**Abgeordnetenhaus von Berlin** **Drucksache 13 / 2918**

**13. Wahlperiode**

# Vorlage – zur Kenntnisnahme –

über **Stellungnahme des Senats**
**zum Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1997**

Der Senat legt nachstehende Vorlage dem Abgeordnetenhaus zur Besprechung vor:

Gemäß § 29 des Berliner Datenschutzgesetzes erstattet der Datenschutzbeauftragte dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit. Der Regierende Bürgermeister führt eine Stellungnahme des Senats zu dem Bericht herbei und legt diese innerhalb von drei Monaten dem Abgeordnetenhaus vor.

Die Veröffentlichungen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin.
Telefon: 6 61 84 84; Telefax: 6 61 78 28.

# Stellungnahme des Senats zum Bericht des Berliner Datenschutzbeauftragten für 1997

**(gemäß § 29 Abs. 2 Berliner Datenschutzgesetz)**

Inhaltsverzeichnis

**Einleitung**

1. **Rechtliche Rahmenbedingungen**
1.1 Deutschland und Europa
1.2 Datenschutz in Berlin

2. **Technische Rahmenbedingungen**
2.1 Tendenzen und Entwicklungen der Informationstechnik
2.2 Datenschutz durch Technik
2.3 Datenverarbeitung in Berlin

3. **Schwerpunkte im Berichtsjahr**
3.1 Der Bürger im Netz der Sozialdatenverarbeitung
3.2 „Spannungsbericht“
3.3 Datenschutz bei Telediensten
3.4 Bankautomation

4. **Aus den einzelnen Arbeitsgebieten**
4.1 Sicherheit
4.1.1 Polizei
4.1.2 Verfassungsschutz
4.2 Ordnung
4.2.1 Meldewesen und Wahlen
4.2.2 Ausländer
4.2.3 Straßenverkehr
4.2.4 Wirtschaftsverwaltung
4.2.5 Veterinäraufsicht
4.3 Justiz und Finanzen
4.3.1 Justiz
4.3.2 Finanzen
4.4 Sozialordnung
4.4.1 Arbeitnehmer und öffentliche Bedienstete
4.4.2 Gesundheit
4.4.3 Sozialverwaltung
4.4.4 Wohnen
4.5 Wissen und Bildung
4.5.1 Wissenschaft und Forschung
4.5.2 Schule
4.5.3 Statistik
4.6 Wirtschaft
4.6.1 Banken und Versicherungen
4.6.2 Verkehrsunternehmen
4.6.3 Werbung contra Markt- und Meinungsforschung
4.6.4 Datenverarbeitung für fremde Zwecke
4.7 Telekommunikation und Medien
4.7.1 Entwicklung des Telekommunikationsrechts
4.7.2 Einzelne Dienstleistungen
4.7.3 Telekommunikation in der Berliner Verwaltung
4.7.4 Datenschutz und Medien
4.8 Organisation und Technik
4.8.1 Datenverarbeitung im Auftrag oder Funktionsübertragung
4.8.2 Defekte Speichermedien

5. **Organisation des Datenschutzes**
5.1 Sicherstellung des Datenschutzes
5.1.1 Betriebliche und behördliche Datenschutzbeauftragte
5.1.2 Dienstanweisung für das bezirkliche Bürgerbüro
5.1.3 Geschäftsordnung
5.1.4 Dateienregister
5.2 Der Berliner Datenschutzbeauftragte
5.2.1 Die Dienststelle
5.2.2 Zusammenarbeit mit dem Abgeordnetenhaus
5.2.3 Kooperation mit anderen Datenschutzbehörden
5.2.4 Öffentlichkeitsarbeit

**Anlagen zum Jahresbericht 1997**

1. **Rede des Berliner Datenschutzbeauftragten vor dem Abgeordnetenhaus am 11. September 1997**

2. **Arbeitsergebnisse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder**
2.1 Entschließungen der 53. Konferenz am 17./18. April 1997
2.1.1 Entschließung zu den Beratungen zum Strafverfahrensänderungsgesetz 1996
2.1.2 Entschließung zu genetischen Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke
2.1.3 Entschließung zur geplanten Verpflichtung von Teledienstean-bietern, Kundendaten an Sicherheitsbehörden zu übermitteln
2.1.4 Entschließung zur Achtung der Menschenrechte in der Europäischen Union
2.1.5 Entschließung zur Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen
2.2 Entschließung der Konferenz vom 20. Oktober 1997 zu den Vorschlägen der Arbeitsgruppe der Arbeits- und Sozialministerkonferenz „Verbesserter Datenaustausch bei Sozialleistungen“
2.3 Entschließungen der 54. Konferenz am 23./24. Oktober 1997
2.3.1 Entschließung zur Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts
2.3.2 Entschließung zur informationellen Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren
2.3.3 Entschließung zur Erforderlichkeit datenschutzfreundlicher Technologien
2.3.4 Thesenpapier zum Allgemeinen Informationszugangsrecht und zum Recht auf informationelle Selbstbestimmung

3. **Arbeitsergebnisse der Europäischen Konferenz der Datenschutzbeauftragten**
3.1 Stellungnahme der Europäischen Konferenz vom 28. Februar 1997 zum Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in audiovisuellen Diensten und Informationsdiensten, zur Mitteilung an das Europäische Parlament u. a. über rechtswidrige und schädliche Inhalte im Internet sowie zur Ratsentschließung vom 28. November 1996 über rechtswidrige und schädliche Inhalte im Internet
3.2 Entschließung der Europäischen Konferenz am 19. September 1997 zum Entwurf der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (früher: ISDN-Richtlinie)

4. **Empfehlungen und Dokumente der Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten nach Art. 29 der EG-Datenschutzrichtlinie**
4.1 Empfehlung 1/97 vom 25. Februar 1997 zu Datenschutzrecht und Medien
4.2 Erste Leitlinien für die Übermittlung personenbezogener Daten in Drittländer vom 26. Juni 1997

5. **Gemeinsame Erklärung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation vom 12. September 1997 zur Kryptographie**

6. **Auszug aus dem Geschäftsverteilungsplan des Berliner Datenschutzbeauftragten**

**Abkürzungsverzeichnis**

**Stichwortverzeichnis**

**Einleitung**

Die Situation des Datenschutzes im Jahr 1997 ist durch ganz widersprüchliche Tendenzen gekennzeichnet.

Auf der einen Seite steht die weitere stürmische Ausbreitung der Informationstechnik im Wirtschaftsleben und in der Verwaltung, wo die Rationalisierungpotentiale dieser Technologie zunehmend erkannt und genutzt, wenn auch lange noch nicht ausgeschöpft werden: Ein neues Beispiel ist die Entwicklung von Spracherkennungssoftware, die gerade im vergangenen Jahr erhebliche Fortschritte gemacht hat und die in nicht allzu ferner Zukunft einen weiteren flächendeckenden Schub beim Verlust von Arbeitsplätzen verursachen wird. So wird im Bürobereich die Nachfrage nach Schreibdiensten, künftig wohl auch die nach anderen sprachverarbeitenden Diensten (z. B. Übersetzung, Auskunftserteilung, Beratung) drastisch zurückgehen.

Auch im persönlichen Umfeld ist die Informationstechnik dabei, sich über die gewohnten Geräte wie Fernsehen, Telefon und PC (den man inzwischen schon zum üblichen Haushaltsinventar rechnen muß) hinaus auszubreiten. Das Hereindringen von Fernwirkdiensten zeichnet sich ab. So ist gerade in diesen Tagen eine neue Generation von Haushaltsgeräten mit Computerschnittstellen auf den Markt gekommen, mit deren Hilfe die Heizung, der Küchenherd oder der Videorecorder aus der Ferne (z. B. vom Schreibtisch aus) bedient werden können; auf die hierfür erforderlichen Standards hat man sich in den letzten Monaten geeinigt[1]. Die bisher geläufigen Computerspiele werden in ihrer Eindringlichkeit erheblich übertroffen durch die Tamagochis und ähnliche Apparätchen, die im vergangenen Jahr die Kinderzimmer erobert haben und mitunter auch Erwachsene in Dauerstreß halten.

All das geschieht vor dem Hintergrund einer sich ebenfalls explosionsartig ausdehnenden Vernetzung der verschiedensten Techniken weltweit im Internet, aber auch in abgeschlossenen Netzen der verschiedensten Art, für die sich der Begriff „Intranet“ herausgebildet hat.

Die Folgen dieser Entwicklung reichen weit über diejenigen Aspekte hinaus, die von den klassischen Prinzipien des Datenschutzes abgedeckt werden. Daß dieser weiterentwickelt werden muß zu einem Regelungsinstrumentarium, das die Gesellschaft und das einzelne Individuum umfassender als bisher vor den unerwünschten Folgen der Datenverarbeitung bewahrt[2], ist inzwischen weitgehend anerkannt.

