffenen erheben. Es lagen keine Anhaltspunkte für einen der in § 75 Abs. 2 AuslG genannten Ausnahmefälle vor, in denen eine Erhebung auch ohne Mitwirkung der betroffenen Ausländer zulässig gewesen wäre.

Vor allem aber kam eine Übermittlung hier schon deshalb nicht in Betracht, weil es sich um Daten handelte, die der ärztlichen Schweigepflicht i.S. von § 203 StGB unterlagen. Nach § 77 Abs. 1 AuslG muß eine Übermittlung personenbezogener Daten nach § 76 unterbleiben, soweit besondere gesetzliche Verwendungsregelungen – in diesem Fall § 203 StGB – entgegenstehen. § 77 Abs. 2 AuslG, demzufolge personenbezogene Daten, die von einem Arzt einer öffentlichen Stelle zugänglich gemacht worden sind, unter bestimmten Voraussetzungen an die Ausländerbehörde übermittelt werden dürfen, war nicht einschlägig, da sich die Daten noch innerhalb des psychiatrischen Krankenhauses befanden, mit dem ein Behandlungsvertrag bestand.

Ich konnte den Leiter der Ausländerbehörde sofort von der Rechtswidrigkeit der Aktion überzeugen. Er erklärte mir, daß die derzeitige Rechtslage in vielen Punkten unübersichtlich und verwirrend sei und er insbesondere auf den baldigen Erlaß verbindlicher und praktikabler Verwaltungsvorschriften hoffe. Diese Hoffnung teile ich.

5.3
Ausländerzentralregister-Gesetz (AZRG)

Die größte Sammlung personenbezogener Ausländerdaten ist das beim Bundesverwaltungsamt in Köln geführte Ausländerzentralregister (AZR). Es enthält Angaben über mehr als 10 Millionen Ausländer. Gespeichert sind dort nicht nur Daten von Ausländern, die in der Bundesrepublik leben, sondern auch von Ausländern, die in ihren Heimatstaat zurückgekehrt sind oder sich dort z.B. an eine Vertretung der Bundesrepublik gewandt haben. Außer Informatione n zur Identifizierung sind insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren registriert. Nicht nur die Ausländerbehörden, sondern auch die unterschiedlichsten öffentlichen Stellen haben

Zugang zu dem Register. Ein Teil der Ausländerbehörden sowie die Grenz- und Polizeibehörden, die Verfassungsschutzämter, das Zollkriminalinstitut und das Bundesamt für die Anerkennung ausländischer Flüchtlinge können über Online-Anschlüsse sogar direkt auf die automatisiert gespeicherten Daten zugreifen.

Für das Register gibt es noch immer keine gesetzlichen Datenverarbeitungsvorschriften, obgleich die Datenschutzbeauftragten schon vor Jahren auf das Regelungsdefizit hingewiesen haben (vgl. 15. Tätigkeitsbericht, Ziff. 7). Die Bundesregierung brachte zwar 1989 einen Entwurf für ein Ausländerzentralregistergesetz im Bundestag ein, besonders wegen der massiven Kritik aus den Reihen der Betroffenen und der Datenschutzbeauftragten kam es jedoch nicht zur Verabschiedung des Gesetzes. Am 15. Juli 1991 hat daher das Bundesinnenministerium ein Arbeitspapier für einen Gesetzentwurf vorgelegt. Da das Papier im wesentlichen dem Gesetzentwurf der Bundesregierung entspricht und dieser wiederum den Empfehlungen , die eine Arbeitsgruppe 1986 in einem Bericht zur Neukonzeption des AZR gegeben hat, gilt die im 15. Tätigkeitsbericht geäußerte Kritik an dem Bericht von 1986 gleichermaßen für das neue Arbeitspapier.

5.3.1
Aufgaben des Registers

Die im Arbeitspapier des Bundesinnenministeriums für das Register vorgesehenen Aufgaben gehen weit über ein bloßes Aktenhinweissystem hinaus. Das Register soll hauptsächlich unmittelbar Auskunft über bestimmte Sachverhalte geben und damit den Rückgriff auf die Akte bei den Ausländerbehörden ersetzen.

Die Gefahren, die damit verbunden sind, liegen auf der Hand: Die anfragende Behörde erhält die Daten direkt aus dem Register, ohne sie im Kontext des Aktenvorgangs, aus dem sie stammen, beurteilen zu können. Das kann dazu führen, daß verkürzte, aus dem Zusammenhang gerissene Informationen zur Grundlage von Entscheidungen gemacht werden. Hinzu kommt, daß die Informationen im Fall des automatisierten Abrufs nicht auf Richtigkeit und Aktualität überprüft werden können. Die Registerbehörde hat nur logische Widersprüche im Datensatz aufzudecken und sicherzustellen, daß Daten nicht ungewollt gelöscht oder unrichtig werden. Sie muß sich auf die korrekte und zeitgerechte Anlieferung bzw. Nachberichtigung der Daten durch die anliefernde Stelle verlassen. Kommt diese ihrer Pflicht nur in einem Fall nicht nach, kann das zu einem Fehler im Datensatz führen, der sich ohne Kenntnis der Registerbehörde immer weiter fortsetzt. So stellte beispielsweise der Bundesdatenschutzbeauftragte bei einer Prüfung des Ausländerzentralregisters fest, daß in immerhin 34 von 600 ausgewählten Fällen die Einbürgerung eines Ausländers dem AZR nicht mitgeteilt worden war.

5.3.2
Inhalt des Registers

Der direkte Zugriff der anfragenden Behörde erscheint noch problematischer, sieht man sich einzelne der nach dem Entwurf im Register zu speichernde Daten an. Denn neben den Stammdaten des Betroffenen und den Angaben zum Meldestatus, Aufenthalts- und Asylrecht sollen z.B. auch Einreisebedenken registriert werden, ohne daß der Entwurf sagt, was darunter zu verstehen ist. Sieht man sich die Fälle an, die das Bundesverwaltungsamt bereits heute unter dem Merkmal "Einreisebedenken" erfaßt, z.B. Verdacht auf Scheinehe oder Prostitution, zeigt sich, daß es hier nicht um Feststellungen geht, die in einem rechtsstaatlich formalisierten Verfahren getroffen worden sind, sondern um subjektive, äußerst fehleranfällige Wertungen und Einschätzungen einzelner Sachbearbeiter.

Positiv zu bewerten ist, daß der neue Entwurf nunmehr ausschließlich die Speicherung der Ablehnung des Antrags auf Feststellung als Deutscher oder auf Übernahme oder Anerkennung als Vertriebener vorsieht. Nach dem früheren Entwurf war noch die Angabe zu speichern, daß ein entsprechender Antrag wegen "erheblicher Zweifel am Bestehen der erforderlichen Voraussetzungen voraussichtlich abgelehnt werden wird."

Bedenken gegen den vorgesehenen Datensatz ergeben sich jedoch noch aus einem weiteren Grund: Das bereits in den Vorarbeiten zum Gesetzentwurf der Bundesregierung formulierte Ziel, das AZR für den Sicherheitsbereich nutzbar zu machen, ist konsequent realisiert worden. Es geht nicht nur darum, was bisher schon zunehmend der Fall war, daß Polizei- und Verfassungsschutzbehörden Zugriff auf Daten erhalten, die primär ausländerrechtliche Fragen betreffen. Geplant ist darüber hinaus, bestimmte Erkenntnisse der Sicherheitsbehörden über Ausländer im AZR zu speichern. So sollen die Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung aus dem INPOL-Fahndungsbestand des BKA in das AZR übernommen werden. Gleiches gilt für Angaben zu Personen, bei denen "tatsächliche Anhaltspunkte für den Verdacht bestehen", daß sie Straftaten begehen könnten.

Die Integration dieser Informationen der Sicherheitsbehörden in das AZR ist aus datenschutzrechtlicher Sicht sehr problematisch. Im Ergebnis bedeutet dies, daß Ausländerbehörden und andere Stellen Hilfsfunktionen für die Polizei übernehmen. So wird z.B. die Ausländerbehörde vor der Erteilung oder Verlängerung der Aufenthaltserlaubnis zu der Prüfung veranlaßt, ob zu dem Ausländer bestimmte polizeiliche Erkenntnisse vorliegen. Die Verknüpfung von zu derart unterschiedlichen Zwecken gesammelten Informationen bedeutet für den Betroffenen, daß Informationen über ihn aus ganz verschiedenen Lebensbereichen zusammengeführt werden. Je vielfältiger die gesammelten Daten zu einer Person und je unterschiedlicher ihre Herkunft, um so vollständiger und damit auch aufschlußreicher ist das Bild, das mit ihrer Hilfe von der Persönlichkeit des einzelnen erstellt werden kann. Nach der Rechtsprechung des Bundesverfassungsgerichts ist aber sowohl die Erstellung von Persönlichkeitsprofilen als auch das Anfertigen von Teilabbildern der Persönlichkeit unzulässig (BVerfGE 65, 1, 53).

5.3.3
Datenübermittlungen

Der Kreis der Behörden, die Daten an das Register übermitteln oder Angaben aus ihm erhalten sollen, ist aus datenschutzrechtlicher Sicht viel zu weit. Informationen liefern und erhalten sollen nach dem Arbeitspapier beispielsweise die Grenzbehörden, das Bundesamt für die Anerkennung ausländischer Flüchtlinge, das Bundeskriminalamt und die Verfassungsschutzbehörden.

Viel zu großzügig werden den Behörden Direktanschlüsse für Abfragen erlaubt. Ausreichend ist nach dem Arbeitspapier, daß die "Vielzahl der Übermittlungsersuchen" oder die "besondere Eilbedürftigkeit" einen Online-Anschluß angemessen erscheinen lassen. Solche Anschlüsse sind jedoch nur akzeptabel, wenn ein darüber hinausgehendes besonderes Bedürfnis an ihrer Einrichtung besteht. Das ist in dem Arbeitspapier weder für die Bundesanstalt für Arbeit noch für das Zollkriminalinstitut, die Verfassungsschutzämter oder den Bundesnachrichtendienst dargelegt. Es genügt nicht, wie etwa bei den Geheimdiensten, darauf hinzuweisen, der Online-Anschluß sei für diese Einrichtungen auch deshalb erforderlich, weil dadurch die besondere Vertraulichkeit der Aufgabenstellung der Geheimdienste gewahrt würde, denn mit diesem Argument ließen sich für die Geheimdienste Direktanschlüsse zu allen möglichen Datenbanken rechtfertigen.

6. Sozialverwaltung: Reform des Kinder- und Jugendhilferechts

6.1
Die Datenschutzregelungen im 8. Buch des Sozialgesetzbuchs

Am 1. Januar 1991 ist als Kern der lange diskutierten Reform des Jugendhilferechts das 8. Buch des Sozialgesetzbuches (SGB VIII): "Kinder- und Jugendhilfe" in Kraft getreten (BGBl. I (1990) S. 1163). Nicht zuletzt dank der Intervention der Datenschutzbeauftragten des Bundes und der Länder zu den vorgelegten Entwürfen waren noch während des Gesetzgebungsverfahrens bereichsspezifische Datenschutzregelungen in das Gesetz eingefügt worden. Für den Bereich der Kinder- und Jugendhilfe existieren nunmehr Datenschutzregelungen, die den Anforderungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts gerecht werden. Das 4. Kapitel des SGB VIII "Schutz personenbezogener Daten" (§§ 61 bis 68) konkretisiert die Zweckbindung (§ 63 Abs. 2). Gleichzeitig werden die Offenbarungsnormen des SGB X eingeschränkt, wenn eine Offenbarung den Erfolg der Leistung der Jugendhilfe in Frage stellen könnte (§ 64 Abs. 2). Für die Erhebung ist zudem der grundsätzliche Vorrang der Erhebung beim Betroffenen festgelegt (§ 62 Abs. 2).

Hervorzuheben ist schließlich der durch § 65 gewährleistete "Besondere Vertrauensschutz in der persönlichen und erzieherischen Hilfe". Festgeschrieben wird das Verhältnis von beruflicher Schweigepflicht (§ 203 Strafgesetzbuch) einerseits und der Einbindung der schweigepflichtigen Personen in die Strukturen der Verwaltung andererseits. Das Gesetz entscheidet sich für den Vorrang der Schweigepflicht und damit auch für ein innerbehördliches Schweigerecht der betroffenen Mitarbeiter (zu ersten Erfahrungen mit den praktischen Auswirkungen des § 65 SGB VIII vgl. Ziff. 6.3).

6.2
Hessisches Ausführungsgesetz zum SGB VIII

Das SGB VIII überläßt an verschiedenen Stellen die konkrete Ausgestaltung dem Landesgesetzgeber. Im Mai 1991 hat das Hessische Ministerium für Jugend, Familie und Gesundheit deshalb einen Entwurf für ein Ausführungsgesetz vorgelegt. Bei der Überarbeitung des Entwurfs, der im wesentlichen die Verwaltungsstruktur, wie z.B. die Organisation des Landesjugendamtes, regelt und die Grundsätze zur Finanzierung einiger besonderer Leistungsarten bzw. zur Beteiligung des Landes bei entstehenden Kosten festlegt, wurden meine Anregungen berücksichtigt.

6.3
Konsequenzen des § 65 SGB VIII für kommunale Erziehungsberatungsstellen

§ 65 SGB VIII sichert einen besonderen Vertrauensschutz in der persönlichen und erzieherischen Hilfe, die die Jugendämter gewähren. Die Regelung lehnt sich an der beruflichen Schweigepflicht in § 203 StGB an, geht jedoch darüber hinaus. Sie richtet sich an alle Mitarbeiter eines Trägers der öffentlichen Jugendhilfe unabhängig von der beruflichen Ausbildung des Mitarbeiters oder dem konkreten Charakter der Beratungsstelle. Immer dann, wenn Daten zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind, gilt der Vertrauensschutz. "Persönliche Hilfe" ist dabei i.S.d. § 11 SGB I zu verstehen als eine besondere Art der Dienstleistung.

Der Kreis der Personen, die sich auf § 65 SGB VIII berufen können, ist damit sehr weit gefaßt. Bedeutsam ist auch, daß sich diese Regelung, anders als die übrigen Datenschutzvorschriften, nicht an den Leistungsträger, sondern an die Mitarbeiter wendet. Damit sind einige Probleme der täglichen Praxis von Beratern gelöst. Die Erfahrungen haben jedoch gezeigt, daß dies nicht ohne weiteres für alle Schwierigkeiten, die sich aus der Verschwiegenheitspflicht für bestimmte Berufsgruppen ergeben, gilt. Vor allem aus dem Bereich von Erziehungsberatungsstellen in kommunaler Trägerschaft bin ich mehrmals um Klärung von Einzelfragen gebeten worden.

Bei der Beurteilung der Konflikte kann nicht unberücksichtigt bleiben, daß die Beratungsstellen in die Kommunalverwaltung integriert sind und sich somit Fragen der Dienstaufsicht ebenso wie der Fachaufsicht stellen; ähnliches gilt für haushaltsrechtliche Probleme bzw. die Rechnungsprüfung. Andererseits ist auch kein Grund ersichtlich, warum das Verhältnis Berater – Bürger bei diesen Beratungsstellen anders, weniger vertraulich, sein sollte als bei entsprechenden Angeboten freier Träger. Entscheidend muß sein, wie diese Stellen nach außen auftreten, mit welchen Erwartungen der Bürger sie aufsucht. Durch entsprechende Organisationsformen muß der Träger dafür sorgen, daß es keine Konflikte mit der üblichen Behördenstruktur gibt.

6.3.1
Keine Verwendung der anvertrauten Daten für Zwecke der Rechnungsprüfung

Die Reform des Kinder- und Jugendhilferechts hat mit der Regelung in § 64 Abs. 3 SGB VIII klargestellt, daß auch die sensiblen Sozialdaten zur Erfüllung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung und zur Durchführung von Organisationsuntersuchungen zur Verfügung stehen, soweit sie für die Durchführung der Maßnahmen erforderlich sind. Diese Regelung ist jedoch auf die Daten, die i.S.v. § 65 SGB VIII einem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe anvertraut worden sind, nicht anwendbar. Das folgt zum einen aus der systematischen Stellung des § 65 SGB VIII: Er ist eine Spezialregelung für den Schutz derjenigen personenbezogenen Daten, die zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind. Zum anderen folgt dies auch daraus, daß, wie erwähnt, § 65 SGB VIII sich nicht an die datenverarbeitende Stelle "Jugendamt" richtet, sondern als Adressaten den einzelnen Mitarbeiter hat. Eines der Ziele des § 65 SGB VIII ist gerade, dem Mitarbeiter nicht nur eine Verpflichtung gegenüber den Bürgern aufzuerlegen, sondern ihm ausdrücklich ein persönliches Schweigerecht gegenüber seinem Vorgesetzten und der Dienststelle zu geben.

6.3.2
Zusammenarbeit mit anderen Teilen der Verwaltung

Die Tätigkeit der Erziehungsberatungsstellen ist teilweise abhängig von Entscheidungen des Jugendamtes. Die Erziehungsberatungsstellen müssen daher die zur Vorbereitung solcher Entscheidungen vom Jugendamt benötigten Daten gemäß § 60 SGB I übermitteln. Solche Daten sind jedoch strikt zu trennen von den Informationen, die der Betroffene im Verlaufe der Beratung dem einzelnen Mitarbeiter "anvertraut". Anvertraut sind alle die Informationen, die dem Mitarbeiter bekannt werden, weil der Betroffene auf seine Verschwiegenheitspflicht vertraut – und auch vertrauen durfte. Dabei ist es unerheblich, ob der Bürger bei der Bekanntgabe der Einzelinformation ausdrücklich darauf hinweist, daß er dieses als vertraulich ansieht. Insoweit ist auch die Verantwortung der Berater gefragt. Bei Situationen oder Informationen, die unter die Mitwirkungspflicht des § 60 SGB I fallen (können), muß er den Betroffenen rechtzeitig darauf hinweisen, daß es hier notwendig sein kann, diese Informationen an Dritte für Entscheidungen des Jugendamtes weiterzugeben. Dabei gilt auch für die Beratungsstellen in kommunaler Trägerschaft grundsätzlich, daß schon allein die Tatsache, ob bzw. wann ein Bürger diese Beratungsstelle aufsucht, der Schweigepflicht unterliegt. § 65 SGB VIII steht der Weitergabe von Informationen jedoch dann nicht entgegen, wenn die Beratungsstelle von Dritten um ein Gutachten gebeten wird und dem Betroffenen dies auch bekannt ist.

Dies alles hat auch Konsequenzen für die Organisation der Beratung, die Aktenführung, notwendige Abrechnungsmodalitäten sowie das Verhältnis zu den anderen Stellen der Kommunalverwaltung.

6.3.3
Datenweitergabe aufgrund einer Einwilligung

Eine Durchbrechung der Verschwiegenheitspflicht ist gem. § 65 SGB VIII möglich, wenn die Voraussetzungen des § 203 StGB vorliegen. Dies ist u.a. dann gegeben, wenn eine Einwilligung des Betroffenen vorliegt. Dabei ist darauf zu achten, daß der Betroffene nur dann wirksam einwilligen kann, wenn ihm bewußt ist, in welchem Umfang welche Information an wen offenbart werden soll. Es kann auf keinen Fall davon ausgegangen werden, daß einem Klienten, der eine kommunale Beratungsstelle aufsucht, bewußt ist, daß diese in die normale Verwaltungsorganisation einschließlich Dienst-/Fachaufsicht und Rechnungsprüfung eingebunden ist. Das Gegenteil ist in der Regel der Fall: Der Klient rechnet mit der Vertraulichkeit, nicht zuletzt auch deshalb, weil sich die Beratungsstellen in den letzten Jahren ausdrücklich bemüht haben, ihre innere Unabhängigkeit gegenüber der Verwaltung deutlich zu machen.

Daher ist die Organisation der Beratung so zu gestalten, daß einerseits dem Klienten bewußt wird, wer welche Informationen bekommen kann, und andererseits auch nur im wirklich erforderlichen Umfang personenbezogene Informationen zur Organisation der Beratungsstelle verwendet werden. Über die Strukturen der Beratungsstelle, aber auch über notwendige Kontakte mit anderen Teilen der Verwaltung muß der Bürger informiert werden. Nur dann kann er eine Vorstellung davon entwickeln, wie mit seinen Informationen umgegangen wird.

6.3.4
Zur inneren Organisation der Beratungsstellen

Die eigentliche Beratung ist eine persönliche Hilfe, die von einer Person und nicht von einer Organisaton geleistet wird. Soweit aus fachlichen Gründen ein Austausch über den Inhalt oder die Umstände einer Beratung stattfinden

soll, muß der Klient darüber informiert sein. Sieht das Konzept der Beratungsstelle vor, daß in der Regel die Behandlung bzw. die Beratung durch ein Team erfolgt, ist der Betroffene vorab darüber zu informieren. Danach kann ein Austausch im Team stattfinden. Dient der Austausch im Team jedoch im wesentlichen der Reflexion des eigenen Verhaltens des Beraters, dem fachlichen Meinungsaustausch oder findet eine Supervision gegebenenfalls auch mit Außenstehenden statt, ist dies in aller Regel nur in anonymisierter Form zulässig.

Von der Organisation der konkreten Beratungsstelle hängt es auch ab, ob der Leiter einer Beratungsstelle, der hauptsächlich Verwaltungsaufgaben wahrnimmt, noch zum Team dieser Beratungsstelle gehört. Zum Team gehört in aller Regel nicht ein Abteilungsleiter innerhalb des Jugendamtes, der nicht in die konkrete Beratungstätigkeit integriert ist. Unerheblich ist insoweit, welche beruflichen Qualifikationen dieser Abteilungsleiter hat. Eine Durchbrechung der Schweigepflicht i.S.d. § 65 SGB VIII findet nämlich auch dann statt, wenn der Empfänger selbst einer entsprechenden beruflichen Schweigepflicht unterliegt.

Bei der Organisation der Abläufe in der Beratungsstelle sowie der Aktenführung ist entsprechend zu verfahren. Zu trennen ist zwischen den Unterlagen und Informationen, die für die reine Organisation notwendig sind, und den Unterlagen, die sich auf die Inhalte der Beratung beziehen.

Zur Organisation gehören u.a. Termine, zuständiger Betreuer, soweit notwendig Vertretungsregelungen, unter bestimmten Voraussetzungen auch Daten zur Abrechnung besonderer Sachverhalte. Auch diese Informationen sind zwar vom Bereich der Schweigepflicht und dem besonderen Vertrauensschutz umfaßt; eine Mitteilung an die Mitarbeiter, die für die organisatorische Abwicklung zuständig sind, ist jedoch zulässig. Der Klient läßt sich auf die Beratung in dieser Beratungsstelle mit der vorgegebenen Organisationsstruktur ein, damit erklärt er auch seine Zustimmung zur Datenweitergabe für diese Zwecke im notwendigen Umfang.

6.3.4.1
Terminkalender

Manche Beratungsstellen führen Anmeldebücher. Dort werden Namen, Telefonnummern, Datum der telefonischen Anmeldung sowie Datum und Berater des Erstgesprächs eingetragen. Dies soll der internen Kontrolle dienen, ob und mit wem ein erstes Beratungsgespräch stattgefunden hat. Dies hilft u.a. bei Auskünften, die aufgrund telefonischer Nachfrage an die Klienten zu geben sind, etwa zu vereinbarten Terminen u.ä. Auf diese Weise läßt sich auch feststellen, wer für den Betroffenen Ansprechperson in der Beratungsstelle ist. Allerdings ist darauf zu achten, daß diese Terminbücher nicht unbegrenzt aufbewahrt werden dürfen.

6.3.4.2
Klientenkartei

In größeren Kommunen sind oft mehrere Beratungsstellen vorhanden, die meist für bestimmte Gebiete regional zuständig sind. Hier ist es grundsätzlich zulässig, in einer zentralen Kartei den Namen und die Tatsache des Erstkontaktes festzuhalten. Dies kann jedoch nur erfolgen, wenn die Bürger darüber informiert sind. Wenn dann, etwa durch einen Umzug, später eine andere Beratungsstelle zuständig wird, hat diese damit die Möglichkeit zu erfahren, daß schon vom Beratungsangebot Gebrauch gemacht wurde. Ein Austausch zwischen dem damaligen und dem späteren Betreuer über den Fall ist jedoch auch dann nur mit ausdrücklicher Zustimmung des Betroffenen möglich.

Solche Unterlagen können jedoch nicht von Dritten benutzt werden, etwa vom externen Abteilungsleiter im Jugendamt. Er dürfte z.B. die Kartei nicht als Hilfsmittel zum Heraussuchen von Akten verwenden, da ihm ein Einsichtsrecht in diese Beratungsakten gerade nicht zusteht.

6.3.4.3
Aktenführung durch die Berater

Die Unterlagen, die zur Organisation der Beratungsstelle, sowie die Informationen, die im Rahmen der Mitwirkungspflichten notwendig sind, sind strikt zu trennen von allen Unterlagen, die der Berater für sich als Hilfe im Beratungsprozeß erstellt. Die Aufzeichnungen, die sich der einzelne Berater über Abläufe und Entwicklungen des Beratungsprozesses macht, dürfen nur ihm zugänglich sein. Dazu ist es notwendig, daß ihm die Beratungsstelle eine Gelegenheit gibt, solche Unterlagen so aufzubewahren, daß sie vor dem Zugriff anderer Personen geschützt sind. Diese Beratungsunterlagen sind nicht ohne ausdrückliche Zustimmung des Betroffenen anderen Beratern, etwa im Vertretungsfall, zugänglich. Sie müssen deutlich kürzer als sonstige Verwaltungsunterlagen aufbewahrt und dürfen nicht mit diesen vermischt werden.

6.3.5
Fachliche Beratung der Mitarbeiter

Die Mitarbeiter müssen aus der Schweigepflicht auch Konsequenzen für ihren Umgang mit Kollegen und Vorgesetzten ziehen. Genausowenig wie der Vorgesetzte von sich aus Einblick in die Beratungsakten nehmen darf, ist es dem Berater erlaubt, in Fällen, in denen er von sich aus meint, eine Unterstützung zu benötigen, diese "zur Entscheidung" dem Vorgesetzten vorzulegen. Fachliche Unterstützung zur weiteren Gestaltung des Beratungsverlaufs

kann er sich sowohl beim Vorgesetzten als auch bei Kollegen, die nicht selbst mit dem Fall befaßt sind, in anonymisierter Form holen. Wo dies aus fachlichen Gesichtspunkten als nicht ausreichend erscheint, muß der Berater mit dem Klienten klären, ob er für diesen Zweck die Schweigepflicht aufheben darf.

6.3.6
Gebührenabrechnung für therapeutische Behandlung

Bei einigen Erziehungsberatungsstellen müssen sich die Eltern mit bestimmten Beträgen an den Kosten für die Therapiestunden beteiligen. Die Abrechnung der zu erbringenden Eigenleistung erfolgt über die Amtskasse. Dazu sind Name, Geburtsdatum, die pro Monat geleisteten Behandlungsstunden sowie die Anschriften der Eltern an die Amtskasse weiterzuleiten.

Ein solches Abrechnungsverfahren ist grundsätzlich zulässig. Die Therapie im Rahmen der Beratungsstelle ist für den Bürger kostenpflichtig. Soweit ein Bürger eine kostenpflichtige Leistung der Verwaltung in Anspruch nimmt, ergibt sich zwangsläufig die Folge, daß für die Abrechnung dieser Leistung Daten verarbeitet werden müssen. Eine Verletzung der Schweigepflicht bzw. des Vertrauensschutzes aus § 65 SGB VIII wäre nur dann gegeben, wenn keine Befugnis zur Weitergabe der für die Abrechnungszwecke benötigten Daten vorhanden wäre. Eine solche ist jedoch gegeben, wenn die betroffenen Bürger vor Aufnahme der Therapie über die Organisation des Abrechnungsverfahrens informiert werden und somit entscheiden können, ob sie unter diesen Voraussetzungen die Leistungen in Anspruch nehmen wollen. Mit der Erklärung, die Therapie beginnen zu wollen, ist dann auch das Einverständnis in dieses Abrechnungsverfahren verknüpft. Dabei muß sichergestellt sein, daß der Umfang der dafür verwendeten Daten auf das notwendige Maß beschränkt wird und auch nur diejenigen Stellen innerhalb der Verwaltung Zugang zu diesen Daten haben, die diese für ihre Aufgabenerfüllung wirklich benötigen.

6.3.7
Arbeitsnachweis für Honorarkräfte

Mitunter arbeiten in den Beratungsstellen stundenweise Honorarkräfte mit besonderer Qualifikation. Für diese Beschäftigten ist es erforderlich, daß der Umfang ihrer Tätigkeit der Stelle innerhalb der Kommunalverwaltung mitgeteilt wird, die für die Abrechnung des Honorars zuständig ist. Diese Abrechnungsnachweise dürfen jedoch keine personenbezogenen Klientendaten enthalten. Dies widerspräche dem Grundsatz, daß schon allein die Tatsache, daß eine solche Beratungsstelle aufgesucht wird, der Schweigepflicht bzw. dem besonderen Vertrauensschutz unterliegt. Für die Abrechnungszwecke der Honorarkräfte sind Aufstellungen von Art und Umfang der Tätigkeit pro Arbeitstag ausreichend, die für die beratenen Klienten eine Kennziffer enthalten. Den berechtigten Forderungen der Rechnungsprüfung kann dann auch dadurch nachgekommen werden, daß in der Beratungsstelle Unterlagen vorhanden sind, aus denen nachvollziehbar ist, wer behandelt worden ist. Weiter gehen die Rechte auch der Rechnungsprüfung jedoch nicht. Die Beratungsunterlagen dürfen auch in diesem Zusammenhang nicht zu Zwecken der Rechnungsprüfung eingesehen werden.

7. Beteiligung des Hessischen Datenschutzbeauftragten bei der Einführung automatisierter Personaldatenverarbeitung (§ 34 Abs. 5 HDSG)

Nachdem seit nunmehr 5 Jahren alle hessischen öffentlichen Stellen gemäß § 34 Abs. 5 HDSG verpflichtet sind, vor der Einführung, Anwendung, Änderung oder Erweiterung einer automatisierten Verarbeitung von Beschäftigtendaten dem Hessischen Datenschutzbeauftragten Gelegenheit zur Stellungnahme zu geben, ist eine Bilanz aus den vielfältigen Erfahrungen, die in dieser Zeit mit der Anwendung der Vorschrift gesammelt werden konnten, angebracht.

Ohne Zweifel sind die von mir durchgeführten präventiven Überprüfungen der Automationsmaßnahmen im Bereich der Personaldatenverarbeitung eine erhebliche Hilfe für die datenverarbeitenden Stellen, aber auch für die Personalräte, die dadurch eine bessere Informationsbasis für die Wahrnehmung ihrer Mitbestimmungsrechte bei der Einführung von technischen Einrichtungen, mit denen eine Verhaltens- oder Leistungskontrolle möglich ist (§ 74 Abs. 1 Nr. 17 Hessisches Personalvertretungsgesetz – HPVG), und bei der Einführung der automatisierten Verarbeitung personenbezogener Daten der Beschäftigten (§ 81 Abs. 1 HPVG) erhalten.

Die Probleme, die sich in der Praxis ergeben haben, betreffen zum einen den Anwendungsbereich der Vorschrift, da der Wortlaut jegliche automatisierte Verarbeitung von Beschäftigtendaten erfaßt. Zum anderen häufen sich durch den verstärkten Einsatz von Personalcomputern die Verfahren, bei denen Beschäftigtendaten automatisiert verarbeitet werden, und oft wird ein und dasselbe Verfahren in einer Vielzahl von Behörden eingesetzt.

Probleme resultieren auch daraus, daß mir in vielen Fällen nicht die für eine Beurteilung notwendigen Unterlagen oder nur unstrukturierte Materialien vorgelegt werden. Dadurch entsteht oft eine erhebliche Belastung durch die erforderliche Sichtung des Materials. Ausgangspunkt der Beurteilung ist gemäß § 34 Abs. 5 HDSG die Dateibeschreibung nach § 6 HDSG. Sie reicht jedoch zum Teil nicht aus, da aus den geforderten Angaben, vor allem wenn das Registermeldeformular verwendet wird, der Verwendungszusammenhang nicht immer eindeutig hervorgeht. Gerade dies kann aber für die Zulässigkeit der Verarbeitung von Beschäftigtendaten in einzelnen Verfahren von entscheidender Bedeutung sein.

Es gibt zwei Schwerpunkte bei der Beurteilung: die Zulässigkeit der konkreten Verarbeitung i.S. des § 34 Abs. 1 HDSG einschließlich der vorgesehenen Auswertungen bzw. deren Verwendung, sowie die Realisierung eines angemessenen Datenschutzkonzeptes. Für die Überprüfung solcher Konzepte bzw. der getroffenen Datensicherungsmaßnahmen ist ein Herstellerprospekt in der Regel wenig hilfreich. Andererseits aber sind die häufig vorgelegten kompletten Programmdokumentationen oder Anwendungshandbücher in der Regel viel zu umfangreich und erfordern einen erheblichen Aufwand bei der Feststellung der in diesem Zusammenhang wichtigen Einzelpunkte.

7.1
Regelungsziel des § 34 Abs. 5 HDSG

Eine Bilanz muß in erster Linie eine Antwort auf die Frage geben, ob derzeit das ursprüngliche Ziel der Regelung des § 34 Abs. 5 HDSG errreicht wird.

In der Begründung zum Gesetzentwurf (Landtags-Drucksache 11/4749, S. 36) heißt es: "Die automatisierte Verarbeitung von Daten von Beschäftigten birgt besondere Gefahren für das Persönlichkeitsrecht in sich, deren Beurteilung einen besonderen Sachverstand voraussetzt. Daher müssen alle Stellen innerhalb und außerhalb der Verwaltung, bei denen die erforderlichen Kenntnisse vorhanden sind, in den Entscheidungsprozeß einbezogen werden." Zwei Punkte sind daraus hervorzuheben: "die besonderen Gefahren für das Persönlichkeitsrecht" und der notwendige "besondere Sachverstand" für deren Beurteilung. Die Regelung knüpft damit an die ausführlichen Diskussionen an, die zur automatisierten Datenverarbeitung insgesamt und die notwendigen personalvertretungsrechtlichen Beteiligungsmöglichkeiten, vor allem bei der Einführung von Personalinformationssystemen, geführt wurden.

Die automatisierte Datenverarbeitung erleichtert die Möglichkeiten des Dienstherrn, auf die bei ihm vorhandenen Beschäftigtendaten zu unterschiedlichen Zwecken zuzugreifen, erheblich. Bei der automatisierten Speicherung bleiben Pauschalierungen – etwa durch vorgegebene Schlüssel – für einen bestimmten Sachverhalt nicht aus. Andererseits steigt die Gefahr des Kontextverlustes und einer gegebenenfalls falschen Bewertung einzelner Tatsachen bei späteren Auswertungen in anderen Zusammenhängen. Die Kontrolle der Verwendungszwecke bzw. Auswertungen, z.B. bei Datenbanken mit freien Abfragesprachen, wird erschwert. Allerdings handelte es sich bei der Mehrzahl der Verfahren, die bis jetzt vorgelegt worden sind, gerade nicht um solche umfassenden Projekte, die im eigentlichen Sinne als Personalinformationssystem einzustufen wären. Das zeigt sich auch an der datenschutzrechtlichen Kritik, die zu den einzelnen Verfahren anzumerken war. Vielfach gab es kein ausreichendes organisatorisches Datensicherungskonzept. Dies ist kein spezifisches Problem der Personaldatenverarbeitung. Soweit sich die Bedenken auf die Zulässigkeit oder den Umfang der Verarbeitung einzelner Daten bezogen, ergaben sie sich in der Regel auch nicht aus der automatisierten Verarbeitung, sondern bereits die manuelle Verarbeitung dieser Daten in Akten, Listen usw. war nicht rechtmäßig. Es bietet sich daher an, bei der Entscheidung über die Notwendigkeit eines Stellungnahmeverfahrens nach Verfahrenstypen bei der Verarbeitung von Personaldaten zu differenzieren.

7.2
Verfahrenstypen

7.2.1
Neuentwicklungen für die Personalverwaltung

Es steht außer Frage, daß umfangreiche Verfahren, z.B. zur Organisation der Personalverwaltung, vorab für eine entsprechende Begutachtung mir vorzulegen sind. In letzter Zeit betraf dies zum Beispiel die Reorganisation der Lehrerdatenverarbeitung (vgl. 18. Tätigkeitsbericht Ziff. 9.13) sowie die Automatisierung der Personalverwaltung beim Regierungspräsidium Darmstadt, die als Pilotprojekt für die hessische Landesverwaltung entwickelt wird. Dazu gehören aber auch Vorhaben der Büroautomation (Bürokommunikation), die die Arbeitsabläufe in einer Personalverwaltung reorganisieren sollen.

7.2.2
Einsatz von landesweiten Verfahren

Ein wiederholtes Stellungnahmeverfahren erscheint mir jedoch dann entbehrlich, wenn ein von vielen Anwendern genutztes und zentral entwickeltes Verfahren – wie z.B. das Gehaltsabrechnungsprogramm HESPA – von einem neuen Anwender genutzt werden soll. Wichtig ist hierbei, daß sichergestellt sein muß, daß durch den jeweiligen Anwender keine wesentlichen Änderungen des Verfahrens möglich sind. Außerdem müssen dem Anwender ausreichende Anleitungen für ein Datenschutzkonzept zur Verfügung gestellt werden. Diese können auch für den Personalrat nützlich sein und sind zudem Grundlage der Beurteilung der verwirklichten technischen und organisatorischen Datensicherungsmaßnahmen gemäß § 10 HDSG bei der Überprüfung der Registermeldung.

7.2.3
Verfahrensentwicklung für eine Vielzahl von Anwendern

Eine Vereinfachung des Verfahrensablaufes, auch im Interesse der Bewältigung einer Vielzahl von Verfahren, ist in den Fällen möglich, in denen eine Stelle für viele Anwender neue Verfahren entwickelt. Dies gilt z.B., wenn das

Hessische Institut für Bildungsplanung und Schulentwicklung (HIBS) Verfahren für den Einsatz an Schulen entwickelt. Eine rechtzeitige Einbeziehung meiner Dienststelle bei der zentralen Verfahrensentwicklung und (soweit erforderlich) eine Überprüfung der Realisierung vor Ort im Zusammenhang mit der Registermeldung können den Zweck des 34 Abs. 5 HDSG adäquat erfüllen.

7.2.4
Automatisierte Verarbeitung zur Organisation der Abläufe der Personalverwaltung

Es gibt eine Vielzahl von Verfahren, in denen (auch) Beschäftigtendaten verarbeitet werden, ohne daß dadurch besondere Gefahren für das Persönlichkeitsrecht der Betroffenen entstehen.

Ein formales Stellungnahmeverfahren halte ich im Regelfall dann für verzichtbar, wenn nur wenige Stammdaten für einen genau eingrenzbaren Zweck verarbeitet werden sollen. Dies gilt etwa für die Organisation einzelner Abläufe in der Personalabteilung oder der Dienststelle insgesamt oder die Abwicklung von Kassengeschäften, wie z.B. die Auszahlung von Reisekosten. In diesen Fällen kann in der Regel davon ausgegangen werden, daß der Sachverstand zur Beurteilung der Zulässigkeit der Verwendung dieser Daten für den jeweils angegebenen Zweck bei den datenverarbeitenden Stellen und den Personalvertretungen vorhanden ist. Nach meinen derzeitigen Erfahrungen kommt etwa folgender Datenkatalog in Betracht: Name, Anschrift, Zimmernummer, dienstliche Rufnummer, Amtsbezeichnung, Zuständigkeit, Bankverbindung.

Das schließt nicht aus, daß im Einzelfall ein Personalrat ausdrücklich um die Einholung einer Stellungnahme bittet, etwa weil die technische Umsetzung sehr komplex ist. Dann ist auch entsprechend zu verfahren. Bevor die Stellungnahme vorliegt, hat der Personalrat nicht alle erforderlichen Unterlagen i.S. des § 62 HPVG erhalten, so daß ihm auch eine Entscheidung noch nicht abverlangt werden kann.

7.2.5
Verwendung von Personaldaten bei der Organisation anderer Verwaltungsverfahren

Zu Zwecken der Organisation des Verwaltungsablaufs (etwa zur Zuordnung von Vorgängen), aber auch als Serviceleistung für den Bürger werden häufig einige wenige Daten als Bearbeiterkennzeichen verwendet: Name, Amtsbezeichnung, Rufnummer, Zimmernummer. Die Darstellung erfolgt in unterschiedlicher Form, zum Teil als Kürzel zur Kennzeichnung eines Vorgangs im Bürokommunikationssystem, zum Teil im Anschreiben an den Bürger, um den zuständigen Ansprechpartner zu benennen. Häufig ist sie in großen Anwendungsprogrammen eingebunden – z.B. beim automatisierten Baugenehmigungsverfahren.

Auch hier ist die Frage der Zulässigkeit der Verwendung dieser Daten für die angegebenen Zwecke leicht zu entscheiden, so daß zusätzlicher Sachverstand zur Unterstützung der datenverarbeitenden Stellen und der Personalräte nicht erforderlich ist. Probleme könnten sich im Einzelfall aus der technischen Realisierung des Gesamtverfahrens ergeben. Denn selbstverständlich gilt auch hier die Zweckbindung, mit der Folge, daß etwa Auswertungen dahingehend – wie schnell arbeitet ein Mitarbeiter, wie oft wird gegen von ihm vorbereitete Bescheide Widerspruch eingelegt und ähnliches – unzulässig sind. Soweit dann aufgrund der besonderen Umstände bzw. der Komplexität des Verfahrens zusätzlicher Sachverstand nötig erscheint, empfiehlt sich auch hier ein Stellungnahmeverfahren.

7.3
Personaldatenverarbeitung im Rahmen der technischen und organisatorischen Maßnahmen zum § 10 HDSG

Kein Stellungnahmeverfahren nach § 34 Abs. 5 HDSG ist erforderlich, wenn Daten der Beschäftigten nicht zur Organisation des Beschäftigungsverhältnisses oder zur Durchführung innerdienstlicher Maßnahmen verwendet werden. Dies gilt vor all em für die Daten, die im Rahmen der technischen und organisatorischen Maßnamen nach § 10 HDSG gespeichert werden, also z.B. für die Protokolldaten oder Tabellen mit der Festlegung von Zugriffsrechten für einzelne Nutzer einer DV-Anlage. Faktisch sind diese Daten zur Kontrolle der Beschäftigten geeignet. Der hier auftretende Gegensatz zwischen den gesetzlichen Anforderungen des § 10 HDSG, die der Sicherstellung der Grundrechte der Betroffenen dienen, deren Daten mit dem jeweiligen Verfahren bearbeitet werden, und den berechtigten Interessen der Beschäftigten, die diese Daten verarbeiten, läßt sich nicht zugunsten einer Seite auflösen. Das Verbot, solche Daten zur Verhaltens- und Leistungskontrolle zu nutzen, das § 34 Abs. 7 HDSG enthält, entschärft diesen Konflikt auch nur teilweise. Nach § 10 HDSG ist zu entscheiden, welche konkreten Maßnahmen jeweils erforderlich sind. Dabei ist im Rahmen der Verhältnismäßigkeitsabwägung auch das Interesse der betroffenen Beschäftigten zu berücksichtigen.

8. Hochschulen und Bibliotheken

8.1
Prüfung der Datenverarbeitung des Fachbereichs Wirtschaftswissenschaften der Frankfurter Universität

1991 habe ich eine bereits Ende des vorangegangenen Jahres begonnene Prüfung der Datenverarbeitung des Fachbereichs Wirtschaftswissenschaften der Frankfurter Universität abgeschlossen. Der Fachbereich war ausgewählt

worden, weil er mit ca. 5.800 Studenten, 96 wissenschaftlichen Mitarbeitern und 50 Professoren der größte der Universität Frankfurt ist und seine Datenverarbeitung im Verwaltungsbereich in stärkerem Maße als andere Fachbereiche automatisiert hat. Geprüft wurden sowohl das Dekanat als auch das Prüfungsamt. Von den festgestellten Mängeln dürften die folgenden durchaus repräsentativ für andere Fachbereiche an der Universität Frankfurt oder anderer hessischer Universitäten sein.

8.1.1
Dekanat

8.1.1.1
Studentendatenverarbeitung

Das Dekanat verarbeitet nur in relativ geringem Umfang personenbezogene Studentendaten. Außer bei Beschwerden und Eingaben von Studenten sowie Studentenaustauschprogrammen hat es keinen Anlaß, Studentendaten in personenbezogener Form zu verarbeiten. Bis auf die haushaltstechnische Abwicklung der Stipendien erfolgt die gesamte Studentendatenverarbeitung in Sachakten. Zu monieren war, daß die Unterlagen zum Teil zu lange aufbewahrt wurden. Nach dem Hessischen Archivgesetz (§ 10 Abs. 1) müssen Materialien, die zur Aufgabenerfüllung nicht mehr erforderlich sind, unverzüglich ausgesondert und dem zuständigen Archiv zur Übernahme angeboten werden.

8.1.1.2
Datenverarbeitung im Rahmen des Promotionsverfahrens

Öffentliche Stellen dürfen personenbezogene Daten nur verarbeiten, wenn dies zur Aufgabenerfüllung und für einen damit verbunden Zweck erforderlich ist. Die Datenverarbeitung im Promotionsverfahren entsprach nicht in allen Punkten diesem Erforderlichkeitsgrundsatz des Hessischen Datenschutzgesetzes. So müssen nach der Promotionsordnung des Fachbereichs die Bewerber ein Reifezeugnis vorlegen. In der Mehrzahl der Fälle dürfte das jedoch nicht nötig sein, sondern allenfalls, wenn bei ausländischen Bewerbern die Gleichwertigkeit der Vorbildung zweifelhaft ist.

Die Promotionsordnung verlangt außerdem die Vorlage eines polizeilichen Führungszeugnisses oder eines von der Universität ausgestellten Leumundszeugnisses. Abgesehen davon, daß unklar blieb, was die Universität in dem Leumundszeugnis bestätigen sollte, ist auch nach Auffassung des Dekanats weder das eine noch das andere Zeugnis für die Durchführung des Promotionsverfahrens erforderlich.

Die Pflichtexemplare der Dissertationen enthielten im Anhang einen Lebenslauf des Doktoranden. Die Beschreibungen waren weder nach Form noch nach Umfang einheitlich. In der Promotionsordnung des Fachbereichs findet sich keine Bestimmung zum Lebenslauf in den Pflichtexemplaren der Dissertationen. Eine Regelung, die zwingend vorschreibt, daß die Doktoranden ihren Lebenslauf in den zur Veröffentlichung bestimmten Pflichtexemplaren darstellen müssen, wäre nicht zulässig, da sie gegen den Erforderlichkeitsgrundsatz des höherrangigen Datenschutzgesetzes verstoßen würde. Das HDSG versteht unter Datenverarbeitung jede Verwendung gespeicherter oder zur Speicherung vorgesehener personenbezogener Daten. Die Universität veröffentlicht in den Pflichtexemplaren der Dissertation den Lebenslauf des Doktoranden und verarbeitet damit dessen personenbezogene Daten. Als Zweck der Dissertation definiert die Prüfungsordnung des Fachbereichs Wirtschaftswissenschaften den Nachweis einer wissenschaftlichen Leistung und der Fähigkeit des Bewerbers zur selbständigen wissenschaftlichen Arbeit. Es ist nicht zu erkennen, daß zur Erfüllung dieses Zwecks die Veröffentlichung des Lebenslaufs des betroffenen Doktoranden erforderlich sein könnte.

Für die Durchführung des Promotionsverfahrens ist die Aufnahme des Lebenslaufs in die Pflichtexemplare ebenfalls nicht erforderlich, denn nach der Promotionsordnung muß bereits dem Gesuch auf Zulassung zur Promotion ein Lebenslauf einschließlich einer Beschreibung des Bildungsgangs beigefügt werden. Die Prüfer können sich somit aus der Prüfungsakte über den Lebenslauf und beruflichen Werdegang des Doktoranden informieren.

Auch die Voraussetzungen des § 16 Abs. 1 HDSG sind nicht erfüllt. Danach dürfen öffentliche Stellen zwar unabhängig von ihrer Aufgabenerfüllung privaten Dritten personenbezogene Daten übermitteln, wenn die Empfänger ein berechtigtes Interesse an der Kenntnis der Daten haben. Es dürfen jedoch keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange der Betroffenen beeinträchtigt werden können. Selbst wenn man von einem berechtigten Interesse der Leser der Dissertation ausgeht, den Lebenslauf zu erfahren, ist zumindest die zweite Voraussetzung hier nicht erfüllt. Das zeigen insbesondere auch Beschwerden, die ich von Doktoranden gegen die in manchen Promotionsordnungen vorgesehene Verpflichtung zur Veröffentlichung ihres Lebenslaufs erhalten habe.

Der Lebenslauf darf deshalb in den Pflichtexemplaren der Dissertation nur mit ausdrücklicher Einwilligung des Doktoranden veröffentlicht werden.

8.1.1.3
Personaldatenverarbeitung

8.1.1.3.1
Akten über das Lehrpersonal und die Dekanatsmitarbeiter

Für jede Person, die seit Gründung der Universität am Fachbereich gelehrt hat, war im Dekanat eine Akte vorhanden. Darin waren enthalten: Kopien des Schriftverkehrs mit den Betroffenen im Rahmen des Berufungsverfahrens, alle Vorgänge zu Bleibeverhandlungen, Änderungen der Lehrstuhlausstattungen, Angaben über die Zuteilung von Mitteln usw. Das Dekanat sah in der Aktensammlung eine notwendige Dokumentation der Geschichte des Fachbereichs. Die Unterlagen wurden außerdem zur Vorbereitung von Jubiläumsveranstaltungen und zur Information des Dekans bei Ehrungen verwendet. Mitunter wurde aus den Materialien auch die Entwicklung eines Lehrstuhls (Stiftungsprofessur, Mittelausstattung etc.) rekonstruiert und als Grundlage für Verhandlungen mit dem Wissenschaftsministerium über die Weiterentwicklung des Fachbereichs oder zur Vorbereitung von Haushaltsverhandlungen verwertet.
Die Akten über die Dekanatsmitarbeiter enthielten den in Personalangelegenheiten geführten Schriftwechsel zwischen Dekanat, Präsidialabteilung und Mitarbeitern. Diese Unterlagen wurden nach dem Ausscheiden der Betroffenen noch 15 Jahre im Dekanat aufbewahrt.

Auch die Aufbewahrung der Personalunterlagen durch ein Dekanat muß sich am Erforderlichkeitsgrundsatz des Hessischen Datenschutzgesetzes und den Aussonderungs- und Abgabebestimmungen des Hessischen Archivgesetzes orientieren. Solange die Betroffenen noch am Fachbereich bzw. im Dekanat tätig sind, ergeben sich keine Probleme. Fraglich ist lediglich, wie lange das Dekanat die Unterlagen nach dem Ausscheiden der Betroffenen aus dem Hochschuldienst noch aufbewahren darf.

Im vorliegenden Fall wurden mit der unbegrenzten Aufbewahrung der Akten der Lehrenden unterschiedliche Zwecke verfolgt. Für eine Aufbewahrung der Unterlagen zu wissenschaftshistorischen Zwecken im Dekanat (um die Geschichte des Fachbereichs nachzeichnen zu können) gibt es keine Rechtsgrundlage.

Für Verwaltungszwecke dürfen die Daten allerdings solange aufbewahrt werden, wie dies u.a. zur Abwicklung des Dienstverhältnisses oder zur Durchführung innerdienstlicher organisatorischer und personeller Maßnahmen erforderlich ist (§ 34 Abs. 1 HDSG). Nr. 11.1 der Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes vom 20. 10. 1986 (StAnz 1986 S. 2107) schreibt für Personalakten eine Aufbewahrungsdauer von fünf Jahren nach Ablauf des 65. Lebensjahres des Beamten bzw. von fünf Jahren nach Ablauf des Todestages des Betroffenen vor. Da der Erlaß für die Selbstverwaltungskörperschaft Universität nicht bindend ist, sondern nur empfehlenden Charakter hat, können für ein Dekanat durchaus andere – auch längere – Fristen in Betracht kommen. Das Dekanat darf die Unterlagen jedoch nicht zeitlich unbegrenzt aufbewahren. Es muß festlegen, in welchem Umfang und wielange die Akten über ausgeschiedene Hochschullehrer für Verwaltungszwecke des Dekanats zur Verfügung stehen sollen.

Eine 15jährige Aufbewahrungsfrist für Akten über Dekanatsmitarbeiter ist erheblich zu lang.

8.1.1.3.2
Telefonabrechnungen

Der Büroleiter bewahrte alle Einzelgesprächsnachweise der Telefonapparate des Dekanats in einem Ordner auf. Das entsprach nicht den Nrn. 6.6.4 und 6.6.5 der Fernsprechvorschriften für die Verwaltung des Landes Hessen vom 3. März 1986 (StAnz 1986 S. 720). Danach müssen die Nachweise den Nebenstelleninhabern ausgehändigt werden, wenn die Stichprobenkontrolle keinen Anlaß zur näheren Überprüfung ergibt. Die Nachweise für Privatgespräche erhält er direkt in einem verschlossenen Umschlag. Nutzen mehrere einen Apparat, so ist ein Verfahren festzulegen, wie die Betroffenen intern die Verteilung bzw. Begleichung der Gebühren vorzunehmen haben.

Für die Abrechnung und Haushaltsüberwachung usw. reichen Summenlisten mit den im Bereich des Dekanats angefallenen Gebühren. Die Einzelgesprächsnachweise waren daher zu vernichten.

8.1.1.3.3
Urlaubsliste

In einer Urlaubsliste notierte der Büroleiter die jeweils gewährten Urlaubstage der Mitarbeiter im Dekanat. Die aufgezeichneten Daten erfaßten mehrere Jahre, bis das DIN-A-4-Blatt gefüllt war.

Ein solches Verfahren ist unzulässig. Beschäftigtendaten, die für die Aufgabenerfüllung der speichernden Stellen nicht mehr erforderlich sind, müssen grundsätzlich dem Universitätsarchiv angeboten und, wenn dieses die Übernahme ablehnt, vernichtet werden (§ 10 Abs. 1 und 2 Hessisches Archivgesetz, § 34 Abs. 4 Hessisches Datenschutzgesetz). Nach Ablauf des Urlaubsjahres genügt die Feststellung der verbleibenden bzw. zu übertragenden Resttage. Die Aufzeichnungen über die jeweils gewährten Urlaubstage werden dagegen, nachdem die Richtigkeit der Abrechnung mit den betroffenen Mitarbeitern festgestellt worden ist, nicht mehr benötigt. Vermutlich wird auch das Universitätsarchiv kein Interesse an der Übernahme dieser Unterlagen haben, so daß sie vernichtet werden müßten. Diese Entscheidung trifft allerdings das Archiv.

Ich habe deshalb gefordert, die Aufzeichnungen über die gewährten Urlaubstage künftig in einer Form vorzunehmen, die eine regelmäßige Aussonderung zum Ende des Urlaubsjahres ermöglicht.

8.1.1.4
Datensicherheit bei der automatisierten Datenverarbeitung

Im Bereich des Dekanats waren drei PCs im Einsatz, die alle für Textverarbeitung genutzt wurden. Auf keinem der PCs existierten Produkte, mit denen Datenschutzmaßnahmen vorgenommen werden konnten. Es gab auch keine Regelungen, nach denen sich die Mitarbeiter richten konnten, um selbst entsprechende Maßnahmen vorzunehmen.

Mit dem ersten PC wurden nur auf Disketten gespeicherte personenbezogene Daten verarbeitet. Die Disketten wurden in einem Stahlschrank aufbewahrt. Auf der Festplatte befanden sich zwar keine personenbezogenen Daten, dafür aber die Utility PC-Tools.

Auf dem zweiten PC befanden sich auf der Festplatte ungeschützt diverse Schreiben und Sitzungsprotokolle mit personenbezogenen Angaben. Außerdem existierte ein Directory, in dem ohne Wissen der Dekanatsleitung nur Spiele gespeichert waren. Die Gefahr besteht darin, daß Spielprogramme oft unkontrolliert kopiert oder verändert werden und deshalb häufig mit Programmviren "infiziert" sind. Das vorgefundene Spiel "Larry" fällt in diese Kategorie. Es gibt Berichte über Fälle, in denen bei diesem Spiel nach Erreichen einer bestimmten Punktzahl die Festplatte gelöscht worden sein soll.

Auch auf dem dritten PC waren auf der Festplatte einige Adreßlisten und Schreiben ungeschützt gespeichert.

Ferner kam es etwa zweimal im Monat vor, daß ein Tutor, der in keinem Terminalraum der Universität einen freien Bildschirm gefunden hatte, auf einem der PCs arbeitete. Über einen Akustikkoppler und die Kommunikationssoftware "Kermit" wurde mit dem Rechner der Fernuniversität Hagen eine Verbindung aufgebaut, um Übungen für Fernstudiengänge zu bearbeiten. Während dieser Zeiten waren weder der zuständige Sachbearbeiter noch ein anderer Mitarbeiter des Dekanats im Raum anwesend.

Aus den getroffenen Feststellungen ergaben sich folgende Forderungen:

1. Die personenbezogenen Daten auf den PCs sind gegen unberechtigte Zugriffe zu schützen. Bei der Planung der Datenschutzmaßnahmen ist auch der Einsatz einer Datenschutzsoftware zu prüfen. Zwar kann eine Speicherung personenbezogener Daten auf Disketten mit den entsprechenden organisatorischen Schutzmaßnahmen (Aufbewahrung in Safes, physisches Löschen usw.) bei einigen Anwendungen eine praktikable Lösung sein. Es ergibt sich jedoch bei neuen Anwendungen immer die Frage, ob diese Maßnahme ausreicht und durchführbar ist. Sollte dies zu verneinen sein, kann in vielen Fällen durch eine Datenschutzsoftware ein adäquater Sicherheitsstandard geschaffen werden. Im Regelfall ist daher eine Datenschutzsoftware einzusetzen.

2. Utilities wie PC-Tools dürfen normalen Nutzern nicht zugänglich sein, sondern nur dem Systemverwalter auf Disketten zur Verfügung stehen.

3. Die Spiele sind umgehend zu löschen.

4. Dekanatsfremde Personen dürfen die Rechner nicht benutzen.

5. Art und Umfang der Datenverarbeitung müssen geregelt werden. Hierzu gehört auch eine Dienstanweisung mit folgenden Punkten:

   - welche Software eingesetzt werden darf (Verbot von nicht freigegebener Software)
   - Regelungen zur Sicherstellung der Maßnahmen nach § 10 HDSG
   - Datensicherung
   - Datenträgerverwaltung
   - Dokumentation (Verfahrensverzeichnis)
   - Löschvorschriften (Art und Weise; Fristen)
   - Regelungen zu den Funktionen Systemverwaltung, Revision (Kontrollinstanz), Anwendungsentwicklung (falls vorhanden).

8.1.1.5
Reaktion des Dekans

Das Dekanat zeigte sich sehr kooperativ und offen für meine Hinweise und Anregungen. In seiner Stellungnahme vom August 1991 teilte mir der Dekan mit, daß die meisten der von mir aufgezeigten Mängel beseitigt worden seien oder demnächst behoben würden. So wird z.B. künftig im Promotionsverfahren im Regelfall (d.h. Bewerber besitzen ein Diplom einer deutschen wissenschaftlichen Hochschule) auf die Vorlage eines Reifezeugnisses verzichtet, ebenso wird kein polizeiliches Führungszeugnis oder Leumundszeugnis mehr verlangt. Für alle PCs wird eine Datenschutzsoftware beschafft. Die Akten über die Dekanatsmitarbeiter werden fünf Jahre nach dem Ausscheiden der Betroffenen ausgesondert und dem Universitätsarchiv zur Übernahme angeboten.

In diesem Zusammenhang muß allerdings erwähnt werden, daß es ein den Anforderungen des Hessischen Archivgesetzes entsprechendes Archiv an der Universität Frankfurt noch nicht gibt. Da das Archivgesetz mittlerweile mehr als zwei Jahre in Kraft ist, kann die Einrichtung eines gesetzeskonformen Archivs nicht mehr länger hinausgeschoben werden, sonst muß die Universität ihre Unterlagen dem Hessischen Staatsarchiv anbieten. Dies ist allerdings keine Aufgabe des Fachbereichs, sondern der zentralen Universitätsverwaltung.

Lediglich die vom Dekan für die Veröffentlichung des Lebenslaufs in den Pflichtexemplaren der Dissertation vorgeschlagene Regelung in der Promotionsordnung ist noch korrekturbedürftig. Der Entwurf des Dekans sieht eine Pflicht zur Veröffentlichung des Lebenslaufs vor, von der der Doktorand nur auf Antrag befreit werden kann. Das Hessische Datenschutzgesetz erfordert jedoch die umgekehrte Regelung: Der Lebenslauf darf nur mit Einwilligung des Doktoranden in die Pflichtexemplare aufgenommen werden.

8.1.2
Prüfung der Datenverarbeitung des Prüfungsamtes des Fachbereichs Wirtschaftswissenschaften

Erwähnenswert ist zunächst, daß als Ergebnis der Prüfung künftig bei der Anmeldung zur Zwischenprüfung, zur Diplomarbeit und zum Examen kein Reifezeugnis mehr vorgelegt werden muß. Es bestand Konsens mit dem Prüfungsamt, daß die bisherige Praxis nicht mit dem Erforderlichkeitsprinzip des Hessischen Datenschutzgesetzes vereinbar ist.

Im Mittelpunkt der Prüfung der Datenverarbeitung des Prüfungsamtes stand jedoch die automatisierte Datenverarbeitung und dort wiederum das vom Fachbereich selbst entwickelte Prüfungsverwaltungssystem, dessen Entwicklung frühzeitig mit mir abgestimmt worden war.

Das Prüfungsamt verfügte zur Zeit der Prüfung über drei PCs und ein Terminal, das an das Hochschulrechenzentrum angeschlossen war. Alle PCs wurden im stand-alone Betrieb genutzt. Eine Vernetzung war nicht geplant.

8.1.2.1
Prüfungsverwaltungssystem (PVS)

8.1.2.1.1
Aufgaben des PVS

Das für einen Rechner mit dem Betriebssystem MS-DOS und der Datenbank-Software CONCEPT 16 entwickelte Prüfungsverwaltungssystem soll dem Prüfungsamt zur effektiveren Gestaltung seiner Arbeit einen leichteren und schnelleren Zugang zu den Prüfungsergebnissen und die automatisierte Erstellung der folgenden Listen und Bescheide ermöglichen:

Anmeldeliste
Teilnehmerliste
Notenliste
Leistungsbescheide
Liste der Rücktritte
Zwischenprüfungszeugnisse
Bescheide über nicht bestandene Prüfungen.

8.1.2.1.2
Gespeicherte Daten

Im PVS gab es zur Zeit der Prüfung eine Grundstudiumsdatei, eine Klausurdatei, eine Sekretariatsdatei und eine Archivdatei.

Ein Teil der im PVS gespeicherten Daten stammte vom Studentensekretariat, die übrigen Angaben hatte das Prüfungsamt selbst erhoben. Das Studentensekretariat lieferte regelmäßig auf einer Diskette Änderungen zur Grundstudiumsdatei. Aber auch das Prüfungsamt selbst änderte Daten in der Grundstudiumsdatei. In der Klausurdatei speicherte das Prüfungsamt die handschriftlich von den Professoren auf den Teilnehmerlisten vermerkten Noten. Zwei Mitarbeiter überprüften unabhängig voneinander die automatisiert gespeicherten Prüfungsergebnisse und die Belege auf Übereinstimmung.

Außer in der Klausurdatei, in der sich auch Klausurergebnisse von Studenten anderer Fachbereiche befanden, speicherte das Prüfungsamt nur Daten von Studenten des Fachbereichs Wirtschaftswissenschaften. Nach der Zwischenprüfung wurden die Prüfungsergebnisse aus der Klausurdatei in die Archivdatei übergeben. Die Löschung erfolgte fünf Semester nach der Zwischenprüfung.

8.1.2.1.3
Datenschutzmaßnahmen

Benutzerkontrolle:

Der für das PVS eingesetzte PC befand sich in einem abschließbaren Schreibtisch. Zum Zeitpunkt der Prüfung war der PC mit seinem Betriebsschloß abgeschlossen. Als Datenschutzsoftware war OCULIS-Plus in der aktuellen Version installiert. Bei einem Systemstart wurde die Eingabe eines Paßwortes durch OCULIS verlangt. Um dann die Anwendung selbst unter CONCEPT aufrufen zu können, mußte eine Benutzerkennung und das zugehörige Paßwort eingegeben werden. Von beiden Paßwörtern konnte der Benutzer das OCULIS-Paßwort selbst ändern. Es fehlte in der installierten Version jedoch ein Automatismus, der zeitgesteuert Paßwortveränderungen verlangt.

Zugriffskontrolle:

Sowohl OCULIS als auch die Datenbank CONCEPT 16 besaßen die Möglichkeit, den Benutzern Zugriffsrechte zu geben und diese zu kontrollieren. Es gab jedoch Probleme, die entsprechenden Sicherheitsmechanismen einzusetzen. Da CONCEPT 16 mit einem 'hidden'-Directory arbeitete, konnte ein OCULIS-Benutzer die Anwendung nur aufrufen, wenn er unter OCULIS die höchste Berechtigung besaß. Die Zugriffsrechte in der Anwendung waren hiervon unberührt. Diese Konstellation bedingte, daß jeder Benutzer auf der Betriebssystem-Ebene beliebige Befehle eingeben konnte.

Bei der Kontrolle der vergebenen Zugriffsrechte ergab sich, daß die Anwendungsentwicklung die Berechtigung zur Benutzerpflege hatte. Es ist aber erforderlich, die Verwaltungsfunktionen nur den zuständigen Benutzern zugänglich zu machen, in diesem Fall also dem Systemverwalter.

Speicherkontrolle:

Es erfolgte ein SIGNOFF, wenn länger als zehn Minuten nicht mit der Anwendung gearbeitet wurde. Eine Weiterarbeit war nur nach einer neuerlichen Anmeldung möglich.

PC-Dienstanweisung:

Es existierte eine PC-Dienstanweisung, die nur in einigen wenigen Punkten ergänzt werden mußte. Insbesondere waren folgende Punkte noch nicht geregelt:

- Welche Software darf eingesetzt werden? Es darf nur freigegebene Software verwendet werden. Die Dienstanweisung muß definieren, was unter freigegebener Software zu verstehen ist. (Dienstlich beschafft; evtl. noch weitere Kriterien wie Verbot von Spielen und Public-Domain-Software ...)
- Dokumentation der eingesetzten Software (Verfahrensverzeichnis)
- Beschreibung der Datensicherung
- Vorgesehene Protokollierungen und ihre Kontrolle
- Verbot, private Datenträger einzusetzen.

Die personelle Funktionstrennung von Anwendungsentwicklung und Systemverwaltung war nicht erfüllt. Durch die neue Stelle eines Systemverwalters sollte das Problem beseitigt werden.

Protokollierung:

Auf der Ebene von CONCEPT 16 wurden alle Anmeldungen, normale und fehlerhafte, protokolliert. Weitere Protokollfunktionen waren weder unter OCULIS noch unter der Datenbank aktiviert.

Forderungen:

Aus den Feststellungen ergab sich eine Reihe von Forderungen:

- Das Problem des Zusammenspiels zwischen OCULIS und den 'hidden'-Directories von CONCEPT 16 mußte behoben werden.
- Die Berechtigung zur Benutzerpflege war nur den Systemverwaltern zu geben.
- Die vergebenen Berechtigungen waren regelmäßig zu kontrollieren.
- Weitere Protokollierungen, so beispielsweise für Verstöße gegen Zugriffsrechte, waren vorzusehen.
- Die PC-Dienstanweisung war anzupassen.

8.1.2.2
Textverarbeitung

Die beiden restlichen PCs dienten der Textverarbeitung mit dem Programm Word. Auf ihnen waren Formbriefe und vereinzelt normale Schreiben gespeichert. Es wurde als Schutzsoftware OCULIS eingesetzt. Die Erfordernisse des Datenschutzes waren soweit ersichtlich erfüllt.

8.1.2.3
Anschluß an das Hochschulrechenzentrum (HRZ)

Auf dem Rechner des HRZ lief die Anwendung PAWI, mit der die Prüfungspläne für das Examen erstellt wurden.

Die Anmeldeprozedur an den Rechner und die Zugriffsmöglichkeiten erfüllten soweit ersichtlich die Anforderungen des Datenschutzes. Es wurde allerdings nicht geprüft, wie die Schutzfunktionen auf dem Rechner insgesamt implementiert waren.

Mängel gab es bei der Dokumentation des Verfahrens. Die Dokumentation bestand aus der zugrundeliegenden Examensarbeit und dem Quell-Code der Programme. Es fehlten aber bespielsweise Dateibeschreibungen, in denen die Bedeutung der einzelnen Datenfelder genannt wurde und es gab keine schriftliche Übersicht zum Verfahrensablauf. Da das Verfahren durch eine PC-Anwendung abgelöst wird, war eine Nachbesserung der Dokumentation entbehrlich.

8.1.2.4
Reaktion des Prüfungsamtes

Das Prüfungsamt teilte mir in seiner Stellungnahme vom August 1991 mit, daß die meisten Mängel behoben worden seien. Es schilderte außerdem die Maßnahmen, die zur Beseitigung der noch bestehenden Defizite ergriffen wurden. Bemerkenswert in diesem Zusammenhang ist, daß, um das Zusammenspiel zwischen der Datenbank und der Datenschutzsoftware sicherzustellen, der Kopierschutz der Datenbank verändert werden mußte. Erst nachdem dies geschehen war, konnten die Sicherungsmechanismen der Datenbank und der Schutzsoftware aktiviert werden.

8.2
Prüfung des Hessischen Bibliotheksinformationssystems HEBIS-Leih

Seit 1989 installieren die wissenschaftlichen Bibliotheken des Landes Hessen (das sind die Universitäts- und Fachhochschulbibliotheken sowie die beiden Landesbibliotheken in Fulda und Wiesbaden) sukzessive das neue automatisierte Ausleihverfahren HEBIS-Leih. HEBIS steht für Hessisches Bibliotheksinformationssystem. Das Ausleihverfahren soll Baustein eines integrierten autonomen lokalen Bibliotheksinformationssystems sein, das auch für die Katalogisierung, Recherchen im Benutzerkatalog und Erwerbung der Bücher, Zeitschriften etc. eingesetzt werden kann.

Noch vor den Bibliotheken des Landes hatte die Stadt- und Universitätsbibliothek der Stadt Frankfurt das neue Ausleihverfahren eingeführt. Deshalb habe ich dort im Sommer 1991 das Verfahren exemplarisch geprüft.

8.2.1
Hardware

Die Stadt- und Universitätsbibliothek verwendet für das Verfahren HEBIS-Leih, mit dem sie ca. 1.2 Mio. Ausleihen pro Jahr bearbeitet, einen Rechner der Firma Norsk Data vom Typ ND-500 mit dem Betriebssystem SINTRAN. Zur Zeit der Prüfung war der Rechner nicht vernetzt und wurde ausschließlich für HEBIS-Leih eingesetzt, so daß sich aus der Hardwarekonfiguration keine Datensicherheitsprobleme ergaben.

8.2.2
Programme und Daten

Bei HEBIS-Leih handelt es sich um eine Software, die aus einzelnen Programm-Modulen besteht, aus denen entsprechend den von der Bibliothek geforderten Funktionen das Programm zusammengestellt wird.

Das Programm befand sich als Object-Code auf dem Rechner und konnte von der Stadt- und Universitätsbibliothek nicht geändert werden. Es umfaßte nicht alle in der Vollversion existierenden Funktionen. Die in Frankfurt installierte Version speicherte im wesentlichen folgende personenbezogene Leserdaten:

- Leserstammdaten (Name, Adresse, Ausweisdaten, Sperren ...)
- Daten der laufenden Ausleihen nach Benutzern
- Daten über vorgemerkte und bestellte Medien nach Benutzern
- Daten über zu zahlende Gebühren nach Benutzern
- Daten über laufende Mahnungen nach Benutzern.

Aus dem bei der Ausleihe eines Buches gespeicherten Datensatz ging hervor, welcher Leser das Buch ausgeliehen hatte. Bei der Rückgabe wurde der Datensatz gelöscht. Die Zuordnung zwischen Leser und Literatur war in der installierten Programmversion nicht zu rekonstruieren. Wenn es zu Leser und Buch einen Mahnvorgang gab, der noch nicht abgeschlossen war, befand sich die Information redundant im Mahnkonto. Zu Statistikzwecken wurden Informationen über Ausleihen in Summenfeldern der Mediensätze und spezieller Statistikdatensätze gespeichert. Die dort vorhandenen Daten waren, soweit ersichtlich, nicht reidentifizierbar und daher nicht personenbezogen. Als wichtigstes Ergebnis der Prüfung ist daher festzuhalten: Leserprofile konnten anhand der Daten nicht erstellt werden.

Die Software war zwar funktionell eingeschränkt, die Datenbank jedoch für eine Vollversion vorhanden. So gab es beispielsweise einen Datenbereich, der zur Speicherung der Daten einer Ausleihe je Benutzer und Medium über die Rückgabe hinaus vorgesehen war, ohne daß er genutzt wurde. Da derartige Daten zu einer anderen Wertung des Gesamtverfahrens geführt hätten, habe ich Vorkehrungen verlangt, die eine entsprechende Speicherung ausschließen. Dazu zählen z.B.:

- Wenn eine neue Version der Software eingespielt wird, muß kontrolliert werden, daß sie den geforderten Funktionsumfang besitzt.

- Die Datenbank muß entsprechend dem Funktionsumfang der Programmversion für die Stadt- und Universitätsbibliothek generiert sein. Das bedeutet: Es sind die Datenbereiche festzulegen, die nicht genutzt werden dürfen. Diese müssen in der Datenbank undefiniert bleiben oder als Dummy-Bereiche vorgesehen werden (d.h. die Definitionen sind vorhanden, es gibt aber keinen Platz, um Datensätze zu speichern).

- Es ist zu kontrollieren, daß die nicht genutzten Datenbereiche leer bleiben. Dies wäre beispielsweise mit der Datenbankstatistik zu erreichen.

8.2.3
Sonstige Mängel

Die ansonsten gefundenen Mängel waren nicht spezifisch für das Verfahren. Sie bewegten sich im Rahmen dessen, was bei Prüfungen häufig festzustellen ist:

- Zum Rechnerraum hatten Personen Zugang, deren Aufgaben dies nicht erforderten.

- Benutzerkennungen waren mehreren Personen zugeordnet, ohne daß dies erforderlich war. Die mit den Kennungen verknüpften Rechte waren allerdings gering.

- Mögliche Protokolle wurden nicht erstellt bzw. nicht ausgewertet.

- Wartungstätigkeiten wurden nicht protokolliert, obwohl ein Wartungsbuch vorhanden war.

- Es fehlte eine Dienstanweisung.

8.2.4
Stellungnahme der Stadt- und Universitätsbibliothek

Die Bibliothek hat mir Ende November 1991 mitgeteilt, sie habe das Verfahren HEBIS-Leih auf den neuesten Stand gebracht und dabei meinen Forderungen entsprechend die Datenbank geändert. Auch die übrigen Mängel seien beseitigt worden. Lediglich an der Dienstanweisung und den Regelungen zu den Protokollen werde noch gearbeitet. Ich werde im Frühjahr 1992 die vollständige Umsetzung meiner Forderungen überprüfen.

9. Gesundheit

9.1
Telefax in Krankenhäusern

9.1.1
Unzureichender Zugriffsschutz

Wie bereits im 18. Tätigkeitsbericht (Ziff. 16.1) beschrieben, birgt Telefax neue Risiken für den Datenschutz. Nicht nur daß die Gefahr, daß ein Telefax an einen falschen Adressaten gerät, größer ist als beim konventionellen Brief, da man sich leichter verwählen als bei der Anschrift eines Briefes verschreiben kann. Der Empfänger kann ein falsch adressiertes Telefax ohne weiteres lesen, da es offen bei ihm ankommt, was bei einem Brief nicht der Fall ist. Die größten Probleme macht jedoch beim Telefax der Zugriffsschutz, und zwar besonders dann, wenn z.B. in einer Behörde ein Telefaxgerät für verschiedene Ämter oder in einem Krankenhaus für verschiedene Abteilungen vorhanden ist.

Das hat auch eine Prüfung gezeigt, die ich im Herbst1991 in den Städtischen Kliniken Kassel durchgeführt habe. Auf einem Telefaxgerät, das im Sekretariat des Verwaltungsleiters stand, kamen Arztbriefe an. Ein anderes Telefaxgerät stand in einem allgemein zugänglichen und stark frequentierten Raum der Wirtschafts- und Verwaltungsabteilung. Telefaxe, die hier eingingen, wurden in unregelmäßigen Abständen an die behandelnden Ärzte oder Fachabteilungen weitergeleitet.