Kein Dokument zur Informationsgesellschaft kommt mehr ohne den Hinweis aus, daß der Datenschutz eine zentrale Rolle bei deren Weiterentwicklung spielt. Das belegt eindrucksvoll die Erklärung der Europäischen Ministerkonferenz, die im Juli vergangenen Jahres in Bonn tagte. Sie widmete dem Datenschutz ein ganzes Kapitel, in dem es heißt:

Die Minister betonen mit Nachdruck, daß personenbezogene Daten der Nutzer globaler Informationsnetze nur dann gesammelt und verarbeitet werden sollten, wenn der Benutzer in Kenntnis der Sachlage seine ausdrückliche Genehmigung hierzu gegeben hat oder wenn die Sammlung und Verarbeitung gesetzlich zulässig ist, darüber hinaus sind entsprechende Sicherheitsvorkehrungen im rechtlichen und technischen Bereich zu treffen, um den Schutz der Privatsphäre zu wahren, auf den der Benutzer einen Anspruch hat.

Der amerikanische Präsident hatte kurz zuvor in einer vielbeachteten Rede erklärt:

„In dem Maße, wie das Internet sich auf jedes Unternehmen und jeden Haushalt erstreckt und wir vor der erschreckenden Aussicht stehen, daß private Informationen – sogar Patientenakten – sofort weltweit zur Verfügung gestellt werden könnten,

1 Richtlinien der European Installation Bus Association (EIBA), einem herstellerübergreifenden Zusammenschluß für die Etablierung eines Standards für die Gebäudesystemtechnik auf dem europäischen Markt; die Haushaltsgeräte werden zusammen mit einem PC zu einem „Home Electronic System“ – HES – vernetzt

2 Bereits Steinmüller u. a. definieren in dem Gutachten „Grundfragen des Datenschutzes“ aus dem Jahr 1971, das die wissenschaftliche Basis des deutschen Datenschutzrechtes schuf, den Datenschutz umfassend als Kehrseite der Datenverarbeitung: „Wo Datenverarbeitung, da Datenschutz. Wie der Schatten notwendig dem Licht folgt, und ohne Licht kein Schatten bestehen kann, so begleitet Datenschutz die Datenverarbeitung“ – BT-Drs. VI/3826, S. 34

müssen wir neue Schutzvorkehrungen für die Privatsphäre angesichts der neuen technischen Realität entwickeln."

In erstaunlichem Gegensatz zu dieser weltweiten Entwicklung steht eine umgekehrte Tendenz: In den letzten Monaten wurde der Datenschutz in Deutschland von manchen Stimmen geradezu als gesellschaftliches Übel angeprangert. Von den Sicherheitsbehörden war der Datenschutz schon immer als Hemmschuh der eigenen Aktivitäten betrachtet worden. Ihnen fehlt häufig die Einsicht, daß eine hinreichende Sicherung des Datenschutzes die Voraussetzung dafür ist, daß auch neue, technikgestützte Methoden auf allgemein anerkannte und rechtsstaatliche Weise eingesetzt werden können. Datenschutz als Akzeptanzkriterium, in der Wirtschaft ein zunehmend anerkanntes Unternehmensziel, ist eine Maxime, mit der man sich schwertut. Dabei müßte diese vor dem Hintergrund der drängenden Forderungen der Sicherheitsbehörden nach neuen informationstechnischen Befugnissen, etwa zum Großen Lauschangriff[3] oder zum Zugriff auf Telekommunikationsnetze und -dienste[4], ein besonderes Anliegen sein.

Neu war im vergangenen Jahr die Art und Weise, in der gerade in der Bundeshauptstadt Berlin das „Spannungsverhältnis zwischen Datenschutz und schutzwürdigen Belangen der Allgemeinheit" erörtert wurde[5]. Selbst der Innensenator scheute sich nicht, in einer offiziellen Pressemitteilung seines Hauses titeln zu lassen: „Datenschutz darf nicht zum Täterschutz verkommen"; die Befolgung datenschutzrechtlicher Vorschriften „gefährde den sozialen Frieden" oder sie „lege das Feuer an eine Lunte, von der niemand wissen kann, wie lang sie ist"[6]. In Berlin, dem traditionell den Freiheitsrechten verbundenen Gemeinwesen, schmerzt das besonders.

Daß sich die Aversionen in besonderer Weise gegen den Datenschutzbeauftragten richten, dessen Aufgabe der Nachweis von Mängeln bei der Informationsverarbeitung ist – auch und gerade bei den Sicherheitsbehörden –, verwundert nicht. Der von einem Berliner Hochschullehrer in den Anfangstagen des Datenschutzes formulierte Vergleich mit einem Fußballspiel ist aktueller denn je: Der Datenschutz befinde sich „in einer Rolle des Schiedsrichters, der Regelverstöße aufzeigen und ahnden und dafür gelegentlich auch einmal die gelbe oder die rote Karte zeigen soll. Diese Rolle ist bei niemandem sonderlich beliebt. Die Akteure schätzen sie nicht, weil sie sich durch den Schiedsrichter die rechtlichen Grenzen ihres Tuns aufzeigen lassen müssen und auch das Publikum registriert selten mehr als nur die vermeintlichen oder wahren Fehlleistungen des Schiedsrichters und pflegt ihn dann allenthalben zum Prügelknaben für das empfundene Ungemach zu machen[7]."

Auch andere Verwaltungen versuchen, selbst die bisher anerkannten Restriktionen abzuschütteln. Der vorgebliche massenhafte Mißbrauch von Sozialleistungen wird zur Rechtfertigung von Datenabgleichen herangezogen, die noch vor wenigen Jahren für ausgeschlossen gehalten wurden[8]. Mit Rationalisierung und Verwaltungsreform wird begründet, daß selbst die Verarbeitung medizinischer Daten ohne Rücksicht auf datenschutzrechtliche Überlegungen in die Hände von Privatunternehmen gegeben („outgesourced") wird[9]. Trotz aller Warnungen der Datenschutzbeauftragten werden die Rechner der öffentlichen Verwaltung an das Internet angeschlossen und damit die auf diesen Rechnern verarbeiteten personenbezogenen Daten der Gefahr des weltweiten unbefugten Zugriffs ausgesetzt[10].

In der Privatwirtschaft, die auf Grund der bestehenden Beschränkungen des Datenschutzrechts in diesem Bereich ohnehin nur schwer kontrollierbar ist, sind ähnliche Tendenzen erkennbar. Mit bescheidenen Prämien werden die Bürger dazu gebracht, ihr gesamtes Privatleben zu offenbaren und den Rechnersystemen des Adreßhandels zur Verfügung zu stellen[11]. Ein Unternehmen vertreibt eine CD-Rom mit Daten aller deutschen Telefonkunden unbeeindruckt von Entscheidungen der Aufsichtsbehörde und der angerufenen Gerichte, nach denen diese

3 vgl. unten 1.1
4 vgl. unten 4.7
5 vgl. unten 3.2
6 Pressemitteilung der Senatsverwaltung für Inneres vom 5. Februar 1997
7 Eggert Schwan in: Datenschutz und Datensicherung, 2/1980, S. 64
8 vgl. unten 3.1
9 vgl. unten 4.3.1
10 vgl. unten 2.3
11 vgl. unten 4.6.3

Die warnenden Ausführungen des Berliner Datenschutzbeauftragten sollten nach Meinung des Senats nicht als Aufforderung mißverstanden werden, auf diese auch für die Verwaltung wichtigen Kommunikationsmöglichkeiten zu verzichten. Das wäre ohnehin nicht durchsetzbar, weil auch ohne direkte Verbindung zum Internet über bereits bestehende Netzanbindungen (X.25, X.400, Online-Dienste) und deren Gateways die Kommunikation zum Internet möglich ist. Stattdessen sollte dieser Hinweis als Aufforderung verstanden werden, die Fragen der Netzsicherheit mit besonderer Sorgfalt und Verantwortlichkeit zu betrachten.

Die Nutzung des Internet birgt in der Tat große Nutzenpotentiale für eine schnellere und effektivere Aufgabenerfüllung der Verwaltung. Den bestehenden erheblichen Risiken der Internet-Nutzung muß mit entsprechenden Sicherheitskonzepten begegnet werden. Verbleibt trotz der Sicherheitsmaßnahmen ein unakzeptables Restrisiko, muß auf die Nutzung verzichtet werden.

Die Senatsverwaltung für Inneres hat sowohl in dem als Entwurf vorliegenden „IT-Sicherheitsrahmenkonzept" als auch in detaillierten Rundschreiben zur „Nutzung des Internet" die technisch-organisatorischen Mindestanforderungen an eine Nutzung des Internets für Verwaltungsaufgaben festgelegt. Diese Anforde-

nicht nur wettbewerbswidrig sondern auch datenschutzrechtlich unzulässig ist: Es setzt seine Aktivitäten nunmehr von Österreich aus fort, wo der Datenschutz im Privatbereich noch schwächer ausgestaltet ist als in Deutschland[12].