In beiden Fällen wurde gegen Datenschutzrecht verstoßen. Das Krankenhaus ist keine rechtliche Einheit, innerhalb der personenbezogene Daten von jedem Beschäftigten zur Kenntnis genommen und weitergegeben werden dürfen. Auch innerhalb des Krankenhauses ist die ärztliche Schweigepflicht (§ 203 StGB) und das Datengeheimnis (§ 12 KHG, § 9 HDSG) zu beachten. Zudem schreibt das Hessische Krankenhausgesetz ausdrücklich vor, daß die Datenbestände der Fachabteilungen voneinander zu trennen sind und zwischen den Fachabteilungen die Regelungen über die Übermittlung personenbezogener Daten entsprechend Anwendung finden (§ 12 Abs. 3 KHG). Jeder im Krankenhaus Beschäftigte darf deshalb nur die personenbezogenen Daten erfahren, die er für seine konkrete Aufgabenerfüllung benötigt. So braucht etwa die Verwaltungsabteilung lediglich die Daten, die für die verwaltungsmäßige Abwicklung des Behandlungsvertrages erforderlich sind, jedoch keine detaillierten medizinischen Daten über Patienten. Eine Fachabteilung, die einen Patienten nicht behandelt, darf dessen Daten nicht erhalten. Diese rechtlichen Vorgaben sind bei der Organisation der Postverteilung im Krankenhaus, bei der Archivierung der Krankenakten etc. zu berücksichtigen. Mit der Post eingehende Arztbriefe werden daher auch generell nicht in der Verwaltung, sondern in der betreffenden Fachabteilung geöffnet.

Der Einsatz des Mediums Telefax darf nicht dazu führen, daß die rechtlichen Vorgaben nicht mehr beachtet werden und sich der Schutz der Patientendaten verschlechtert. In den beiden geschilderten Fällen in Kassel war nicht gewährleistet, daß nur die jeweils Berechtigten die Patientendaten zur Kenntnis nehmen konnten. Ich habe daher von den Städtischen Kliniken Kassel gefordert, umgehend den Schutz der Patientendaten durch geeignete Maßnahmen sicherzustellen. Da die Vermutung naheliegt, daß die Situation in Kassel kein Einzelfall war, werde ich auch 1992 den Einsatz von Telefax in öffentlichen Stellen prüfen.

9.1.2
Anforderungen an die Benutzung von Telefaxgeräten im Krankenhausbereich

Da die medizinischen Daten besonders schutzwürdig sind, muß durch organisatorische Maßnahmen sichergestellt werden, daß bei der Übermittlung von Patientendaten per Telefax unbefugte Dritte die Daten nicht zur Kenntnis nehmen können. Das Krankenhaus muß gewährleisten, daß ein ankommendes Telefax nur an die zuständigen Bediensteten gelangt. Die Verantwortung dafür, daß das Telefax nur Befugten zugeht, trägt freilich nicht nur das Krankenhaus, sondern auch die übermittelnde Stelle. Zu beachten sind insbesondere folgende Punkte:

- In Räumen mit Publikumsverkehr darf überhaupt kein Telefax mit Patientendaten empfangen werden.

- Grundsätzlich dürfen im gesamten Verwaltungsbereich des Krankenhauses keine medizinischen Daten per Telefax empfangen werden. Im Einzelfall kann dies bei Vorliegen besonderer Gründe allenfalls dann akzeptiert werden, wenn die unmittelbare Entgegennahme des Telefaxes durch einen Mitarbeiter aus der betreffenden Fachabteilung gewährleistet ist.

- Steht ein Telefaxgerät in einer Fachabteilung des Krankenhauses, so darf dieser Apparat nicht ohne weiteres durch eine andere Fachabteilung mitbenutzt werden. Wünschenswert ist auf jeden Fall, daß das Telefax direkt in der Fachabteilung ankommt, die den Patienten behandelt. Solange dies aus technischen, organisatorischen oder finanziellen Gründen nicht realisierbar ist, ist die Mitbenutzung eines Apparates durch eine andere Fachabteilung dann zulässig, wenn es im Krankenhaus eine schriftliche Regelung über die Zuständigkeit für die Entgegennahme von Telefaxsendungen und den Umgang mit Patientendaten gibt.

- Das Krankenhaus muß in einer Dienstanweisung die Modalitäten der zulässigen Verwendung der Telefaxgeräte entsprechend den rechtlichen Vorgaben festlegen.

- In jedem Fall, in dem ein Schreiben mit medizinischen Daten in einem nicht dafür bestimmten Telefaxgerät eingeht, muß das Krankenhaus den Absender darauf hinweisen, welche Telefaxnummer korrekt gewesen wäre.

- Nicht nur der Empfänger, sondern auch der Absender der Patientendaten, z.B. ein (mit-)behandelnder niedergelassener Arzt, ist für die Einhaltung der ärztlichen Schweigepflicht im Sinne von § 203 verantwortlich. Der Absender darf seine Patientendaten nur an die zur Kenntnisnahme Berechtigten übermitteln. Bei dem heutigen Stand der Technik der Telefaxgeräte und der Ausstattung der Krankenhäuser mit Telefaxgeräten darf der absendende Arzt nicht ohne weiteres davon ausgehen, daß die Daten nur von zugriffsberechtigten Personen zur Kenntnis genommen werden können. Bevor er erstmals medizinische Daten per Telefax an ein bestimmtes Krankenhaus verschickt, muß er sich daher erkundigen, wo dieses Gerät steht bzw. ob das Krankenhaus generell Verfügungen getroffen hat, die sicherstellen, daß die Daten nur an die Empfangsberechtigten gelangen. Will der Absender diese generelle Klärung nicht vornehmen, so muß er es entweder bei einem normalen Brief belassen oder im konkreten Einzelfall vor Absendung des Telefaxes den behandelnden Arzt telefonisch verständigen, so daß eine unmittelbare Entgegennahme des Telefaxes durch den behandelnden Arzt gewährleistet ist.

9.1.3
Telefax mittels Personal-Computer

Die technische Entwicklung und Liberalisierung im Telekommunikationsbereich hat die geschilderten Datenschutzprobleme, die Telefax bereitet, noch vergrößert. Denn sowohl die Möglichkeit, einen Personal-Computer mittels Hard- und Software (eine Steckkarte und ein dazu passendes Programm) zu einer telefaxfähigen Einrichtung zu erweitern, als auch der Einsatz eines solchen "Fax-PCs" in modernen DV-Netzwerken schaffen neue Sicherheitsrisiken.

Das Bundesministerium für Post und Telekommunikation hat durch die Anpassung der technisch betrieblichen Funktionsbedingungen an die vorhandene Technik die Voraussetzungen für die massenhafte Verbreitung von Fax-PCs geschaffen. Seit dem 1. Januar 1991 dürfen Fax-PCs an das öffentliche Netz angeschlossen werden, die nicht rund um die Uhr empfangsbereit sind und eingehende Telefaxe nicht zwangsweise ausdrucken. Gleichzeitig entfiel die Anforderung, daß an jeder Telefax-Einrichtung ein externer Fernsprechapparat angeschlossen sein muß.

9.1.3.1
Der "Stand-Alone Fax-PC"

Fax-PCs als Einzelplatzgeräte werfen neben den organisatorischen Telefax-Problemen auch die bekannten Fragen zur Datensicherheit beim Einsatz von PCs auf, da die Telefaxe sinnvollerweise vor der Versendung oder nach dem Empfang gespeichert werden bzw. bleiben. Lösungsmöglichkeiten, die sich hier anbieten, habe ich bereits in meinem 15. (vgl. Ziff. 9) und 17. Tätigkeitsbericht (vgl. Ziff. 12) eingehend behandelt.

Der Einsatz eines Fax-PCs muß unter den gleichen organisatorischen Bedingungen erfolgen, wie der eines herkömmlichen Telefax-Gerätes. Um unbefugte Zugriffe auszuschließen, ist außerdem in der Regel eine Datenschutzsoftware notwendig. Dies gilt insbesondere dann, wenn der Fax-PC für mehrere Fachabteilungen oder zum zeitversetzten Senden genutzt wird. Die Zuständigkeiten und Aufgaben der mit dem Betrieb und der Verteilung der empfangenen Telefaxe beauftragten Personen sind schriftlich zu regeln.

Ein Fax-PC bietet gegenüber dem einfachen Standard-Telefaxgerät allerdings auch Vorteile für den Datenschutz: Die eingehenden Telefaxsendungen werden nicht, wie bei Standardgeräten, sofort und deshalb häufig unbemerkt ausgedruckt, sondern es muß zuvor ein Druckbefehl eingegeben werden. Dadurch verringert sich die Gefahr, daß Unbefugte ein längere Zeit offen daliegendes Telefax lesen können. Mit dem Fax-PC können die Sendungen außerdem direkt vom Arbeitsplatz ohne schriftliche Vorlage erfolgen. Das Schreiben muß nicht an eine zentrale Telefaxstelle im Haus weitergegeben werden.

Darüber hinaus bietet das Gerät seinen Nutzern je nach Leistungsfähigkeit der Programme noch zusätzlichen Komfort, wie z.B. die programmgesteuerte Verlegung der Versendung in die kostengünstigeren Tarifzeiten.

9.1.3.2
Der Fax-PC als Bestandteil eines DV-Netzes

Durch die Verbindung des Fax-PCs mit einem Datenverarbeitungsnetzwerk soll der Telefax-Dienst allen oder einigen ausgewählten Benutzern des Systems zur Verfügung gestellt werden. Dazu muß der Fax-PC eine besondere Anbindung an das PC-Netzwerk haben, die den Übergang vom und zum Netz ermöglicht. Das Gerät wird, wie jede andere Workstation, an das Netz angeschlossen und eine Benutzerkennung mit bestimmten Zugriffsrechten im Netzwerkbetriebssystem eingetragen und eingelogt (d.h. die Benutzerkennung wird am System angemeldet). Auf dem PC wird ein Programm gestartet, das eine vorhandene Fax-Software ansteuert oder eine solche zum Inhalt hat, und auf den Plattenspeichern des Servers werden zusätzlich die von diesem Programm benötigten Verzeichnisse und Dateien angelegt. Da der Fax-PC im Netz ständig empfangsbereit sein soll, steht er damit für keine andere Nutzung zur Verfügung.

Aus der Einbindung der Fax-PCs in Datenverarbeitungsnetze ergeben sich dadurch, daß für mehrere Netzbenutzer ein gemeinsames "Sendeverzeichnis" existiert und Telefaxe für verschiedene Netzbenutzer empfangen, gespeichert und im Netz verteilt werden können, besondere Schwierigkeiten. Dies hat auch eine von mir im Universitätsklinikum Gießen durchgeführte Überprüfung eines Fax-PCs, der in ein PC-Netzwerk mit dem Betriebssystem Novell Netware integriert ist, gezeigt. Zu den aus dem Einsatz solcher Netzwerke resultierenden Risiken vgl. den 18. Tätigkeitsbericht, Ziff. 16.3.

9.1.3.2.1
Der Sendevorgang

Die Versendung eines Telefax erfolgt in der geprüften Konstellation folgendermaßen:

Eine sendeberechtigte Person erstellt einen Text und versieht ihn mit den von der Fax-Software benötigten zusätzlichen Informationen, z.B. der Zielnummer. Danach kopiert sie das so vorbereitete Telefax in ein Sendeverzeichnis, das auf der Festplatte des Servers angelegt ist. Das Programm, das auf dem Fax-PC für den Netzübergang verantwortlich ist, überprüft dieses Verzeichnis in regelmäßigen Abständen auf neu zu versendende

Telefaxe und kopiert diese in das Sendeverzeichnis auf der Festplatte des Fax-PC. Danach gibt es dem eigentlichen Fax- Programm den Auftrag, dieses Telefax zu versenden. Das Fax- Programm startet danach den Sendevorgang und quittiert dem auftraggebenden Programm die erfolgte Versendung oder einen Code für die Ursache eines Sendeabbruchs. Bei erfolgreicher Versendung wird der Text im Sendeverzeichnis des Servers gelöscht. Ist der Anschluß des Empfängers besetzt, wird der Aufruf des Fax-Programms mit einstellbaren Intervallen wiederholt. Erfolgte ein Sendeabbruch aus anderen Gründen, weil z.B. die angegebene Zielnummer kein Telefax-Gerät ist, erhält der Absender eine entsprechende Nachricht und kann das gegebenenfalls geänderte Telefax zur erneuten Versendung vorbereiten.

Bei diesem Ablauf lassen sich – eine entsprechende Administration des Netzwerkes vorausgesetzt – die Verzeichnisse des Servers ausreichend gegen unberechtigte Zugriffe sperren. Lediglich das Sendeverzeichnis auf dem Server kann von allen Sendeberechtigten angesprochen werden, d.h. Telefaxe, die noch nicht versandt werden konnten, liegen im geschilderten Fall im lesenden Zugriff aller Sendeberechtigten. Dies widerspricht den in Ziff. 9.1.1 dargelegten rechtlichen Vorgaben für die Kenntnisnahme und die Weitergabe personenbezogener Daten im Krankenhaus. Es müßte daher eine Fax-Software den Nutzern jeden weiteren Zugriff auf ein einmal in das Sendeverzeichnis übertragenes Telefax verwehren. Wenn dies durch die eingesetzten Systeme ausgeschlossen ist, besteht noch die Möglichkeit, die Absender in verschiedene Gruppen einzuteilen, d.h. z.B. für jede Fachabteilung ein eigenes Sendeverzeichnis anzulegen. Die verschiedenen Sendeverzeichnisse können dann jeweils gegen unberechtigte Zugriffe geschützt werden.

9.1.3.2.2
Empfangsvorgang

Der Ablauf bei eingehenden Telefaxen ist zwar wesentlich einfacher, aber die damit verbundenen datenschutzrechtlichen Probleme sind mit den vorhandenen technischen Möglichkeiten noch nicht sämtlich befriedigend zu lösen.

Ein eingehendes Telefax wird zunächst von der Fax-Software aufgenommen und dann direkt in einem zentralen "Empfangsverzeichnis" abgespeichert. Dieses Verzeichnis befindet sich in der Regel, so auch in Gießen, auf der Festplatte des Servers, da der Server normalerweise die größeren Speicherkapazitäten hat. Damit liegen die eingehenden Telefaxe auch in einem Bereich, der durch das Netzwerkbetriebssystem vor unberechtigten Zugriffen geschützt werden kann.

Wenn ein Fax-PC abteilungsübergreifend im Krankenhaus eingesetzt wird, liegt das Problem in der weiteren Bearbeitung dieser Telefaxe, die gegenwärtig automatisiert noch nicht möglich ist. Ein Programm, das eine Verteilung innerhalb des Netzes vornehmen soll, muß dazu ein Kennzeichen für den jeweiligen Empfänger auswerten können. Die Übertragung und Auswertung dieses Kennzeichens im Verbindungsprotokoll oder im Telefax selbst erweist sich jedoch als Problem. In den USA werden zwar für das dortige Fernsprechnetz entwickelte Verfahren angeboten, und die Industrie arbeitet an verschiedenen Verfahren für den hiesigen Markt, aber mir ist bis heute kein zugelassenes Produkt bekannt, das ein derartiges Leistungsmerkmal anbietet.

Solange eine automatisierte Verteilung nicht möglich ist, ist eine gemeinsame Benutzung des Fax-PC durch mehrere Fachabteilungen nur zulässig, wenn dafür, wie bei einzelnen Telefax-Geräten, eine schriftliche organisatorische Regelung existiert, in der u.a. die Einzelheiten für den Umgang mit empfangenen Telefaxen und deren Verteilung durch die dazu beauftragte Person beschrieben sind.

9.1.3.2.3
Sonstige Maßnahmen

Um ein Telefax zu versenden oder empfangene Telefaxe zu verteilen, ist es, anders als beim normalen Faxgerät, nicht erforderlich, den Fax-PC zu bedienen. Er kann daher in besonders geschützten Räumen, die nur den Berechtigten zugänglich sind, untergebracht werden. Damit ist er vor unmittelbaren unberechtigten Zugriffen geschützt, aber es muß auch sichergestellt werden, daß keine Zugriffe über das vorhandene Netzwerk möglich sind.

Beim Einsatz von Fax-PCs im Datenverarbeitungs-Netz gelten zunächst die gleichen Bedingungen wie beim Stand-Alone Fax-PC. Da die Systemverantwortlichen des Netzwerkbetriebssystems jedoch zusätzliche Zugriffsmöglichkeiten auf das Sende- und Empfangsverzeichnis haben, müssen auch ihre Zuständigkeiten und gegebenenfalls die Kontrolle ihrer Zugriffe in die schriftlichen Regelungen zum Einsatz von Telefax eingearbeitet werden.

9.2
Prüfung der Datenerhebung in Krankenhäusern

1991 habe ich in einer Reihe von Krankenhäusern die Datenerhebung bei der Patientenaufnahme überprüft und dabei mehrere typische Mängel festgestellt.

9.2.1
Unnötige Datenerhebungen

Auf den von mir geprüften Aufnahmeformularen war häufig die Erhebung von Daten vorgesehen, die für die Durchführung des Behandlungsvertrages nicht erforderlich waren. So wurde z.B. häufig routinemäßig von jedem Patienten der Arbeitgeber erfragt .

Nach § 12 Hessisches Krankenhausgesetz (HKHG), § 11 HDSG dürfen die Kliniken personenbezogene Daten der Patienten erheben, soweit dies für die Durchführung des Behandlungsvertrages erforderlich ist. Dazu gehören neben Name, Geburtsdatum und Adresse des Patienten auch solche Daten, die zur Abrechnung mit dem Kostenträger erforderlich sind, ferner im medizinischen Bereich des Krankenhauses selbstverständlich Anamnesedaten und Daten über den Behandlungsverlauf etc. Eine routinemäßige Erhebung des Arbeitgebers bei der Aufnahme des Patienten ist für die Durchführung der Behandlung jedoch nicht erforderlich. Sie kann lediglich einmal im Einzelfall notwendig sein, z.B. wenn sich Unklarheiten über die für den Patienten zuständige Krankenkasse ergeben. Ebensowenig sind z.B. detaillierte Angaben zum Familienstand auf dem Aufnahmeformular für die Durchführung der Behandlung erforderlich. In einem Formular wurde etwa erfragt, ob der Patient ledig, verheiratet, geschieden, getrennt lebend oder verwitwet ist. Allenfalls kann bei Selbstzahlern die Angabe "verheiratet" wegen der möglichen Mithaftung des Ehegatten für die Behandlungskosten in Betracht kommen. Im übrigen ist jedoch die Erhebung solcher Angaben nicht zulässig.

9.2.2
Keine klare Kennzeichnung der freiwilligen Angaben

Häufig war auf den Aufnahmeformularen eine Erhebung von zusätzlichen Daten auf freiwilliger Basis vorgesehen, ohne daß für den Patienten klar ersichtlich war, daß es sich um freiwillige Angaben handelte. Hierbei ging es z.B. um Angaben zur Konfession, zum Hausarzt oder zu Angehörigen.

Rechtlich geboten ist eine strikte Trennung zwischen denjenigen Daten, die für die Durchführung des Behandlungsvertrages erforderlich sind, und denjenigen Daten, die auf freiwilliger Basis vom Patienten erfragt werden: Nach § 12 HKHG, § 11 HDSG dürfen die Kliniken personenbezogene Daten der Patienten erheben, soweit dies für die Durchführung des Behandlungsvertrages erforderlich ist. Für die Erhebung von personenbezogenen Daten, die nicht zur Durchführung des Behandlungsvertrages benötigt werden, bietet der Behandlungsvertrag keine Rechtsgrundlage. Es bedarf vielmehr einer besonderen Einwilligung des Patienten (§ 12 HKHG, § 7 HDSG). Auf den Aufnahmeformularen müssen daher die freiwilligen Angaben klar und deutlich als solche gekennzeichnet sein. Es reicht z.B. nicht aus, daß eine entsprechende Erläuterung auf der Rückseite des Formulars steht.

9.2.3
Unzureichende Information der Patienten

In vielen Aufnahmeformularen wurden Daten, die für die Durchführung des Behandlungsvertrages nicht erforderlich waren, erfragt, ohne daß dem Betroffenen der Zweck der Datenerhebung mitgeteilt wurde. So wurde z.B. nach der Konfession gefragt, ohne dem Patienten zu erläutern, daß seine Daten an die entsprechende Religionsgemeinschaft weitergegeben würden. Auf mehreren Formularen war die Angabe des Hausarztes vorgesehen, ohne daß der Zweck dieser Datenerhebung – etwa die Möglichkeit von Rückfragen der behandelnden Krankenhausärzte oder die Übersendung von Krankenhausentlassungsberichten – für den Patienten ersichtlich war.

Unter diesen Umständen ist die Einwilligung des Patienten in die Datenerhebung unwirksam. Nach § 12 HKHG, § 7 Abs. 2 HDSG muß der Bürger über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufgeklärt werden. Dies ist im Grunde auch eine Selbstverständlichkeit, denn eine echte Entscheidungsfreiheit des Bürgers ist nur dann gegeben, wenn er die konkreten Folgen seiner evtl. Einwilligung auch übersehen kann.

Der Patient hat nicht nur ein Recht auf Information über die Erhebung freiwilliger Angaben auf dem Aufnahmeformular, sondern über jede Verarbeitung personenbezogener Daten im Krankenhaus. Die Aufklärungspflicht der Krankenhäuser umfaßt bei beabsichtigten Übermittlungen auch den Empfänger der Daten (§ 12 Abs. 4 HDSG). Darüber hinaus ist der Bürger nach § 18 Abs. 2 HDSG schriftlich zu benachrichtigen, wenn seine personenbezogenen Daten in einer automatisierten Datei gespeichert werden. Diese Vorschriften sind gerade in Krankenhäusern besonders wichtig, denn die personenbezogenen Daten der Patienten werden im arbeitsteiligen Krankenhaus in vielen Bereichen – z.B. in Verwaltung, Labor, Pathologie, verschiedenen Fachabteilungen etc. – und in zahlreichen automatisierten Dateien verarbeitet. Für den Patienten ist dies in der Regel nicht transparent, wenn er nicht darüber speziell informiert wird. Die Information und Benachrichtigung des Patienten kann z.B. bei der Aufnahme ins Krankenhaus erfolgen. Wird die Benachrichtigung nicht während des Krankenhausaufenthaltes vorgenommen, so ist das Krankenhaus nach den gesetzlichen Bestimmungen verpflichtet, dies schriftlich in jedem Einzelfall nachzuholen, was selbstverständlich mit zusätzlichen Kosten verbunden ist.

In den überprüften Krankenhäusern war die Umsetzung dieser Vorschriften unzureichend, die Patienten wurden nicht ausreichend über die Verarbeitung ihrer Daten im Krankenhaus informiert.

9.2.4
Konsequenzen

Eine Abänderung der Aufnahmeformulare ist auf jeden Fall erforderlich. Darüber hinaus muß in jedem Krankenhaus geklärt und festgelegt werden, wie die Informationsrechte der Patienten umgesetzt werden sollen.

Da die dargelegten Probleme in zahlreichen Krankenhäusern bestehen, habe ich mich im Zusammenhang mit der erfolgten Neufassung der Allgemeinen Vertragsbedingungen (AVB) für die Krankenhäuser an die Hessische Krankenhausgesellschaft gewandt und gemeinsam mit ihr ein Muster für die Datenerhebung bei der Krankenhausaufnahme sowie ein Muster für einen dem Patienten bei der Aufnahme auszuhändigenden Hinweis zur Verarbeitung personenbezogener Daten, der zugleich eine Benachrichtigung des Patienten nach § 18 Abs. 2 HDSG zum Inhalt hat, erarbeitet. Diese Muster wurden von der Hessischen Krankenhausgesellschaft zusammen mit einer Darlegung der neuen Rechtslage in einem Sonderrundschreiben an alle Krankenhäuser in Hessen versandt und den Kliniken zur Übernahme empfohlen.

Die Praxis in den Kliniken werde ich weiterhin überprüfen.

10. Novellierung der Abgabenordnung

Noch immer fehlen für die Finanzverwaltung bereichsspezifische Datenschutzvorschriften. Der 1988 vom Bundesfinanzministerium vorgelegte Entwurf zur Novellierung der Abgabenordnung (vgl. 17. Tätigkeitsbericht, Ziff. 11.1) ist mittlerweile mehrfach überarbeitet worden. Die neueste Fassung datiert vom 25. November 1991.

Sie folgt in vielen Punkten den Anregungen der Datenschutzbeauftragten. Der Entwurf enthält beispielsweise nun nicht mehr die besonders kritisierte Einschränkung der Kontrollbefugnisse der Landesdatenschutzbeauftragten. Bislang sollten die Datenschutzbeauftragten die Finanzbehörden nach den Vorschriften des Bundesdatenschutzgesetzes (BDSG) kontrollieren . Nach dem BDSG ist z.B. eine Überprüfung der Verarbeitung personenbezogener Daten in Akten nur zulässig, wenn dazu ein Anlaß besteht, d.h. wenn entweder die Betroffene dem Datenschutzbeauftragten dargelegt hat, daß sie durch die Datenverarbeitung in ihren Rechten verletzt worden ist, oder dem Datenschutzbeauftragten hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen. Das Hessische Datenschutzgesetz sieht eine solche Beschränkung nicht vor. Die nach dem HDSG dem Datenschutzbeauftragten zustehende Befugnis, aus eigener Initiative auch die Datenverarbeitung in Akten zu überprüfen, bleibt nach dem neuen Entwurf unberührt. Für die Finanzbehörden gelten somit die gleichen Kontrollbedingungen wie für die übrige hessische Verwaltung.

Die Regelungen in § 30 Abs. 5 und 6 bedeuten gegenüber den Vorentwürfen insofern eine Verbesserung, als sie erkennen lassen, daß das Bundesfinanzministerium vom Grundsatz der Einheit der Finanzverwaltung abgerückt ist und nunmehr anerkennt, daß eine zweckändernde Datenverarbeitung auch innerhalb der Finanzverwaltung einer Rechtsgrundlage bedarf.

Trotz der Verbesserungen sind allerdings immer noch einige Mängel verblieben:

Die neue Regelung des § 30 Abs. 6 erlaubt eine nahezu unbegrenzte Verwendung von Daten, die dem Steuergeheimnis unterliegen, auch wenn nach der nun vorliegenden Fassung des Gesetzentwurfs die Offenbarung nur noch zulässig ist, wenn dies zur Durchführung eines anderen Verfahrens erforderlich ist. Nach dem Wortlaut des Absatz 6 Satz 2 ist eine Offenbarung geschützter Daten für andere Zwecke auch ohne Ersuchen des Empfängers zulässig. Das ist schon deshalb bedenklich, weil aus Sicht der offenbarenden Stelle die Erforderlichkeit der Datenverarbeitung für eine andere Stelle häufig gar nicht beurteilt werden kann. Dadurch entsteht für den Empfänger der Anreiz zur Sammlung umfangreicher personenbezogener Daten "auf Vorrat", die dann abgerufen werden könnten, wenn sich in Zukunft die Erforderlichkeit ergeben sollte. Datensammlung auf Vorrat ist jedoch nach einhelliger Meinung unzulässig. Durch Satz 3 wird zusätzlich die Möglichkeit beliebig vieler weiterer zweckändernder Weitergaben von Daten eröffnet. Für die von der Datenübermittlung Betroffenen ist damit überhaupt nicht mehr nachvollziehbar, wer wann welche Daten verarbeitet. Zudem ist der Katalog, wann Daten zu anderen Zwecken offenbart und verwendet werden dürfen, derartig umfangreich, daß Datenübermittlungen innerhalb der Finanzverwaltung praktisch keine Grenzen gesetzt sind.

Bedenklich ist auch § 88 Abs. 3, der die Finanzverwaltung ermächtigt, für Ermittlungszwecke, aber auch "zur Gewinnung von Vergleichswerten" geschützte Daten zu speichern, zu offenbaren und zu verwenden. Diese Vorschrift ermöglicht es der Finanzverwaltung ebenfalls, praktisch unbegrenzt Daten auf Vorrat zu sammeln. Die Ermächtigung zur Datensammlung "zur Gewinnung von Vergleichswerten" ist unbestimmt. Der Zweck des Vergleichs ist keinesfalls gewichtig genug, um eine derart weitgehende Einschränkung des Rechts auf informationelle Selbstbestimmung zu rechtfertigen.

Ursprünglich sah der Entwurf zu § 93 Abs. 1, der die Auskunftspflicht anderer Personen als der Beteiligten regelt, eine Ergänzung des Satzes 3 vor. Die Auskunftspflicht sollte nur dann gelten, wenn nach Prüfung durch die

Finanzbehörde "keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden". Diese Bestimmung ist im neuesten Entwurf bedauerlicherweise wieder gestrichen worden.

Nach § 93 Abs. 1 AO haben alle öffentlichen Stellen der Finanzbehörde die Auskünfte zu erteilen, die zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes erforderlich sind. § 105 Abs. 1 AO hebt insoweit die besonderen Verschwiegenheitspflichten gegenüber den Finanzbehörden auf. Es fehlt eine klare Formulierung zum Umfang der Auskunftspflicht der Behörden. Dies ist vor allem deshalb bedeutsam, weil § 105 Abs. 1 eine weitgehende Durchbrechung von gesetzlich besonders geregelten Schweigepflichten (z.B. Aufhebung des Sozialgeheimnis gegenüber den Finanzbehörden) vorsieht. Da die Regelung des § 30 Abs. 6 weitgehend die zweckgebundene Datenverarbeitung aufhebt, ist diese umfangreiche Durchbrechung anderer Schweigepflichten besonders schwerwiegend.

11. Umweltschutz: Verdachtsflächendatei

Der von der Hessischen Landesregierung begonnene Aufbau einer sogenannten "Verdachtsflächendatei", in der Grundstücke mit gefährlichen chemischen Ablagerungen erfaßt werden (vgl. 19. TB, Ziff. 12.1), hat eine Reihe datenschutzrechtlicher Fragen aufgeworfen. Das gilt insbesondere für die Phase der Datenerhebung: Um eine einigermaßen zuverlässige Übersicht über Verunreinigungen ehemaliger Gewerbegrundstücke zu erhalten, müssen die bei den Kommunen – etwa seit 1850, dem Beginn der Industrialisierung – geführten Gewerbekarteien ausgewertet werden. Diese zeitraubende Aufgabe, die den Gemeinden durch § 17 Abs. 1 Hessisches Abfallwirtschafts- und Altlastengesetz (HAbfAG) auferlegt ist, können die meisten von ihnen nicht mit eigenem Personal in einem vertretbaren Zeitraum bewältigen.

Daher war zu prüfen, ob aus datenschutzrechtlicher Sicht die Datenerhebung durch andere Stellen, wie z.B. den Umlandverband Frankfurt am Main oder private Stellen (auf Umweltschutz spezialisierte Datenerhebungsfirmen) durchgeführt werden kann.

Für den Umlandverband Frankfurt, der nach § 1 Abs. 2 Satz 1 und 2 HAbfAG anstelle der ihm angehörenden Städte und Landkreise zum Kreise der "Entsorgungspflichtigen" gehört, besteht sogar die Pflicht zur Erhebung der betreffenden Daten für seine Mitgliedsgemeinden und Landkreise (§ 17 Abs. 1 Satz 3 HAbfAG).

Anders ist die Rechtslage bei Übernahme der Datenerfassungsarbeiten durch eine darauf spezialisierte private Firma. Hier handelt es sich um Datenverarbeitung im Auftrag, so daß die Voraussetzungen des § 4 HDSG erfüllt sein müssen:

1. Der Auftraggeber – die Kommune – muß sich vor Auftragserteilung davon überzeugen, daß die Firma die nach § 10 HDSG vorgeschriebenen Maßnahmen der Datensicherung getroffen hat.

2. Der Auftraggeber muß den Hessischen Datenschutzbeauftragten über die Beauftragung unterrichten.

3. Der Auftraggeber muß vertraglich sicherstellen, daß die beauftragte Firma die Bestimmungen des Hessischen Datenschutzgesetzes befolgt und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft.

Bisher haben – außer dem Umlandverband Frankfurt – zwei im Rhein-Main-Gebiet ansässige Spezialfirmen für eine Anzahl von Städten und Gemeinden die Daten für die Verdachtsflächendatei aus den Gewerbekarteien der abgemeldeten Betriebe erhoben. Beide Firmen habe ich überprüft und dabei lediglich einige kleinere Mängel festgestellt, die aufgrund meiner Beratung unverzüglich behoben worden sind. Ich werde mich auch künftig bei den Firmen durch Stichproben von der Einhaltung des Datenschutzes, insbesondere der Maßnahmen der Datensicherung, überzeugen.

Ein weiteres Problem, das zwischen Umweltministerium, Sozialministerium und dem Hessischen Datenschutzbeauftragten einvernehmlich gelöst werden konnte, war die Datenerhebung der Landesanstalt für Umwelt bei den Gewerbeaufsichtsämtern. Die Landesanstalt für Umwelt wird nach einem Stufenverfahren vorgehen: Nur wenn im Einzelfall weitere Angaben über die Verdachtsflächendatei notwendig sind und diese sich nicht aus den Gewerberegistern der Gemeinden ermitteln lassen, ist es nach § 26 Abs. 1 Satz 1 sowie Satz 3 Ziff. 2 HAbfAG zulässig, diese Daten bei den Gewerbeaufsichtsämtern zu erheben. Nach der Speicherung der Daten auf elektronischen Datenträgern werden die Erhebungsbogen vernichtet.

Einzelheiten über den Aufbau und die Führung der Verdachtsflächendatei enthält die am 1. Oktober 1991 erlassene Verdachtsflächendatei-Verordnung (GVBl. I S. 314), deren datenschutzrechtliche Aspekte zwischen dem Umweltministerium und mir ausführlich erörtert worden sind.

Im Rahmen des hessischen Datenverarbeitungsverbundes läuft im Kommunalen Gebietsrechenzentrum Starkenburg in Darmstadt ein Pilotprojekt zur Automation der (aktuellen) Gewerbedatei der Gemeinden. Im Einvernehmen mit der Landesanstalt für Umwelt und dem Hessischen Datenschutzbeauftragten wird das KGRZ prüfen, inwieweit

künftig die Daten abgemeldeter Gewerbebetriebe aus diesem Verfahren für die Aktualisierung der Verdachtsflächendatei genutzt werden können.

12. Landwirtschaft: Datensicherheit in den Landwirtschaftsämtern

Bei einer Prüfserie in allen Ämtern für Landwirtschaft und Landentwicklung zur Feststellung des Standes der Datensicherheit im Jahre 1988 (vgl. 17. Tätigkeitsbericht, Ziff. 12.2.1) hatten sich bei fast allen Dienststellen erhebliche Mängel gezeigt, insbesondere in der Aktenaufbewahrung und bei der Aktenvernichtung. Diese Mängel hatte ich nach § 27 HDSG beanstandet und das Ministerium aufgefordert, für eine durchgreifende Verbesserung der Datenschutzsituation in der Landwirtschaftsverwaltung mehr Haushaltsmittel bereitzustellen. Das Ministerium hatte dies zugesagt, aber darauf verwiesen, daß hinsichtlich des erheblichen Umfangs an Haushaltsmitteln, die zur Gewährleistung einer sicheren Aufbewahrung von Akten mit personenbezogenen Daten erforderlich seien (Anschaffung von Stahlschränken), ein Zeitraum von mehreren Jahren ins Auge gefaßt werden müsse.

Nach Ablauf von drei Jahren haben sich bei den meisten Ämtern für Landwirtschaft und Landentwicklung erfreuliche Verbesserungen in der Datensicherung gezeigt. Dies konnte ich durch Kontrollbesuche bei etwa der Hälfte der betroffenen Ämter feststellen. In drei Ämtern war die Datensicherheit einwandfrei. In den übrigen waren zwar für die entsprechenden Haushaltsmittel – die zweckgebunden zur Verfügung gestellt worden waren – Stahlschränke angeschafft worden; es bedarf dort aber noch weiterer Maßnahmen, bis alle Akten mit personenbezogenen Daten sicher untergebracht sein werden.

Solange – mangels zugriffssicherer Aktenschränke – der unbefugte Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, kommt der Frage des Verschließens der Diensträume bei Abwesenheit besondere Bedeutung zu. Das Ergebnis meiner Kontrolle war insoweit bei den meisten Dienststellen unbefriedigend: Die meisten Zimmertüren sind nicht mit modernen Sicherheitsschlössern, sondern nur mit herkömmlichen sogenannten Bartschlössern ausgestattet; auch diese werden bei Abwesenheit der Beschäftigten meist nicht abgeschlossen, oder sie werden zwar abgeschlossen, aber der Schlüssel bleibt stecken. Die Folge ist, daß Unbefugte ohne Schwierigkeit die nicht besetzten Dienstzimmer betreten können, was meinen Prüfern in zahlreichen Fällen möglich war.

Auch wenn das Abschließen der Diensträume bei Abwesenheit für die Betroffenen eine gewisse Unbequemlichkeit mit sich bringt und auch wenn in manchen Ämtern erst organisatorische Maßnahmen (Anschaffung von Zweitschlüsseln bei Diensträumen, die mit mehreren Personen besetzt sind; Schlüsselbrett beim Pförtner usw.) getroffen werden müssen, kann nicht auf das Verschließen der Dienstzimmer bei Abwesenheit als einer wichtigen Maßnahme der Datensicherheit verzichtet werden. Dies gilt für alle Büroräume, in denen personenbezogene Daten verarbeitet werden. Das geschilderte Problem besteht freilich nicht nur bei den Landwirtschaftsämtern, sondern ist bei Prüfungen in den verschiedensten Verwaltungsbereichen immer wieder anzutreffen.

Was die Aktenvernichtung anbetrifft, so haben zwar inzwischen fast alle Landwirtschaftsämter Entsorgungsverträge mit entsprechenden Firmen abgeschlossen; dennoch bleibt hier ein gewisser Unsicherheitsfaktor erhalten, nicht so sehr was aussonderungsreife Altakten anbetrifft, als vielmehr im Hinblick auf Entwürfe, Notizen und nicht mehr gebrauchte Handakten: Der Weg vom Schreibtisch über den Papierkorb und die Mülltonne zum Aufbewahrungsraum bis zur Abholung durch die Firma bietet vielfältige Möglichkeiten dafür, daß die in den Akten enthaltenen personenbezogenen Daten von Unbefugten eingesehen werden können. Aus diesem Grund besteht nach wie vor aus der Sicht des Datenschutzes die Forderung, daß jedes Amt für Landwirtschaft und Landentwicklung mit wenigstens einem Reißwolf ausgestattet werden sollte, der eine sofortige Vernichtung entsprechenden Materials ermöglicht. Solche Geräte in Bürogröße sind heute zu einem Preis, der dem einer Schreibmaschine entspricht, zu haben und daher auch bei sparsamer Haushaltsführung erschwinglich.