Diese der weltweiten Anerkennung des Datenschutzes gegenläufige Tendenz wird gefördert durch die Arbeitsweise des Internet, das zunehmend in allen Lebensbereichen genutzt wird, obwohl einzelne Funktionen selbst den von den Vereinten Nationen anerkannten Grundprinzipien des Datenschutzes[13] Hohn sprechen: Die *Richtigkeit* der Daten kann wegen der Manipulierbarkeit im Netz nicht gewährleistet werden. Die *Zweckbestimmung weder* der Inhaltsdaten noch der bei der Nutzung entstehenden Daten kann gesichert werden, die Suchmaschinen im Netz ermöglichen jedem Nutzer die Erstellung von *Persönlichkeitsprofilen.* Ein *Auskunftsanspruch* über die im Netz vorhandenen Daten der Betroffenen ist völlig illusorisch, schon allein deswegen, weil es keine Verantwortlichen im Netz gibt, an die man sich wenden könnte[14].

Dieser zwiespältigen Befund über die Situation des Datenschutzes muß ergänzt werden um eine andere Entwicklungslinie des Regulierungsrahmens für die Informationsverarbeitung. Immer größeres Gewicht bekommt die Forderung nach freiem Zugang zu den Informationen, soweit nicht überwiegende private oder öffentliche Interessen entgegenstehen. International hat sich hierfür der Begriff der *Informationsfreiheit* eingebürgert. Während andere Staaten nach dem Vorbild des schwedischen Pressegesetzes von 1766 bereits den Zugang zu den staatlichen Informationssammlungen geöffnet haben[15] tut sich Deutschland hiermit besonders schwer, wenn auch hier ein Umdenken unausweichlich ist. Als erstes Bundesland hat das Land Brandenburg den freien Zugang zu den Informationen der Verwaltung in die Verfassung aufgenommen (Art. 11 Abs. 1 Brandenburgische Verfassung), ein entsprechender Gesetzesentwurf ist zu Beginn des neuen Jahres verabschiedet worden. In Berlin liegt dem Abgeordnetenhaus ein Gesetzesentwurf vor[16], dem Bund und die anderen Länder werden folgen müssen. Im Amsterdamer Vertrag hat sich die Europäische Union für die eigenen Institutionen auf das Prinzip der Informationsfreiheit festgelegt (Art. 191 a). Der Ausgleich zwischen dem Grundrecht auf informationelle Selbstbestimmung einerseits und der ebenfalls grundrechtlich verankerten Informationsfreiheit andererseits ist dabei das zentrale Problem der Gesetzgebung[17].

Zusammen betrachtet ergibt sich ein diffuses Bild der Lage des Datenschutzes, das sich in einer Stadt wie Berlin in besonderem Maße zeigt: Weltweite Anerkennung eines Menschenrechts steht gegen den Widerstand bei vielen Detailproblemen; große Lösungen stehen neben vielem Kleinkarierten; das Bedürfnis nach politischer Akzentuierung behindert die nüchterne Diskussion der angemessenen rechtlichen und technischen Umsetzung des Grundrechts auf informationelle Selbstbestimmung. Der vorliegende Tätigkeitsbericht für das Jahr 1997 schildert die Situation deutlicher als in den vergangenen Jahren. Die Kontroversen, die er aufzeigt, sollten einen Anstoß dafür geben, daß die Bundeshauptstadt Berlin gerade auf dem zukunftsweisenden Gebiet der Beherrschung der Informationstechnik einen Führungsanspruch anstrebt.

## 1. Rechtliche Rahmenbedingungen

### 1.1 Deutschland und Europa

Man hätte erwarten können, daß die Umsetzung der europäischen *Richtlinie zum Datenschutz*[18] das zentrale Thema der Datenschutzdiskussion im vergangenen Jahr war. Tatsächlich

rungen stimmen weitestgehend mit entsprechenden Empfehlungen des Berliner Datenschutzbeauftragten überein. Ein umgesetztes Sicherheitskonzept ist Voraussetzung für die Nutzung des Internet durch die Behörden der Berliner Verwaltung. Der Landesbetrieb für Informationstechnik LIT bietet eine entsprechende Dienstleistung zum sicheren Übergang ins Internet an.

12 vgl. unten 4.7.2

13 Richtlinien betreffend personenbezogene Daten in automatisierten Dateien (von der Generalversammlung der Vereinten Nationen am 14. Dezember 1990 beschlossen)

14 vgl. unten 3.3 sowie 4.7

15 z. B. USA: Freedom of Information Act von 1967, Frankreich: Loin 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal

16 vgl. unten 1.2

17 Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu den Bericht einer eigens eingerichteten Arbeitsgruppe unter dem Vorsitz des brandenburgischen Landesbeauftragten entgegengenommen, vgl. Anlage 2.3.4

18 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, AblEG Nr. L 281/31, v. 24. November 1995

wurden zwar mehrere interne Entwürfe des Bundesinnenministeriums zur Neufassung des *Bundesdatenschutzgesetzes* (BDSG) bekannt[19], zu denen die Datenschutzbeauftragten auch Stellung genommen haben[20]; angesichts der Vorgabe des Ministeriums, diese Novellierung auf das Mindestmaß des Erforderlichen zu beschränken[21], entwickelte sich jedoch kaum eine Diskussion über eine grundsätzliche Neugestaltung des deutschen Datenschutzrechts. Vielmehr verlor sie sich in den eher nebensächlichen Details einer formalen Mindestanpassung. Mitgespielt mag hier haben, daß offensichtlich alle Beteiligten davon überzeugt waren, daß eine grundsätzliche Neuorientierung, die auch die in der Einleitung angesprochenen Aspekte berücksichtigt, in der laufenden Legislaturperiode nicht mehr möglich ist.

Gleichwohl ist die Bundesregierung bemüht, die Vorgaben der Richtlinie einzuhalten, die eine Umsetzung in das nationale Recht binnen drei Jahren, das heißt bis zum 24. Oktober 1998, vorsieht. Auf alle Fälle sollten dabei die wesentlichen Innovationen der Richtlinie im Sinne einer Verbesserung des Datenschutzes umgesetzt werden: die weitestgehende Gleichbehandlung von öffentlichem und privatem Sektor, die Erstreckung des Gesetzes auf die Phase der Datenerhebung auch im privaten Bereich, der besondere Schutz sensibler Daten, die völlige Unabhängigkeit der Datenschutzkontrolle auch im privaten Bereich, effektive Eingriffsmöglichkeiten für alle Kontrollinstanzen[22]. Darüber hinaus sollte auch im privaten Bereich die Beschränkung des Gesetzes bei der Verarbeitung von Daten in Akten, auf Videobändern und anderen nicht besonders strukturierten Datensammlungen aufgehoben werden. Hierauf kann es angesichts der Möglichkeiten moderner Informationstechnik (wenn man etwa an die Video- oder Scanner-Technik denkt) nicht mehr ankommen. Auch der in der EU-Richtlinie angelegte, aber europapolitisch eher nach rückwärts gewandte Ausschluß der „zweiten und dritten Säule“, also des Bereichs der Außen- und Sicherheitspolitik sowie der Justiz, aus dem bindenden Umsetzungssektor darf auf keinen Fall dazu führen, daß Errungenschaften der Richtlinie nicht auf diese Bereiche erstreckt werden: Die Beschränkung automatisierter Entscheidungen gegen den Betroffenen kann beispielsweise gerade im Sicherheitsbereich besondere Bedeutung entfalten.

Die Frage, ob der *„Große Lauschangriff“*, also die akustische Überwachung der Wohnräume zur Strafverfolgung mit technischen Hilfsmitteln, zugelassen werden soll, beherrschte die Diskussion über die Grenzen staatlicher Befugnisse in den besonders geschützten Bereichen der Privatsphäre. Das Grundrecht auf die Unverletzlichkeit der Wohnung, das bisher (außer für die Durchsuchung) für Zwecke der Strafverfolgung nicht begrenzt ist (Art. 13 Abs. 3 Grundgesetz – GG), soll nach einer Übereinkunft der Regierungsparteien mit der SPD nunmehr auch hierfür beschränkt werden. Die ursprünglichen Entwürfe für die Grundgesetzänderung sowie die Anpassung der Strafprozeßordnung (StPO)[23] waren Kritik von allen Seiten ausgesetzt. Die Kritik richtete sich insbesondere dagegen, daß auch die Personen, denen ein Zeugnisverweigerungsrecht im Strafverfahren zukommt (§§ 52, 53 StPO), abgehört werden konnten und damit die Rechte der Betroffenen hätten umgangen werden können. Auf Grund der heftigen Proteste wurden Nachbesserungen vereinbart, die jedoch die beteiligten Verbände immer noch nicht zufriedenstellten. Der Ausgang des Gesetzgebungsverfahrens war bei Redaktionsschluß noch offen.

Unsere Auffassung zur Einführung des Großen Lauschangriffs war von Anfang an unverändert. Mit seiner Einführung wird auch der letzte *unantastbare Bereich privater Lebensgestaltung* zum heimlichen Abhören freigegeben. Mehrfach haben wir auch in der Öffentlichkeit vor der Einführung dieser Maßnahme gewarnt. Wenn die Bürger sich nicht mehr sicher sind, ob sie in ihren Wohnungen unbelauscht leben können, wird dies zu einer Verunsicherung führen: Es ist ein Irrglaube anzunehmen, daß sich der Große Lauschangriff auf „Gangsterwohnungen“ begrenzen lassen wird. Im Ermittlungsverfahren handelt es sich ausschließlich

Der Senat hat anläßlich der vorangegangenen Berichte des Berliner Datenschutzbeauftragten wiederholt seine Position zur Einführung des „Großen Lauschangriffs“ dargelegt. Die zwischenzeitlich verabschiedete gesetzliche Regelung beinhaltet einen Kompromiß zwischen den unterschiedlichen Interessen.