13. Der neue Rundfunkstaatsvertrag – mehr Datenschutz für die Teilnehmer

Mit dem Zustimmungsgesetz vom 13. Dezember 1991 (GVBl. I S. 367) hat der Hessische Landtag den "Staatsvertrag über den Rundfunk im vereinten Deutschland" ratifiziert. Der Staatsvertrag, der sechs Einzelverträge umfaßt, ist am 1. Januar 1992 in Kraft getreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit ihrem "Arbeitskreis Medien" intensiv an der Diskussion um die Formulierung der Datenschutzbestimmungen im Staatsvertrag beteiligt. Neben der Mitarbeit in diesem Arbeitskreis habe ich wiederholt zu Einzelfragen gegenüber der Hessischen Staatskanzlei Stellung genommen.

Folgende Kernpunkte der Neuordnung des Rundfunks sind – aus datenschutzrechtlichem Blickwinkel – hervorzuheben:

1. § 28 des Rundfunkstaatsvertrages enthält für den gesamten privaten Rundfunk in der Bundesrepublik eine einheitliche Regelung über die Zulässigkeit der Verarbeitung von Verbindungs- und Abrechnungsdaten. Bisher

war der Datenschutz bei privaten Rundfunkveranstaltern – wenn überhaupt – in den einzelnen einschlägigen Landesgesetzen geregelt und dabei im Detail unterschiedlich ausgestaltet. Wichtigste Norm ist § 28 Abs. 3, der die Speicherung der Abrechnungsdaten in einer Form vorschreibt, die die Möglichkeit der Erstellung eines "Teilnehmerprofils" an Hand von Zeitpunkt, Art, Inhalt und Häufigkeit der eingeschalteten Sendungen ausschließt, wenn nicht ausdrücklich eine detaillierte Rechnung verlangt wird. Die Bestimmung entspricht der Regelung in § 53 Abs. 2 des Hessischen Privatrundfunkgesetzes. Die §§ 50ff. dieses Gesetzes gelten übrigens nach wie vor für Hessen ergänzend zu § 28.

2. § 8 des Rundfunkgebührenstaatsvertrages klärt das Verhältnis der öffentlich-rechtlichen Landesrundfunkanstalten zur Gebühreneinzugszentrale (GEZ) in Köln, bei der bundesweit die Daten aller angemeldeten Teilnehmer gespeichert sind, es sich mithin um eine der größten Datenbanken in Deutschland handelt. Die GEZ wird ausschließlich als Auftragnehmer der jeweiligen Landesanstalt tätig; letztere bleibt also für die Rechtmäßigkeit der Verarbeitung der Daten ihrer Gebührenzahler verantwortlich.

   Da für die Überwachung der Einhaltung der Datenschutzbestimmungen bei den Teilnehmerdaten des Hessischen Rundfunks wiederum meine Zuständigkeit gegeben ist (vgl. § 3 Abs. 6 Satz 2 HDSG; dazu zuletzt 18. Tätigkeitsbericht, Ziff. 2.6), besteht für mich Veranlassung, im Jahr 1992 die Datenverarbeitung bei der GEZ zu überprüfen. Dabei kann der interne Datenschutzbeauftragte behilflich sein, den die GEZ nach § 8 Abs. 2 des Staatsvertrages zu bestellen hat und der zur Zusammenarbeit mit der nach Landesrecht zuständigen Kontrollinstanz verpflichtet ist.

   Festgelegt wird in § 8 Abs. 1 auch die Rechtsstellung der im Außendienst der Rundfunkanstalten zur Ermittlung von bisher nicht angemeldeten Teilnehmern – vielfach auf freiberuflicher Basis – eingesetzten Mitarbeiter. Sie sind bei der Registrierung der Personalien usw. – datenschutzrechtlich gesehen – Auftragnehmer. Dies entspricht der bisherigen Rechtsauffassung und Praxis des Hessischen Rundfunks; dessen Verantwortlichkeit wird mit dem Gebührenstaatsvertrag jetzt auch ausdrücklich klargestellt.

3. Im neuen Bildschirmtextstaatsvertrag (§ 10) wird die bewährte Datenschutzregelung des bisherigen Vertrages (§ 9) unverändert übernommen. Wegen der vergleichsweise geringen Verbreitung des Mediums Btx ist die Bedeutung dieser Vorschrift in der Praxis allerdings nicht sehr groß. Die Länder unterstreichen mit der Bekräftigung der bisherigen Norm erneut ihre Auffassung, daß hier nach dem Grundgesetz die Landeskompetenz für die Mediennutzung gegeben ist, und zwar ungeachtet der Tatsache, daß der Datenschutz bei Bildschirmtext (auch) bundesrechtlich – früher in der TKO, seit 1. Juli 1991 in § 12 der Telekom-Datenschutzverordnung (TDSV) – festgelegt ist (zu diesem Kompetenzstreit vgl. 13. Tätigkeitsbericht, Ziff. 3.3.1 und 14. Tätigkeitsbericht, Ziff. 13.1.3, zur TDSV vgl. unten Ziff. 14.2).

Unverändert bleibt meine Kontrollzuständigkeit für den Einsatz von Bildschirmtext durch öffentliche Stellen in Hessen. Artikel 5 des Zustimmungsgesetzes übernimmt insoweit die im bisherigen Gesetz zum Staatsvertrag über den Bildschirmtext vom 24. Juni 1983 enthaltene Regelung.

Auch wenn nicht alle Anregungen der Datenschutzbeauftragten aufgegriffen worden sind, läßt sich insgesamt eine positive Bilanz ziehen. Die Datenschutzsituation der Rundfunkteilnehmer hat sich in Deutschland – insbesondere in den neuen Bundesländern – mit dem Inkrafttreten der neuen Staatsverträge spürbar verbessert.

14. Kriterien für die Sicherheit von Systemen der Informationstechnik

Wer seine Datenverarbeitungsanlage mit einer Sicherheitssoftware schützen möchte, findet zwar auf dem Markt eine Vielzahl von Produkten, kann aber oft nicht einschätzen, welches Produkt gut und für ihn das passende ist. Eine Beurteilungshilfe bieten hier die von der Zentralstelle für Sicherheit in der Informationstechnik (ZSI), einer Bundesbehörde, herausgegebenen "Kriterien für die Sicherheit von Systemen der Informationstechnik" (IT-Sicherheitskriterien).

14.1
Die IT-Sicherheitskriterien der Zentralstelle für Sicherheit in der Informationstechnik

Die vor knapp drei Jahren von der Zentralstelle für Sicherheit in der Informationstechnik herausgegebenen "Kriterien für die Sicherheit von Systemen der Informationstechnik (IT)" sind eine Fortentwicklung des amerikanischen, nach seiner Umschlagfarbe benannten "Orange Book" (Originaltitel: Trusted Computer System Evaluation Criteria) des amerikanischen Verteidigungsministeriums.

Diese IT-Sicherheitskriterien wurden als Maßstab zur Beurteilung der Sicherheit informationstechnischer Systeme im Auftrag der Bundesregierung erarbeitet. Hier werden Sicherheitsanforderungen ausgehend von den drei Grundbedrohungen entwickelt, denen ein IT-System ausgesetzt ist, nämlich

– unbefugter Informationsgewinn (Verlust der Vertraulichkeit),

– unbefugte Modifikation (Verlust der Integrität),

– unbefugte Beeinträchtigung der Funktionalität (Verlust der Verfügbarkeit).

Die folgenden Grundfunktionen

1. Identifizierung und Authentisierung,

2. Rechteverwaltung,

3. Rechteprüfung,

4. Beweissicherung,

5. Wiederaufbereitung,

6. Fehlerüberbrückung,

7. Gewährleistung der Funktionalität und

8. Übertragungssicherung

werden beschrieben und mit Hinweisen versehen, was in den Sicherheitsanforderungen für ein System bezüglich dieser Grundfunktionen festgelegt sein kann.

Für die Grundfunktion "Beweissicherung" beispielsweise kann in den Sicherheitsanforderungen eines Systems beschrieben sein:

– welche Ereignisse protokolliert werden sollen,

– welche Informationen dabei aufgezeichnet werden sollen,

– wo diese Informationen aufgezeichnet werden sollen,

– wer, wie und wann auf die Informationen zugreifen darf,

– nach welchen Kriterien diese Informationen ausgewertet werden sollen.

Die Funktionalitätsklassen beschreiben jeweils Anforderungen an die verschiedenen Grundfunktionen. Sie sollen "Anhaltspunkte" sein, die

– dem Anwender die Systemauswahl erleichtern sowie

– dem Hersteller bei der Konzeption und Einordnung seines Systems helfen.

Hierarchisch geordnet sind von den zehn Funktionalitätsklassen nur die Klassen F1 bis F5, die aus dem Orange Book abgeleitet sind.

Zur Beurteilung der Qualität der Sicherheitsfunktionen sind Qualitätsstufen (Q0-Q7) definiert. Sie beschreiben für verschiedene Einzelaspekte, wie z.B. Qualität der verwendeten Mechanismen, des Herstellungsvorgangs, der Algorithmen, der anwenderbezogenen Dokumentation etc., jeweils unterschiedlich hohe Anforderungen an den Auftraggeber, also den Hersteller oder Vertreiber, und den Prüfvorgang. Diese Qualitätsstufen sind aufsteigend geordnet, d.h. für eine höhere Qualitätsstufe steigen sowohl die Anforderung an den Hersteller als auch der Aufwand beim Prüfvorgang an.

14.2
Verwendungsmöglichkeiten für den Anwender

Was kann man nun als Anwender mit diesem, von seiner Struktur und seinen vielen Begriffen zunächst kompliziert und abstrakt anmutenden Werk anfangen? Zunächst können – wenn eine Schwachstellen- oder Bedrohungsanalyse für ein DV-Projekt vorliegt – Sicherheitsanforderungen formuliert und den verschiedenen Grundfunktionen zugeordnet werden. Für einen solchen maßgeschneiderten Maßnahmenkatalog bieten die IT-Sicherheitskritierien Anregung und Unterstützung. Weiter lassen sich eine oder mehrere Funktionalitätsklassen festlegen, die den gestellten Anforderungen am besten entsprechen, sowie die erforderlichen Qualitätsstufen.

Die Hauptbedeutung wird aber zukünftig nicht in der Unterstützung solcher eher hausinternen Abläufe liegen. Vielmehr ist ein Instrumentarium geschaffen, mit dem auch gegenüber Dritten, beispielsweise

– für Ausschreibungen,

– für Gespräche mit Herstellern und

– für Vertragsverhandlungen

die Anforderungen an die IT-Sicherheit hinreichend kurz und präzise formuliert werden können. Dabei wird bei nicht besonders sensiblen personenbezogenen Daten die Funktionalitätsklasse F2 mit der Qualitätsstufe Q3 anzustreben sein.

14.3
Zertifizierung von Produkten

Am 1. Januar 1991 ist das Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI – Errichtungsgesetz BSIG) in Kraft getreten (BGBl. I (1990) S. 2834). Damit wurde die Anbindung der Vorgänger, der Zentralstelle für das Chiffrierwesen (ZfCh) und der Zentralstelle für Sicherheit in der Informationstechnik (ZSI), an den Sicherheitsbereich aufgegeben. Das BSI ist dem Bundesminister des Innern unterstellt. Es hat u.a. die Aufgabe, die Sicherheit von informationstechnischen Systemen oder Komponenten zu prüfen und zu bewerten und Sicherheitszertifikate zu erteilen. Das BSI kann im Einvernehmen mit dem Antragsteller sachverständige Stellen mit der Prüfung und Bewertung beauftragen. Die Zertifizierung nimmt es selbst vor. Das könnte im Idealfall bedeuten: Hersteller und Vertreiber können für informationstechnische Systeme oder Komponenten ein Sicherheitszertifikat bei einer zentralen Stelle, dem BSI, beantragen. Diese prüft nach einheitlichen Kriterien. Der Anwender braucht "nur noch" aus der Menge der in Frage kommenden Produkte eines auszuwählen, dessen Zertifikat bezüglich der Funktionalitätsklassen und Qualitätsstufen seinen Anforderungen entspricht, und es vernünftig zu implementieren. Er muß also nicht mehr für alle angebotenen Produkte selbst prüfen, ob sie wirklich seinen Sicherheitsanforderungen genügen. Leider handelt es sich hier nur um ein Szenario, denn es fehlt eine ausreichende Zahl zertifizierter Sicherheitssoftware für die verschiedenen Funktionalitätsklassen und Qualitätsstufen. Dafür gibt es mehrere Gründe:

Zum einen sind die Gebühren für die Evaluierung und Zertifizierung den Herstellern/Vertreibern zu hoch. Ein Hersteller hat angemerkt, daß die Zertifizierung ihn mehr als einen ganzen Jahresgewinn für sein Produkt kostet. Diese Investition ist ihm zu hoch, zumal er sein Produkt auch ohne Zertifikat gut verkauft.

Außerdem gilt ein Zertifikat nur für ein ganz bestimmtes Produkt in einer ganz bestimmten Hard- und Software-Umgebung, nämlich in jener, die der Evaluation/Zertifikation zugrunde lag. Für veränderte bzw. weiterentwickelte Versionen ist das Zertifikat nicht mehr gültig; sie müßten also wieder zertifiziert werden. Über den Zeit-, Anforderungs- und Kostenrahmen der Zertifizierung solcher Nachfolgeversionen müssen Regelungen getroffen werden.

Nach Redaktionsschluß wurde bekannt, daß ab dem 1. Januar 1992 das BSI europäische Sicherheitskriterien, die "Information Technology Security Evaluation Criteria" (ITSEC), zunächst für zwei Jahre anwendet. Die bisherigen IT-Sicherheitskriterien sind maßgeblich in die Formulierung der ITSEC eingeflossen. Es gibt keine klaren Aussagen, ob Zertifikate auf Grundlage der IT- Sicherheitskriterien "umgeschrieben" oder nachzertifiziert werden müssen oder wie ein solches Verfahren aussehen wird. Fazit: Die Hersteller werden erst einmal abwarten.

14.4
Probleme und Forderungen

14.4.1
Überforderte Anwender

Es gibt fast keine zertifizierten Produkte, und daran wird sich auch in absehbarer Zukunft nichts ändern. Der DV-Anwender kann die IT-Sicherheitskriterien bzw. die ITSEC zur Ausschreibung verwenden, muß aber weiterhin selbst evaluieren, ob die Angebote seinen Anforderungen genügen. Dies ist besonders bei Personal Computern äußerst problematisch, denn es gibt eine fast unüberschaubare Anzahl von Sicherheitsprodukten für übliche PCs, darunter aber nur ein einziges zertifiziertes, das lediglich mit der Qualitätsstufe Q1 alle Forderungen von F1 und teilweise Forderungen von F2 erfüllt. Das heißt aber auch, daß in diesem Bereich kein einziges Produkt existiert, dessen Zertifikat auch nur annäherungsweise bei F2/Q3 liegt.

Für den Bereich der PC-Netze fehlen nach wie vor einheitliche, übergreifende Lösungen, die die lokalen und zentralen Ressourcen als integriertes System wirksam schützen können. Es gibt (Stand: Herbst 1991) für lokale Netze kein zertifiziertes Produkt.

Für die Mehrzahl der Anwender dürfte der Zeitaufwand für die Produkt- oder gar Marktanalyse zu groß sein. Den meisten Anwendern fehlen zudem die erforderlichen DV- und Systemkenntnisse. Auch muß berücksichtigt werden, daß der Hersteller aussagefähige vertrauliche Unterlagen, wie sie für eine Evualation/Zertifizierung nötig sind, in der Regel nicht zur Verfügung stellen wird.

14.4.2
Lösungsansätze

Da es nach meinen Informationen in absehbarer Zeit nicht zu erwarten ist, daß der Bund die aufgezeigten Probleme zu lösen vermag, sollte überlegt werden, einen – wenn auch nur vorläufigen – "hessischen" Weg zu finden, da der derzeitige Zustand auf Dauer nicht hingenommen werden kann.

Das Land Hessen könnte eine oder mehrere öffentliche (oder auch private) Stellen, die über das erforderliche Personal- und Fachwissen verfügen, beauftragen, entsprechende Untersuchungen vorzunehmen, und die hierfür notwendigen finanziellen Mittel bereitstellen. Hier wäre insbesondere an die hessischen Großrechenzentren zu denken, die dann mit ihrem so erworbenen Hintergrundwissen ihre Kunden auch bei einer sinnvollen Implementierung und Generierung vor Ort – gegebenenfalls gegen Entgelt – unterstützen könnten.

Diese Lösung hat – das sei noch einmal betont – den Mangel, daß die Rechenzentren sicherlich in der Regel nicht die von den IT-Sicherheitskriterien für eine Zertifizierung vorgeschriebenen Unterlagen zur Verfügung gestellt bekommen; denn diese für eine fundierte Bewertung zentralen Informationen werden wegen der damit verbundenen wirtschaftlichen und rechtlichen Firmeninteressen in aller Regel als Betriebsgeheimnisse eingestuft.

Statt genauer Kenntnis beschriebener Mechanismen kann man dann mit einer Probeinstallation versuchen, die internen Abläufe nachzuvollziehen und Defizite zu finden. Die Qualität der auf einer solchen Grundlage möglichen Aussagen ist mit der eines offiziellen Zertifikats nicht vergleichbar. Von daher kann es sich nur um eine Übergangslösung handeln, bis es hinreichend viele zertifizierte Produkte gibt. Diese Lösung hätte aber immerhin den Vorteil, daß nicht jede Behörde, jede Gemeinde entweder selbst diese Tests vornimmt oder irgendein oder gar überhaupt kein Produkt beschafft.

Auch der Hessische Datenschutzbeauftragte hat in der Vergangenheit Testinstallationen von Sicherheitsprodukten vorgenommen und sich mit ihrem Leistungsumfang und ihren Konzepten beschäftigt. Im Berichtsjahr gehörten dazu wieder eine Reihe von Gesprächen mit verschiedenen Software-Herstellern über Möglichkeiten zur Verbesserung insbesondere der Sicherheit und des Datenschutzes ihrer Produkte. Die Ergebnisse und Erkenntnisse dieser Recherchen fließen selbstverständlich auch in meine Beratung der Anwender ein. Bei der Fülle der vorhandenen Produkte ist es mir aber – insbesondere im PC-Bereich – nicht möglich, die Aufgaben des BSI bzw. der DV-Anwender zu übernehmen, eine Vielzahl entsprechender Produkte zu prüfen und zu bewerten und für die Landesregierung und ihre DV-Anwender im Einzelfall konkrete Empfehlungen zu geben.

Zusätzlich zu den dringend erforderlichen speziellen Produktuntersuchungen ist es wichtig, das im öffentlichen Bereich des Landes Hessen vorhandene Wissen über Sicherheitslücken und Schwachstellen von Software einerseits und mögliche Maßnahmen zu deren Vermeidung andererseits zusammenzutragen und auszutauschen. Dazu müßte zunächst für die verschiedenen Betriebssysteme geklärt werden, wer im Bereich der Landesverwaltung und der Kommunen über die erforderlichen gründlichen Systemkenntnisse und praktischen Erfahrungen verfügt. Dann könnten spezifische Arbeitsgruppen gebildet werden, die ihre Arbeit selbst konkretisieren und damit auch die Art des Wissenstransfers für weniger kundige Systembetreiber und -benutzer festlegen.

Auf jeden Fall muß das Problem der Sicherheit lokaler Netze dringend gelöst werden. Hier ist baldmöglichst zu prüfen, ob neben entsprechenden Ausschreibungen gezielte Entwicklungsaufträge erforderlich sind.

15. Datensicherheit

15.1
Fernwartung

Die Oberfinanzdirektion (OFD) Frankfurt hat für die hessischen Finanzämter das Verfahren BEA (Bearbeitereingabe Arbeitnehmerveranlagung) entwickelt. Es handelt sich dabei um ein Online-Verfahren, das die Bearbeiter von Anträgen auf Lohnsteuerjahresausgleich bzw. von Einkommensteuererklärungen unterstützt. Das Verfahren soll nun in allen 46 Finanzämtern eingeführt werden. Erfahrungsgemäß werden besonders in der ersten Zeit häufig Fehler auftreten. Deshalb soll sich Personal der OFD in Frankfurt um die Fehlerbeseitigung in allen Finanzämtern kümmern. Um für das Wartungspersonal Zeitverluste durch lange Anfahrten zu den Finanzämtern zu vermeiden und mit dem vorhandenen Personal auszukommen, wird eine Fernwartung der Anlagen erwogen.

Die Möglichkeit der Fernwartung zog auch ein Krankenhaus in Betracht. Dort wurden über Nacht automatisch Blutproben analysiert. Die Ergebnisse wurden auf einem Laborrechner gespeichert und mußten am nächsten Morgen zur Vorbereitung von Operationen und anderen Behandlungen zur Verfügung stehen. Es kam immer wieder vor, daß der Rechner nachts ausfiel. In diesen Fällen wurde der Rechnerbetreuer durch die Labornachtschicht angerufen. Er mußte dann sofort kommen, damit die Analyseergebnisse noch rechtzeitig zur Verfügung standen. Durch die Fernwartung erhoffte sich das Krankenhaus eine schnellere Fehlerbehebung und für den Mitarbeiter eine geringere Belastung.

Der Begriff "Fernwartung" wird für unterschiedliche Sachverhalte verwendet. Zum einen wird darunter die Ferndiagnose verstanden, d.h. es werden Fehler- und Statusmeldungen von einer Wartungszentrale aus überwacht. Zur Fehlerbehebung muß aber weiterhin das Personal vor Ort erscheinen. Zum anderen meint Fernwartung im engeren Sinne: Von einer Wartungszentrale aus werden Fehler festgestellt und auch Änderungen an Softwarekomponenten vorgenommen. Nur noch in Ausnahmefällen kommt Wartungspersonal zum Betreiber.

15.1.1
Für und Wider der Fernwartung

Die Fernwartung kann sowohl für den Betreiber als auch für die Stelle, die eine Wartung vornimmt, vorteilhaft sein. Das Wartungspersonal muß nicht mehr in allen Fällen zum Aufstellungsort des Rechners fahren, und wenn es doch kommen muß, kann es oft gleich alle erforderlichen Ersatzteile, Werkzeuge oder andere Hilfsmittel mitbringen, da der Fehler bekannt ist. Fehler lassen sich so im allgemeinen schneller beheben. Es wird weniger Wartungspersonal benötigt und die Wartung wird kostengünstiger.

Den Vorteilen stehen allerdings auch Nachteile gegenüber. Die resultieren vor allem daher, daß ein neuer Zugang zum Rechner geschaffen wird, über den sich Personen anmelden, die eine hohe Priorität und weitgehende Rechte auf dem Rechner besitzen müssen. Der Rechnerbetreiber kann nur begrenzt kontrollieren, welche Person tatsächlich eine Fernwartung vornimmt. Er kann nicht mit Sicherheit wissen, welches Gerät sich am anderen Ende der Datenleitung befindet und welche Daten eventuell dorthin übertragen werden. Ihm ist nicht bekannt, welche Sicherungsmaßnahmen in der Wartungszentrale getroffen sind. "Hacker" könnten über die Wartungsleitung Zugriff auf den Rechner erhalten.

Das Wartungspersonal hat weitgehende Zugriffsrechte auf einem Rechner. Ein Zugriff auf personenbezogene oder andere wichtige Daten auf dem Rechner kann daher meist nicht ausgeschlossen werden. Das hat folgende Gründe: Soll ein Fehler in einer Anwendung behoben werden, ist es in der Regel erforderlich, zur Fehlerfindung den Fehler mit echten Daten zu rekonstruieren. Um dann die Programme anzupassen, müssen Hilfsmittel des Betriebssystems genutzt und die geänderten Programme wieder mit den echten Daten getestet werden. Werden durch die Anwendung personenbezogene Daten verarbeitet, so kann ein Zugriff auf diese Daten generell kaum ausgeschlossen werden. Gibt es Probleme im systemnahen Bereich, so z.B. bei Datenbanken, müssen dem Techniker zur Fehlerbehebung die Möglichkeiten des Betriebssystems offen stehen. Je nach dem eingesetzten Betriebssystem kann damit ein weitgehender Zugriff auf Daten verbunden sein. Schließlich müssen dem Wartungspersonal bei Fehlern am Betriebssystem alle Möglichkeiten des Betriebssystems und eventuell sogar der Microcode zur Verfügung stehen. Ein umfassender Zugriff auf Daten kann hierbei in der Regel nicht ausgeschlossen werden. Gleiches gilt auch für Wartungen an Speichermedien. Hier kann prinzipiell auf alle Daten zugegriffen werden.

Bei einer Ferndiagnose ist es dagegen sehr wohl denkbar, daß kein Zugriff auf personenbezogene Daten möglich ist, da der Zugriff auf die Dateien mit Fehlermeldungen eingeschränkt werden kann.

Es muß in beiden Fällen jeweils geklärt werden, ob und auf welche personenbezogenen Daten zugegriffen wird oder werden kann.

15.1.2
Ausgestaltung der Fernwartung

Angesichts der mit der Fernwartung verbundenen besonderen Gefahren für die Datensicherheit muß in jedem Einzelfall geprüft werden, ob es problemlosere adäquate Maßnahmen gibt. Außerdem muß eine Abwägung erfolgen zwischen den sich aus einer Fernwartung ergebenden Risiken, die von der Sensibilität der gespeicherten Daten und der Ausgestaltung der Fernwartung abhängen, und den Folgen, die ein Verzicht auf die Fernwartung haben würde. Erst danach läßt sich beantworten, ob und wie eine Fernwartung erfolgen kann. Bei der Ausgestaltung der Fernwartung sind folgende Anforderungen zu berücksichtigen:

- Eine Fernwartung darf nur mit Wissen und Willen des Betreibers der Anlage erfolgen. Die Initiative zu einer Fernwartung muß von ihm ausgehen.

- Durch eine Anmeldeprozedur am Rechner muß sichergestellt werden, daß nur berechtigte Personen als Wartungspersonal arbeiten können.

- Die Aktivitäten des Wartungspersonals sind zu protokollieren und zu kontrollieren.

- Können die Möglichkeiten des Wartungspersonals, auf Daten zuzugreifen oder Programme aufzurufen, eingeschränkt werden, so muß dies geschehen.

- Es gibt Funktionen, die für normale Wartungen gesperrt sein müssen. So ist es in der Regel nicht nötig, daß das Wartungspersonal Benutzerkennungen einrichten, Zugriffsrechte setzen oder die Protokolldateien der Schutzsoftware einsehen und löschen kann.

Darüber hinaus gibt es weitere Fragen, die im Einzelfall bei der Beurteilung eine Rolle spielen.

- Existiert ein Fernwartungskonzept?
- Wie kann der Zugriff des Wartungspersonals auf personenbezogene Daten, soweit er möglich ist, kontrolliert werden?
- Können die Aktivitäten des Wartungspersonals an einem Bildschirm verfolgt werden?
- Ist es dem Betreiber jederzeit möglich, den Wartungsvorgang abzubrechen?
- Wird eine laufende Fernwartung angezeigt?
- Wie wird die Einhaltung getroffener Regelungen kontrolliert?

Auch neue technische Entwicklungen können die Fernwartung sicherer machen. Dazu gehören:

- Sicherere Datenleitungsnetze, sowohl bei der Anmeldung am Netz als auch bei der Übertragung von Daten. Die Gefahr, daß unberechtigte Personen mit einem Rechner eine Verbindung aufbauen, wird dadurch geringer.
- Differenzierte Zugriffsmöglichkeiten, d.h. das Wartungspersonal hat eingeschränkte Rechte.
- Verschlüsselung sensibler Daten, so daß die Vertraulichkeit gewahrt bleibt, selbst wenn das Wartungspersonal Zugriff auf die Daten erhält.

15.1.3
Konsequenzen für die beiden Fälle

15.1.3.1
Fernwartung bei den Finanzämtern

Die Oberfinanzdirektion hat mir versichert, bei einer Fernwartung würden folgende Sicherungsmaßnahmen getroffen:

- Es wird ein Rückrufmodem eingesetzt, daß der Bediener des Rechners im Finanzamt vor einer Fernwartung aktivieren muß. Wird das Modem angewählt, so trennt es die Verbindung und wählt eine fest vorgegebene Telefonnummer an, eben die der OFD.
- Für die Fernwartung muß der Bediener außerdem einen Hebel an der Systemkonsole umlegen. Dadurch wird der Bildschirm in der OFD zur Systemkonsole. Um selbst wieder arbeiten zu können, muß der Bediener wieder den Hebel umlegen. Das kann auch während einer Wartung geschehen.
- Der Mitarbeiter der OFD muß sich am Rechner mit Benutzerkennung und Paßwort anmelden.
- Auf dem Bildschirm im Finanzamt sind alle Eingaben und Anzeigen zu verfolgen, die bei der OFD erfolgen.
- Die Tätigkeit des OFD-Mitarbeiters wird protokolliert.
- Anhand der Protokolle wird überprüft, ob nur in dem zur Fehlerbehebung erforderlichen Umfang auf Daten zugegriffen wurde und Funktionen ausgeführt wurden.
- Die OFD bestimmt die Personen, die mit der Fernwartung betraut werden und stellt sicher, daß die nach § 10 HDSG erforderlichen Maßnahmen bei der OFD getroffen sind.

Mit diesen Maßnahmen kann ein Zugriff auf den Rechner durch Personen, die nicht bei der OFD mit der Fernwartung betraut sind, mit großer Sicherheit ausgeschlossen werden. Dem Wartungspersonal können allerdings bei der Fernwartung personenbezogene Daten bekannt werden. In Anbetracht der vorgesehenen Auswertungen der Protokolle könnte ein Mißbrauch der Fernwartung jedoch festgestellt werden. Bei einer konsequenten Umsetzung der Sicherungsmaßnahmen und der nötigen organisatorischen Vorkehrungen, insbesondere bei der Revision, ist die Fernwartung der Rechner der Finanzämter unbedenklich.

15.1.3.2
Fernwartung des Laborrechners im Krankenhaus

Bei einer näheren Untersuchung stellte sich heraus, daß nachts häufig Spannungsschwankungen auftraten. Der Laborrechner reagierte auf diese Schwankungen mit Programmabbrüchen und Stillstand. Eine USV-Anlage (unterbrechungsfreie Stromversorgung) wurde daraufhin installiert und sorgte dafür, daß die Spannungsschwan-

kungen ausgeglichen wurden und der Rechner nicht mehr ausfiel. Durch diese Maßnahme war die geplante Fernwartung nicht mehr erforderlich, ja die Verarbeitung lief sogar besser als sie mit der Fernwartung hätte laufen können.

15.2
Prüfung der Datensicherheitsmaßnahmen in einem kommunalen Gebietsrechenzentrum

Im Herbst 1991 habe ich die Datensicherheitsmaßnahmen des Kommunalen Gebietsrechenzentrums Frankfurt überprüft. Das KGRZ Frankfurt ist eines der größten Rechenzentren im öffentlichen Bereich in Hessen. Es verarbeitet die Daten von mehr als 200 Stellen, zu denen viele Kommunalverwaltungen gehören. Die eingesetzten Verfahren reichen z.B. von der Personaldatenverarbeitung über das Einwohnermelderegister, Ordnungswidrigkeitenverfahren bis hin zu PC-Anwendungen, um nur einige zu nennen. Zur Zeit können mehr als 1.500 Personen mit den Verfahren arbeiten.

Der Prüfungsschwerpunkt lag bei den systemseitigen Datensicherheitsmaßnahmen für den Großrechner, also den Sicherheitsmaßnahmen, die alle Anwendungen und alle Anwender des Großrechners betreffen. In diesem Zusammenhang hatte ich bereits im 16. Tätigkeitsbericht (Ziff. 4.2) einige Anforderungen formuliert.

15.2.1
Technisches Umfeld, das Betriebssystem MVS

In den Rechenzentren des hessischen DV-Verbundes und somit auch im KGRZ Frankfurt wird das Betriebssystem MVS (Multiple Virtual Storage) eingesetzt. Es handelt sich um ein Betriebssystem, das es vielen Benutzern gestattet, mit vielen verschiedenen Programmen gleichzeitig auf dem DV-System zu arbeiten. MVS übernimmt die Verwaltung der Betriebsmittel und Ressourcen wie Hauptspeicher, Plattenspeicher, Datenträger, Ausgabegeräte und Systemprogramme gegenüber den Anwendungsprogrammen, die von Benutzern eingesetzt werden.

Das von IBM entwickelte Betriebssystem MVS ist seit 1974 auf dem Markt. Im Laufe der Zeit wurde es immer weiter entwickelt, aber wesentliche Grundzüge haben sich fast zwanzig Jahre erhalten. Die Ursprünge reichen also noch in die Zeit zurück, als den Rechnern mit Lochkarten Programme und Daten eingespielt wurden. Damals hatten nur die Maschinenbediener Kontakt zu dem Rechner, und einem normalen Benutzer lagen Ergebnisse eigentlich nur in Form von Listen vor, d.h. es gab keine Dialogverarbeitung von Daten. Eine vorrangige Anforderung an MVS war folglich sicherzustellen, daß die verschiedenen Programme sich nicht gegenseitig stören, während die Kontrolle von Benutzern und deren Zugriffen auf Dateien kaum berücksichtigt wurden. Die Belange des Datenschutzes und der Datensicherheit sind im MVS selbst nicht ausreichend berücksichtigt.

15.2.1.1
Schutzfunktionen von MVS

Es sind unter MVS sogenannte Adreßräume eingerichtet, in denen jeweils die durch MVS zu trennenden Programme ablaufen. Die Ressourcenverwaltung des MVS stellt sicher, daß die Programme isoliert sind, d.h. die verschiedenen Adreßräume sind bezüglich der Ausführung von Problemprogrammen oder Dateizugriffen getrennt.

In einem Adreßraum können die unterschiedlichsten Programme ablaufen. Beispiele sind

- Anwendungsprogramme, die in einem festen Ablauf als sogenannter Job Daten verarbeiten (Jobs sind Verarbeitungsaufträge an das Betriebssystem),
- Datenbankmanagementsysteme, die Programmen aus anderen Adreßräumen Daten zur Verfügung stellen. Im Fall des KGRZ Frankfurt ist hier ADABAS (der Firma Software AG) zu nennen,
- TP(Teleprocessing)-Monitore, die Programme steuern, die von Benutzern im Dialog aufgerufen und genutzt werden. Beim KGRZ Frankfurt werden die TP-Monitore Com-Plete (der Fa. Software AG) und CICS (Customer Information Control System der Fa. IBM) genutzt.

MVS ordnet einem Adreßraum zum Ausführungszeitraum Dateien zu, die bearbeitet werden sollen. Neben anderen Steuerungsinformationen wird je Adreßraum eine Kennung gespeichert, die u.a. den Prüfungen durch die Schutzsoftware zugrunde gelegt wird. Sie läßt sich auf unterschiedliche Arten generieren; so kann es beispielsweise die Kennung sein, die ein Benutzer bei der Anmeldung eingegeben hat.

15.2.1.2
Grenzen der Schutzfunktionen von MVS

Solange es keine Zugriffskollisionen gibt, erlaubt es MVS jedem Programm, auf (fast) jede Datei zuzugreifen. Wenn also ein Benutzer selbst bestimmen kann, welche Dateien verarbeitet werden sollen, hat er umfassende Zugriffsmöglichkeiten. Um doch noch Einschränkungen vornehmen zu können, ist es erforderlich, eine Schutzsoftware einzusetzen.

Das Problem ist hinreichend bekannt, so daß es Zusatzprogramme mehrerer Anbieter gibt, mit denen die Sicherheit erheblich verbessert werden kann. Hier sind insbesondere ACF2 (Access Control Facility), Top Secret und RACF (Resource Access Control Facility) zu nennen. Von diesen Produkten wird auf den Rechnern des hessischen DV-Verbundes ACF2 eingesetzt (vgl. 16. Tätigkeitsbericht, Ziff. 4.2). In den USA wurde ACF2 hinsichtlich seiner Sicherheitsfunktionen untersucht und auf dem Level C2 (nach dem "Orange Book") eingestuft. Dies entspricht nach den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) angewandten Kriterien für die Sicherheit von Systemen der Informationstechnik (IT-Sicherheitskriterien) der Stufe F2/Q2. Die Software ist also geeignet, einen ziemlich hohen Stand bei den Sicherheitsmaßnahmen zu erreichen (vgl. Ziff. 14.1).

Es können sich unter MVS auch bei einem guten Schutzprodukt immer wieder Lücken ergeben, die es erlauben, den Schutz zu umgehen. Um diese zu erkennen und auszunutzen, sind aber tiefgehende Systemkenntnisse erforderlich, über die nur wenige Personen verfügen. Außenstehende müssen installationsspezifische Systeminformationen besitzen, um die Kenntnisse umsetzen zu können. Vor diesem Hintergrund reicht es nicht, Systemdateien gegen unberechtigte Änderungen zu schützen, sondern im Regelfall sollte ein Leseschutz vorhanden sein.

Ohne weitere Schnittstellen kann eine Kontrolle nur auf der Ebene der MVS bekannten Strukturen vorgenommen werden. Hierzu gehört auch der Adreßraum. Wenn sich an einem TP-Monitor also mehrere Benutzer anmelden und ihre Programme ausführen, so kennt MVS, und damit auch die Schutzsoftware, nur den Adreßraum mit seiner Kennung und kann diese Benutzer nicht unterscheiden. Eine differenzierte Behandlung der Zugriffe ist nicht möglich.

Um bei der Umsetzung systemseitiger Schutzmaßnahmen das Problem zu lösen, muß über eine Schnittstelle der Schutzsoftware mitgeteilt werden, welcher Benutzer einen Zugriff verlangt. Um welchen Benutzer es sich handelt, wird anhand der Benutzerkennung (User-Id) festgestellt. Die Güte der gesamten Zugriffskontrolle hängt daher davon ab, wie sicher die Identität eines Benutzers festgestellt werden kann (vgl. 19. Tätigkeitsbericht, Ziff. 15.4) und daß den Schutzprodukten bekannt ist, welche Person einen Zugriff vornimmt.

MVS muß daher zusammen mit einer Schutzsoftware eingesetzt werden. Die Software muß natürlich richtig implementiert sein, um das Schutzziel zu erreichen.

15.2.2
Festgestellte Mängel

Die Prüfung des KGRZ Frankfurt war seit längerer Zeit die erste Prüfung eines Großrechenzentrums, bei der die systemseitigen Sicherheitsmaßnahmen geprüft wurden. Ob das Ergebnis repräsentativ für andere Rechenzentren des hessischen DV-Verbundes ist, können nur weitere Prüfungen zeigen. Es kann derzeitig weder der Schluß gezogen werden, daß in den anderen Rechenzentren ähnliche Mängel vorkommen, noch daß beim KGRZ Frankfurt mehr Mängel vorhanden waren als in den anderen Rechenzentren.

Die festgestellten Mängel im organisatorisch-konzeptionellen Bereich und im technischen Bereich waren gravierender als bei den räumlichen Sicherheitsmaßnahmen. Dies lag nicht zuletzt an den Sicherheitsanalysen, die das KGRZ hatte erstellen lassen und die schwerpunktmäßig die räumlichen Gegebenheiten untersucht hatten.

Die Ergebnisse der Sicherheitsanalysen waren in ein Sicherheitskonzept eingeflossen, das folgerichtig räumliche Sicherungsmaßnahmen festlegte. Die vorgefundenen Mängel bei den räumlichen Sicherungsmaßnahmen werden bei der Umsetzung des Sicherheitskonzepts mit beseitigt.

15.2.2.1
Gesamtkonzept

Bei der Prüfung wurden mehrere Mängel festgestellt, die den Verantwortlichen bereits seit längerem bekannt waren. Andere Geschäftsinteressen hatten bei der Abwägung mit den Sicherheitsmaßnahmen den Vorrang erhalten. Es ist klar, daß nicht jede denkbare Sicherheitsmaßnahme gleich umgesetzt werden kann, aber in einigen Fällen hätte der Datenschutz eine höhere Priorität erhalten müssen. Die Tragweite der Mängel wurde zum Teil nicht erkannt (dies gilt z.B. für die Freigabe der Editierfunktion unter Com-Plete für normale Benutzer), oder die Mängel wurden einfach akzeptiert (wie im Fall von unzureichenden Namenskonventionen).

Um hier eine einheitliche Linie zu erreichen, muß ein Datenschutzkonzept erstellt werden. Darin sollte die Sicherheitspolitik des KGRZ festgelegt werden. Daraus ergeben sich Anforderungen, die zusammen mit den Ergebnissen einer Sicherheitsanalyse zu den Mitteln führen, mit denen die Umsetzung erfolgen kann. Ergänzt werden sollte das Konzept um einen Zeitplan für die Realisierung.

15.2.2.2
Revision

Eine wesentliche Komponente eines Sicherheitssystems ist die Revision. Das Ziel der Revision besteht, kurz gesagt, darin, festzustellen, WER hat WANN von WO mit WELCHEN MITTELN WAS veranlaßt und WORAUF zugegriffen. Die Revision stützt sich dabei in weiten Bereichen auf die Ergebnisse von Protokollierungen.

Die Prüfung beschränkte sich hier auf eine Kontrolle von ACF2, wobei die Frage beantwortet werden sollte, wie mit den Protokollen, die ACF2 erzeugt, verfahren wird. Im vorliegenden Fall wurden die ACF2-Protokolle einmal im Monat erstellt und durch den ACF2-Administrator kontrolliert. Die Protokolle und Auswertungen waren prinzipiell geeignet, viele Fragen zu beantworten, die sich einer Revision stellen. In zweierlei Hinsicht ergaben sich aber Probleme.

- Die Auswertung wurde zu selten vorgenommen. Die Listen waren daher so umfangreich, daß es kaum noch möglich war, den Überblick zu behalten. Darüber hinaus war auch die Verfolgung von Verstößen gegen eingeräumte Rechte erschwert, da die Verstöße zu lange zurücklagen.

- Der ACF2-Administrator kontrolliert seine eigene Tätigkeit. Einige der Kontrollen betreffen die Tätigkeiten des ACF2-Administrators selbst. In diesen Fällen lag ein Interessenkonflikt vor. Mehrere Auswertungen, auch Reports genannt, sind sowohl für die Revision als auch für die Administration wichtig. Sie können daher beiden Stellen zugehen.

Daraus resultierte die Forderung, ein Revisionskonzept zu erstellen. In einer ersten Stufe könnte sich das Konzept auf ACF2 beschränken, um dann zu einem Konzept für das gesamte System erweitert zu werden. Es sollte dabei geregelt werden:

- Welche Instanz wird mit der Revision (von ACF2) beauftragt? E s darf kein Interessenkonflikt durch die Tätigkeit entstehen. Insofern ist diese Funktion nicht bei der ACF2-Administration, in der Anwendungsentwicklung oder dem RZ-Betrieb anzusiedeln.

- Welche (ACF2-)Reports sind wann dieser Instanz zuzuleiten?
  Hier sind vor allem in Betracht zu ziehen:
  Reports von Zugriffsschutzverletzungen,
  Reports der abgewiesenen Anmeldungen,
  Reports der Aktivitäten mit besonders privilegierten Kennungen,
  Reports der Nutzung sensibler Programme,
  Reports vom Anlegen, Ändern und Löschen von Zugriffsregeln, der ACF2-Parameter, sonstiger Ressourcen und bei den Definitionen der Benutzerkennungen.

- Welche weiteren Kontrollen sind durchzuführen? Es muß das Ziel sein festzustellen, inwieweit ACF2 auf dem System aktiv ist. Neben einer Feststellung des Ist-Zustands zu bestimmten Zeitpunkten sollte eine Überwachung der Änderungen von sensiblen Bereichen zum Umfang der Kontrollen gehören. Hier sind u.a. zu nennen: APF-autorisierte Bibliotheken, PPT, Exits und SVCs. Insbesondere müssen die Benutzer mit besonderen Rechten und die Parameter, die ACF2 steuern (Einträge in den GSO – Records-Global System Options –), beachtet werden. Die Kontrolle von Zugriffsregeln für sensible Dateien können nach und nach intensiviert werden.

- Es muß geregelt werden, wie zu verfahren ist, wenn Unregelmäßigkeiten festgestellt werden.

15.2.2.3
Anmeldung am System; Zusammenspiel der vorhandenen Schutzprodukte

Die verschiedenen Schutzprodukte befanden sich noch weitgehend isoliert auf dem System. Eine sichere Benutzerkontrolle oder Zugriffskontrolle ist jedoch nur zu erreichen, wenn die Schutzprodukte ein Gesamtsystem bilden (vgl. 16. Tätigkeitsbericht, Ziff. 4.2 und 19. Tätigkeitsbericht, Ziff. 15.4).

Die Benutzerkontrolle und damit verbunden die sichere Feststellung der Identität des Benutzers durch den Rechner sind von zentraler Bedeutung für die Güte der technischen Schutzmaßnahmen. Die Prüfung benutzerspezifischer Rechte und die Auswertung von Protokollen setzen voraus, daß sich tatsächlich die Person angemeldet hat, der eine Kennung zugeordnet wurde.

Die Identität eines Benutzers wird während der Anmeldung am Rechner ermittelt. Dies geschieht durch eine Identifikation (Eingabe der Kennung) und eine Authentifikation (zur Zeit in der Regel die Eingabe eines Paßwortes).

Je nach dem angewählten TP-Monitor erfolgte die Benutzerkontrolle durch unterschiedliche Schutzprodukte. Bei TSO (Timesharing Option) und dem Test-Com-Plete wurde ACF2 genutzt, bei den anderen Com-Pletes und im Fall von CICS gab es jeweils eigene Prüfroutinen. Zusätzlich gab es auf der Anwendungsebene noch verschiedene Programme zur Zugriffskontrolle, an denen ebenfalls eine "Anmeldung" erfolgen mußte. Hier sind u.a. die Vorstellungsdatei und die FINPA zu nennen.

Die Qualität der Authentifikationsfunktion, die sicherstellen soll, daß sich tatsächlich die Person anmeldet, der eine Kennung zugeordnet wurde, war bei den verschiedenen Produkten sehr unterschiedlich. Von den genannten Produkten wurden bei ACF2 die Sicherheitsanforderungen am besten umgesetzt. Die anderen Produkte hatten demgegenüber alle ihre Schwächen.

Um mit einer Anwendung arbeiten zu können, mußte ein normaler Benutzer ein mehrstufiges Anmeldeverfahren durchlaufen. Bei dem Verfahren Gewerberegister erfolgte zuerst die Anmeldung an dem TP-Monitor CICS. Anschließend mußte die Anmeldung bei der Vorstellungsdatei vorgenommen werden. Da kein Abgleich der Kennungen erfolgte, war es möglich, mit unterschiedlichen Kennungen zu arbeiten. Ein Benutzer konnte sich am CICS als Benutzer "Meier" der Gemeinde A anmelden und gegenüber der Vorstellungsdatei mit dem Schlüssel, der dem Benutzer "Müller" der Gemeinde B zugeordnet war. Ein "Identitätswechsel" war möglich (vgl. 19. Tätigkeitsbericht, Ziff. 15.4).

Die Unzulänglichkeiten bei der Benutzerkontrolle, also der Anmeldung am Rechner und dem Zusammenspiel der verschiedenen Schutzprodukte, können nur abgestellt werden, wenn ein Gesamtkonzept existiert und umgesetzt wird.

Die Schutzprodukte auf der Anwendungsebene können derzeit aus verschiedenen Gründen nicht ersetzt werden. Die Lage ändert sich spätestens, wenn Anwender die Möglichkeit erhalten, direkt Abfragen an das Datenbanksystem zu richten. Es stehen ihnen dann sogenannte Query-Languages zur Verfügung. In diesem Fall gibt es kein Schutzprodukt auf der Anwendungsebene, das eine Kontrolle vornehmen könnte. Eine Kontrolle kann dann nur noch über das Datenbankmanagementsystem erfolgen. Zu diesem Zeitpunkt wird die Frage akut, ob auch die Zugriffskontrolle in den Anwendungen besser über das Datenbankmanagementsystem erfolgen sollte.

15.2.2.4
Implementierung von ACF2

Auf dem Rechner war als MVS-Schutzsoftware ACF2 installiert. AC F2 ist geeignet, die Anmeldung am System und die Nutzung von MVS weitgehend zu kontrollieren. In der vorgefundenen Implementierung war ACF2 jedoch fast wirkungslos, was Dateizugriffe betraf. Die unter 15.2.2.3, 15.2.2.5, 15.2.2.6 und 15.2.2.8 geschilderten Mängel beruhen teilweise darauf, daß ACF2 noch nicht vollständig aktiviert war. Darüber hinaus gab es noch Defizite bei der Definition von Benutzern. Kurz gesagt, das Schutzprodukt ACF2 war so implementiert, daß es den Erfordernissen des Datenschutzes in einigen Punkten nicht genügte.

15.2.2.4.1
Zugriff auf Dateien

Zum Zeitpunkt der Prüfung waren nur für einen Teil der Dateien Zugriffsregeln definiert, die festlegen, welcher Benutzer wie auf die Daten zugreifen kann. Insbesondere im Bereich der Produktionsdateien und der Systemdateien existierten nur wenige Zugriffsregeln. Dies ist normalerweise unproblematisch, da ACF2 einen Zugriff abweist, wenn keine Zugriffsregel existiert, die ihn erlaubt (Verbot mit Erlaubnisvorbehalt). Um trotz der fehlenden Regeln mit dem Rechner arbeiten zu können, war jedoch der Parameter gesetzt, der für eine Übergangszeit die Philosophie von ACF2 umkehrt: Es war die ACF2-Option MODE (RULE QUIET ABORT) gesetzt, die für den Fall, daß zu einer Datei keine Zugriffsregel existiert, den Zugriff erlaubt. Von den vorhandenen Regeln waren darüber hinaus viele mit dem Modus QUIET definiert, wodurch wiederum jedem Benutzer der Zugriff erlaubt wurde. Es ist durchaus sinnvoll, daß diese Möglichkeiten existieren, da sie es erlauben, im laufenden Betrieb eine Schutzsoftware einzuführen.

Im vorliegenden Fall war ACF2 aber vor mehr als zwei Jahren installiert worden, so daß die Übergangszeit verstrichen war, in der die Option akzeptiert werden konnte.

In einigen Fällen war zwar eine Protokollierung von Dateizugriffen vorgesehen, diese war allerdings nur bedingt aussagefähig (vgl. Ziff. 15.2.2.2).

Eine solche Generierung hat weitreichende Konsequenzen. So hatten unberechtigte Personen Zugriff auf Produktionsdateien, wodurch die Zugriffskontrolle nicht sichergestellt war. Zusätzlich ergaben sich nicht so offensichtliche Lücken, die es ermöglichen, den Rechnerbetrieb selbst zu beeinträchtigen. Hier sind zu nennen:

- Es konnten Dateien gelesen werden, die MVS parametrisieren. Die Kenntnis dieser Informationen erleichtert es, das MVS selbst zu beeinflussen oder ACF2 zu umgehen.

- Systemdateien konnten geändert werden. Teile des Betriebssystems konnten geändert werden und es war möglich, Programme zu erstellen, die die Schutzmechanismen von MVS und ACF2 umgehen können. Das Betriebssystem selbst war daher nicht ausreichend geschützt.

- Es war auch möglich, den Inhalt der CICS-Tabellen einzusehen. Daraus ergab sich, daß viele Personen (Benutzer, die editieren konnten, Mitarbeiter des KGRZ) CICS-Kennungen und deren Paßwort sich beschaffen konnten. Eine Anmeldung unter einer fremden CICS-Kennung, wie der des CICS-Systemprogrammierers, wäre möglich gewesen.

- Der Zugriff auf die SMF-Dateien, d.h. die Protokolldateien des MVS, war kontrolliert. Jedoch waren die "Backups", d.h. die Sicherungskopien der SMF-Dateien, auf denen dann die Auswertungen aufbauten, nicht geschützt. Es war folglich möglich, Protokollinformationen abzuändern.

- Die Dateien, in den die Sourcen und die Lademodule der Produktionsprogramme gespeichert wurden, konnten durch einen zu großen Personenkreis geändert werden.

- Es gibt besonders sensible Hilfsprogramme, die nur in begründeten Fällen genutzt werden dürfen. Diese Programme befanden sich in Dateien, die allgemein zugänglich waren. Die Benutzung wurde zwar für einige Programme durch ACF2 protokolliert, es darf aber nur berechtigten Personen möglich sein, die Programme auszuführen. Die Programme müssen in lesegeschützten Dateien stehen.

Für die meisten Dateien war folglich der Zugriffsschutz von ACF 2 nicht aktiv. Um das zu ändern, ergaben sich folgende Forderungen:

- Wenn keine Zugriffsregel existiert, muß der Zugriff abgewiesen werden.

- Wird einem Benutzer kein Zugriffsrecht eingeräumt, so ist der Zugriff abzuweisen. Nur in begründeten Ausnahmefällen darf trotzdem der Zugriff erlaubt werden. Dann muß aber eine Protokollierung hierüber erfolgen.

- Die Zugriffsrechte für Produktionsdateien sind restriktiv zu vergeben.

- Auch die Zugriffsrechte auf Systemdateien sind restriktiv zu vergeben. So muß erreicht werden, daß nur berechtigte Benutzer sie lesen und ändern können. Das bedeutet: Systemdateien müssen im Regelfall lesegeschützt sein. Besonders sensible Programme gehören in Programm-Bibliotheken, die lesegeschützt sind. Ihre Anwendung ist zu kontrollieren.

15.2.2.4.2
Definition der Benutzerkennungen

Ein weiterer Bereich, der unter ACF2 zu beachten ist, betrifft die Definition von Benutzerkennungen. Es werden den Kennungen ACF2-Rechte, auch Privilegien genannt, zugeordnet. Beim KGRZ wurden noch nicht alle Optionen von ACF2 genutzt, so daß nicht alle möglichen Privilegien zur Anwendung kamen. Einige der Privilegien sind wegen der damit verbundenen Möglichkeiten besonders restriktiv zu vergeben. Im Zusammenhang mit der Prüfung waren besonders zu beachten:

SECURITY Das Privileg müssen ACF2-Administratoren haben. Der Benutzer kann alle Einträge in ACF2 vornehmen. Er hat Zugriff auf alle Dateien, geschützte Programme und Ressourcen. Ein Dateizugriff, der nicht durch eine Zugriffsregel erlaubt ist, wird protokolliert (Eine Einschränkung kann das Privileg RULEVLD erzwingen, durch das Zugriffe eines Benutzers nur im Rahmen der Regeln erlaubt werden; dies gilt auch für Kennungen mit SECURITY).

NON-CNCL Dem Benutzer wird jeder Dateizugriff erlaubt. Es wird aber protokolliert, wenn der Zugriff nicht durch eine Regel erlaubt wurde.

RESTRICT Die Kennung kann nur in Jobs genutzt werden. Es ist kein Paßwort zur Anmeldung erforderlich. Wenn ein Job mit einer derartigen Kennung gestartet wird, erfolgt ein Protokolleintrag.

TAPE-BLP Der Benutzer kann auf Banddateien unter Umgehung des Labels, d.h. des Dateinamens, zugreifen. Es ist damit möglich, den ACF2-Schutz vor Banddateien zu umgehen.

Es stellte sich heraus, daß einige Benutzereinträge angepaßt werden mußten.

- Das Privileg SECURITY war zu oft vergeben.

- Es war noch die Standardkennung von ACF2 aktiv, die umfassende Rechte unter ACF2 besaß. Die Kennung ist inzwischen deaktiviert.

- Das Privileg TAPE-BLP war mehr als dreißig Benutzern zugeordnet. Um den Schutz der Banddateien zu verbessern, habe ich gefordert, nur den Benutzern dieses Privileg zu geben, für deren Tätigkeit es unbedingt erforderlich ist.

- Es waren fünf Kennungen mit dem Privileg NON-CNCL definiert. Die gleichen fünf Kennungen waren mit RESTRICT definiert, was bedeutet, daß keine Paßwortprüfung erfolgt. Mit diesen Kennungen könnte Mißbrauch betrieben werden, da sie in einen Job eingetragen werden können, ohne ein Paßwort zu kennen und trotzdem jeder Zugriff erlaubt wird. Ich habe daher gefordert sicherzustellen, daß ein Mißbrauch ausgeschlossen wird. Eine Lösung wäre, diese Kombination von Privilegien abzuschaffen.

- Die Parameter zur Kontrolle des Paßwortes entsprachen nicht den Anforderungen, die ich in meinem 19. Tätigkeitsbericht (Ziff. 15.5) aufgestellt habe. So wurde für Paßwörter lediglich eine Länge von vier bzw. fünf Stellen erzwungen, und es gab keinen Wert für die maximale Gültigkeitsdauer eines Paßwortes. Es gab

Kennungen, bei denen das Paßwort mehr als zwei Jahre nicht geändert worden war. Das Defizit war aber bereits längere Zeit bekannt, und es waren Maßnahmen ergriffen worden, um es abzustellen. Noch während der Prüfung wurden die entsprechenden Änderungen vorgenommen.

15.2.2.4.3
Namenskonventionen

Es waren unter ACF2 über 1.500 Benutzerkennungen eingerichtet. Eine Regelung, die den Aufbau der Kennungen festlegte, existierte nicht. Die Kennungen waren fünf oder sechs Stellen lang und in unterschiedlichster Weise aufgebaut. Als Folge davon konnten ACF2-Regeln nur aufwendig erstellt und nur mit viel Aufwand kontrolliert werden. Es ist nötig, Namenskonventionen zu erstellen.

15.2.2.5
Zugriffsmöglichkeiten für Mitarbeiter der Verwaltungen

Normalerweise werden Benutzern auf einem Großrechner bestimmte DV-Verfahren zugeordnet, und sie können nur diese benutzen. Den Benutzern sind lediglich einige Anwendungsfunktionen zugänglich, und es gibt keine Möglichkeit, auf die Systemebene zu gelangen. Es sind auch die Dateien fest vorgegeben, mit denen gearbeitet werden kann. Innerhalb der Verfahren gibt es meist noch Kontrollen, die sicherstellen, daß ein Zugriff nur im Rahmen von eingeräumten Berechtigungen möglich ist.

Dieser Regelfall wurde am Beispiel des Verfahrens Gewerberegister geprüft. Soweit ersichtlich, waren die Sicherheitsmaßnahmen ausreichend. In einigen anderen Verfahren gab es aber eine Konstellation, in der Benutzer zu weitgehende Zugriffsmöglichkeiten besaßen. So war häufig Benutzern die Möglichkeit eröffnet worden, für diese Verfahren die Steuerungsanweisungen selbst zu erfassen oder auch eine einfache Textverarbeitung vorzunehmen. Es gab aber keine Zugriffsbeschränkung auf vorgegebene Dateien, sondern es konnten beliebige Dateien angewählt werden. Da ACF2 nicht vollständig aktiviert war und es keine Schnittstelle zwischen dem Com-Plete und ACF2 gab, hatten die Benutzer weitreichende Zugriffsmöglichkeiten. Die Benutzer mit den Editierfunktionen konnten auf fast alle Dateien zugreifen. Es handelte sich um Dateien anderer Anwender, sonstige Produktionsdateien (Programmbibliotheken, Dateien mit Jobs, ...) und Systemdateien.

Auf viele Dateien konnten sie im Dialog zugreifen und, da es auch möglich war Jobs zu erstellen und zu starten, war der Zugriff auf die restlichen Dateien mit einem Job möglich. Der Zugriff war dabei nicht nur lesend, es war auch möglich, die Daten anderer Anwender und in vielen Fällen Systemdateien abzuändern. Der fast uneingeschränkte Zugriff auf die Systemebene war somit gegeben.

In diesen Fällen war es nötig, umgehend tätig zu werden. Neben Einträgen unter ACF2 mußte auch die Schnittstelle zwischen Com-Plete und ACF2 aktiviert werden, damit ACF2 die Information übergeben wird, welche Kennung (und damit welche Person; vgl. 15.2.2.3) einen Zugriff beansprucht. Die Anpassungen ziehen aber durchaus noch weitere Änderungen nach sich, so bei der Anmeldung am Com-Plete, bei der dann ACF2 die Kontrolle hat (vgl. Ziff. 15.2.1 und 15.2.2.4). Das KGRZ hat sofort Maßnahmen ergriffen und innerhalb kürzester Zeit die Schnittstelle in Betrieb genommen.

15.2.2.6
Funktionstrennung; Zugriffsmöglichkeiten für Mitarbeiter des KGRZ

In den geprüften Bereichen war die Funktionstrennung für die Mitarbeiter organisatorisch sichergestellt. Eine Ausnahme stellte der Datenschutzbeauftragte dar, dem die Funktion des stellvertretenden ACF2-Administrators zugewiesen war. In diesem Fall war ein Interessenkonflikt gegeben, da zu den Aufgaben des Datenschutzbeauftragten u.a. gehört, bei der Überwachung der nach § 10 HDSG erforderlichen Datensicherungsmaßnahmen mitzuwirken. Dies bedeutet aber, daß er seine Tätigkeit als ACF2-Administrator kontrollieren müßte (vgl. 15.2.2.2). Die Aufgaben des Datenschutzbeauftragten müssen entsprechend abgeändert werden, da der interne Datenschutzbeauftragte nach § 5 Abs. 2 HDSG keinem Interessenkonflikt ausgesetzt sein darf.

Die organisatorisch gegebene Funktionstrennung war nicht durch technische Sicherungsmaßnahmen unterstützt. Die Zugriffsmöglichkeiten der KGRZ-Mitarbeiter entsprachen im wesentlichen denen der oben beschriebenen Benutzer. So konnten z.B. Mitarbeiter der Anwendungsentwicklung prinzipiell auf Produktionsdaten auch ändernd zugreifen.

Im Fall der Administration der Vorstellungsdatei (vgl. 15.2.2.3) war für jede Anwendung ein Anwendungsbetreuer bestimmt, der als Oberberechtigter für die jeweilige Anwendung Zugriffsrechte vergeben sollte. Ein Oberberechtigter ist aber eine Person, die in der Vorstellungsdatei Zugriffsrechte für alle Verfahren vergibt. Es gab keine Möglichkeiten, die Rechte der Oberberechtigten im nötigen Umfang einzuengen. Dies muß geändert werden. Eine Lösung ließe sich durch organisatorische Maßnahmen oder Änderungen in den Programmen der Vorstellungsdatei erreichen.

15.2.2.7
Magnetbandverwaltung

Es wurde die Magnetbandverwaltung für den Rechenzentrumbetrieb geprüft. Die Maßnahmen bei Disketten oder anderen Datenträgern, die nicht im Verantwortungsbereich des Rechenzentrumbetriebs lagen, blieben unberücksichtigt. Für die ausgewählten Magnetbänder wurde im Datenträgerarchiv der richtige Aufbewahrungsort angegeben. Die Magnetbänder waren auch ausreichend gekennzeichnet, so daß es im Regelfall keine Schwierigkeiten bereitete festzustellen, wo sich ein Magnetband befand. Es gab aber Probleme beim Datenträgeraustausch und bei der Trennung zwischen Bändern für Test und Produktion:

- Bei der Überprüfung von Magnetbändern, die nach den Unterlagen verschickt worden waren, wurden unrichtige Angaben gefunden.
- In den Räumen der Anwendungsentwicklung befanden sich Magnetbänder, die vorher bei der Sicherung von Produktionsdaten genutzt worden waren. Die Magnetbänder waren nicht gelöscht.
- Die Magnetbänder waren nicht gegen irrtümliches Überschreiben vor der Freigabe geschützt.

15.2.2.8
Versionskontrolle von Produktionsprogrammen

Die Versionskontrolle wurde aufbauend auf der aktuellen Programmversion mittels Listen durchgeführt. Welche Version bei einem bestimmten Programmlauf vorgelegen hatte, ergab sich aus dem Joblog, d.h. dem Protokoll der Systeminformationen zu einem Job.

Die Produktionsprogramme lagen als Ladeprogramme und in Sourceform in Produktionsdateien vor. Bei der Versionskontrolle und der Freigabe von Produktionsprogrammen wurden kaum Mängel festgestellt. Es mußten aber noch die folgenden Punkte angegangen werden, damit die Versionskontrolle revisionssicherer wird:

- Die Programmversionen im Rahmen der Versionskontrolle umfaßten nicht die Schnittstellendefinitionen (Includes) und die Datenbankdefinitionen.
- Die Schnittstellendefinitionen befanden sich nur im Testbereich, wo sie der Anwendungsentwicklung zur Verfügung standen. Es war dabei auch möglich, in alten Versionen zu ändern.
- Die Dateien mit den Produktionsprogrammen waren nicht durch ACF2 geschützt, sondern durch die Vergabe eines Expirationdate (Verfalldatums). Es waren daher Programmänderungen möglich, die durch die Versionskontrolle unbemerkt geblieben wären.

15.2.3
Fazit

Wenn man sich vor Augen hält, wie viele Benutzer mit welchen Anwendungen arbeiten und welche Komponenten reibungslos ineinandergreifen müssen, war es kaum zu erwarten, daß keine Mängel bei der Prüfung festgestellt würden.

Die festgestellten Mängel sind sicherlich nicht spezifisch für das KGRZ Frankfurt. In dieser oder ähnlicher Ausprägung dürften sie bei Prüfungen unabhängig vom eingesetzten Rechner oder der Größe der Installation auch anderswo vorkommen. Verallgemeinert lassen sie sich so darstellen:

- Es fehlte ein Datenschutzkonzept.
- Es fehlte ein Revisionskonzept.
- Die verschiedenen Schutzprodukte bildeten kein Gesamtsystem, so daß die Qualität der Sicherheitsmaßnahmen sich am schwächsten Produkt ausrichtete. (So wurde insbesondere bei der Benutzerkontrolle der Stand der Technik nicht erreicht.)
- Vorhandene Schutzprodukte wurden so administriert, daß Benutzern zu oft Sonderrechte gegeben wurden und die Zugriffsmöglichkeiten auf Dateien zu weitgehend waren.
- Normale Benutzer hatten Zugang zur Betriebssystemebene des Rechners.
- Die Funktionstrennung im Rechenzentrum war nicht technisch sichergestellt.

– Es wurde nicht zwischen Magnetbändern für Test und Produktion unterschieden.

– Es wurden im Rahmen einer Versionskontrolle nicht alle erforderlichen Informationen vorgehalten.

Es zeigt sich hieran, daß Datensicherheit noch nicht heißt, ein (zertifiziertes) Schutzprodukt auf einem Rechner einzuspielen. Die Qualität der Sicherheitsmaßnahmen ergibt sich durch das Zusammenspiel aller Komponenten. Hier sind zu nennen:

– organisatorische Maßnahmen wie das Erstellen von Konzepten oder Dienstanweisungen,

– technische Sicherheitsmaßnahmen und deren richtiger Einsatz,

– räumliche Sicherheitsmaßnahmen und

– die Kontrolle der Maßnahmen.

Es steht noch eine Stellungnahme aus, in der das KGRZ u.a. die Maßnahmen beschreibt, die zur Behebung der Mängel ergriffen wurden bzw. vorgesehen sind. Ich werde die Umsetzung der Maßnahmen kontrollieren und die Erfahrungen bei weiteren Prüfungen einbringen.

15.3
Auftragsdatenverarbeitung

Städte und Gemeinden beauftragen nicht selten private Firmen mit der Verarbeitung personenbezogener Daten. Das geschieht zum Beispiel, wenn ein privates Rechenzentrum eingeschaltet wird oder die Gemeinde ein privates Unternehmen mit der Erhebung bestimmter Daten beauftragt (vgl. hierzu z.B. Ziff. 11). Dagegen ist nichts einzuwenden, solange die besonderen Bestimmungen, di e das Hessische Datenschutzgesetz hierfür enthält, befolgt werden. Ich mußte jedoch auch im Jahr 1991 wieder mehrfach feststellen, daß zumeist aus Unkenntnis die gesetzlichen Vorgaben für die Auftragsdatenverarbeitung nicht beachtet wurden.

Übersehen wurde beispielsweise, daß der Auftraggeber, also die Stadt oder die Gemeinde, auch für die Datenverarbeitung, die das beauftragte Unternehmen durchführt, verantwortlich bleibt. Die Privatfirma übt lediglich eine Hilfsfunktion aus. Die auftraggebende Stelle bleibt auch der zuständige Ansprechpartner für den von der Datenverarbeitung betroffenen Personenkreis. We nn ein Betroffener sein Recht auf Auskunft (§ 18 Abs. 1 HDSG), Benachrichtigung (§ 18 Abs. 2 HDSG), Berichtigung, Sperrung und Löschung (§ 19 HDSG) sowie Schadensersatz (§ 20 HDSG) geltend machen will, so muß er sich nicht an die im Auftrag der Stadt/Gemeinde tätige private Firma wenden, sondern an die Gemeinde selbst. Verstöße gegen Datenschutzbestimmungen muß sich der Auftraggeber stets zurechnen lassen. Es empfiehlt sich deshalb, den Auftragnehmer besonders sorgfältig auszuwählen, auch wenn das Hessische Datenschutzgesetz in § 4 dies nicht ausdrücklich vorschreibt (anders das Bundesdatenschutzgesetz: § 11 Abs. 2 Satz 1 BDSG verlangt ausdrücklich die sorgfältige Auswahl des Auftragnehmers). Der Auftraggeber muß außerdem seinem Auftragnehmer klare Weisungen hinsichtlich der durchzuführenden Datenverarbeitung erteilen. Weiterhin hat er darauf zu achten, daß beim Auftragnehmer die nach § 10 HDSG erforderlichen technischen und organisatorischen Maßnahmen, die die Datensicherheit gewährleisten sollen, getroffen sind.

Da die Vorschriften des Hessischen Datenschutzgesetzes nicht für Privatfirmen gelten, hat der Auftraggeber vertraglich sicherzustellen, daß der Auftragnehmer die Bestimmungen des HDSG befolgt und sich der Kontrolle durch den Hessischen Datenschutzbeauftragten unterwirft (§ 4 Abs. 2 HDSG). Anderenfalls hieße dies, daß beliebig viele Datenverarbeitungsvorgänge im Wege der Auftragsdatenverarbeitung der Kontrolle durch den Hessischen Datenschutzbeauftragten entzogen werden könnten. Damit der Hessische Datenschutzbeauftragte diese Kontrolle wirksam ausüben kann, hat die auftraggebende Stadt oder Gemeinde die zusätzliche Verpflichtung, dem Hessischen Datenschutzbeauftragten mitzuteilen, welche Stelle/Firma mit der Datenverarbeitung beauftragt wurde.

15.4
Versendung von Unterlagen als Massendrucksachen

Eine Gemeinde bat mich im vergangenen Jahr um Stellungnahme zu der Frage, ob sie die anfallenden Steuerbescheide als Massendrucksache versenden könne. Das Landesversorgungsamt beabsichtigte, Schriftstücke mit personenbezogenen Daten als verschlossene Drucksache zu verschicken. Dies sind nur zwei von mehreren mir im letzten Jahr bekannt gewordenen Fällen, in denen erwogen wurde, aus Gründen der Kostenersparnis die Massenpost – selbst wenn sie Unterlagen mit personenbezogenen Angaben enthielt – per Drucksache zu versenden.

Ich habe in allen Fällen klargestellt, daß Schriftstücke mit personenbezogenen Daten nicht als Drucksache versandt werden dürfen; denn die Post kann solche Sendungen jederzeit zu Prüfzwecken öffnen. Wer eine derartige Versendungsform wählt, gibt damit zu erkennen, daß der Inhalt des Briefes nicht besonders schützenswert ist. In den beiden Beispielen geht es aber um besonders schützenswerte Angaben. Steuerbescheide enthalten Daten, die dem Steuergeheimnis (§ 30 Abgabenordnung) unterliegen. Die Schreiben des Landesversorgungsamtes werden in aller Regel Daten enthalten, die dem Sozialgeheimnis (§ 35 Sozialgesetzbuch I) unterliegen und die deshalb ebenfalls besonders schützenswert sind. Aber auch wenn für die Daten keine besondere Geheimhaltungsvorschrift gilt, sollte

die Versendungsform Drucksache nicht gewählt werden; denn es gehört zum wesentlichen Inhalt des Rechts auf informationelle Selbstbestimmung, daß der einzelne darauf vertrauen kann, daß Unbefugte keinen Einblick in ihn betreffende Daten erlangen. Die Postbediensteten, die bei Drucksachen zu Überprüfungszwecken jederzeit Einblick nehmen könnten, sind in diesem Zusammenhang Unbefugte.

16. Bilanz

16.1
Hessisches Personalinformationssystem – HEPIS
(16. Tätigkeitsbericht Ziff. 8.2.2, 19. Tätigkeitsbericht Ziff. 16.4.1)

Im letzten Tätigkeitsbericht hatte ich über meine Beanstandung der Verwendung der beim Landespersonalamt geführten HEPIS-Datei berichtet und darauf hingewiesen, daß seit Inkrafttreten des novellierten Hessischen Datenschutzgesetzes am 1. Januar 1987 für das Verfahren HEPIS in der ursprünglichen Konzeption keine ausreichende Rechtsgrundlage besteht. Die Beanstandung hatte zwar dazu geführt, daß der archivierte Datenbestand verändert wurde, um einen Personenbezug zu verhindern. Auch werden seit einiger Zeit keine namensbezogenen Sonderauswertungen für Verwaltungszwecke für die einzelnen Ressorts mehr erstellt. Doch trotz wiederholter Ankündigungen durch das Landespersonalamt, daß eine Rechtsgrundlage für HEPIS in einem Artikelgesetz zur Landesstatistik geschaffen werde, ist dies bis heute nicht geschehen. Ende 1991 hat mir das Landespersonalamt mitgeteilt, daß eine baldige gesetzliche Regelung für die Verarbeitung der Personaldaten in HEPIS nicht mit dem seit langem ausstehenden Landesstatistikgesetz II erreicht werden könne. Man habe deshalb jetzt dem Hessischen Ministerium des Innern und für Europaangelegenheiten vorgeschlagen, eine entsprechende Regelung in das geplante Gesetz zur Änderung dienstrechtlicher Vorschriften aufzunehmen.

Da HEPIS nunmehr seit fünf Jahren ohne Rechtsgrundlage ist, kann ein Übergangsbonus nicht mehr wesentlich länger in Anspruch genommen werden. Sollte es im Laufe des Jahres 1992 immer noch nicht zu einer gesetzlichen Regelung kommen, müßten die personenbezogenen Daten in HEPIS gelöscht werden. Unabhängig davon, in welches Gesetz eine Rechtsgrundlage für HEPIS aufgenommen wird, muß der sehr umfangreiche Datensatz der gegenwärtigen Datei künftig reduziert werden.

16.2
Datenschutz in der Telekommunikation
(18. Tätigkeitsbericht, Ziff. 6.2.3; 19. Tätigkeitsbericht, Ziff. 16.5.1)

16.2.1 TELEKOM-Datenschutzverordnung (TDSV)

Die im letzten Tätigkeitsbericht angemahnten beiden Datenschutzverordnungen nach dem Poststrukturgesetz sind inzwischen in Kraft getreten. Seit dem 1. Juli 1991 gilt die "Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM" (TDSV; BGBl. I S. 1390). Sie regelt den Schutz personenbezogener Daten der an der Telekommunikation (TK) Beteiligten für den Bereich der als öffentlich-rechtliches Unternehmen tätigen TELEKOM. Das notwendige Pendant für die in privatrechtlicher Rechtsform tätigen Netzbetreiber und TK-Diensteanbieter, die "Teledienstunternehmen-Datenschutzverordnung (UDSV)" stammt vom 18. Dezember 1991 (BGBl. I S. 2337).

Die Historie beider Verordnungen ist ein erneuter Beleg für die Schwierigkeit, gegenüber der Deutschen Bundespost elementare Datenschutzerfordernisse durchzusetzen. Schon bei der Umsetzung des Bildschirmtextstaatsvertrages von 1983 in verbindliche Regelungen der Post gab es ähnliche Probleme (dazu eingehend 13. Tätigkeitsbericht für 1984, Ziff. 3.1.1.2).

16.2.2
Rufnummernanzeige

Wichtigstes Beispiel: Im ISDN-Netz (Integrated Services Digital Network) der TELEKOM, d.h. im Fernmeldenetz mit digitalisierter Vermittlungstechnik, ist bei entsprechender technischer Ausstattung des Telefonapparats eine sog. Rufnummernanzeige möglich. Dabei wird die Telefonnummer des Anrufers bis zum Angerufenen durchgeleitet und erscheint dort auf dem Display des Apparats. Die datenschutzrechtlichen Anforderungen sind jedoch nur erfüllt, wenn der Anrufer die Anzeige fallweise unterdrücken kann. Er soll bei jedem Telefonat entscheiden können, ob er sich identifiziert. Dem Angerufenen steht es frei, nicht-identifizierte Gespräche anzunehmen oder nicht. Nur diese Lösung entspricht dem sogenannten Euro-ISDN-Standard; sie ist in Frankreich ebenso vorgesehen wie im ISDN-Richtlinienvorschlag der EG-Kommission (Bundesrats-Drucks. 690/90). Dennoch wollte das Bundesministerium für Post und Telekommunikation (BMPT) noch in der TDSV-Entwurfsversion vom 28. Februar 1991 das Gegenteil vorschreiben, daß nämlich auf dem Markt nur solche ISDN-Anschlüsse angeboten werden dürften, die die Rufnummer obligatorisch bei jedem Telefonat übermitteln.