Insbesondere sind entgegen früheren Vorstellungen weitere nach § 53 Abs. 1 StPO im Zusammenhang mit ihrer beruflichen Tätigkeit zur Zeugnisverweigerung Berechtigte von der akustischen Wohnraumüberwachung grundsätzlich ausgenommen.

Der Senat begrüßt, daß nach den langwierigen Diskussionen auf politischer Ebene die gesetzlichen Bestimmungen, wenn auch in eingeschränktem Maß, nunmehr verabschiedet worden sind. In welchem Umfang der „Große Lauschangriff“ künftig zu einer verbesserten Strafverfolgung im Bereich der Schwerkriminalität beitragen wird, läßt sich derzeit nicht sicher beurteilen. Durch die verschiedenen gesetzlichen Kontroll- und Berichtspflichten ist aber sichergestellt, daß sich die Maßnahmen streng im Rahmen der Verhältnismäßigkeit bewegen.

19 Letzte Fassung vom 8. Dezember 1997
20 Anlage 2.3.1
21 vgl. JB 1996, 1.1
22 vgl. JB 1995, 1.2
23 BT-Drs. 13/8650 bzw. 8651

um Tatverdächtige, bei denen noch nicht feststeht, ob sie sich strafbar gemacht haben. Es ist darüber hinaus unvermeidlich, daß auch Unschuldige abgehört werden und natürlich alle Personen ihres Umfeldes – Familie, Freunde, Kollegen. Auch technisch ist der Große Lauschangriff fragwürdig. Die Schwerstkriminellen, die erfaßt werden sollen, werden sich mit Ortungs- und Störtechnik wehren – Maßnahmen, die auch anderen Personen jederzeit zur Verfügung stehen. Interessanterweise hat das Bundesamt für die Sicherheit in der Informationstechnik (BSI) selbst Tips veröffentlicht, wie man sich gegen Lauschangriffe zur Wehr setzen kann[24].

Wie problematisch der Einsatz der akustischen Überwachung im Einzelfall ist, zeigt die Überprüfung, die wir im vergangenen Jahr bei einer Maßnahme im Bereich der Gefahrenabwehr durchgeführt haben, wo der Große Lauschangriff unter bestimmten Voraussetzungen bereits jetzt zulässig ist[25].

Einige Bundesgesetze mit datenschutzrechtlichem Gehalt sind im vergangenen Jahr verabschiedet worden, darunter das Gesetz über das *Bundeskriminalamt*[26] und das *Justizmitteilungsgesetz*[27], mit denen seit vielen Jahren bestehende Gesetzgebungslücken geschlossen wurden. Mehrere Gesetze zur Umsetzung der *Europol-Konvention* sind in Kraft; lediglich das Gesetz zur Gewährung einer beschränkten Immunität für Europol-Bedienstete ist noch in Diskussion[28], so daß das zweite große europäische Informationssystem der Polizei neben dem Schengener Informationssystem in die Realisierung gehen kann. Das neue *Straßenverkehrsgesetz*[29] ermöglicht den von den Datenschutzbeauftragten kritisierten Aufbau eines zentralen Fahrerlaubnisregisters, enthält aber andererseits längst überfällige Regelungen zum Umgang mit Daten in der Führerscheinakte. Das neue *Arbeitsförderungsgesetz*[30], das nunmehr als Drittes Buch in das Sozialgesetzbuch eingegliedert ist, vermehrt die Zahl der Bestimmungen zum Schutz des Sozialgeheimnisses, das *Erste Gesetz zur Änderung des Dritten Buches Sozialgesetzbuch*[31] hingegen sieht neue Meldepflichten zwischen den verschiedenen Stellen vor.

Ein bedeutsames weiteres Kapitel der Telekommunikationsgesetzgebung wurde mit der Verabschiedung des *Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste* aufgeschlagen, das unter anderem den Datenschutz bei Telediensten *(Teledienstdatenschutzgesetz* – TDDSG) und die *digitale Signatur* regelt[32]. Parallel dazu schlossen die Länder einen *Mediendienstestaatsvertrag* mit hinsichtlich des Datenschutzes nahezu gleichlautendem Inhalt[33]. Neue Detailregelungen zur Netzebene finden sich im *Telekommunikationsbegleitgesetz*, das allerdings die wesentliche Neuregelung des Zugangs der Sicherheitsbehörden zu Verkehrsdaten bei der Telekommunikation vorläufig ausgeklammert hat[34]. Für die traditionelle Post gilt nunmehr die *Postdienstunternehmen-Datenschutzverordnung.*

Weitere Rechtsgebiete warteten auch im vergangenen Jahr vergeblich auf einen Abschluß oder gar überhaupt erst einen Beginn des Gesetzgebungsverfahrens: So fehlen nach wie vor angemessene Datenschutzregelungen in der *Strafprozeßordnung* (je ein Entwurf der Bundesregierung und des Bundesrat liegen derzeit im Bundestag), im *Strafvollzugsrecht* (es liegen bisher nur ein Referentenentwurf zum Strafvollzugsgesetz, Vorarbeiten zum Jugendstrafvollzug und ein Referentenentwurf zur Untersuchungshaft vor), im *Personenstands- und Staatsangehörigkeitsrecht* (im Stadium von Vorentwürfen), im *Steuerrecht* (der Bundesrat hat den Entwurf einer Steuerdaten-Abrufverordnung an die Bundesregierung zurückgegeben, die Erörterung datenschutzrechtlicher Regelungen in der Abgabenordnung wird vom Bundesfinanzministerium verweigert). Angesichts der Reichweite am bedeutsamsten, ist das Fehlen eines *Arbeitnehmerdatenschutzgesetzes*, das die vielfältigen Datenschutzbestimmungen in Arbeits-

Der Senat begrüßt ausdrücklich, daß einige überfällige, auch aus datenschutzrechtlicher Sicht unverzichtbare Gesetze, in jüngster Zeit durch die Bundesregierung eingebracht und relativ zügig verabschiedet wurden. Dies gilt insbesondere für das Gesetz über das Bundeskriminalamt und das Justizmitteilungsgesetz. Verschiedene Änderungsgesetze zur Strafprozeßordnung, die ebenfalls eine Vielzahl datenschutzrechtlicher Detailregelungen enthalten, befinden sich dagegen noch in den Beratungen im Bundestag. Die Justizminister der Länder haben wiederholt den Bundestag aufgefordert, diese Entwürfe vorrangig zu behandeln, um den teilweise nicht hinnehmbaren Zustand der Rechtsunsicherheit für die Strafverfolgungspraxis, aber auch für Betroffene, zu beenden. Zum Bedauern des Senats ist eine kurzfristige Umsetzung dieser Entwürfe nicht zu erwarten. Der Senat wird sich aber weiter nachdrücklich für eine Anpassung strafprozessualer Regelungen an den angesichts der Rechtsentwicklung gebotenen datenschutzrechtlichen Standard einsetzen.

Die Bundesregierung hat am 23. Januar 1998 einen Gesetzentwurf zur datenschutzrechtlichen Ergänzung des Strafvollzugsgesetzes (4. StVollzGÄndG) vorgelegt, zu dem der Bundesrat am 6. März 1998 Stellung genommen hat. Er ist jetzt dem Deutschen Bundestag zur Beratung zugeleitet worden. Es bleibt zu hoffen, daß das Gesetzgebungsverfahren noch in dieser Legislaturperiode abgeschlossen werden kann.

Der Bundesrat hatte das Bundesministerium für Finanzen wegen Bedenken der kommunalen Spitzenverbände gegen Regelungen der vorgesehenen Steuerdaten-Abrufverordnung gebeten, den hierfür vorgelegten Verordnungsentwurf nochmals mit diesen zu erörtern. Ein diesbezüglich überarbeiteter Text für eine Steuerdaten-Abrufverordnung ist jetzt von den kommunalen Spitzenverbänden gebilligt worden.

Um jedoch endlich dem Bereich des Bundes und der Länder, in dem der Schwerpunkt der automatisierten Abrufe von Steuerdaten liegt, eine zwischen diesen unter Beteiligung der Datenschutzseite abgestimmte Regelung für die Praxis zur Verfügung stellen zu können, ist geplant, diese zunächst als Verwaltungsregelung alsbald in Kraft zu setzen. Parallel dazu soll das Verfahren zum Erlaß einer Rechtsverordnung unter Einbeziehung der Gemeinden in die Regelungen über den automatisierten Abruf von Steuerdaten eingeleitet werden.