Es bedurfte nachdrücklicher Interventionen u.a. aus dem Bundestag und von den Datenschutzbeauftragten, um in diesem Punkt einen halbwegs akzeptablen Kompromiß zu erzielen: Die fallweise Rufnummernunterdrückung ist nach 9 Abs. 1 S. 2 TDSV bis spätestens 1. Januar 1994 einzuführen.

Dem Druck der Kirchen wiederum, die zu Recht um die Anonymität der telefonischen Kontakte mit ihren Seelsorge- und Beratungseinrichtungen fürchteten, ist es zu danken, daß der Kreis der Organisationen, die auf Antrag die Übermittlung der Telefonnummern zu ihren (ISDN-)Anschlüssen generell unterdrücken lassen können (dazu u. Ziff. 16.2.4), maßgeblich erweitert wurde. Nach § 9 Abs. 1 Satz 3 TDSV gehören jetzt dazu alle Institutionen, deren Mitarbeiter besonderen Verschwiegenheitsverpflichtungen unterliegen und die Beratungsaufgaben in sozialen oder kirchlichen Bereichen ganz oder überwiegend über Telefon abwickeln.

16.2.3
Einzelentgeltnachweis und "Geheimnummer"

Für diese Organisationen gilt weiterhin die Besonderheit, daß Telefonate, bei denen ihre Rufnummer angewählt wurde, nicht aus dem sogenannten Einzelentgeltnachweis ersichtlich sein dürfen (§ 6 Abs. 9 Satz 5 TDSV). Auch damit soll die Identifizierbarkeit des Gesprächspartners – etwa durch Familienmitglieder des Anrufers oder sonstige Mitbenutzer des Anschlusses – verhindert werden. Im übrigen aber kann der Telefonkunde dann, wenn er einen Einzelentgeltnachweis beantragt, eine Gebührenrechnung mit der kompletten Auflistung aller Zielnummern erhalten. Die Datenschutzbeauftragten haben sich in diesem Punkt mit ihrer Forderung, in den Gebührenrechnungen die Angabe der Zielrufnummer nur verkürzt um die letzten vier bzw. drei Ziffern zuzulassen, nicht durchsetzen können. Nur so hätte sich das Risiko, Telefonprofile herzustellen und zur Kontrolle des Kommunikationsverhaltens etwa von Mitbewohnern, Arbeitnehmern etc. heranzuziehen, verringern lassen.

Einen wichtigen Fortschritt gibt es bei den Telefonbüchern, jetzt "öffentliches Kundenverzeichnis" genannt. Der Zwangseintrag jedes Anschlußinhabers, der Ausnahmen nur mit spezieller Begründung zuließ, wurde abgeschafft. Jeder Telefonkunde kann nach § 10 Abs. 3 TDSV verlangen, daß der Eintrag seiner Nummer ganz oder teilweise unterbleibt, ohne dafür Gründe angeben zu müssen.

16.2.4
Antragsvoraussetzung

Die neuen rechtlichen Möglichkeiten nach der TDSV sind noch wenig bekannt. Ich habe Anfang Januar 1992 die Ministerien für Frauen, Arbeit und Sozialordnung sowie für Jugend, Familie und Gesundheit auf die geänderte Rechtssitutation aufmerksam gemacht. Beide Ressorts habe ich außerdem gebeten, Wohlfahrtsverbände, Beratungsstellen und andere einschlägige Institutionen bzw. deren Verbände darüber zu informieren, daß sie bei der TELEKOM den Ausschluß der Rufnummernanzeige sowie die Streichung ihrer Telefonnummern auf den Einzelentgeltnachweisen der Anrufer beantragen können; dies wurde mir inzwischen zugesagt. Die Geltendmachung der Rechte nach der TDSV ist von der Stellung eines solchen Antrags abhängig.

16.2.5
Teledienstunternehmen-Datenschutzverordnung (UDSV)

Die UDSV ist in weiten Teilen wortgleich mit der TDSV. Allerdings wollte der Bundesrat (Bundesrats-Drucks. 416/91 – Beschluß –) u.a. die in § 16 Abs. 2 TDSV vorgesehene Übergangsfrist für die technische Realisierung der Rufnummernunterdrückung bei Beratungsstellen in der UDSV nicht akzeptieren (a.a.O., Ziff. 2). Diese Frist bis 1. Juli 1992 wurde der TELEKOM wegen der notwendigen Umstellung ihrer Programme für die Vermittlungstechnik konzediert. Es war aber nicht einzusehen, warum sie auch privaten TK-Anbietern, die ihre Software schon vor dem Markteinstieg auf die Vorgaben der UDSV einstellen können, eingeräumt werden sollte. Der Bundesrat lehnte auch die Regelung ab, wonach der Katalog der zulässigen Verbindungsdaten erweitert werden konnte, soweit es die technische Entwicklung erfordere (a.a.O., Ziff. 1, zu § 5 Abs. 1 S. 2 und 3 des Entwurfs).

Darüber hinaus hat der Bundesrat die Bundesregierung in einer Entschließung aufgefordert, § 12 des Fernmeldeanlagengesetzes auf die durch die Einführung des ISDN eintretende neue Situation anzupassen (Bundesrats-Drucks. 416/91 – Beschluß –, S. 3ff.). Diese Vorschrift erlaubt dem Richter und bei Gefahr im Verzug auch dem Staatsanwalt, "Auskunft über den Fernmeldeverkehr" zu Strafverfolgungszwecken zu verlangen, und zwar ohne die weiteren Voraussetzungen, wie sie etwa für Abhörmaßnahmen nach §§ 100a, 100b Strafprozeßordnung gegeben sind. Diese Vorschrift spielte bisher wegen der weitgehenden Anonymität des Telefonverkehrs im analogen Telefonnetz kaum eine Rolle. Da im ISDN-Netz aber jedenfalls temporär die Verbindungsdaten aller über das Telefonnetz laufenden Kontakte gespeichert werden, könnte § 12 FAG eine ursprünglich nicht vorgesehene Bedeutung erhalten.

Sichergestellt werden muß, daß auch diese Norm einschränkenden Voraussetzungen unterworfen wird, etwa nur bei einem Katalog schwerer Straftaten anwendbar ist. Gelegenheit zur Änderung des § 12 FAG besteht im Rahmen der zur Zeit im Bundestag laufenden Beratungen über den Entwurf für ein Gesetz zur Bekämpfung der Organisierten Kriminalität (Bundestags-Drucks. 12/989), da dort ohnehin eine Änderung der Bestimmungen über die Kontrolle des Fernmeldeverkehrs vorgesehen ist (a.a.O. S. 17, Art. 9).

Beide Abweichungen der UDSV gegenüber der TDSV im Beschluß des Bundesrates sowie in der jetzt in Kraft getretenen Fassung beruhen auf Vorschlägen bzw. – was die Korrektur des FAG angeht – auf einem Antrag des Landes Hessen, die von einer Arbeitsgruppe, bestehend aus Vertretern des Innen- und des Wirtschaftsministeriums sowie der Staatskanzlei und des Hessischen Datenschutzbeauftragten, vorbereitet worden sind.

16.3
Europäische Gemeinschaft: Richtlinienentwürfe zum Datenschutz
(19. Tätigkeitsbericht, Ziff. 2)

Im ganzen Jahr 1991 wurde in den zuständigen EG-Gremien, d.h. der Arbeitsgruppe "Wirtschaftsfragen (Datenschutz)" des Ministerrats und vier Ausschüssen des Europaparlaments – federführend war der Rechtsausschuß – intensiv über das Vorschlagspaket der Kommission (KOM (90) 314 endg.) beraten. Schwerpunkt der Diskussion war der Vorschlag einer Rats-Richtlinie "zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" (a.a.O., SYN 287).

Auch die Datenschutzbeauftragten der EG-Mitgliedstaaten haben die bereits 1990 begonnene intensive Auseinandersetzung mit den Vorstellungen der Kommission fortgesetzt. Dazu fanden 1991 unter Vorsitz des damaligen Hessischen Datenschutzbeauftragten, Professor Simitis, Sitzungen in Brüssel, Manchester und Straßburg statt. Der deutsche Standpunkt als Basis der Konsensbildung mit den EG-Kollegen wurde zu Beginn des Jahres in dem Beschluß einer Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder festgelegt (abgedruckt unter Ziff. 17.1.1).

Am 16./17. Dezember 1991 sind die Beratungen auf Ausschußebene mit der Verabschiedung des Berichts des Rechtsausschusses abgeschlossen worden. Debatte und Votum im Plenum des Europaparlaments werden für Februar 1992 erwartet. Die letzte Gelegenheit, Standpunkte der EG-Datenschutzinstitutionen mit der Chance der Beeinflussung der Willensbildung des Rechtsausschusses zu formulieren, wurde bei einer Sitzung Ende November in Den Haag unter Leitung des niederländischen Datenschutzbeauftragten Hustinx genutzt.

Der Bericht des Rechtsausschusses enthält gegenüber dem ursprünglichen Kommissionsentwurf einige Verbesserungen, aber auch eine Reihe von Punkten, in denen die strikte Haltung der Kommission aufgeweicht bzw. Interventionen einflußreicher Lobbies wie etwa den Direkt-Marketing-Verbänden nachgegeben wurde.

Ich werde mich an den Arbeiten der EG-Datenschutzkonferenz zum Richtlinienpaket auch 1992 intensiv beteiligen. Dabei wird es in erster Linie darum gehen, die Kommission bei ihrem Versuch zu unterstützen, den Grundansatz einer Harmonisierung des Datenschutzes "nach oben" auch angesichts im Ministerrat zu erwartender massiver Widerstände durchzuhalten. Auf keinen Fall darf es zu einer bloßen Minimallösung kommen, bei der lediglich die inzwischen veraltete Europaratskonvention von 1981 zum Datenschutz – eventuell mit kleineren Modifikationen – EG-weit verbindlich gemacht wird.

16.4
Prüfung der klinischen Krebsregister in den Städtischen Kliniken Darmstadt und Kassel sowie dem Universitätsklinikum Gießen
(19. Tätigkeitsbericht Ziff. 5.1)

Bei Prüfungen der klinischen Krebsregister in den Städtischen Kliniken Darmstadt und Kassel sowie dem Universitätsklinikum Gießen hatte ich 1990 festgestellt, daß das 1989 vom Hessischen Sozialministerium, der Kassenärztlichen Vereinigung, den betroffenen Kliniken und mir erarbeitete Datenschutzkonzept für alle klinischen Tumorregister in Hessen (siehe hierzu 15. Tätigkeitsbericht Ziff. 4.2, 17. Tätigkeitsbericht Ziff. 5.3, 18.Tätigkeitsbericht Ziff. 18.3) nur unvollständig umgesetzt war. Die rechtlichen, technischen, organisatorischen und räumlichen Mängel sind in der Zwischenzeit nur in zwei der geprüften Kliniken ganz bzw. überwiegend beseitigt worden.

- Im Universitätsklinikum Gießen ist im neuen Tumordokumentationssystem nunmehr sichergestellt, daß jede an das Tumorregister angeschlossene Fachabteilung nur noch auf die personenbezogenen Daten ihrer eigenen Patienten Zugriff hat. Damit ist eine Abschottung der Datenbestände der verschiedenen Fachabteilungen untereinander vorgenommen worden, wie sie die ärztliche Schweigepflicht im Sinne von § 203 StGB und § 12 Abs. 2 und 3 Hessisches Krankenhausgesetz vorschreibt. Ferner erfolgt jetzt eine automatisierte Protokollierung der im Krebsregister vorgenommenen Auswertungen, mit der festgestellt werden kann, welche Auswertungen tatsächlich erstellt wurden und von wem. Auch die notwendigen räumlichen Sicherungsmaßnahmen sind erfolgt.

- In den Städtischen Kliniken Darmstadt ist ebenfalls inzwischen sichergestellt, daß jede an das dortige Tumorregister angeschlossenen Fachabteilung nur noch auf die personenbezogenen Daten ihrer eigenen Patienten zugreifen kann. Eine automatisierte Protokollierung der aus dem Krebsregister vorgenommenen Auswertungen findet jetzt statt. Die von mir kritisierte Möglichkeit, daß jeder Benutzer durch Betätigung der "CRTL-Y"-Taste auf die Systemebene gelangt und damit die Sicherheitsvorkehrungen umgehen kann, ist beseitigt worden. Alle notwendigen räumlichen Sicherungsmaßnahmen sind getroffen worden.

- In den Städtischen Kliniken Kassel liegen nunmehr schriftliche Verträge zwischen den niedergelassenen Ärzten, die die Daten ihrer Patienten mit deren Einwilligung an das Krebsregister weitergeben, und den Städtischen Kliniken über den konkreten Umgang der von den Städtischen Kliniken durchzuführenden Datenverarbeitung im Auftrag vor.

Im Gegensatz zu Darmstadt und Gießen konnte zum Zeitpunkt meiner Nachprüfung im Herbst 1991 jede Fachabteilung nach wie vor auf die Patientendaten anderer Fachabteilungen zugreifen. Ich habe die Kliniken nochmals nachdrücklich darauf hingewiesen, daß diese Zugriffsmöglichkeit mit der ärztlichen Schweigepflicht und der Regelung im Krankenhausgesetz nicht vereinbar und daß eine Abänderung unerläßlich ist.

Das Problem, daß jeder Benutzer durch Betätigung der "CRTL-Y"- Taste auf die Systemebene gelangt, war in Kassel zum Zeitpunkt meiner Nachprüfung für eine Mitarbeiterin noch nicht befriedigend gelöst. Inzwischen haben mir die Kliniken mitgeteilt, daß der Mangel beseitigt wurde. Die von mir geforderten räumlichen Sicherungsmaßnahmen waren bis zum Zeitpunkt der Nachprüfung nicht umgesetzt. Ich werde weiterhin auf die vollständige Beseitigung der Mängel dringen und den Sachstand in Kassel erneut überprüfen.

16.5
Richtlinien für den Datenschutz in Schulen
(19. Tätigkeitsbericht, Ziff. 6.3)

In ihrer Stellungnahme vom 5. September 1991 (Drucks. 13/583, S. 7) zu meinem 19. Tätigkeitsbericht hat die Landesregierung angekündigt, daß der Entwurf eines neuen Schulgesetzes auch die von mir geforderten bereichsspezifischen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im Schulbereich enthalten werde. Deshalb sei die Herausgabe der Richtlinien vorläufig zurückgestellt worden. Die Landesregierung behalte sich aber vor, bei einer Verzögerung des Gesetzgebungsverfahrens die Richtlinien bereits vor Verabschiedung des Gesetzes zu erlassen.

Die Koalitionsfraktionen SPD und GRÜNE haben am 4. November 1991 dem Landtag einen Gesetzentwurf für ein hessisches Schulgesetz vorgelegt (Drucks. 13/858), der im 6. Teil Datenverarbeitungsnormen enthält. Ich gehe davon aus, daß ich Gelegenheit haben werde, mich im Rahmen der für das Frühjahr 1992 angekündigten Anhörung im Landtag ausführlich zu dem Entwurf zu äußern.

16.6
Weitergabe von Volkszählungs- und Mikrozensusdaten – Neue Möglichkeiten der Anonymisierung
(19. Tätigkeitsbericht, Ziff. 16.6.2.2)

Das Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz – BStatG) vom 22. Januar 1987 (BGBl. I S. 462) hat in § 16 Abs. 6 der Wissenschaft einen erleichterten Zugang zu Einzelangaben aus der amtlichen Statistik verschafft. Die Statistikämter dürfen Hochschulen oder sonstigen Einrichtungen mit der Aufgabe unabhängiger Forschung für wissenschaftliche Vorhaben "faktisch anonymisierte" statistische Einzelangaben mitteilen. Die Daten dürfen nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten Person zuordenbar sein, müssen also nicht völlig anonym sein.

Das Gesetz sagt allerdings nicht, wie die faktische Anonymität in einem konkreten Datensatz sichergestellt werden kann. Deshalb wollte das Statistische Bundesamt unter Beteiligung des Zentrums für Umfragen, Methoden und Analysen – ZUMA – der Universität Mannheim durch ein Forschungsprojekt eine Lösung dazu finden. Begleitet wurde das Vorhaben von einem Beirat, in dem Vertreter der statistischen Ämter des Bundes und der Länder, der Datenschutzbeauftragten von Bund und Ländern, der Wissenschaft und des Bundesministeriums für Forschung und Technologie zusammengearbeitet haben. Auch ich habe mich an dieser Diskussion und der datenschutzrechtlichen Beurteilung der Ergebnisse beteiligt.

Bei den Untersuchungen ging es um die Feststellbarkeit von Überschneidungsmerkmalen bei der Gegenüberstellung anonymer mit personenbezogenen Datensätzen. Als zu deanonymisierendes Datenmaterial dienten Angaben des Mikrozensus von Nordrhein-Westfalen. Bei den Datensätzen des Mikrozensus fehlten nur Name und Anschrift der Betroffenen. Die vergleichsweise differenzierten Regionalinformationen – z. B. Bundesraumordnungsregion und Gemeindegrößenklasse – waren noch enthalten. Als öffentlich zugängliche Informationsquellen für Zusatzwissen beim Reidentifizierungsversuch wurde Kürschners Deutscher Gelehrtenkalender 1987 herangezogen. Er enthält – bezogen auf Hochschullehrer – zehn auch im Mikrozensus erfragte Angaben wie z.B. Geburtsjahr, Beruf, Religion usw.

Bei den 8.000 dem Gelehrtenkalender entnommenen Datensätzen gab es bei Verwendung einer einfachen Zuordnungstechnik lediglich 14 Fälle mit der gleichen einzigartigen Merkmalskombination auch im Mikrozensus. Die Überprüfung dieser Zuordnungen durch einen Treuhänder ergab jedoch, daß die Überschneidungen nur in vier Fällen die gleiche Person betrafen. Dies entspricht einer Reidentifikationsquote von 0.0005. Die vier korrekten Identifikationen kamen jedoch nur dann zustande, wenn neben der Löschung von Namen und Anschrift keine weiteren Anonymisierungsmaßnahmen getroffen waren. Wurden beispielsweise die Regionalinformationen auf die Ebene des Bundeslandes aggregiert, konnte auch bei Einbeziehung der sehr differenzierten Merkmale Geburtsjahr, Beruf und Wirtschaftszweig kein Fall eindeutig zugeordnet werden.

Nach den Ergebnissen dieses Projekts übersteigt der Aufwand, der für eine korrekte Deanonymisierung von Mikrozensusdaten bei Unkenntnis der Personalien betrieben werden müßte, bei weitem den Betrag, der für eine alternative Informationsbeschaffung aufzuwenden wäre. Damit kann das Kriterium der faktischen Anonymität als erfüllt angesehen werden.

Allerdings beziehen sich die Ergebnisse des Forschungsprojektes ausschließlich auf die Einkommens- und Verbrauchsstichprobe (EVS) und den Mikrozensus. Bei personenbeziehbaren Statistiken mit anderen Samples (z.B. Bevölkerungs- und Beherbergungsstatistik) bedürfte es einer erneuten Überprüfung, ob das Anonymisierungsverfahren ausreicht. Dies gilt auch für die regionale Aufschlüsselung von Einzelangaben bei der Übermittlung von Daten aus kleinen Bundesländern bzw. den Stadtstaaten. Die Übertragbarkeit dieses Modells auf den Bereich der Kommunalstatistik wäre ebenfalls gesondert zu untersuchen. Darauf habe ich in meiner Stellungnahme zu den Ergebnissen des Projektes hingewiesen.

Wiesbaden, den 5. März 1992
Professor Dr. Hassemer
gez. Hassemer

17. Materialien

17.1
Beschluß und Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und Beschluß mehrerer Datenschutzbeauftragter

17.1.1
Beschluß der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29. Januar 1991 zu dem von der EG-Kommission vorgelegten Vorschlag für eine Rats-Richtlinie zum Datenschutz

I.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Vergangenheit zu wiederholten Malen die Untätigkeit der Europäischen Gemeinschaft im Bereich des Datenschutzes kritisiert. Kernpunkt dieser Kritik war die Befürchtung, daß die Dynamik der wirtschaftlichen Entwicklung in Richtung auf den vollendeten Binnenmarkt zu einem "informationellen Großraum" mit einem engen Netzwerk grenzüberschreitender Datenflüsse führt, ohne daß gleichzeitig der Grundrechtsschutz in der Gemeinschaft bei der Verarbeitung und dem Austausch persönlicher Daten gewährleistet wird.

II.
Daher begrüßt die Konferenz, daß die EG-Kommission im Juli 1990 den "Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt hat. Der Kommissionsvorschlag geht in einer Reihe von Punkten über die Konvention des Europarats zum Datenschutz von 1981 hinaus und berücksichtigt insoweit die technische und rechtliche Entwicklung des vergangenen Jahrzehnts. Positiv bewertet die Konferenz vor allem die Intention des Entwurfs, den Datenschutz in der EG nicht auf dem kleinsten gemeinsamen Nenner, sondern auf einem möglichst hohen Niveau zu harmonisieren. Sie legt allerdings entscheidenden Wert darauf, daß die Mitgliedstaaten die Möglichkeit behalten, den Datenschutz in der nationalen Gesetzgebung weiterzuentwickeln.

III.
Zahlreiche bewährte Vorschriften und Instrumente aus dem deutschen Datenschutzrecht sind in den Richtlinientext aufgenommen worden. Die Bewertung der einzelnen Bestimmungen des Richtlinienentwurfs kann jedoch nicht isoliert aus dem Blickwinkel des deutschen Datenschutzrechts erfolgen. Jeder nationale Gesetzgeber muß bei Rechtsharmonisierung auf europäischer Ebene bereit sein, einzelne seiner Regelungen auf dem Hintergrund der Erfahrungen und Vorstellungen anderer Mitgliedstaaten in Frage zu stellen. Zur Abstimmung der Auffassungen auf EG-Ebene besteht ein intensiver Meinungsaustausch zwischen der Konferenz und den Datenschutzinstitutionen der Partnerländer.

IV.
Die Konferenz hält, abgesehen von der Bereinigung von redaktionellen Unstimmigkeiten, einige Änderungen im Richtlinienvorschlag für notwendig, um die Gleichwertigkeit des Schutzes auf dem Niveau, das die Mitgliedsländer mit bestehender Datenschutzgesetzgebung bereits erreicht haben, sicherzustellen. Folgende Korrekturen sind dabei vorrangig:

1. Datenschutz muß, jedenfalls im Bereich der öffentlichen Verwaltung, für alle Unterlagen mit personenbezogenen Daten gelten. Die in der Richtlinie vorgesehene Beschränkung des Anwendungsbereichs auf die Verarbeitung personenbezogener Daten in "Dateien" ist ebenso technisch überholt wie Anlaß zu einer Fülle von Interpretationsproblemen.

2. Für die Verwendung und Weitergabe persönlicher Daten muß das Prinzip strikter Zweckbindung gelten und ausdrücklich statuiert werden. Wenn der Entwurf die bloße Vereinbarkeit der Zwecke von Erhebung, Speicherung und Übermittlung genügen läßt, werden inakzeptable Verarbeitungsfreiräume eröffnet; die Transparenz des Datenumgangs geht für den einzelnen verloren.

3. Der Anspruch auf Auskunft über die gespeicherten Daten ist das elementarste Individualrecht der Betroffenen. Nur gravierende Interessen der Allgemeinheit oder Dritter dürfen im Ausnahmefall diesen Auskunftsanspruch

einschränken. Der im Entwurf vorgesehene Katalog von Fällen der Auskunftsverweigerung muß daher deutlich vermindert werden.

4. Der Forderung des Entwurfs, daß die Erhebung von Daten nur "nach Treu und Glauben" erfolgen darf, kann uneingeschränkt zugestimmt werden. Doch muß dieses Prinzip im Interesse des einzelnen konkretisiert werden. Es gilt klarzustellen, daß persönliche Angaben vorrangig beim Betroffenen selbst zu erheben sind. Die Ausnahmefälle, in denen Informationen ohne Kenntnis des Betroffenen beschafft werden dürfen, sollten soweit wie möglich in der Richtlinie konkret benannt werden.

5. Der Datenschutz der EG-Bürger darf nicht an den Gemeinschaftsgrenzen haltmachen. Ziel der Richtlinie muß neben der EG-internen Harmonisierung auch sein, den Schutz des Betroffenen beim Datenexport in Drittländer zu gewährleisten. Dies setzt voraus, daß im Empfängerland ein dem EG-Standard gleichwertiges Datenschutzniveau besteht. Daß der Richtlinienentwurf sich mit einem "angemessenen" Schutz im Zielland zufriedengibt, genügt nicht. Notwendig ist schließlich, das Verfahren zur Feststellung des Datenschutzstandards in Drittländern übersichtlich und praktikabel auszugestalten.

6. Auf der EG-Ebene bedarf es einer unabhängigen Datenschutzinstanz, die alle EG-Organe in Datenschutzfragen berät und für die Überwachung der Einhaltung sowie die einheitliche Anwendung der Richtlinie sorgt. Die im Richtlinienvorschlag vorgesehene "Gruppe für den Schutz personenbezogener Daten" erfüllt – betrachtet man ihre Struktur, Aufgaben und Kompetenzen – diese Anforderungen nicht. Die Unabhängigkeit der Datenschutzkontrolle auf EG-Ebene wird in Zweifel gezogen, wenn den Vorsitz nicht ein gewähltes Mitglied dieser – aus den nationalen Datenschutzorganen zusammengesetzten – "Gruppe", sondern ein Vertreter der EG-Kommission führt. Klargestellt werden muß weiter, daß das Votum der "Gruppe" im vorhinein bei allen den Datenschutz betreffenden Initiativen und Entwürfen der Kommission einzuholen ist. Ansprechpartner der "Gruppe" darf nicht ausschließlich die EG-Kommission, sondern muß auch das Europäische Parlament sein.

7. Da die Kommission die entsprechende Anwendung der Richtlinie auf die personenbezogene Datenverarbeitung ihrer eigenen Dienststellen beschlossen hat, muß sie auch umgehend für eine unabhängige Kontrolle dieses Bereichs Sorge tragen.

V.
Die Konferenz weist darauf hin, daß die vorliegende Richtlinie durch Regelungen für besondere Anwendungsbereiche ergänzt werden muß. Sie sind insbesondere für den Arbeitnehmer- und Sozialdatenschutz vordringlich. Die Kommission sollte schon jetzt ihre Bereitschaft erklären, entsprechende Regelungen zu treffen, und möglichst bald erste Vorschläge vorlegen.

VI.
Die Konferenz begrüßt die Gesprächsbereitschaft der Kommission und geht davon aus, daß der bereits begonnene Dialog zu einer substantiellen Verbesserung des Richtlinienvorschlags führen wird. Die Konferenz wird diese Entschließung der EG-Kommission, dem Europäischen Parlament sowie der Bundesregierung zuleiten. Informiert werden ebenfalls die Datenschutzkontrollinstitutionen der Partnerländer in der Gemeinschaft.

17.1.2
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 8. März 1991 zu Telekommunikation und Datenschutz

I.
Die Telekommunikation hat außerordentlich stark an Bedeutung gewonnen und ersetzt häufig den Brief oder auch das persönliche Gespräch: Über die dreißig Millionen deutschen Telefone werden monatlich rund drei Milliarden Gespräche geführt. Für die Privatsphäre des Bürgers in einer freiheitlichen Gesellschaft ist es unverzichtbar, daß Telefongespräche unkontrolliert und unbeobachtet geführt werden können. Von existentieller Bedeutung wird dies, wenn der Bürger in Notlagen gerät, aus denen er sich nur mit vertraulicher Beratung und Hilfe befreien kann. Daher unterstützen sowohl die Kirchen als auch Hilfs- und Beratungsorganisationen die Forderung, das "Grundrecht auf unbeobachtete Kommunikation" zu sichern.

Dieser Forderung muß die technische Ausgestaltung der Telekommunikationsnetze und -dienste folgen, und die rechtlichen Regelungen müssen diesen sich aus der Verfassung ergebenden Auftrag erfüllen. Der Gesetzgeber hat in dem am 1. Juli 1989 in Kraft getretenen Poststrukturgesetz die Bundesregierung aufgefordert, "Rechtsverordnungen zum Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten" zu erlassen. Der Ausschuß für Post und Telekommunikation und der Innenausschuß des Deutschen Bundestages haben mehrfach den Schutz des Fernmeldegeheimnisses angemahnt.

Die vom Bundesminister für Post und Telekommunikation vorgelegten Entwürfe von Verordnungen über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TDSV) und über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (UDSV), widersprechen in wesentlichen Punkten dem Grundrecht auf unbeobachtete Kommunikation. Dabei ist besonders unverständlich, daß der Bundesminister von bereits früher gemachten Zusagen an den Deutschen Bundestag wieder abgerückt ist.

Die Entwürfe bleiben in wichtigen Punkten unter dem Datenschutzniveau, das von der EG-Kommission in ihrem Richtlinienentwurf zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen für den europäischen Binnenmarkt angestrebt wird.

II.
Ein wesentlicher Mangel besteht in der beabsichtigten Vollerfassung aller Verbindungsdaten von Telefongesprächen: Für jedes Telefonat soll bis zur Versendung der Entgeltrechnung bei der Deutschen Bundespost TELEKOM festgehalten werden dürfen, wer wann wie lange und mit wem telefoniert hat, nach Wahl des Kunden achtzig Tage darüber hinaus. Eine monatliche Auflistung dieser dem Fernmeldegeheimnis unterliegenden Informationen (Einzelentgeltnachweis) sollen Kunden – auch Arbeitgeber – auf Wunsch erhalten können. Außerdem können nach § 12 Fernmeldeanlagengesetz (FAG) auch Gerichte und Staatsanwaltschaften bei strafrechtlichen Ermittlungen jeder Art, also auch bei Bagatelldelikten, ohne besondere Voraussetzungen auf diese Daten zugreifen.

Abzulehnen ist auch die vorgesehene Beschränkung des Kunden auf die Alternative, daß von einem Anschluß die Telefonnummer des Anrufers immer oder nie beim Angerufenen angezeigt wird. Dem Recht auf informationelle Selbstbestimmung entspricht es, daß der Anrufer in jedem Einzelfall entscheiden kann, ob seine Rufnummer beim Angerufenen angezeigt wird. Umgekehrt hat jeder Angerufene selbstverständlich das Recht, nur Gespräche entgegenzunehmen, bei denen die Nummer des Anrufers angezeigt wird.

III.
Die Datenschutzbeauftragten fordern:

1. Alle – durch die computergesteuerte Vermittlungstechnik entstehenden – Verbindungsdaten sind nach dem Ende der Verbindung mit folgender Maßgabe unverzüglich zu löschen:

   In die Entgeltdatenverarbeitung dürfen nur diejenigen Daten eingehen, die zur Berechnung der Entgelte in Summenform unerläßlich sind. Auf Antrag des Kunden darf zur Prüfung der Richtigkeit des in Rechnung gestellten Entgelts oder zur Erstellung des Einzelentgeltnachweises die Rufnummer des Angerufenen nur in einer zumindest um die letzten vier Ziffern verkürzten Form gespeichert werden. Die Daten sind spätestens achtzig Tage nach dem Absenden der Entgeltrechnung zu löschen.

   Die Entscheidung des Kunden über die Form der Abrechnung muß auch bei der Abrechnung zwischen verschiedenen Netzbetreibern respektiert werden.

2. Die Erstellung von "Kommunikationsprofilen", die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, muß ausgeschlossen sein.

3. Bei der Anzeige der Rufnummer des Anrufers beim Angerufenen müssen beide die Wahlmöglichkeit haben, diese Anzeige entweder auf Dauer oder im Einzelfall "auf Knopfdruck" zu unterdrücken.

4. Ausnahmen von diesen Grundsätzen – z.B. zur Aufklärung telefonischer Bedrohungen oder in Notfällen – müssen begründet, ausdrücklich geregelt und für den Betroffenen transparent sein.

5. Die Konferenz bekräftigt ihre Forderung (Beschluß vom 4./5. Oktober 1990), Eingriffe in das grundgesetzlich geschützte Fernmeldegeheimnis (Art. 10 GG) auf das unerläßliche Maß zu beschränken und insbesondere nicht schon im Bereich der Bagatellkriminalität zuzulassen. Die Regelung des § 12 FAG hat im Zuge der technischen Entwicklung eine verfassungsrechtlich bedenkliche neue Qualität erhalten, da sie nunmehr auch die bei Einsatz neuer Kommunikationstechniken anfallenden Abrechnungs-, Verbindungs-, Nutzungs- und Inhaltsdaten umfaßt. Statt im FAG sollten die Eingriffsmöglichkeiten in das Fernmeldegeheimnis im Rahmen der Strafverfolgung – schon aus Gründen der Normenklarheit – in der Strafprozeßordnung unter engen Voraussetzungen und Beschränkungen abschließend geregelt werden.

17.1.3
Entschließung der 42. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes

I.
Die Daten von Arbeitnehmern werden im Laufe ihres beruflichen Lebens in vielfältiger Weise vom Arbeitgeber verarbeitet. Allein schon im Hinblick auf die große Zahl der über Arbeitnehmer erhobenen Daten und mit Rücksicht auf die Abhängigkeit des Arbeitnehmers vom Arbeitgeber ist eine gesetzliche Regelung der Verarbeitung von Personaldaten zwingend erforderlich. Auch gegenüber Beamten und anderen im öffentlichen Dienst Tätigen kann die Verarbeitung ihrer Daten nicht allein auf die hergebrachten Grundsätze des Berufsbeamtentums gestützt oder in Verwaltungsvorschriften geregelt werden. Vielmehr ist eine gesetzliche Grundlage vonnöten. Sie muß um so konkreter sein, je tiefer in das Persönlichkeitsrecht der Betroffenen eingegriffen wird.

II.
In der Auseinandersetzung um das Recht des öffentlichen Dienstes beeinträchtigen zwei grundlegende Fehleinschätzungen eine angemessene Regelung des Datenschutzes. Es trifft nicht zu, daß die Kenntnis des Dienstherrn über

seine Bediensteten alle persönlichen Lebensumstände vollständig und lückenlos umfassen muß. Es ist ferner unrichtig, daß gesetzliche Regelungen überflüssig sind, weil stets die Einwilligung der Betroffenen eingeholt werden kann.

Zum einen wäre es mit der Würde des Menschen unvereinbar, wollte man ihn in seiner ganzen Persönlichkeit registrieren. Zwar ist der Angehörige des öffentlichen Dienstes dem Staat gegenüber besonders eng verpflichtet; er bleibt aber auch gegenüber seinem Dienstherrn Grundrechtsträger: Auch seine personenbezogenen Daten dürfen nur erhoben und verarbeitet werden, soweit das für die Begründung und Abwicklung des Dienstverhältnisses erforderlich ist.

Zum anderen macht der Rückgriff auf die Einwilligung gesetzliche Regelungen keineswegs überflüssig. Zwar ist die Erhebung und Verarbeitung personenbezogener Daten mit Einwilligung des Betroffenen grundsätzlich auch dann zulässig, wenn eine gesetzliche Grundlage fehlt. Die Einwilligung wird jedoch zur Farce, wenn sie faktisch erzwungen wird, weil z.B. eine Bewerbung ohne Einwilligung nicht berücksichtigt wird. Soweit bestimmte Angaben verfügbar sein müssen, sind sie gesetzlich präzise vorzuschreiben, aber zugleich auf den erforderlichen Umfang zu begrenzen.

III.
Neben der Neuordnung des Personalaktenrechts bedürfen auch andere Teilbereiche des öffentlichen Dienstrechts der datenschutzgerechten gesetzlichen Regelung. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere die Lösung folgender Probleme für vorrangig:

1. Bewerbung um Einstellung in den öffentlichen Dienst

   Es ist – für den Bewerber transparent – festzulegen,

   - welche personenbezogenen Informationen von ihm verlangt bzw. über ihn eingeholt, wie sie genutzt werden dürfen und wann sie zu löschen sind,
   - ob und unter welchen Voraussetzungen und in welchem Stadium des Verfahrens der Bewerber sich Tests, Untersuchungen und Überprüfungen zu unterziehen hat,
   - ob und inwieweit private Institutionen daran mitwirken und welche vertraglichen Sicherungen zum Schutz personenbezogener Daten zu vereinbaren sind,
   - daß die Daten jeweils erst zu dem Zeitpunkt, in dem sie für das Verfahren erforderlich werden, und mit dem geringstmöglichen Eingriff erhoben werden.

2. Sicherheitsüberprüfung

   Es ist bereichsspezifisch gesetzlich festzulegen,

   - wer im öffentlichen Dienst einer Sicherheitsüberprüfung unterzogen wird,
   - welche personenbezogenen Daten dafür erhoben und verarbeitet werden,
   - wie das Verfahren gestaltet wird, insbesondere welche Stellen mit welchen Befugnissen am Verfahren beteiligt sind und unter welchen Voraussetzungen Sicherheitsbedenken anzunehmen sind,
   - daß die im Rahmen der Sicherheitsüberprüfung erhobenen Daten grundsätzlich nur für diesen Zweck verwendet werden dürfen,
   - daß der Betroffene über das Ergebnis der Sicherheitsüberprüfung zu unterrichten ist.*

3. Ärztliche Untersuchung

   Es ist durch Gesetz oder ergänzende Rechtsverordnung festzulegen,

   - unter welchen Voraussetzungen die ärztliche Untersuchung eines Bewerbers oder Bediensteten angeordnet werden kann,
   - daß jede ärztliche Untersuchung einen präzisen Untersuchungsauftrag voraussetzt, der Anlaß und Gegenstand der Untersuchung möglichst exakt definiert und den Umfang der Untersuchung eingrenzt,
   - wie das Arztgeheimnis und der Datenschutz sicherzustellen sind,

* Auf ihre Forderungen zur Sicherheitsüberprüfung (Geheimschutzgesetz) in den Entschließungen vom 13. September 1985, 18. April 1986 und 22. März 1990 nimmt die Konferenz Bezug.

- wann und in welchem Umfang Versicherungen und früher behandelnde Ärzte über frühere Untersuchungen und Maßnahmen befragt werden und diese offenbaren dürfen,

- daß die Unterlagen der ärztlichen Untersuchungen nicht für andere Zwecke verwendet werden und nicht mit solchen vermengt werden dürfen, die anderen Zwecken dienen, und daß sie zu vernichten sind, sobald sie nicht mehr benötigt werden,

- daß der Arzt der personalverwaltenden Stelle nur das Endergebnis seiner Untersuchung und – soweit erforderlich – nur tätigkeitsbezogene Risiken mitzuteilen hat,

- daß dem Betroffenen ein Recht auf Einsicht in die beim Arzt verbliebenen Untersuchungsunterlagen zusteht.

4. Beihilfen

Gesetzlich festzulegen sind die Grundlagen eines datenschutzgerechten Beihilfeverfahrens, insbesondere die Abschottung der Beihilfestelle, das Verbot automatisierter Speicherung von Diagnosedaten und anderen medizinischen Einzelangaben, die Zweckbindung der Daten sowie ein eigener Beihilfeanspruch der Angehörigen.

5. Personalinformationssysteme

Es muß dienstrechtlich gewährleistet sein, daß

- automatisierte Systeme zur Verarbeitung von Personaldaten zu unterschiedlichen Zwecken (z.B. Urlaubsdatei, Telefondatenerfassung, PC-Betriebsdaten) nicht zu umfassenden Persönlichkeitsprofilen verknüpft werden,

- alle vorgesehenen Auswertungen von Personaldaten in einer Übersicht, die dem Betroffenen zugänglich sein muß, zusammengefaßt werden,

- Kontrollen der Bediensteten mit Hilfe automatisierter Systeme unzulässig sind; Ausnahmen bedürfen einer gesetzlichen, insbesondere personalvertretungsrechtlichen Regelung.

IV.
Die Datenschutzbeauftragten des Bundes und der Länder fordern die für das Personalrecht zuständigen Minister und den Gesetzgeber auf, die auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts verfassungsrechtlich notwendigen Vorschriften zu erlassen.

17.1.4
Beschluß der Datenschutzbeauftragten der Länder Berlin, Bremen, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen und Schleswig-Holstein vom Mai 1991 zu der im Bundesdatenschutzgesetz vorgesehenen Einschränkung der Kontrollrechte
(Dem Beschluß haben sich im Juni 1991 die Datenschutzbeauftragten der Länder Rheinland-Pfalz und Saarland angeschlossen.)

1.
Das am 1. Juni 1991 in Kraft tretende Bundesdatenschutzgesetz schränkt die Kontrollbefugnisse der Datenschutzbeauftragten an entscheidenden Stellen ein: Widerspricht der Betroffene einer Einsichtnahme durch den Beauftragten, entfällt dessen Kontrollbefugnis beispielsweise bei Daten, die dem Arztgeheimnis unterliegen oder bei Angaben, die aufgrund einer Sicherheitsüberprüfung in Personalakten aufgenommen wurden. Dieses "Widerspruchsrecht" kann nach dem neuen Gesetz ausdrücklich auch gegenüber Kontrollen durch die Landesdatenschutzbeauftragten geltend gemacht werden.

Sowohl das 1. Bundesdatenschutzgesetz aus dem Jahre 1977 als auch die seither erlassenen bereichsspezifischen Datenschutzvorschriften haben dagegen die in den Landesdatenschutzgesetzen eingeräumten Kontrollrechte stets respektiert.

Mit Nachdruck wenden sich die Datenschutzbeauftragten der Länder gegen den verfassungswidrigen Eingriff des Bundesgesetzgebers in ihre Rechte. Dem Bundesgesetzgeber steht eine Kompetenz zur Einschränkung ihrer Kontrollbefugnisse nicht zu.

2.
Auch wenn § 203 des Strafgesetzbuchs den Bruch des Arztgeheimnisses unter Strafe stellt, folgt daraus nicht, daß der Umfang der Kontrollbefugnisse bei medizinischen Daten dem Strafrecht zuzuordnen wäre und dem Bund eine konkurrierende Gesetzgebungskompetenz nach Art. 74 Nr. 1 des Grundgesetzes zustünde. Ebensowenig können die Kontrollrechte bei Personalakten oder Akten über die Sicherheitsüberprüfung öffentlicher Bediensteter der Länder auf die Rahmenkompetenz des Bundes nach Art. 75 Nr. 1 Grundgesetz gestützt werden. Es geht nicht

darum, allgemeine Verarbeitungsbedingungen oder einen wirksamen strafrechtlichen Schutz festzulegen, sondern den Umfang der Kontrollbefugnis durch den Landesdatenschutzbeauftragten zu definieren. Hierzu ist allein der Landesgesetzgeber berufen.

3.
Die Regelung der Kontrollrechte der Datenschutzbeauftragten der Länder ergibt sich auch nicht aus der Kompetenz des Bundes, das Verwaltungsverfahren festzulegen (Art. 84 Abs. 1 GG). Zum einen vermag der Bundesgesetzgeber Verfahren nur dann zu bestimmen, wenn die Verwaltungen der Länder Bundesrecht ausführen. Zum anderen umfaßt das Verwaltungsverfahren lediglich den Ablauf der personenbezogenen Datenverarbeitung von der Erhebung über die Speicherung bis zur Löschung oder Archivierung und begründet Rechte und Pflichten von Verwaltung und betroffenem Bürger. Die Kontrolle durch den Datenschutzbeauftragten dient hingegen nicht nur dem Recht auf informationelle Selbstbestimmung einzelner Betroffener. Gerade die umfassende, präventive Kontrolltätigkeit ohne konkreten Anlaß ist unabdingbarer Bestandteil einer umfassenden Sicherung des Grundrechts auf informationelle Selbstbestimmung über den Einzelfall hinaus. Das vom Gesetzgeber beschlossene "Widerspruchsrecht" gefährdet diese präventive Kontrolle.

Einzelne Landesgesetze verpflichten den Datenschutzbeauftragten, Gutachten und Untersuchungen für Landtag und Landesregierung anzufertigen bzw. durchzuführen. Ohne Einsicht in personenbezogene Unterlagen ist das oft nicht möglich. Weit über die Sicherung der Rechte einzelner hinaus soll der Datenschutzbeauftragte zu einer datenschutzgerechten Informationsverarbeitung beitragen. Die neue Regelung erschwert die Erfüllung dieser Aufgaben erheblich.

Es steht allein dem jeweiligen Gesetzgeber in Bund und Ländern zu, die Kontrollaufgaben seines Datenschutzbeauftragten festzulegen und abzugrenzen. Dabei hat er das gesamte Aufgabenspektrum dieser Institution zu berücksichtigen.

4.
Solange § 24 (6) BDSG nicht aufgehoben ist, sind die sich aus dem Widerspruchsrecht des Betroffenen ergebenden Kontrollbeschränkungen der Datenschutzbeauftragten möglichst restriktiv auszulegen.

Es ist zumindest klarzustellen, daß

- die Kontrollrechte der Datenschutzbeauftragten unabhängig davon bestehen, ob und wann die Betroffenen über ihr Widerspruchsrecht unterrichtet worden sind,

- es ausreicht, wenn die Unterrichtung der Betroffenen durch allgemeinen Hinweis, etwa durch Aushang oder Veröffentlichung im Amtsblatt, erfolgt und

- erst der tatsächlich eingelegte Widerspruch des Betroffenen die Kontrolle der auf ihn bezogenen Daten im Einzelfall ausschließt.

17.2
Zur Aufnahme des informationellen Selbstbestimmungsrechts und der Informationsfreiheit ("Freedom of Information") in das Grundgesetz – Zwischenbericht des Hessischen Datenschutzbeauftragten gemäß § 30 Abs. 1 HDSG anläßlich des vom Hessischen Landtag und von der Hessischen Landesregierung am 30. und 31. Oktober 1991 veranstalteten Verfassungssysmposiums

Inhaltsverzeichnis

I. Gründe für die Aufnahme des informationellen Selbstbestimmungsrechts und der Informationsfreiheit in das Grundgesetz

1. Das informationelle Selbstbestimmungsrecht

Der Gedanke, die Grundregeln über die Verarbeitung personenbezogener Daten in die Verfassung aufzunehmen, ist nicht neu. Spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 (Bundesverfassungsgerichtsentscheidungen Band 65, 1) steht fest: Die Verwendung personenbezogener Angaben tangiert die Grundrechte der Betroffenen, genauer ihre informationelle Selbstbestimmung. Konsequenterweise hat sich zunächst Nordrhein-Westfalen dazu entschlossen, das Recht der einzelnen, selbst über den Umgang mit den ihre Person betreffenden Angaben zu bestimmen, unmittelbar in der Landesverfassung (Art. 4) anzusprechen. Das Saarland (Art. 2) und Berlin (Art. 21b) sind entsprechend verfahren. In die gleiche Richtung deuten auch die Verfassungsentwürfe von Brandenburg (Art. 12 des Entwurfs vom Mai 1991), Sachsen (Art. 32 des Entwurfs vom Juni 1991) und Sachsen-Anhalt (Art. 4 und 37 des Entwurfs vom Juli 1991). Auch bei den parlamentarischen Beratungen über die Novellierung des Bundesdatenschutzgesetzes hat die Frage einer verfassungsrechtlichen Verankerung der Datenschutzvorschriften eine wichtige Rolle gespielt.

Ähnlich ist die Entwicklung im Ausland verlaufen. Sowohl die österreichische (Art. 1) als auch die spanische (Art. 18), die niederländische (Art. 10) und die portugiesische (Art. 35) Verfassung nehmen ausdrücklich zur Verwendung personenbezogener Daten Stellung. Auch das Europäische Parlament hat in einer Entschließung und Erklärung über Grundrechte und Grundfreiheiten vom 12. April 1989 eine Bestimmung über den Datenschutz aufgenommen (Art. 18).

So sehr sich die meisten dieser Bestimmungen ihrem Wortlaut nach unterscheiden, so verschieden ihr Entstehungsprozeß ist und so wenig sich die oft erheblichen Abweichungen in der Entwicklung der Informationstechnologie übersehen lassen, so deutlich spiegelt jede dieser Vorschriften eine gemeinsame, in vielen Fällen auf eine leidvolle historische Erfahrung gegründete Überzeugung wider. Je offener sich der Zugang zu personenbezogenen Daten gestaltet, je leichter es jedem Interessierten fällt, sich jede von ihm gewünschte Information zu beschaffen, desto mehr verflüchtigen sich die Grundrechte der Betroffenen und wächst die Gefahr ihrer Manipulation.

Um noch einmal das Volkszählungsurteil zu zitieren: Wer nicht weiß, von wem, für welche Zwecke und unter welchen Bedingungen Daten zu seiner Person zusammengestellt werden, wird sich nicht nur mehr und mehr überlegen, ob er etwa einer politischen oder gewerkschaftlichen Organisation beitritt, sondern auch zunehmend davon Abstand nehmen, seine Meinung zu äußern (BVerfGE 65, 1, 43). Wenig später hat das Bundesverfassungsgericht in einem grundlegenden Urteil zu der in Art. 8 GG gewährleisteten Versammlungsfreiheit noch einmal ausdrücklich darauf hingewiesen, daß staatliche Observationen und Registrierungen die Versammlungsfreiheit gefährden können (BVerfGE 69, 315, 349). Klare, die informationelle Selbstbestimmung garantierende Regeln zählen deshalb zu den elementaren Funktionsbedingungen "eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich-demokratischen Gemeinwesens" (BVerfGE 6, 1, 43) .

Ohne Zweifel liegt es nahe, die verfassungsrechtliche Garantie der informationellen Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 GG abzuleiten. Allein schon ein Blick in die Rechtsprechung des Bundesverfassungsgerichts zeigt allerdings, welche Schwierigkeiten eine solche Argumentation bereitet. Das Bundesverfassungsgericht hat zunächst einen Schutz der Privat- und Geheimsphäre als Bestandteil des allgemeinen Persönlichkeitsrechts im Sinne von Art. 2 Abs. 1 und Art. 1 GG bejaht (z.B. in BVerfGE Band 27, 344; 32, 373; 44, 353; 33, 367). Nicht von ungefähr hat jedoch das Gericht im Volkszählungsurteil, gerade vor dem Hintergrund einer sich fortlaufend, auch und vor allem durch die Möglichkeit einer multifunktionalen Nutzung der jeweils erhobenen Daten gekennzeichneten Informationstechnologie, seine früheren Positionen überprüft und nicht nur davon abgesehen, die informationelle Selbstbestimmung etwa nur bei Daten anzuerkennen, welche die Geheim- oder Intimsphäre der Betroffenen berühren, sondern sich unmißverständlich für eine klare Zweckbindung jeder Verarbeitung und gegen Vorratsspeicherungen irgendwelcher Art ausgesprochen. Es deshalb weiterhin bei einer Anknüpfung an Art. 2 Abs. 1 in Verbindung mit Art. 1 GG zu belassen, heißt die Garantie der informationellen Selbstbestimmung mit allen Unwägbarkeiten zu belasten, die ein unter anderen Umständen und mit anderen Zielen entwickelter Schutz des Persönlichkeitsrechts unweigerlich mit sich bringt. Es bedeutet aber auch, den Kern der informationellen Selbstbestimmung zu verkennen. Ihr Ziel ist es, die Kommunikationsfähigkeit des einzelnen sicherzustellen. Welche Vorkehrungen zu ihrer Gewährleistung also getroffen werden müssen, kann allein in Kenntnis dieser ihrer Aufgabe entschieden werden. So gesehen, spricht alles dafür, ein selbständiges Grundrecht auf informationelle Selbstbestimmung in das Grundgesetz aufzunehmen.

Sicher gilt es, sich davor zu hüten, die Tragweite einer entsprechenden Ergänzung der Verfassung zu überschätzen. Man darf allerdings auch nicht ihre Bedeutung unterschätzen. Die bloße Ergänzung der Verfassung um ein noch so klar formuliertes Grundrecht auf informationelle Selbstbestimmung löst ohne Zweifel nicht die mit einer Verarbeitung personenbezogener Daten verbundenen Probleme. Ob und in welchem Umfang es wirklich gelingen kann, die Chance der Betroffenen zu wahren, nicht nur den Überblick über die Verarbeitung zu behalten, sondern auch und vor allem Einfluß auf den Verarbeitungsablauf zu nehmen, hängt letztlich von den konkreten gesetzlichen, insbesondere bereichsspezifischen Vorkehrungen ab. Eine verfassungsrechtliche Norm hätte aber eine gerade für den tagtäglichen Respekt vor der informationellen Selbstbestimmung wichtige politisch-psychologische Bedeutung. Der

Verfassungsgeber würde damit offen auf die besonderen Entwicklungs- und Existenzbedingungen des einzelnen in einer hochtechnisierten, durch die zunehmende Informationsverarbeitung gekennzeichneten Gesellschaft reagieren und zugleich unmißverständlich statuieren, daß wer immer personenbezogene Daten haben möchte, sich an die Betroffenen wenden und ihnen die Entscheidung überlassen muß.

Daraus folgt aber: Eine verfassungsrechtliche Garantie der informationellen Selbstbestimmung darf sich nicht auf den öffentlichen Bereich beschränken. Auch im privaten Bereich kommt dem Schutz personenbezogener Daten zentrale Bedeutung zu, vor allem dort, wo die Freiheit der Bürgerin und des Bürgers durch die Ausübung wirtschaftlicher und sozialer Macht gefährdet ist. Ganz gleich, ob man die Verarbeitung von Arbeitnehmerdaten, den konsequenten Ausbau der Kreditinformationssysteme, die Datenerhebungen durch die zunehmenden privaten Sicherheitsdienste, das bundesweite elektronische Telefaxverzeichnis oder die vielfältige Verarbeitung von Patientendaten nimmt, überall zeigt sich, daß es keinen wirklichen Schutz der informationellen Selbstbestimmung geben kann, solange entscheidende Teile der Lebenswelt der Betroffenen ausgespart bleiben. Ganz in diesem Sinn hat das Bundesverfassungsgericht 1991 ausdrücklich klargestellt, daß beispielsweise auch im Rahmen eines Mietverhältnisses auf die informationelle Selbstbestimmung des Mieters Rücksicht genommen werden muß (BVerfG NJW 1991, 2411). Eine Ergänzung des Grundgesetzes darf sich deshalb nicht darauf beschränken, die informationelle Selbstbestimmung lediglich als ein gegen den Staat gerichtetes Abwehrrecht anzusprechen. Sie muß vielmehr auch einen expliziten Auftrag an den Gesetzgeber enthalten, einen gleichwertigen Schutz der informationellen Selbstbestimmung im öffentlichen und im nicht-öffentlichen Bereich zu gewährleisten. Nur unter dieser Voraussetzung kann es gelingen, die immer deutlichere Diskrepanz zwischen dem wachsenden Schutz im öffentlichen Bereich und den evidenten Schutzdefiziten im privaten Bereich zu überwinden.

2. Das Recht auf Informationsfreiheit

So wichtig es erscheint, die informationelle Selbstbestimmung ausdrücklich zu garantieren, so sehr kommt es darauf an, das Grundgesetz zugleich um eine weitere, das Grundrecht auf Informationsfreiheit gewährleistende Bestimmung zu ergänzen. Gemeint ist selbstverständlich nicht jenes bereits in Art. 5 Abs. 1 GG angegesprochene Recht, sich aus "allgemein zugänglichen Quellen ungehindert zu unterrichten". Gemeint ist vielmehr das Recht auf Zugang zu den Daten der Behörden ("Aktenöffentlichkeit", "freedom of information").

Wiederum geht es dabei um eine entweder bereits realisierte oder in der verfassungsrechtlichen Diskussion immer deutlicher formulierte Erwartung. So enthalten die Verfassungsentwürfe von Sachsen (Art. 33, speziell für Umweltakten) und Brandenburg (Art. 22 Abs. 4) Bestimmungen, die ausdrücklich auf die Informationsfreiheit eingehen. Die Informationsfreiheit ist in Schweden, Finnland, Dänemark, Norwegen, den Niederlanden, Kanada und den USA bereits in unterschiedlicher Weise festgelegt (siehe hierzu die Übersicht in meinem 14. Tätigkeitsbericht von 1985, Ziff.11, 15. Tätigkeitsbericht von 1986, Ziff. 10). Schließlich hat sich auch die Europäische Gemeinschaft in der Richtlinie des Rates der Europäischen Gemeinschaften vom 7. Juni 1990 über den Zugang zu Informationen über die Umwelt (siehe hierzu auch meinen 18. Tätigkeitsbericht von 1989, Ziff. 3.3) rechtsverbindlich für eine Informationsfreiheit entschieden. (Art. 3).

Auf den ersten Blick mag es merkwürdig, wenn nicht widersprüchlich erscheinen, gleichzeitig eine Garantie der informationellen Selbstbestimmung und der Informationsfreiheit zu verlangen. Beides paßt, so könnte man meinen, schlecht zusammen: Während im einen Fall eine gezielte, gesetzlich abgesicherte Abschottung bestimmter Daten gefordert wird, steht im anderen Fall ein prinzipiell unbeschränkter Informationszugang zur Debatte. Wer allerdings z.B. die Geschichte der hessischen Datenschutzgesetzgebung genau verfolgt, stellt schnell fest, daß sich der hessische Gesetzgeber von Anfang an keineswegs darauf beschränkt hat, Verarbeitungssperren bei der Verwendung personenbezogener Daten vorzusehen. Er hat sich vielmehr stets auch für Vorkehrungen ausgesprochen, die ein Informationsgleichgewicht zwischen Parlament und Regierung garantieren sollen und deshalb ein Informationszugangsrecht statuieren. Ganz in diesem Sinn hat der Gesetzgeber später, zuletzt in § 33 des 3. HDSG, ein Recht auf Zugang zu personenbezogenen Daten öffentlicher Stellen für wissenschaftliche Forschungsvorhaben anerkannt. Auf der gleichen Ebene bewegen sich die Bestimmungen des Hessischen Archivgesetzes. Kurzum, Datenschutz und Informationsfreiheit werden keineswegs voneinander getrennt oder gar gegeneinander ausgespielt, sondern als Bausteine eines auf die Kommunikationsfähigkeit der Bürgerinnen und Bürger und die Funktionsfähigkeit einer demokratischen Gesellschaft bedachten Regelungssystems. Im einen wie im anderen Fall geht es, anders ausgedrückt, darum, Informationsstrukturen festzulegen, die in Kenntnis der Anforderungen einer demokratischen Gesellschaft, aber auch der Auswirkungen einer sich verdichtenden Informationsverarbeitung, die Voraussetzungen des Zugangs und der Verwertung von Informationen näher bestimmen.

Nicht von ungefähr ordnet der brandenburgische Verfassungsentwurf die Informationsfreiheit dem in Art. 22 geregelten "Recht auf politische Gestaltung" zu und weist damit klar darauf hin, daß die Transparenz der öffentlichen Verwaltung eine entscheidende Bedingung für die Ausübung so fundamentaler Rechte ist wie etwa der Meinungs- und Pressefreiheit oder des Wahlrechts. Ebensowenig überrascht es aber, daß der Hessische Gesetzgeber dort, wo er bereits die Informationsfreiheit anerkannt hat, sich damit nicht begnügt, sondern möglichen Konflikten mit der informationellen Selbstbestimmung durch gezielte Regelungen zuvorzukommen sucht. Konflikte, die also dort durchaus entstehen können, wo der Zugang zu personenbezogenen Daten zur Debatte steht, berechtigen nicht dazu, sich entweder nur für die informationelle Selbstbestimmung zu entscheiden oder sich lediglich für die Informationsfreiheit auszusprechen. Sie verpflichten vielmehr dazu, beides ausdrücklich zu garantieren und in den konkret in Betracht kommenden Verarbeitungsfällen für einen Ausgleich zu sorgen, der Funktion und Verbindung beider Grundrechte berücksichtigt.

II. Textvorschläge mit Erläuterungen

1. Art. 2 a GG Informationelles Selbstbestimmungsrecht

(1.) Jeder Mensch hat das Recht, über die Verarbeitung der auf seine Person bezogenen Daten selbst zu bestimmen.

(2.) Jeder Mensch hat das Recht auf Information über die Verarbeitung der auf seine Person bezogenen Daten und Einsicht in die Akten, die Daten zu seiner Person enthalten.

(3.) Einschränkungen dieser Rechte dürfen nur durch Gesetz oder aufgrund eines Gesetzes erfolgen.

(4.) Der Gesetzgeber ist verpflichtet, einen gleichwertigen Schutz des informationellen Selbstbestimmungsrechts im öffentlichen und im nicht-öffentlichen Bereich zu gewährleisten.

Erläuterungen:

Verarbeitung ist jede Verwendung von Daten, z.B. auch jede Nutzung.

Das in Abs. 1 aufgenommene informationelle Selbstbestimmungsrecht gewährt als Abwehrrecht Schutz vor direkten staatlichen Eingriffen. Darüber hinaus entfaltet es auch – wie es nunmehr auch explizit in der Entscheidung des Bundesverfassungsgerichts vom 11. Juni 1991 (NJW 1991, 2411) bestätigt worden ist – als objektive Norm seinen Rechtsgehalt im Privatrecht und hat damit Einfluß auf die Auslegung und Anwendung privatrechtlicher Vorschriften (sog. "mittelbare Drittwirkung" des Grundrechts).

Das in Abs. 2 enthaltene Recht der Bürgerin und des Bürgers auf Information über die Verarbeitung seiner Daten umfaßt z.B. das Recht auf Auskunft und das Recht auf Benachrichtigung. Bei der Ausgestaltung dieser Rechte im einzelnen hat der Gesetzgeber Gestaltungsspielraum.

Das Recht auf Information über die Verarbeitung der Daten schließt die Auskunft über die konkreten Daten, Herkunft und Weiterverarbeitung der Daten (regelmäßige Empfänger usw.) sowie die rechtlichen Grundlagen der Verarbeitung ein.

Eine Einschränkung des Rechts auf informationelle Selbstbestimmung darf nur durch Gesetz oder aufgrund eines Gesetzes erfolgen. Sie setzt ein überwiegendes Allgemeininteresse an der Einschränkung voraus. Zuständigkeitsvorschriften im Grundgesetz dürfen auf keinen Fall als inhaltliche verfassungsrechtliche Regelungen angesehen werden, die als kollidierendes Verfassungsrecht Grundrechte einschränken können .

Abs. 4 enthält einen an den Gesetzgeber gerichteten Verfassungsauftrag, einen gleichwertigen Schutz des informationellen Selbstbestimmungsrechts im öffentlichen und im nicht-öffentlichen Bereich zu gewährleisten. Konkrete Gesetzgebungsaufträge sind im Grundgesetz bereits in einzelnen Fällen enthalten. So wird z.B. in Art. 6 Abs. 5 GG die Gleichstellung der ehelichen Kinder "durch die Gesetzgebung" verlangt. Ein expliziter Gesetzgebungsauftrag im Sinne einer verbindlichen Weisung der Verfassung an den Gesetzgeber zur umfassenden Realisierung des Schutzes der personenbezogenen Daten ist notwendig, weil der Gesetzgeber bisher im nicht-öffentlichen Bereich keinen gleichwertigen Schutz des informationellen Selbstbestimmungsrechts sichergestellt hat. Auch mit der im Dezember 1990 vom Bundestag verabschiedeten Neufassung des Bundesdatenschutzgesetzes ist ein solcher gleichwertiger Schutz nicht realisiert worden. Das seit langem bestehende und insbesondere von den Datenschutzbeauftragten immer wieder kritisierte Ungleichgewicht zwischen dem Umfang des gewährleisteten Datenschutzes im öffentlichen Bereich einerseits und im nicht-öffentlichen Bereich andererseits wurde vielmehr weiter zementiert, indem – im Gegensatz zum öffentlichen Bereich – für den privaten Bereich weder eine klare Zweckbindung der Daten noch eine Einbeziehung aller Verarbeitungsphasen und -formen in die gesetzliche Regelung vorgenommen und auch keine umfassende, nach den für den öffentlichen Bereich geltenden Grundsätzen funktionierende externe Kontrolle der Datenverarbeitung eingeführt wurde. Es fehlen zudem auch weiterhin wichtige bereichsspezifische Regelungen im nichtöffentlichen Bereich, so z.B. für Arbeitnehmerdaten und für Kreditinformationssysteme.

2. Art. 10
Brief-, Post- und Fernmeldegeheimnis

(2.) Beschränkungen dürfen nur aufgrund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen bis zum Abschluß der Überwachung nicht mitgeteilt wird und daß solange an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt. Danach sind die Betroffenen von der Maßnahme zu unterrichten. Von diesem Zeitpunkt an steht ihnen der Rechtsweg nach Art. 19 Abs. 4 offen.

Erläuterungen:

Die im Text durch Unterstreichungen gekennzeichneten Änderungsvorschläge für Art. 10 stellen eine Konkretisierung des Umfangs des informationellen Selbstbestimmungsrechts der Bürgerin und des Bürgers in einem besonders sensitiven Bereich dar. Zentraler Punkt ist, daß die von Eingriffen in das Brief-, Post- oder Fernmeldegeheimnis Betroffenen künftig auf jeden Fall nach Abschluß der Überwachung von den erfolgten Eingriffen unterrichtet werden und ein endgültiger Ausschluß des Rechtsweges nicht mehr erfolgt.

3. Art. 5 Abs. 2a
Recht auf Informationsfreiheit

Jeder Mensch hat das Recht auf Zugang zu den Daten der vollziehenden Gewalt ohne den Nachweis eines Interesses. Einschränkungen dieses Rechts dürfen nur durch Gesetz oder aufgrund eines Gesetzes erfolgen, wenn öffentliche Geheimhaltungsinteressen dies zwingend gebieten oder die Geheimhaltungsinteressen Dritter überwiegen.

Erläuterungen:

Das Recht auf Informationsfreiheit ("Aktenöffentlichkeit") zielt auf die umfassende Transparenz der staatlichen Verwaltung. Angesichts der Entwicklung der automatisierten Datenverarbeitung kann Bezugspunkt der Regelung allerdings nicht allein die "Akte" im herkömmlichen Sinne, d.h. in Papierform, sein. Die Bestimmung gewährleistet daher allgemein das Recht auf Zugang "zu den Daten" der vollziehenden Gewalt. Daten im Sinne dieser Bestimmung sind alle personenbezogenen und nicht personenbezogenen Daten unabhängig von der Form ihrer Speicherung, z.B. in herkömmlichen Akten in Papierform, manuellen oder automatisierten Dateien oder auf Bild- und Tonträgern.

Der Nachweis eines besonderen "berechtigten Interesses" der Bürgerin und des Bürgers an dem Zugang zu den Daten wird – anders als etwa in dem Verfassungsentwurf von Brandenburg – nicht verlangt. Ein solcher Nachweis würde auch dem unter I. dargelegten Hintergrund der Forderung nach einem Recht auf Informationsfreiheit widersprechen, weil es darum geht, generell die Voraussetzungen für eine effektive Mitwirkung jedes Bürgers an der politischen Willensbildung zu gewährleisten.

Das Recht auf Informationsfreiheit kann durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, wenn öffentliche Geheimhaltungsinteressen dies zwingend gebieten oder die Geheimhaltungsinteressen Dritter überwiegen. In der ersten Alternative ist ein grundsätzlicher Vorrang des Rechts des Bürgers auf Zugang zu den Daten eindeutig festgelegt. Geheimhaltungsinteressen des Staates können das Recht nur dann einschränken, wenn sie dies zwingend gebieten. Dies muß inhaltlich substantiiert begründet werden. Das Vorliegen dieser Voraussetzungen darf nicht pauschal für einzelne Verwaltungsbereiche, wie z.B. Verteidigung oder Verfassungsschutz bejaht werden.

In der zweiten Alternative ist kein grundsätzlicher Vorrang des Rechts auf Informationsfreiheit gegenüber den Geheimhaltungsinteressen Dritter festgelegt. Ein Geheimhaltungsinteresse Dritter kann z.B. das informationelle Selbstbestimmungsrecht Dritter sein, das ebenfalls verfassungsrechtlich gewährleistet ist. Hier hat kein Grundrecht grundsätzlichen Vorrang, beide sind prinzipiell gleichrangig und müssen im konkreten Konfliktfall einander zugeordnet werden.

III. Aufnahme einer Kompetenzregelung für den Bundesbeauftragten für Datenschutz und Informationsfreiheit in das Grundgesetz

So wichtig eine verfassungsrechtliche Garantie der informationellen Selbstbestimmung ist, so wenig reicht sie für sich genommen aus. Nicht etwa deshalb, weil es besonderer gesetzlicher Regelungen zur Verarbeitung personenbezogener Daten bedarf. Das Bundesverfassungsgericht hat vielmehr im Volkszählungsurteil ausdrücklich darauf aufmerksam gemacht, daß eine Gewährleistung der informationellen Selbstbestimmung entscheidend von der Existenz einer unabhängigen Institution abhängt, deren Aufgabe es sein muß, rechtzeitig einzugreifen und damit nicht nur einen "vorgezogenen Rechtschutz" zu verwirklichen, sondern auch eine kontinuierliche Fortentwicklung der normativen Anforderungen an die Datenverarbeitung.

Bundes- und Landesgesetzgeber haben diese Funktion ganz im Sinne des Bundesverfassungsgerichts den Datenschutzbeauftragten übertragen. Der Bundesgesetzgeber hat im Rahmen der Novellierung des Bundesdatenschutzgesetzes zudem die – in einer Reihe von Landesdatenschutzgesetzen seit langem – bestehende Regelung aufgegriffen und sowohl die Bedeutung der Tätigkeit des Datenschutzbeauftragten als auch dessen Unabhängigkeit durch die Notwendigkeit einer parlamentarischen Wahl unterstrichen.

Die Verknüpfung der informationellen Selbstbestimmung mit einer institutionalisierten Kontrolle legt es nahe, es nicht bei der bisherigen Regelung zu belassen. Eine ausdrückliche Aufnahme der informationellen Selbstbestimmung in das Grundgesetz muß auch eine entsprechende auf Funktion und Tätigkeit des Datenschutzbeauftragten bezogene Bestimmung zufolge haben. Die Verankerung in der Verfassung würde besser und deutlicher als bisher die Unabhängigkeit des Datenschutzbeauftragten hervorheben und zugleich den Gesetzgeber an seine Verpflichtung erinnern, die Bedingungen zu schaffen, um eine ebenso uneingeschränkte wie ungehinderte Kontrolle zu ermöglichen.

Was das Bundesverfassungsgericht zur informationellen Selbstbestimmung gesagt hat, gilt genauso für die Informationsfreiheit. Ein Grundrecht auf Informationsfreiheit muß ebenso wie die informationelle Selbstbestimmung durch eine institutionelle Kontrolle abgesichert werden. Dem Datenschutzbeauftragten entspricht so gesehen ein Beauftragter für die Informationsfreiheit. Daraus läßt sich aber nicht folgern, daß es notwendigerweise zwei getrennte Instanzen geben muß. Im Gegenteil: alle bisherigen Erfahrungen sprechen gegen eine solche Lösung. Sowohl in Frankreich als auch in Kanada hat sich zwar gezeigt, wie unentbehrlich die institutionelle Kontrolle ist, aber auch erwiesen, daß getrennte Instanzen eine wirksame Kontrolle erschweren. Gewiß, der Tätigkeitsbereich der beiden Instanzen deckt sich nur partiell, doch gerade dort, wo möglicherweise Konflikte entstehen können, bei der Verarbeitung personenbezogener Daten, kommt es ganz besonders darauf an, von Anfang an einen institutionellen und rechtlichen Rahmen zu schaffen, der auseinandergehende Interpretationen verringert und damit den höchstmöglichen Schutz der Grundrechte erlaubt. Nicht zuletzt deshalb gipfelt die bisherige Kritik etwa im französischen Modell in dem Vorschlag, die beiden Instanzen zu fusionieren.

Unter diesen Umständen erscheint es richtig, eine Trennung zu vermeiden und beide Aufgaben miteinander zu verbinden. Konkret: Der Bundesbeauftragte für den Datenschutz muß zugleich die Aufgaben eines Beauftragten für die Informationsfreiheit wahrnehmen.

IV. Textvorschlag

Einfügung eines Art. 45 d

(1) Der Bundestag wählt auf Vorschlag der Bundesregierung einen Bundesbeauftragten für Datenschutz und Informationsfreiheit mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder für eine Amtszeit von fünf Jahren. Einmalige Wiederwahl ist zulässig.

(2) Vor Ablauf der Amtszeit kann der Bundesbeauftragte für Datenschutz und Informationsfreiheit nur abberufen werden, wenn Tatsachen vorliegen, die bei einem Beamten die Entlassung aus dem Dienst rechtfertigen.

(3) Der Bundesbeauftragte ist unabhängig, frei von Weisungen und nur dem Gesetz unterworfen.

(4) Der Bundesbeauftragte kann sich jederzeit an den Bundestag wenden.

(5) Das Nähere regelt ein Gesetz.

17.3
Rede des Landtagspräsidenten Starzacher vom 22. Oktober 1991 vor dem Hessischen Landtag zum Ausscheiden von Herrn Professor Dr. Simitis aus dem Amt des Hessischen Datenschutzbeauftragten

Zwischen den Fraktionen ist vereinbart, daß wir, bevor wir den von der Landesregierung vorgeschlagenen Kandidaten für dieses Amt wählen, zunächst Gelegenheit nehmen und geben, daß Herr Professor Simitis zu uns spricht, der 16 Jahre lang Datenschutzbeauftragter gewesen ist. Aber bevor ich Herrn Professor Simitis das Wort gebe, möchte ich für den Hessischen Landtag selbst einige Anmerkungen zu seiner Arbeit machen.

Meine Damen und Herren, was den Datenschutz betrifft, hatte Hessen immer eine Spitzenstellung. Es war, wenn ich das so sagen darf, schon immer ein Land der Superlative. Hier im Hessischen Landtag wurde 1970 das erste Datenschutzgesetz der Welt geschaffen, und heute verabschieden wir den dienstältesten Datenschutzbeauftragten der Welt.

Lieber Herr Professor Simitis, vor 16 Jahren, im Jahr 1975, haben Sie das Amt des Hessischen Datenschutzbeauftragten von Ihrem Vorgänger Willi Birkelbach übernommen. Ich freue mich besonders , daß Willi Birkelbach heute auf der Tribüne als Gast an dieser Plenarsitzung teilnimmt.

Ebenso freue ich mich, daß Herr Ministerpräsident a.D. Albert Osswald an der heutigen Plenarsitzung teilnimmt, ebenso wie Herr Dr. Schonebohm, der wesentlichen Anteil am Zustandekommen unseres Datenschutzgesetzes Ende der sechziger Jahre, Anfang der siebziger Jahre gehabt hat. Herzlich willkommen im Hessischen Landtag!

Herr Professor Simitis, nachdem Sie dieses Amt vor 16 Jahren übernommen und seither ununterbrochen wahrgenommen haben, haben Sie Landesregierungen sehr unterschiedlicher politischer Zusammensetzung kritisch begleitet. Daß Sie bei Ihren Wiederwahlen von den jeweiligen Landtagen regelmäßig ein zustimmendes Votum von über 90 Prozent aller Stimmen erhielten – lediglich bei Ihrer ersten Wahl hatten Sie 20 Gegenstimmen zu verzeichnen –, spricht für die hohe Akzeptanz, die Sie durch Ihre unbestreitbare und unbestrittene Kompetenz erworben haben.

16 Jahre sind eine lange Zeit. Es hätten auch mehr Jahre werden können. Über die Zahl der vielen Jahre hinaus ist für Ihr Wirken aber vielleicht noch wesentlich aussagekräftiger, wie Sie von außen gesehen werden, wie Sie beispielsweise nicht selten in den Medien und unter Ihren Kollegen als der "Papst des Datenschutzes" "apostrophiert" wurden. Nach meiner Kenntnis geschah dies kaum deshalb, weil Sie den Anspruch der Unfehlbarkeit erhoben hätten;

vielmehr fanden Sie Anerkennung und Bewunderung vor allem deshalb, weil Ihre Bereitschaft überzeugte, immer dann initiativ zu werden, wenn Ihnen dies im Interesse und zum Wohle des Datenschutzes wichtig erschien.

Sie schalteten sich stets dann in die Diskussion ein, wenn sich bedeutsame Entwicklungen in der von rapiden Veränderungen gekennzeichneten Welt der Datenverarbeitung abzeichneten. Ganz abseits von professoraler Abgeschiedenheit waren Sie stets bereit, auch in den Ausschüssen des Hessischen Landtags noch in den späten Abendstunden bei der Kleinarbeit in der Gesetzgebung mitzuwirken.

Der Datenschutz wandelte sich während Ihrer Amtszeit von einem recht exotischen Gebiet für eine kleine Gruppe von Datenverarbeiterinnen und Datenverarbeitern – es werden in der Regel Männer gewesen sein – und Futurologen zu einem heute anerkannten Bestandteil nicht nur der öffentlichen Verwaltung, sondern auch des Wirtschaftslebens. Meilensteine für uns in Hessen, aber auch für die gesamte Bundesrepublik waren dabei folgende Ereignisse:

1978 wurde mit der Verabschiedung des Bundesdatenschutzgesetzes auch das Zweite Hessische Datenschutzgesetz geschaffen.

1983 war ein besonders bedeutsames Jahr für den Datenschutz: Das Bundesverfassungsgericht bekannte sich im Volkszählungsurteil zum Grundrecht auf informationelle Selbstbestimmung und legte die Grundlage für ein Netz bereichsspezifischer Datenschutzregelungen, das den Gesetzgebern in den Folgejahren ein erhebliches Arbeitspensum abverlangte. Erst in diesen Wochen ergänzte das Gericht dieses Urteil um eine weitere Entscheidung, mit der bekräftigt wurde, daß auch im privaten Bereich das Recht auf informationelle Selbstbestimmung Gültigkeit hat.