24 Faltblatt Ö 05 – 02/98, das auch im Internet abrufbar ist
25 vgl. unten 4.1.1
26 vgl. unten 4.1.1
27 vgl. unten 4.3.1
28 vgl. unten 4.1.1
29 vgl. unten 4.2.3
30 BGBl. 1997 I, S. 594
31 BGBl. 1997 I, S. 2970
32 vgl. unten 3.3
33 vgl unten 4.7.4
34 vgl. unten 4.7.1

verhältnissen, die häufig nur der Rechtsprechung zu entnehmen sind, bündelt. An Ankündigungen aus dem Bundesarbeitsministerium, daß in Kürze ein Entwurf vorgelegt würde, mangelt es seit dem Volkszählungsurteil (also seit 15 Jahren) nicht; der Vollzug steht jedoch noch immer aus. Auch die mehrfachen Aufforderungen des Bundestages zur Vorlage eines Gesetzentwurfs[35] fruchteten nichts.

Von der Bundesrechtsprechung gingen im vergangenen Jahr keine bedeutsamen neuen Impulse für die Fortentwicklung des Datenschutzes aus. Das *Bundesverfassungsgericht* befaßte sich mit der Verwertbarkeit von Daten über Ereignisse in der DDR im Zusammenhang mit Personalüberprüfungen[36], das *Bundesarbeitsgericht* mit dem Verhältnis zwischen Betriebsrat und betrieblichem Datenschutzbeauftragten[37].

In Europa schuf der *Amsterdamer Vertrag* auch für den Datenschutz Neuerungen: Er fügte in den EG-Vertrag einen neuen Artikel 213 b ein, nach dem die EU-Richtlinie ab 1. Januar 1999 auch auf die Organe und Einrichtungen Anwendung findet (bisher gab es für die europäischen Gremien noch keine Datenschutzbestimmungen) und nach dem der Rat eine unabhängige Kontrollinstanz für den Datenschutz einzurichten hat. Ferner wurde Artikel 191 a geschaffen, der allen Personen und Unternehmen, die in der EU einen Wohn- bzw. Unternehmenssitz haben, Zugang zu den europäischen Dokumenten gewährt – allerdings entsprechend den Sonderbestimmungen, die sich jedes Organ im Rahmen eines vom Rat noch zu erlassenden Rechtsakts geben kann.

Nach dem Inkrafttreten der europäischen Datenschutzrichtlinie konzentriert sich die Rechtsetzung der Europäischen Union auf dem Gebiet des Datenschutzes auf einzelne Spezialmaterien. So wurde im vergangenen Jahr nach vielen Diskussionen, bei denen auch wir mitgewirkt haben, die Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der *Telekommunikation* verabschiedet[38]. Die *Zusammenschaltungs-Richtlinie* schreibt die Sicherung des Telekommunikationsgeheimnisses durch alle beteiligten Unternehmen vor, die *Fernabsatz-Richtlinie* schränkt das Direktmarketing durch Telefax und Voice-Mail ein[39]. Weitere gesetzgeberische Aktivitäten zeichnen sich in vorbereitenden Dokumenten ab, etwa zum Jugendschutz im Internet, zur Kryptografie[40] und zur Registrierung von Schiffspassagieren[41].

### 1.2 Datenschutz in Berlin

Seit Jahren haben wir festgestellt, daß die *Sicherheitsüberprüfung* für Bedienstete der Berliner Verwaltung, aber auch für Berliner Unternehmen, die als sicherheitsgefährdet einzustufen sind, der letzte bedeutsame Bereich ist, bei dem angemessene Datenschutzregelungen im Landesrecht fehlen. Diese Lücke ist nunmehr geschlossen. Bis zum Jahresende wurde der bereits in der vergangenen Legislaturperiode vorgelegte Entwurf beraten; in den Erörterungen im Unterausschuß Datenschutz des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses konnten deutliche datenschutzrechtliche Verbesserungen erreicht werden[42]. Das Gesetz wird Anfang 1998 verabschiedet werden.

Die Diskussion um die Verhinderung des Mißbrauchs von Sozialleistungen hat neben vielen politischen Debatten auch Initiativen zur landesrechtlichen Regelung des Datenaustauschs der Sozialämter untereinander und mit anderen Behörden der Verwaltung hervorgebracht, zu denen wir gehört wurden und die zu befriedigenden gesetzgeberischen Lösungen geführt haben[43].

---

35 zuletzt BT-Drs 13/7699 v. 16. Mai 1997
36 vgl. unten 4.4.1
37 ebenda
38 vgl. unten 3.3
39 vgl. unten 4.7.1
40 vgl. unten 3.3
41 Vorschlag für eine Richtlinie des Rates über die Registrierung der an Bord von Fahrgastschiffen befindlichen Personen Kori (96) 574 endg., BR-Drs 994/96
42 vgl. unten 4.1.2
43 vgl. unten 3.1

| Bericht des Berliner Datenschutzbeauftragten | Stellungnahme des Senats |
|---|---|

Die Fraktion Bündnis 90/Die Grünen hat in das Abgeordnetenhaus einen Entwurf für ein *Gesetz zur Förderung der Informationsfreiheit* im Land Berlin (Berliner Informationsfreiheitsgesetz – IFG) eingebracht[44], der entsprechende Initiativen der rot-grünen Koalition von 1990 aufgreift; das damals eingebrachte Gesetz war am Ende der Legislaturperiode aus formalen Gründen nicht verabschiedet worden. Damit wird der von uns bereits im Ersten Bericht über die Aufnahme der Tätigkeit des Berliner Datenschutzbeauftragten[45] erhobenen Forderung Rechnung getragen, daß sich die öffentliche Verwaltung durch Gewährung eines generellen Akteneinsichtsrechtes die für ein demokratisches Gemeinwesen angemessene Transparenz verschaffen sollte. Der nun vorliegende Gesetzentwurf wird unter Berücksichtigung der Thesen zu diskutieren sein, die zu dem Thema „Allgemeines Informationszugangsrecht des Bürgers“ von Datenschutzbeauftragten des Bundes und der Länder erarbeitet worden sind[46].

Die Verwirklichung eines allgemeinen (also jedem unabhängig von einer individuellen Betroffenheit zustehenden) Informationszugangsrechts gewinnt gerade in der heutigen Informationsgesellschaft zunehmend an Bedeutung. Bei der Vielzahl der bei der Verwaltung vorhandenen Informationen kann die Möglichkeit, sich aus allgemein zugänglichen Quellen zu unterrichten, nicht mehr genügen. Je intensiver sich Verwaltung und Bürger der Informationstechnik bedienen und deren erschließbare Informationsressourcen nutzen, um so enger müssen der Zugang zu den Daten und der Schutz der informationellen Selbstbestimmung miteinander verflochten werden. Auch der Gesichtspunkt der *Demokratie* spielt eine Rolle: Der Grundsatz der Öffentlichkeit von Parlamentssitzungen und von Gerichtsverhandlungen gehört zum Grundbestand unserer Rechtsordnung, so daß zumindest gegenüber diesen Gewalten ein Mindestmaß an öffentlicher Kontrolle gewährleistet ist. Hiervon ist bislang lediglich der Bereich der vollziehenden Gewalt weitgehend ausgenommen geblieben. Transparenz der Verwaltung ist aber für die Wahrnehmung der Teilhabe am öffentlichen Leben in einem demokratischen Rechtsstaat unerläßlich.

Bereits mit dem *Umweltinformationsgesetz* von 1994 hat der Bundesgesetzgeber für einen ganzen Bereich die Regel durchbrochen, daß Informationsrechte in Form von Einsichts- und Auskunftsrechten nur Betroffenen oder Beteiligten zustehen.

Es steht allerdings außer Frage, daß ein schrankenloses allgemeines Informationszugangsrecht, das jedem Bürger die Möglichkeit eröffnet, Einsicht in alle Verwaltungsakten zu nehmen, mit dem *Grundrecht auf informationelle Selbstbestimmung* unvereinbar wäre. Ein Personenbezug ist jedoch bei einem Großteil der für den Informationszugang relevanten Unterlagen nicht vorhanden, wie z. B. in Bereichen, in denen es um die Grundlagen des grundsätzlichen Verwaltungshandelns geht (Erlasse, Rundschreiben und andere Verwaltungsvorschriften) oder in Bereichen sachbezogenen Verwaltungshandelns (z. B. Straßenbau, Bildungswesen). Beinhalten Verwaltungsvorgänge personenbezogene Daten Dritter, bedarf die Offenbarung der Daten angesichts des Grundrechts auf informationelle Selbstbestimmung des Betroffenen einer ausdrücklichen normenklaren Rechtsgrundlage. Allerdings können auch in einem Informationszugangsgesetz diejenigen Ausnahmen direkt benannt werden, in denen das Recht auf informationelle Selbstbestimmung hinter dem Informationszugangsrecht zurückzutreten hat. Hierzu gehören z. B. die mit dem Verwaltungsvorgang befaßten Amtsträger. Die Offenlegung ihrer Verantwortlichkeiten für Verwaltungsentscheidungen bzw. für die Sachbearbeitung gehört zu einer transparenten Verwaltung und dient den überwiegenden Interessen der Öffentlichkeit. Darüber hinaus wäre auch daran zu denken, im Einzelfall eine Einwilligung anderer Betroffener in die Offenbarung ihrer Daten einzuholen und sie damit zugleich über das Vorliegen eines Informationsbegehrens zu unterrichten.

Im Rahmen eines Informationzugangsgesetzes muß natürlich auch Aspekten Rechnung getragen werden, die gegen die Gewährung des Informationszugangs sprechen (z. B. *staatliche Sicherheitsinteressen).* Bei derartigen Abweichungen vom Grundsatz

Die Ausführungen sind nur allgemein gehalten und kennzeichnen die derzeitige Rechtslage und den Sachstand. Ein Berliner IFG wird auch von der Innenverwaltung grundsätzlich für wünschenswert gehalten, insbesondere soweit dadurch für die Bürger und Bürgerinnen die allgemeine Transparenz von IT-Verfahren und Daten unter Berücksichtigung des Datenschutzes gefördert werden kann. Ein Entwurf könnte auf die verfügbaren Muster zurückgreifen, seine Vorbereitung würde jedoch trotzdem – zur Zeit anderweitig gebundene – erhebliche Ressourcen benötigen.

44 Drs 13/1623
45 JB 1979, 5.2
46 Anlage 2.3.4

des allgemeinen Informationszugangs sollte jedoch vermieden werden, daß ein Katalog von Ausnahmetatbeständen diesen Grundsatz wieder in sein Gegenteil verkehrt.

Zur Durchsetzung, aber auch zur Abwehr des Informationszugangs kann der Bürger den *Rechtsweg* beschreiten, wobei sich als zusätzliche Möglichkeit anbietet, sich mit dem jeweiligen Anliegen an eine *unabhängige Stelle* zu wenden, die in der Lage ist, die Fragen des Interessenausgleichs oder der Interessenkollision sorgfältig zu prüfen. Es bietet sich hier an, ähnlich wie in Brandenburg die Aufgabenstellung des Datenschutzbeauftragten entsprechend zu erweitern. Jedenfalls wird hervorgehoben, daß das Recht auf informationelle Selbstbestimmung des Einzelnen einerseits und das Recht auf allgemeinen Informationszugang andererseits nur „zwei Seiten der gleichen Medaille“ sind und sich nicht von vornherein gegenseitig ausschließen.

## 2. Technische Rahmenbedingungen

### 2.1 Tendenzen und Entwicklungen der Informationstechnik

Schneller, kleiner, billigere Leistung, vernetzter: Die seit Jahren vermeldeten Trends halten unvermindert an:

Neue Generationen von *Prozessoren* haben die Verarbeitungsgeschwindigkeit der Rechner auch für „Otto Normalverbraucher“ in einer Weise verbessert, daß es schwieriger für ihn wird, überhaupt Verwendungen zu finden, die diese Kapazitäten nutzen können. Der Heim-PC wird zum Spielgerät für Computerspiele mit hochaufgelösten komplexen Graphiken, die die Präzision guter Videobilder oder Filme längst übertreffen. Übliche praktische Anwendungen im privaten Haushalt wie Textverarbeitung, Tabellenkalkulation, Datenverwaltung und darauf aufsetzende konkretere Anwendungen können auch bei hohen Ansprüchen an die graphische Oberfläche nur Bruchteile der Kapazität solcher Rechner in Anspruch nehmen. Im kommerziellen Bereich können solche Leistungsdaten dann von Nutzen sein, wenn die Rechner von vielen Benutzern gleichzeitig in Anspruch genommen werden können, wenn sie also als Server vielfältigen Anforderungen parallel genügen müssen.

*Notebook-Computer* gehören wie Handies zur Standardausstattung des modernen Handelsreisenden.

Die *Chipkartentechnologie* regt die Phantasie der Anwendungsdesigner in dem Maße an, in dem die Leistungsstärke der Kartencomputer anwächst und komplexe multifunktionale Anwendungen möglich macht.

Systeme werden zunehmend *vernetzt.* Der Zugriff auf gemeinsame Ressourcen, vor allem Datenbestände, der Austausch von Nachrichten, der Abruf von Informationen, der betriebsinterne Workflow erzwingen die Kopplung der Systeme. Vom häuslichen Computer geht es auf ferne Datenreisen über das Internet.

Organisationsinterne Netze passen sich in den verwendeten Standards zunehmend dem Internet an. Die aus dem Internet gewohnte Darstellung und Strukturierung der Informationen im HTML-Format findet sich auch in den *Intranets* wieder.

#### Vom Client-Server-System zum Network Computing – die Aufhebung von Zeit und Raum

Waren noch vor wenigen Jahren die Mehrplatzsysteme mit zentralem UNIX-Server und „dummen“ Terminals die Standardarchitektur für die Datenverarbeitung in Büro und Verwaltung, so sind es heute die *Client-Server-Systeme.* In ihnen wird unterschieden zwischen dezentralen Arbeitsplatzrechnern bzw. Workstations (Clients) und zentralen Servern.

An *Clients* arbeiten Menschen an ergonomisch ausgerichteten Benutzeroberflächen und führen die Informationsverarbeitung durch. Sie nehmen dabei verschiedene Dienstleistungen, Hilfsmittel und Datenbestände in Anspruch, die zentral zur Verfügung gestellt werden.

Diese zentralen Dienstleistungen können von den *Servern* bereitgestellt werden: Datenhaltung, Druckersteuerung, Massendrucken, Bereithaltung von Massenspeichern (z. B. CD-Server), externe Kommunikation, zentrale Datensicherung, zentrale Softwareversorgung usw. Je nach Umfang dieser zentralen Dienst-

leistungen und der Anzahl der zu bedienenden Clienten können die Server kleine PCs oder Hochleistungsrechner sein und können eine Standard- oder eine Spezialausstattung haben.

Diese Arbeitsteilung und die unterschiedlichen Ausstattungen und Einsatzbedingungen von Clients und Servern führen zu unterschiedlichen Anforderungen an den technischen und organisatorischen Datenschutz. In unserer neuen Broschüre „Datenschutz und IT-Sicherheit bei PCs“[47] werden Empfehlungen zur Erarbeitung von IT-Sicherheits- und technisch-organisatorischen Datenschutzkonzepten für diese, heute verbreitete Einsatzform moderner Informationstechnik gegeben.

Daß Client-Server-Systeme für die aufkommende Informationsgesellschaft noch nicht die letzte Weisheit sind, beweisen die neueren Entwicklungen, die unter dem Stichwort „*Netzwerk-Computer*“ die Schlagzeilen der Fachpresse füllen. Diese Netzwerk-Computer sind Clients, deren lokale Ausstattungen „abgespeckt“ werden: Interne Massenspeicher werden nicht mehr gebraucht. Alles, was für die Verarbeitung benötigt wird, wird aus dem Netz gezogen, denn irgendwo steht ein Server, der den jeweils gewünschten Dienst leisten kann. Der Netzwerkcomputer stellt die Benutzeroberfläche, dahingehend ist er optimiert. Woher die Dienstleistung gezogen wird, ist für den Benutzer und für die Anwendung völlig unbedeutend. Sie kann aus dem Serverraum nebenan, von irgendeinem Server im abteilungs-, firmen- behörden-, landesweiten Intranet, letzten Endes auch von irgendwoher aus dem globalen Internet abgerufen werden.

Seit 1995 wird das Ziel verfolgt, derartige Computer zu entwickeln, die unabhängig von der Hard- und Software der Netzumgebung den Zugang zu den Anwendungen eines Netzes ermöglichen. Zur Umsetzung des Zieles existieren inzwischen Lösungsansätze von verschiedenen Anbietern. Dabei wird auch deutlich, daß es noch keine scharfen Vorstellungen darüber gibt, wie solche Netzwerk-Computer beschaffen sein sollen. So gibt es Firmenkonsortien, die sich um plattformunabhängige Standards bemühen, aber auch Unternehmen, die ihre proprietären Ansätze weltweit durchsetzen möchten.

Jedoch kristallisieren sich folgende Eigenschaften von Netzwerk-Computern im Vergleich zu normalen PCs heraus:

- Netzwerk-Computer werden vollständig *zentral administriert.* Zum Betrieb des Netzwerk-Computers wird die benötigte Software, u. a. auch das Betriebssystem, von einem zentralen Server geladen. Ein normaler PC dagegen verfügt über eine lokale Datenhaltung. Bestimmte Parameter der Hardware und des Betriebssystems können daher nur lokal administriert werden.
- Netzwerk-Computer müssen daher immer mit einem *Netzzugang* ausgestattet sein, während ein normaler PC auch isoliert (stand-alone) betrieben werden kann.
- Ein Netzwerk-Computer ist ein geschlossenes System, das im Gegensatz zum normalen PC nicht ohne weiteres durch standardisierte Komponenten erweitert werden kann. Das Gehäuse eines Netzwerk-Computers soll versiegelt sein *(closed box).*
- Theoretisch sollen Netzwerk-Computer plattform- und betriebssystemunabhängig sein. Mit der *Programmiersprache Java*[48] soll eine Grundlage dafür geschaffen werden, jedoch ist man von einer Normierung noch weit entfernt. Dafür sind zum Teil noch technische Probleme ausschlaggebend, wie z. B. die verhältnismäßig geringe Geschwindigkeit von Java-Anwendungen. Wichtigster Hinderungsgrund für solche Vereinbarungen sind jedoch gegensätzliche Interessen unterschiedlicher Wettbewerbsteilnehmer.