1984 wurde hier in diesem Plenarsaal ein Symposium der Hessischen Landesregierung veranstaltet, das den Titel "Informationsgesellschaft oder Überwachungsstaat" trug. Vom extremen Kritiker der Informationsgesellschaft – ich erinnere an Professor Joseph Weizenbaum vom Massachusetts Institute of Technology – bis hin zu einem Repräsentanten der modernen polizeilichen Datenverarbeitung, dem früheren Präsidenten des Bundeskriminalamts Horst Herold, diskutierte damals in diesem Hause die "Creme" der Datenschützer und Datenverarbeiter Chancen und Gefahren der modernen personenbezogenen Datenverarbeitung.

1986 schuf Hessen wiederum als erstes Bundesland ein Datenschutzgesetz, das über die automatisierte und manuelle Datenverarbeitung hinaus jede Form von personenbezogener Informationsverarbeitung einbezog.

1990 und 1991 war Hessen wiederum unter den ersten Bundesländern, als es mit dem Hessischen Gesetz über die Öffentliche Sicherheit und Ordnung und dem Hessischen Verfassungsschutzgesetz Maßstäbe für die Polizei- und Verfassungsschutzgesetze der übrigen Länder und des Bundes setzte.

Bei all diesen Vorhaben waren Sie, Herr Prof. Simitis, zwar in unterschiedlicher, aber immer sehr intensiver Weise beteiligt: als Gutachter für das Bundesverfassungsgericht, als Teilnehmer an zahllosen Anhörungen in Bund und Ländern zu projektierten Datenschutzregelungen, als Wissenschaftler bei internationalen Symposien, im Alltag der Gesetzgebungsarbeit und bei Ihrer Kontrolltätigkeit, die heute im Mittelpunkt unserer Betrachtungen stehen soll. Der weite Bogen Ihrer Arbeit fordert uns Bewunderung und Respekt ab.

Nicht zuletzt während der Affäre um die Verwendung eines Telefonabhörprotokolls in der letzten Wahlperiode legten Sie Zeugnis von einer stets unparteiischen, sachorientierten und präzisen Arbeitsweise ab. Daß gerade in der letztgenannten Angelegenheit meines Wissens keinerlei öffentliche Kritik an Ihrem Vorgehen und an Ihren Berichten laut wurde, beweist, mit welchem Respekt Landtag, Landesregierung, aber auch alle Fraktionen bzw. Parteien bei aller unterschiedlichen Betroffenheit Ihre Tätigkeit begleitet haben.

Herr Professor Simitis, Sie waren auch außerhalb der Grenzen der Bundesrepublik erfolgreich für das Markenzeichen Datenschutz made in Hessen. Nicht nur als Vorsitzender der Expertenkommission für Datenschutz beim Europarat in den Jahren 1982 bis 1986 und als Vorsitzender der Arbeitsgruppe der Datenschutzbeauftragten der Mitgliedsländer der Europäischen Gemeinschaften seit 1990, sondern auch als Teilnehmer an einer Vielzahl von Konferenzen haben Sie, meist in der jeweiligen Landessprache, für dieses Markenzeichen Datenschutz geworben.

Lieber Herr Professor Simitis, mit Bedauern mußten wir zur Kenntnis nehmen, daß Sie nun nach 16 Jahren auch die stilvolle Arbeitsatmosphäre in Ihrer Dienststelle in der Uhlandstraße nicht mehr reizt, das Amt für eine weitere Amtsperiode wahrzunehmen. Wir hätten Sie gern – ich bin sicher: mit breiter Zustimmung des ganzen Hauses – wiedergewählt.

In Ihrer Rede in der gestrigen Sitzung des Unterausschusses für Informationsverarbeitung und Datenschutz haben Sie uns mitgeteilt, daß Sie nicht nach neuen Ufern streben, sondern an den Ihnen verbleibenden alten Ufern, vor allem an der Frankfurter Universität Ihre Arbeit intensivieren wollen. Das heißt, Sie werden eine neue Relation zwischen Ihrer Profession und Ihrer Professur herstellen. Hierfür wünschen wir Ihnen Gesundheit und die Kraft, alle geplanten Vorhaben zu realisieren.

Als Präsident des Hessischen Landtags, an den das Amt des Datenschutzbeauftragten angebunden ist, möchte ich Ihnen sehr herzlich für die in den letzten 16 Jahren geleistete Arbeit danken.

Damit verbinde ich auch den Dank an Ihre Mitarbeiterinnen und Mitarbeiter.

Ich bin sicher, daß Sie dem Hessischen Landtag auch künftig Ihren Rat nicht versagen werden, wenn es in den kommenden Jahren wieder einmal darum geht, Gesetze über die personenbezogene Informationsverarbeitung zu schaffen oder zu verändern. Insofern hoffe ich, daß der heutige Tag kein Tag des Abschieds ist, sondern der Beginn einer Zusammenarbeit in neuer Form. Ihre mir in der vergangenen Woche übermittelten Vorschläge zur Aufnahme des informationellen Selbstbestimmungsrechts und der Informationsfreiheit in das Grundgesetz nähren diese Hoffnung beträchtlich.

Noch einmal herzlichen Dank, Herr Professor Simitis. Ich erteile Ihnen jetzt das Wort.

17.4
Rede von Professor Dr. Simitis vor dem Hessischen Landtag am 22. Oktober 1991 anläßlich seines Ausscheidens aus dem Amt des Hessischen Datenschutzbeauftragten

1.
Jahr für Jahr wird in den Plenarsaal des Hessischen Landtags ein Stuhl für den Datenschutzbeauftragten hereingetragen und von den Abgeordnetensitzen deutlich getrennt, wenn auch in deren unmittelbarer Nähe hingestellt. Kaum jemand achtet noch darauf. Und doch ist der Vorgang in doppeltem Sinne symbolisch.

Er symbolisiert vor allem die enge Verbindung des Datenschutzbeauftragten zum Parlament. Früher als jedes andere Parlament hat der Hessische Landtag festgelegt, daß der Bedeutung, die den Aufgaben des Datenschutzbeauftragten zukommt, nur in Gestalt einer parlamentarischen Wahl entsprochen werden könne sowie durch die Verpflichtung des Gewählten, dem Parlament jederzeit Rechenschaft abzulegen. Die Position des Stuhles symbolisiert aber auch die Einsamkeit des Datenschutzbeauftragten. Die Wahl durch das Parlament führt, so paradox dies klingen mag, nicht in die Nähe derer, die den Datenschutzbeauftragten gewählt haben. Im Gegenteil: der Datenschutzbeauftragte hat zu den politischen Parteien sowie zur Regierung und öffentlichen Verwaltung stets ein Höchstmaß an Distanz zu wahren. Doch bedeutet dies keineswegs, daß ihm die Rolle eines interessierten Zuschauers zugedacht wäre. Er muß vielmehr, will er die in ihn gesetzten Hoffnungen erfüllen, jederzeit bereit sein, offen und unmißverständlich zu einzelnen Vorgängen ebenso wie zur generellen Entwicklung der Verarbeitungstechnologie Stellung nehmen, ohne Rücksicht darauf, wie unangenehm eine solche Stellungnahme für die Beteiligten, Dritte oder gelegentlich auch für ihn selbst sein mag.

Die Wahl zum Datenschutzbeauftragten ist, so gesehen, unweigerlich der Beginn eines schwierigen Mittelweges zwischen den Extremen einer bloßen Alibifunktion einerseits und solipsistischer Proteste andererseits. Legt der Datenschutzbeauftragte nämlich nicht nur Wert auf einen kontinuierlichen Dialog mit den einzelnen verarbeitenden Stellen, sondern versucht er auch, die jeweiligen Probleme gemeinsam mit ihnen zu lösen, so kann er sich alsbald den Vorwurf einhandeln, Alibiveranstaltungen zu inszenieren. Entwickelt er dagegen seine Vorschläge im Alleingang und erklärt er sie für die einzig möglichen, die einzig richtigen, läuft er Gefahr, Monologe vor den Toren einer hermetisch sich abschottenden Verwaltung zu halten.

2.
Die Anbindung an das Parlament und die Distanz zur Regierung ebenso wie zur öffentlichen Verwaltung gehören zu den wichtigsten Voraussetzungen, um gerade die Funktion erfolgreich wahrnehmen zu können, die in den Augen des Bundesverfassungsgerichts den Kern der Tätigkeit des Datenschutzbeauftragten ausmacht: einen "vorgezogenen Rechtsschutz" gegen die Gefahren der Verarbeitung personenbezogener Daten sicherzustellen. Der Datenschutzbeauftragte ist, so gesehen, Symbol und Garant jener gesetzlichen Vorschriften, die wohl deutlicher als jede andere Regelung die Fragilität einer demokratischen Gesellschaft illustrieren, eben der Datenschutzgesetze.

Wer systematisch Daten über die Krankheiten von Kassenpatienten zusammenstellt, Informationen darüber erhebt und miteinander verknüpft, wann Schulkinder "auffällig" werden, Angaben über Kauf- oder Urlaubsgewohnheiten zu "life-style-Profilen" verarbeitet, will mehr als nur Fragen entscheiden, die einen bestimmten Einzelfall betreffen. Er will das Verhalten der Kassenpatienten unter Kostengesichtspunkten "optimieren", "kriminogenen" Faktoren in Schule und Familie rechtzeitig entgegenwirken oder gezielt auf Vorstellungen und Reaktionen der Konsumenten Einfluß nehmen. Verständlicherweise ist er deshalb auf ein offenes Verarbeitungsprogramm bedacht, sucht also seine Informationsgrundlage möglichst umfassend anzulegen, um aktuelle Fragen beantworten zu können, aber auch um für potentielle, noch gar nicht absehbare zukünftige Entwicklungen gerüstet zu sein.

In dem Maße, in dem der einzelne, vor dem Hintergrund expandierender administrativer Aufgaben und sich ständig verfeinernder Marketingstrategien nur noch als Informationsobjekt wahrgenommen, ja wie selbstverständlich zum "Informationsschuldner" erklärt wird, verflüchtigen sich seine Grundrechte. Wer nicht mehr weiß, für wen, aus welchen Gründen und mit welchen Konsequenzen Daten zu seiner Person erhoben und verarbeitet werden, wird zunehmend bestrebt sein, nicht aufzufallen. Er wird sich mehr und mehr davor hüten, einer politischen Partei, einer Gewerkschaft oder einer sonstigen Organisation beizutreten, sich an einer Demonstration zu beteiligen oder überhaupt seine Meinung zu äußern. Wo die wachsende Informiertheit über den einzelnen mit dessen zunehmender Desinformiertheit hinsichtlich des Umgangs mit den seine Person betreffenden Daten erkauft wird, minimiert sich die Chance zur Selbständigkeit, während sich der Anpassungsdruck maximiert.

In klarer Erkenntnis dieses Zusammenhangs hat das Bundesverfassungsgericht, wie zuvor schon der hessische Gesetzgeber, die Existenz- und Funktionsfähigkeit einer demokratischen Gesellschaft unmittelbar in Beziehung gesetzt zu den Bedingungen, unter denen personenbezogene Daten verarbeitet werden dürfen. Wenn die einzelnen wirklich die Möglichkeit haben sollen, ihre persönliche Entwicklung selbst zu bestimmen, muß die Begrenzung und nicht die Grenzenlosigkeit Leitmaxime der Informationsverarbeitung sein. Jede der Vorschriften, die den Verarbeitungsablauf regeln, ist insofern ein Indikator für die Bereitschaft, den Zugriff auf personenbezogene Daten nur als besonders begründungsbedürftige Ausnahme zu tolerieren.

Aus dieser Perspektive betrachtet, muß eine auf ihre Substanz bedachte demokratische Gesellschaft Informationsdefizite bewußt in Kauf nehmen. Nur eine konsequent praktizierte Zurückhaltung im Umgang mit personenbezogenen Angaben ebnet dem einzelnen den Weg zur Selbstbestimmung und bewahrt die Gesellschaft zugleich davor, in totalitäre Strukturen abzugleiten. Datenschutz ist also unmittelbar Demokratieschutz. Vor dem Hintergrund der gegenwärtigen Diskussion über eine Revision des Grundgesetzes stellt sich daher die Frage, ob es nicht an der Zeit wäre, der mit dem Hessischen Datenschutzgesetz von 1970 eingeleiteten und durch das Volkszählungsurteil des Bundesverfassungsgerichts eindrucksvoll bestätigten Entwicklung durch einen besonderen Verfassungsartikel Rechnung zu tragen. Ich habe deshalb eine Reihe von Vorschlägen zur Ergänzung des Grundgesetzes in einem Zwischenbericht zusammengefaßt und dem Präsidenten des Hessischen Landtages mit der Bitte zugeleitet, diese Vorschläge in die Verfassungsdebatte einzubringen.

3.
Seit jenem 30. September 1970, an dem der Hessische Landtag das weltweit erste Datenschutzgesetz verabschiedete, hat sich gewiß viel verändert. Längst ist beispielsweise die Vorstellung aufgegeben worden, die polizeiliche Datenverarbeitung ließe sich mit Hilfe einiger weniger Verwaltungsvorschriften regeln. Niemand bestreitet mehr die Notwendigkeit, den Verarbeitungsverlauf an verbindliche, gesetzlich definierte Vorgaben zu knüpfen. Auch die Annahme, ein einziges, allgemeines Datenschutzgesetz reiche aus, gehört mittlerweile der Vergangenheit an.

Die abstrakten, unterschiedlich interpretierbaren Bestimmungen der ersten Datenschutzgesetze sind zunehmend Vorschriften gewichen, die sich direkt auf einzelne, für den Betroffenen freilich besonders wichtige Verarbeitungsvorgänge beziehen und den Interpretationsspielraum einengen. Um nur einige Beispielsbereiche zu nennen: Wenn personenbezogene Daten in Sozial- oder Sicherheitsbehörden verarbeitet werden, im Rahmen einer Krankenhausbehandlung oder bei der Archivierung behördlicher Unterlagen, sind stets in erster Linie Bestimmungen maßgeblich, die für jede dieser Verarbeitungssituationen eigens entwickelt worden sind.

Die hartnäckig wiederholte Behauptung, der gesetzlichen Regelung komme lediglich die Aufgabe zu, den Verarbeitungsmißbrauch zu verhindern, ist mittlerweile ebenfalls fallengelassen worden. In Anlehnung an das Volkszählungsurteil des Bundesverfassungsgerichts hat der hessische Gesetzgeber als Leitlinie aller Verarbeitungsregelungen 1986 die Verpflichtung anerkannt, das Recht des einzelnen zu schützen, über die Preisgabe und Verwendung der sich auf seine Person beziehenden Daten selbst zu bestimmen. Dem hat sich inzwischen nicht nur ein Landesgesetzgeber nach dem anderen angeschlossen, sondern, wenngleich in einer etwas verklausulierten Form, auch der Bundesgesetzgeber.

Es gibt heute also keinen Zweifel mehr an der Verpflichtung aller verarbeitenden Stellen, sich grundsätzlich stets nur an die Betroffenen zu wenden, um die benötigten Informationen zu bekommen. Unstreitig ist gleichermaßen das Recht der Betroffenen, von jeder verarbeitenden Stelle im einzelnen zu erfahren, ob und wenn ja, welche Daten verarbeitet werden. Niemand käme zudem noch auf jene seltsame, jahrelang vor allem vom Bundesgesetzgeber verfochtene Idee, eine Gebühr zu erheben, wenn die Betroffenen ihr gesetzlich verbürgtes Auskunftsrecht ausüben.

4.
Die Geschichte des Datenschutzes ist ein Musterbeispiel für Bedeutung und Leistungskraft eines konsequent praktizierten Föderalismus. Die Landesgesetzgeber haben als erste auf die sich abzeichnenden Folgen der automatischen Verarbeitung personenbezogener Daten reagiert. Sie waren es auch, die seither immer wieder die Initiative ergriffen haben, um die bestehenden Regelungen zu überprüfen und auszubauen. Wohl keine andere Ausrede hat deshalb die Weiterentwicklung des Datenschutzes mehr gefährdet als die Behauptung, erst einmal müsse die Reaktion des Bundesgesetzgebers abgewartet werden. Diesem steht eine "Leitfunktion" nicht zu; auch kann von ihm nicht erwartet werden, Lösungen für alle Datenschutzprobleme anzubieten. Das Grundgesetz stellt seinen Äußerungen eben nicht eine Verpflichtung zur Konformität voran. Vielmehr spricht es sich unmißverständlich für eine Aufteilung der Kompetenzen aus und begründet damit das Recht, aber auch die Pflicht der Länder, ihre Gestaltungsspielräume voll zu nutzen. Zwar ist jedes Land gehalten, die Kompetenzgrenzen zu respektieren, jedoch nicht um den Preis der passiven Hinnahme einer expansiven Gesetzgebungspolitik des Bundes. Die Länder können vielmehr anhand der eigenen Gesetzgebungstätigkeit immer wieder aktiv selbst verdeutlichen, wo die Kompetenzgrenzen verlaufen.

Zwei Beispiele: Alle Fraktionen des Bundestages haben wiederholt an die Bundesregierung appelliert, endlich Vorschläge für eine Regelung der Verarbeitung von Arbeitnehmerdaten vorzulegen. Davon unabhängig hat der hessische Gesetzgeber der Landesverwaltung bereits untersagt, dienst- und arbeitsrechtliche Beurteilungen der Beschäftigten ebenso wie die sie betreffenden medizinischen und psychologischen Befunde automatisiert zu

verarbeiten. Die unstreitige Kompetenz des Bundes für den Datenschutz im nichtöffentlichen Bereich hat der hessische Gesetzgeber gleichfalls nicht zum Anlaß genommen, sich völlig passiv zu verhalten. Vielmehr korrigierte er den Mangel an Transparenz bei einer Verarbeitung personenbezogener Angaben durch nicht-öffentliche Stellen wenigstens teilweise durch die Verpflichtung der Landesregierung, dem Parlament jährlich einen Bericht über die Erfahrungen der für diese Stellen zuständigen Landesbehörden zuzuleiten.

5.
Diese vielen und zweifellos wichtigen Verbesserungen können indessen den Blick dafür versperren, daß die Entwicklung des Datenschutzes nicht etwa gradlinig von Erfolg zu Erfolg verlaufen ist und verläuft, sondern sich nur langsam, ja zuweilen unendlich mühsam, von Rückschritten und Enttäuschungen begleitet, vollzogen hat und vollzieht. Und zwar allein schon deshalb, weil die Forderung, von einer Verarbeitung personenbezogener Daten möglichst abzusehen bzw. sich strikt auf jeweils konkret erforderliche Angaben zu beschränken, mit der tradierten, in den modernen hochtechnisierten Industriegesellschaften nach wie vor weitverbreiteten Vorstellung kollidiert, jede Verarbeitung sei solange legitim und legal, wie sie dazu diene, die eigenen Aufgaben "effizienter" und "wirtschaftlicher" zu erfüllen. Würde man diese Vorstellung weiterhin uneingeschränkt und unbefragt akzeptieren, bestünde wenig Aussicht auf Datenschutz; denn es gibt kaum einen Verarbeitungsvorgang, für den sich diese Kriterien nicht ins Feld führen ließen.

Ich nenne drei Beispiele für solches Argumentieren aus der praktischen Arbeit des Hessischen Datenschutzbeauftragten. Man hat die Speicherung von Selbstmordversuchen in den polizeilichen Informationssystemen damit begründet, die Polizei könne auf diese Weise im Wiederholungsfalle "angemessen" reagieren, bei der Festnahme eines so Gefährdeten entsprechende Haftbedingungen vorsehen oder gegebenenfalls die Todesursache rascher ermitteln. Als man zehnjährige Schülerinnen und Schüler während der Unterrichtszeit Fragebögen zu häuslichen Verhältnissen, zur Beziehung der Eltern untereinander sowie zu den Nachbarn beantworten ließ, hat man angegeben, die möglichst genaue Kenntnis der Lebensbedingungen von Schülern erleichtere die korrekte Einschätzung ihrer schulischen Leistungen. Der Vermerk von Diagnosen auf dem Krankenschein, also eine klare Preisgabe von Patientendaten, ist damit gerechtfertigt worden, auf diese Weise könnten "erbrachte Leistungen" richtig bewertet, unangemessene Honorarforderungen offengelegt und damit weitere Steigerungen der Versicherungskosten verhindert werden.

Nach wie vor gilt das Bestreben, immer mehr Informationen zu erheben und neu zu verarbeiten, als selbstverständlich, und nach wie vor wird die Aufforderung, die eigenen Datenbestände und Informationswünsche fortlaufend kritisch zu überprüfen, gewissermaßen als widernatürlich empfunden. So ist jüngst die Forderung des Datenschutzbeauftragten auf heftige Kritik gestoßen, die für die Jugendämter von Betreuern und Therapeuten erstellten Erziehungsberichte auf die für die Entscheidungen dieser Behörden relevanten Punkte zu beschränken, künftig also etwa auf die bislang übliche überaus detaillierte Darstellung der körperlichen Konstitution und der Persönlichkeitsentwicklung zu verzichten. Das Gegenargument lautete: Die Jugendämter seien auf eine umfassende und präzise Information angewiesen, wollten sie ihre Aufgabe, nicht zuletzt im Hinblick auf den gesetzlich geforderten "Hilfeplan", "sachgerecht" erfüllen. Dem ist entgegenzuhalten: Das Kinder- und Jugendhilfegesetz verlangt zwar tatsächlich einen "Hilfeplan", versteht ihn aber, im Gegensatz zu früher verbreiteten Vorstellungen, als Grundlage einer zeitlich beschränkten, also möglichst bald zu beendenden Intervention. Und gerade deshalb ist es unerläßlich, den Informationsprozeß von vornherein einzuschränken, um der Gefahr einer Stigmatisierung ebenso vorzubeugen wie der Versuchung, den "Hilfeplan" in eine langfristige, administrativ gesteuerte Planung individueller Schicksale zu verwandeln.

Noch massiver formierte sich der Widerstand gegen die Forderung, Familienmitgliedern von Angehörigen des öffentlichen Dienstes einen selbständigen Anspruch gegenüber der Beihilfestelle zu gewähren. Dadurch sollte beispielsweise vermieden werden, daß Gutachten zur psychotherapeutischen Behandlung längst volljähriger Kinder in die Beihilfeakte ihres Vaters gelangten oder in Scheidung lebende Frauen gezwungen würden, ärztliche Befunde an ihren beihilfeberechtigten Ehemann weiterzuleiten. Jeder Versuch, die Ansprüche aufzuteilen, würde, so meinte man zur Abwehr dieser Forderung, gegen die in Art. 33 GG vorgesehene Verpflichtung verstoßen, sich bei der Gestaltung des öffentlichen Dienstes nach den "hergebrachten Grundsätzen des Berufsbeamtentums" zu richten. Der Beihilfeanspruch sei eine Ergänzung des Besoldungsanspruchs und deshalb genau wie dieser ein höchstpersönlicher Anspruch. Das Grundgesetz aber stellt nun einmal die "hergebrachten Grundsätze des Berufsbeamtentums" nicht über die Grundrechte.

6.
Diese der informationellen Selbstbestimmung gegenüber gleichgültige oder gar abweisende Mentalität schlägt immer wieder durch. So überrascht es nicht, daß ständig Versuche unternommen werden, die Anwendung etablierter Datenschutzregelungen einzuschränken und bereits erzwungene Korrekturen rückgängig zu machen. Wohl auf keine andere Vorschrift haben verarbeitende Stellen so schnell reagiert wie auf jene Bestimmung des novellierten Bundesdatenschutzgesetzes, die den Betroffenen das Recht einräumt, der Kontrolle über die Verarbeitung ihrer Daten durch den Bundesbeauftragten zu widersprechen. Just jene Bundespost, die jahrelang nichts von gerade für ihren Bereich dringend notwendigen Datenschutzvorschriften wissen wollte, hat, kaum war die Novellierung verabschiedet, ihre Telefonkunden ausdrücklich auf das ihnen zustehende Widerspruchsrecht aufmerksam gemacht, ohne freilich ein einziges Wort darüber zu verlieren, daß und warum eine generelle und präventive Kontrolle durch den Bundesbeauftragten – eben im Interesse der Betroffenen – unverzichtbar ist.

Bekanntlich hat kein anderes Ereignis die Entwicklung des Datenschutzes nachhaltiger gefördert als die letzte Volkszählung. So mutet es fast paradox an, daß schon jetzt Konzepte für die Volkszählung 2000 entwickelt werden, die über weite Strecken so verlaufen, als habe es die damalige erbitterte Auseinandersetzung über die Notwendigkeit von "Totalerhebungen" gar nicht gegeben. Niemand scheint sich mehr an die vom Bundesverfassungsgericht wie vom Bundestag ausgesprochene Aufforderung zu erinnern, über Alternativen nachzudenken. Was heute einzig interessiert, ist offenbar, wie die für unentbehrlich gehaltene Zählung noch effektiver durchgeführt werden könne als die vorherige. Laptops sollen den Zählern ermöglichen, die Daten direkt einzuspeisen und so das Risiko, daß die Befragten Fehlangaben machen, vollends beseitigen. Daß sich das Bundesverfassungsgericht seinerzeit für das Recht der Befragten ausgesprochen hatte, den Fragebogen persönlich und ungestört auszufüllen, scheint vergessen, ganz zu schweigen von einer Berücksichtigung der gerade unter Datenschutzgesichtspunkten bestehenden Bedenken hinsichtlich der Verwendung von Laptops.

7.
Die zukünftige Entwicklung des Datenschutzes hängt aber nicht allein von Einstellungen und Mentalitäten ab. Sie wird wesentlich von Innovationen im Bereich der Verarbeitungstechnologie bestimmt werden. Schließlich war es diese Technologie, die die Diskussion über die Notwendigkeit gesetzlich gesicherter Anforderungen an die Verarbeitung personenbezogener Daten allererst in Gang gesetzt hat.

Die siebziger Jahre standen ganz im Zeichen der Erwartung, die zunehmende Automatisierung werde im Zuge des Aufbaus großer Datenbanken zu einer Zentralisierung der Verarbeitung führen. Die meisten der seinerzeit ausgearbeiteten und bis heute geltenden Vorschriften zum Ablauf und zur Kontrolle der Verarbeitung wurden im Hinblick auf diese Annahme formuliert. Durch die schnelle Verbreitung des Personal Computers in den achtziger Jahren wurde sie jedoch überraschend ad absurdum geführt. Statt der erwarteten Zentralisierung setzte sich eine Dezentralisierung durch, die nun wichtige, in den Datenschutzgesetzen fest verankerte Regelungsansätze wirkungslos zu machen droht.

Die neunziger Jahre werden, so scheint es, von den sogenannten neuronalen Computern beherrscht werden. Ihr Funktionsprinzip setzt zwei weitere Verarbeitungsprämissen außer Kraft, die in der Datenschutzdiskussion bisher als unveränderlich galten: die Trennung von Hard- und Software sowie die von Prozessor und Speicher. Zudem beginnt sich der Computer auf dieser Stufe sozusagen zu verselbständigen und, ähnlich dem menschlichen Gehirn, mit Hilfe von Regeln zu reagieren, die er sich selbst erarbeitet, etwa über die Korrelation von Beispielen oder durch Nachahmung. Die Konsequenzen liegen auf der Hand: Zwar dürfte es nach wie vor möglich sein, die Ausgangsgrundlage des Verarbeitungsprozesses zu überprüfen. Dagegen läßt sich weder der Verarbeitungsablauf genau verfolgen, noch gar die Entscheidungsfindung exakt rekonstruieren. Und damit entfallen gerade jene Bedingungen, die es bislang erlaubt haben, präzise Anforderungen an die Verarbeitung personenbezogener Daten zu stellen und deren Einhaltung zu kontrollieren.

Nur wenn es gelingt, der sich verändernden Verarbeitungstechnologie mit neuen Regelungskonzepten zu begegnen, wird Datenschutz auch in Zukunft gewährleistet werden können. Die Zeit hierfür ist freilich knapp, denn nach den vorliegenden Informationen werden neuronale Computer bereits praktisch erprobt. Zu den Testfällen gehört unter anderem die Überprüfung der Kreditwürdigkeit von Kunden bestimmter Banken. Eines hat uns die Erfahrung inzwischen gelehrt: Wenn Datenschutzvorschriften fehlen, hat sich noch keine Behörde, kein privates Unternehmen bei der Erprobung neuer Verarbeitungswege von selbst Beschränkungen auferlegt. Mit erheblicher Zeitverschiebung nachträglich Korrekturen einzuführen, ist nicht nur kostspielig, sondern vor allem unweigerlich mit Konzessionen verbunden, die sich in der Regel zu Lasten des Datenschutzes auswirken.

8.
Ich möchte mit einigen Dankesworten schließen. Zuerst an die Adresse des Landtags. Kein anderes Parlament hat sich so nachdrücklich für den Datenschutz eingesetzt und den Datenschutzbeauftragten derart konsequent unterstützt: Ohne die Initiative des Hessischen Landtags wäre es nicht zur Anbindung des Datenschutzbeauftragten an das Parlament gekommen; ohne seine Intervention hätten anderswo noch immer bestehende Einschränkungen der Verarbeitungskontrolle nicht überwunden werden können; ohne seine Bemühungen wäre es nicht möglich gewesen, den Forderungen des Bundesverfassungsgerichts fristgerecht Rechnung zu tragen. Ausdrücklich danken möchte ich aber auch meinen Mitarbeiterinnen und Mitarbeitern für ihr waches Interesse, ihre fordernden Fragen, ihre ständige Bereitschaft, Zeit und Mühe zu opfern. Ohne ihre tatkräftige und kompetente Mitwirkung in all den Jahren hätte ich meine Aufgaben nicht erfüllen können.

17.5
Rede von Professor Dr. Hassemer vor dem Hessischen Landtag am 22. Oktober 1991 anläßlich seiner Wahl zum Hessischen Datenschutzbeauftragten

Ich freue mich auf dieses Amt. Die Zeiten sind für den Datenschutz stürmisch, aber nicht unbedingt schlecht, der Ort ist für den Datenschutz unbedingt gut.

Zum Ort: Datenschutz in Hessen ist fast ein Markenzeichen, ist für den Kenner, zu dem ich mich langsam heranbilde, ein Mekka:

In Hessen ist der Datenschutz gewissermaßen geboren worden, und meine Vorgänger Birkelbach und Simitis waren die kundigsten und kräftigsten, nicht aber die einzigen Geburtshelfer; der Datenschutz war und ist bis heute eine Institution, die nicht zwischen den Parteien zerrieben, sondern von ihnen gemeinsam gepflegt wird – auch wenn die Dünger bisweilen zwischen Chemie und Herzblut wechseln mögen. Diese Gemeinsamkeit hat dazu geführt, daß wir in Hessen ein Datenschutzgesetz haben, das man – wie immer im Leben natürlich nicht ohne jede Einschränkung – als musterhaft bezeichnen darf, musterhaft nicht nur im theoretischen Verständnis inhaltlicher Güte, sondern auch in der praktischen Anschauung eines Vorbilds für Gesetze außerhalb unseres Landes. Spiros Simitis hat dieses Gesetz nicht nur – im doppelten Sinn des Wortes – "gebildet"; er hat auf seiner Klaviatur auch mit einer Souveränität und zugleich Solidität gespielt, die den Nachfolger einerseits zum Nachmachen verführen muß, die ihm andererseits aber auch angst und bange machen könnte. Gleichviel: Daß der Datenschutz in Hessen insgesamt gut aufgehoben ist, dürfte in diesem Hause außer Streit sein.

Was die Zeiten angeht, so gibt es diesen Streit, und es gibt Turbulenzen. Der mächtige Schub, den der Datenschutz in der Form des Rechts auf "informationelle Selbstbestimmung" durch das Bundesverfassungsgericht erfahren hat, ist nach acht Jahren immer noch spürbar – zum Glück: Seine Kraft nämlich hat bislang noch nicht gereicht, alle die Bereiche in Bewegung zu bringen, auf denen der Datenschutz seine Rolle zu spielen hätte; es bleibt noch viel zu tun.

Das Recht auf informationelle Selbstbestimmung ist – und darin liegt der Schub, den ich meine – zu einem Menschenrecht geworden, dessen Struktur und Verständnis "modern" ist: der Zeit angemessen, in der wir leben. Es geht nicht mehr nur um persönliche Geheimnisse (die gehörten schon immer zum Kernbereich der Person), und es geht schon gar nicht um Informationen, die man vor anderen verbergen muß (darauf läßt sich ein Grundrecht schlecht begründen). Es geht vielmehr um nichts weniger als um die Sicherung der Menschenwürde in der Informationsgesellschaft.

Das heißt: Die ehrwürdigen Grundsätze der Würde und Freiheit der Person haben sich im Recht auf informationelle Selbstbestimmung neu konstituiert, sie haben die Gestalt angenommen, die den Gefährdungen der Persönlichkeitsrechte in der modernen Gesellschaft angemessen ist, sie sind um unsere heutigen Gefährdungserfahrungen bereichert und an ihnen konkretisiert worden. In dieser Gesellschaft braucht der Mensch nicht nur Brot und Freiheit, sondern auch einen stabilen Schutz gegen fremde, ihm weit überlegene Neugier. Die schnell wachsenden Informationstechnologien sind nämlich für uns nur insoweit ein Heil, wie es uns gelingt, das technische Können an die Kette des rechtlichen Dürfens zu legen: Informationen über Personen ist heute nicht nur Informiertheit, sie ist Herrschaft, und Herrschaft muß im Rechtsstaat gebunden und notfalls gebrochen werden. Das ist meine Sicht auf den Datenschutz.

Daraus ergibt sich eine kleine Reihe von Folgerungen.

In dem kalten, gleichsam technischen Wort von der "informationellen Selbstbestimmung" kommt ganz gut zum Ausdruck, daß es hier um etwas geht, mit dem wir nicht aufgewachsen sind. Rechtsgüter wie Gesundheit, Ehre oder auch sexuelle Selbstbestimmung sind uns vertraut, und von ihrem Wert für unser Leben brauchen wir nicht erst überzeugt zu werden. Die informationelle Selbstbestimmung hat es dagegen schwer, sich als unverzichtbares Recht im menschlichen Alltag einzuprägen; dazu sind die informationellen Gefährdungen – anders als beispielsweise die gesundheitlichen – zu dunkel, zu technisch, zu neu.

Datenschutz fordert deshalb heute zuerst einmal, daß das Recht auf informationelle Selbstbestimmung als Grundrecht allgemein verständlich gemacht wird: Nur wenn und nur insoweit den Bürgerinnen und Bürgern einleuchtet, daß es beim Datenschutz um ihre eigenen Interessen und um ihren eigenen Alltag geht, wird die Institution Datenschutz politisch wachsen und überleben. Das verständlich zu machen, ist keine leichte Aufgabe.

Sie ist um so schwerer, als der Datenschutz derzeit immer tiefer in eine Schlinge gerät, die ihn auf die Dauer strangulieren kann: Er reimt sich für eine schlichte Denkungsart auf "Tatenschutz" und wird so von den Strudeln um die "innere Sicherheit" erfaßt. Der in der Öffentlichkeit verbreitete Eindruck, Datenschutz sei eine Mischung aus Hinderung erfolgreicher Polizeiarbeit einerseits und fremdwörtlich-elitärer "informationeller Selbstbestimmung" andererseits, ist politisch explosiv.

Datenschutz fordert deshalb heute, daß das Recht auf informationelle Selbstbestimmung von dem Ruch freigehalten wird, auf "Kriminelle" oder "Spinner" konzentriert zu sein – jedenfalls auf einen anderen Typ von Menschen als man selber einer ist. Das setzt voraus, daß man die Ängste der Leute ernst nimmt und sich offensiv mit ihnen auseinandersetzt. Und dies wiederum erfordert Überzeugungsarbeit und gemeinsames Bemühen um die konkrete und praktische Sicherung der Bürgerrechte in der Risikogesellschaft:

Überzeugungsarbeit für die Einsicht, wonach jede und jeder einzelne für sich selbst vital daran interessiert sein muß, daß die rechtsstaatlichen Bindungen der Exekutive politisch überleben und daß das Recht auf informationelle Selbstbestimmung heute zu diesen Bindungen gehört. Und ein gemeinsames Bemühen aller darum, daß man die

unfruchtbare, verschleiernde und diffamierende Alternative von "Datenschutz" und "Tatenschutz" überwindet zugunsten von Lösungen, welche auf das jeweilige Problemfeld achten, die konkreten Informationsbedürfnisse zur Kenntnis nehmen und die Konturen des Rechts auf informationelle Selbstbestimmung in der alltäglichen Praxis fundieren. Wir dürfen einander den Datenschutz nicht um die Ohren schlagen; wir müssen vielmehr streitend herausarbeiten, was er hier und heute zu bedeuten hat.

Noch ein Drittes folgt aus den Besonderheiten des Rechts auf informationlle Selbstbestimmung. Das Hessische Datenschutzgesetz ist aus guten verfassungsrechtlichen Gründen auf die "öffentlichen Stellen" konzentriert. Das Recht auf informationelle Selbstbestimmung und seine Gefährdungen nehmen an dieser Konzentration aber nicht teil, im Gegenteil: Die moderne Informationsgesellschaft verwirklicht sich im gesellschaftlichen und im privaten Bereich noch geschwinder als im staatlichen, die Schwerfälligkeit der "öffentlichen Hand" ist unter dem Blickwinkel technologischer Beschleunigung der Informationsverarbeitung fast schon ein Schutz für die betroffenen Menschen, und man darf überdies annehmen, daß die normalen alltäglichen Gefährdungen informationeller Selbstbestimmung eher auf den leisen Sohlen des Privaten daherkommen als in den schweren Schuhen des Öffentlichen.

Datenschutz fordert deshalb heute die Revision seiner Anwendungsgebiete. Wir müssen überlegen, wie die Erfolge, welche vor allem die Landesgesetzgebung für den Datenschutz im Bereich der öffentlichen Verwaltung zweifellos gebracht hat, schrittweise in den Bereich des Gesellschaftlichen und Privaten übersetzt werden können. Die Erfahrungen reichen, so denke ich, aus, damit wir über neue Strukturen verantwortlich nachdenken dürfen.

Damit bin ich am Schluß. Ich hoffe, daß hinter den grundsätzlichen Überlegungen die Linie einer künftigen Praxis sichtbar geworden ist und daß diese Linie sich auch in der Praxis werden umsetzen lassen wird.

Nach meinem derzeitigen Verständnis ist eine der wichtigsten Vorschriften unseres Datenschutzgesetzes die Gewähr für alle, sich jederzeit an den Hessischen Datenschutzbeauftragten wenden zu können. Dies wird meine erste Praxis sein, und ich wünsche mir, daß sich die Grundsätze an und aus dieser Praxis bereichern.