Netzwerk-Computer sind Clients in Client-Server-Systemen. Sie können zusammen mit herkömmlichen PC-Clients und Terminals in einem Netzwerk eingesetzt und damit Einsparungen bei der Administration von Netzwerken erzielt werden. So können Bedienungsfehler bei der Konfigurierung der Rechner vermieden, zumindest aber mit geringerem Aufwand korrigiert werden.

47 Die Broschüre behandelt die IT-Sicherheit und den Datenschutz von Personal Computern in verschiedenen Einsatzformen: als Stand-Alone-PC, als Client oder Server in Client-Server-Netzen, als tragbare Systeme.

48 JB 1996, 4.8.4

Aus der Sicht des technischen Datenschutzes sind verschiedene Risiken zu erkennen:

Netzwerk-Computer sind für einen Anschluß an das *Internet* vorgesehen. Eine solche Schnittstelle ist auf Grundlage einer Kommunikationsanalyse sorgfältig zu planen. Auf die „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[49] sei im Zusammenhang mit den vielfältigen internetspezifischen Risiken ausdrücklich hingewiesen.

Netzwerk-Computer laden die Programme und Daten, mit denen sie arbeiten, aus dem Netz, u. U. sogar aus dem Internet heraus. Die Herkunft der Daten und Programme ist daher nicht immer genau bestimmbar, so daß Zweifel an der *Authentizität der Daten* angebracht sein können. Dies würde bedeuten, daß eine Nachvollziehbarkeit der Datenverarbeitungsprozesse, die für die Sicherstellung der ordnungsgemäßen Datenverarbeitung obligatorisch ist, nicht gegeben ist. Die Authentizität der Daten und Programme ist daher durch elektronische Unterschriften abzusichern.

Auch die *Integrität der Daten und Programme* ist in Frage gestellt, wenn sie aus unbekannten Quellen stammen und/oder auf unbekannten Wegen transportiert werden. Auch hier helfen kryptographische Verfahren zur Entdeckung unautorisierter Änderungen (z. B. *Checksummen-Verfahren).* Außerdem sind Netzwerk-Computer als Einfallstore für *Computerviren* anzusehen und bedürfen daher entsprechender Schutzprogramme.

Die plattformübergreifende Programmiersprache Java eignet sich sehr gut zum Aufbau von netzfähigen Systemen. Doch gerade die sog. *Java-Applets oder Java-Scripts,* welche in Web-Seiten enthalten sein können, lösen u. U. unerwünschte Aktivitäten bei der Ausführung auf dem Netz-Computer aus. Es könnten z. B. Programme geschrieben werden, die das unerlaubte Ausspähen personenbezogener Daten ermöglichen.

Mit dem Einsatz von Netzwerk-Computern steigen die *Kapazitätsanforderungen* an das bestehende Netzwerk extrem an, da neben dem eigentlichen Datenverkehr auch die Anwendungen und Betriebssystemteile über das Netzwerk übertragen werden müssen. Um eine akzeptable Verfügbarkeit und Performanz des Netzes zu gewährleisten, muß die Leitungskapazität dementsprechend ausreichend ausgebaut werden. Inakzeptable Antwortzeiten stehen der Akzeptanz des Systems und der Motivation der Mitarbeiter entgegen und sind damit eine Quelle personell bedingter Sicherheitsrisiken.

Ein wichtiger Nachteil des Netzwerk-Computers ist seine *Abhängigkeit vom Netzwerk.* Fallen entscheidende Komponenten im Netz aus, so ist auch kein lokaler Einsatz möglich.

Die Stellung der *Systemadministration* wird mit dem Einsatz von Netz-Computern wesentlich verstärkt, denn individuelle Einstellungen im Clientbereich sind dort nicht mehr möglich. Die Verantwortung der Systemverwalter wächst in dem Umfang, in dem sie sich auch um die dezentralen Arbeitsumgebungen kümmern müssen. Viele verbreitete Netzbetriebssysteme gewähren den Systemverwaltern umfassende Befugnisse, deren Mißbrauch eine besondere Gefahr für die Funktion des Gesamtsystems bedeuten würde. Vorbeugende technische Maßnahmen gibt es dagegen häufig nicht, selbst die Protokollierung der Systemverwalteraktivitäten ergibt nur dann gegen vorsätzliches Handeln einen Sinn, wenn die Protokolle selbst nicht manipuliert werden können.

Das letztgenannte Risiko zeigt, daß bestimmte Leistungsmerkmale aus der Sicht der informationstechnischen Sicherheit aber auch unübersehbare Vorteile mit sich bringen.

Die zentrale Administration bietet vielfältige Vereinfachungen für den Systemverwalter (Fehler an der Konfiguration der Rechner z. B. durch Fehlbedienungen können mit geringerem Personalaufwand korrigiert werden, zentrale Einspielung und Konfiguration neuer Software usw.) und fördert damit die Verfügbarkeit und Integrität der Systeme.

Den auch vom Senat anerkannten Risiken muß mit wirksamen, umgesetzten Sicherheitskonzepten begegnet werden. Entsprechende Ausführungen werden Bestandteil des erwähnten „IT-Sicherheitsrahmenkonzepts“ sein.

49 Die Orientierungshilfe ist beim Berliner Datenschutzbeauftragten erhältlich und kann auch aus unserem Internetangebot abgerufen werden.

Der Einsatz von Netz-Computern bietet noch weitere Chancen für die informationstechnische Sicherheit und damit für den Datenschutz:

- Die Software kann nur im Netz installiert werden und ist somit gegen *Manipulationen* von den Arbeitsplatzsystemen aus besser geschützt.
- Manipulationen am Endgerät können verhindert werden, da der Administrator bei einer *Fernkontrolle* solche Veränderungen feststellen kann.
- Im Normalfall enthalten Netzwerk-Computer keine Festplatten und keine Laufwerke für bewegliche Datenträger *(medialess system)* und sind lediglich mit einer Netzwerkkarte, Tastatur, Maus und Monitor ausgestattet. Eine lokale Datenhaltung ist nicht möglich. Die Manipulation der personenbezogenen Daten kann dann nur am Server, der die Daten vorhält, erfolgen, der jedoch unter besonderen Sicherheitsbedingungen betrieben werden kann.
- Verschiedene Hersteller bieten *versiegelte* Geräte auf dem Markt an. Dadurch wird eine Manipulation durch Einspielung von Software von externen Laufwerken oder durch den unerlaubten Einbau von Hardwarekomponenten unterbunden oder zumindest erschwert.

Obwohl die meisten Anwender dem Netzwerk-Computer heute eher zurückhaltend gegenüberstehen, prognostizieren die neueren Statistiken und Analysen zum Jahr 2000 einen starken Anstieg des Einsatzes dieser Technik. Im Jahr 2001 könnte demzufolge die Anzahl der heute üblichen Client-Server-Systeme erreicht und überflügelt werden.

Allerdings ist bis heute das Angebot an Software für solche Systeme vergleichsweise gering. Das Konzept der Netzwerk-Computer kann nur erfolgreich durchgesetzt werden, wenn Anwendungen hinreichend verfügbar sind.

Neueste Visionen zeigen die globale Vernetzung aller Kommunikations- und Computersysteme auf: In Verbindung mit einer Chipkarte soll der Anwender von einem beliebigen Computer aus unter seiner gewohnten Bedieneroberfläche und den entsprechenden Zugriffsrechten über das Internet mit dem heimatlichen System arbeiten können. Z.B. kann sich ein Mitarbeiter auf Dienstreise von einem Hotelzimmer aus bei seiner Firma einloggen und damit arbeiten, als säße er an seinem eigentlichen Arbeitsplatz.

**Schürfen in Banken und Warenhäusern**

In der aufziehenden Informationsgesellschaft ist niemand in der Gefahr, nicht hinreichend mit Daten-, Nachrichten- und Informationsmaterial versorgt zu werden. Zeitungen, Zeitschriften, Bücher, graue und grelle Literatur, Briefe, Postwurfsendungen, Telefaxe, elektronische Post, Datenströme, Datenträger, automatisierte Datenverarbeitungsprozesse, Internet und vieles anderes mehr sorgen dafür, daß jede Information, die jemanden erreichen soll, ihm zumindest physisch auch erreicht.

Aber nur ein geringer Bruchteil der Informationen, die uns erreichen, kann auch real zur Kenntnis genommen werden. Es kommt also darauf an, diejenigen Informationen herauszufiltern, die man braucht. Dies gilt auch für elektronisch verfügbare Daten. Diese stehen in Behörden und Unternehmen in ungeheuren Massen zur Verfügung. Gesucht sind also Instrumente, die aus den Datenmassen gezielt die Daten bereitstellen, die gerade gebraucht werden. Diese Aufgabe ist weit schwieriger zu lösen als das Sammeln und Speichern der Daten. Bereits in den 70er Jahren ist der Versuch, unter dem Begriff *„Management-Informationssysteme“* Entscheidungsträgern die vermeintlich gebrauchten Informationen am Arbeitsplatz bereitzustellen, kläglich gescheitert.

Das klassische Instrument der Datenhaltung und Datenerschließung ist das *Datenbanksystem*. Die dahinterstehenden Datenmodelle haben sich im Laufe der letzten Jahrzehnte wesentlich gewandelt. Gemeinsam ist ihnen jedoch, daß eine einheitliche Strukturierung der Daten in Tabellen, Sätzen, Feldern notwendig war. Aktuelle Datenbanksysteme arbeiten mit Tabellen, die untereinander relational zu neuen Tabellen verknüpft

werden können und auf diese Weise Bezüge zwischen den Daten aufdecken können, die anders vielleicht nicht erkennbar wären. Diese relationalen Datenbanken sind heute Standard für die gezielte Datenbereitstellung.

Die Erschließung unstrukturierter Datenbestände wie z. B. von Textmengen erfolgt mit *Volltext-Retrievalsystemen.* Heute lassen sich die Vorteile relationaler Datenbanken mit Volltext-Retrievalsystemen kombinieren, indem einzelne Felder relationaler Datenbanken mit großen Textmengen gefüllt werden, die ihrerseits mit Volltextrecherche erschlossen werden können.

Mittlerweile füllen neue Begriffe die Schlagzeilen der Fachpresse: *Data-Warehouses* sollen mit Methoden des *Data-Mining*[50] relevante Informationen aus den verfügbaren, mit unterschiedlichen Methoden und unterschiedlicher Intensität strukturierten, also heterogenen Datenmassen „herausgraben“ und bereitstellen.

Data-Warehousing soll bisher nicht erschließbare und demzufolge eben auch nicht erschlossene Daten über Konkurrenten und Kunden gezielt bereitstellen. Was dem einen die „Rasterfahndung nach dem Kunden“ ist, bedeutet für Unternehmen das „Wir wollen alles über den Kunden wissen, damit wir ihn besser bedienen können“.

Mit den Werkzeugen des Data-Warehousing können die verschiedenen Datenressourcen eines Unternehmens zusammengeführt und analysiert werden. Diese Analysen können exakte Aussagen über das Verhalten von Mitbewerbern, vor allem aber über die Kunden eines Unternehmens treffen. Ihr Kaufverhalten kann beobachtet, vorhergesagt und damit – z. B. im Rahmen des Direkt-Marketing – beeinflußt werden. Die eigene Serviceleistung kann auf der vollständig verfügbaren Datenbasis analysiert und gegebenfalls korrigiert werden.

Solche kundenbezogenen Analysen können bis zur einzelnen Person verfeinert werden und führen so zu neuen personenbezogenen Daten. Aber selbst dann, wenn die Analysen nur zu statistischen Summendaten zu bestimmten Kundenkategorien und -gruppen führen: In der Konsequenz ordnen sie individuell erfaßbare Menschen einer bestimmten Gruppe zu, ordnen ihnen damit Merkmale zu, nutzen dies zu Entscheidungen über eine individuelle Kundenbetreuung, -beratung und -umwerbung.

Aus datenschutzrechtlicher Sicht ist dieses Data-Mining höchst problematisch. Die weitgefaßten Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im Bundesdatenschutzgesetz erlauben die Verarbeitung personenbezogener Daten bereits dann, wenn berechtigte Interessen der Verarbeiter vorliegen und eine Abwägung ergibt, daß die schutzwürdigen Interessen der Betroffenen nicht unangemessen beeinträchtigt werden. Diese Kategorien gehen von einem bestimmten Anwendungszusammenhang oder einer bestimmten Zwecksetzung aus. Mögen die Daten in den Data-Warehouses im einzelnen in bestimmten Anwendungszusammenhängen oder für bestimmte Zwecke erhoben und gespeichert worden sein, bei der Zusammenführung dieser Daten und der Analyse zur Aufdeckung neuer, vorher unbekannter Zusammenhänge lösen sich die Daten jedoch von den ursprünglichen Zwecken und werden zur Gewinnung beliebiger neuer Erkenntnisse über Personen zusammengeführt. Dabei kann nicht mehr automatisch davon ausgegangen werden, daß die schutzwürdigen Interessen der Betroffenen den berechtigten Interessen der Verarbeiter hintanstehen können. Data Warehouses sind im Zusammenhang mit der Verarbeitung personenbezogener Daten – seien es Personen in ihrer Rolle als Kunden, als Mitarbeiter oder als Bürger – ein besonderes Risiko für die informationelle Selbstbestimmung.

### 2.2 Datenschutz durch Technik

Die letzten Ausführungen zum Data-Warehousing mögen ein Indiz dafür sein, daß mit dem technischen Fortschritt ebenso fortschreitend Risiken für die informationelle Selbstbestimmung verbunden wären. Eine solche, in einzelnen Medien auch immer wieder angedeutete Auffassung, die Technik an sich sei eine Gefahr für die Privatsphäre und die immanenten IT-Sicherheitsrisiken der Infrastrukturen der Informationsgesellschaft seien nicht beherrschbar, trifft die Wirklichkeit nicht.

50 Verfahren zur Datenverdichtung, um mit statistischen Methoden aus großen Datenbeständen neue Zusammenhänge herauslesen zu können

Wie bereits im Vorjahr ausführlich behandelt[51], kommt es vielmehr darauf an, die Informationstechnik für die Ziele des Datenschutzes zu nutzen. Dies bedeutet, daß nicht nur defensive Absicherungen für die Verfügbarkeit, Integrität und Vertraulichkeit der Systeme, Programme und Daten mit technischen Mitteln umgesetzt werden, um Bedrohungen und Risiken für diese Sicherheitsziele entgegenzutreten, sondern daß die technischen Möglichkeiten offensiv dazu genutzt werden, solche Bedrohungen und Risiken gar nicht erst aufkommen zu lassen.

In zwei umfassenden Arbeitspapieren haben sich die Datenschutzbeauftragten des Bundes und der Länder mit der Thematik der datenschutzfreundlichen Technologien befaßt, zum einen in einem allgemein auf die Informationstechnik bezogenen Ansatz[52], zum anderen speziell zur Telekommunikation[53]. Die wichtigsten Thesen sind in einem Beschluß der Konferenz der Datenschutzbeauftragten zur „Erforderlichkeit datenschutzfreundlicher Technologien“ des Bundes und der Länder zusammengefaßt[54].

Die Ziele in der Entwicklung der Informationstechnik waren bisher davon bestimmt, immer mehr Daten mit immer komplexeren Strukturen verarbeiten zu können, einerseits um immer genauere und umfassendere Informationen über Gegenstände des jeweiligen Interesses (und das sind in den meisten Fällen Personen) zu gewinnen und zu nutzen, andererseits aber auch, um differenziertere und damit in der Regel gerechtere Fallunterscheidungen bei der Entscheidungsfindung zu ermöglichen. Wer heute versuchen wollte, z. B. Lohn-und Gehaltszahlungen in einem mittleren oder größeren Unternehmen so zu berechnen, daß allen rechtlichen Anforderungen genügt wird, wird sich klar werden, daß dies nur deshalb so kompliziert sein darf, weil es eben Computerprogramme gibt, die dieser Komplexität noch Herr werden können. Gäbe es die Computer nicht, müßten solche Vorgänge einfacher bearbeitet werden können.

Da die Informationstechnologie Kapazitätsengpässe kaum noch kennt, die nicht mit geringem finanziellen Aufwand behoben werden könnten, sind die Planer von Anwendungsverfahren eher großzügig, wenn es darum geht, welche Daten dabei verwendet werden sollen und welche Verarbeitungen damit ermöglicht werden sollen. Auch der Gesetzgeber tendiert zur Großzügigkeit, wenn es darum geht, den Begehrlichkeiten den erforderlichen rechtlichen Rahmen zu geben.

Die Diskussion um datenschutzfreundliche Technologien soll hier jedenfalls für bestimmte Anwendungsbereiche eine Trendwende initiieren. Die Informationstechnologie soll dabei helfen, daß

- in bestimmten Anwendungen auf personenbezogene Daten verzichtet werden kann, ohne daß die Ziele der Datenverarbeitung dabei in Frage gestellt werden *(Datenvermeidung);*
- anderenfalls in Hinsicht auf Umfang und Verbreitung sparsam mit personenbezogenen Daten umgegangen wird, ebenfalls, ohne daß die Ziele der Datenverarbeitung dabei in Frage gestellt werden *(Datensparsamkeit)*;
- die Datenverarbeitung so organisiert wird, daß auftretende personenbezogene Daten nur dort auf einzelne Personen beziehbar sind, wo dieses auch erforderlich ist, ansonsten aber *anonym* oder zumindest *pseudonym* gespeichert, übertragen und verarbeitet werden.

Diese Zielsetzungen sind von der Bundesregierung auch schon aufgegriffen worden. In dem Bericht zu „Info 2000 – Deutschlands Weg in die Informationsgesellschaft“ formuliert das Bundesministerium für Wirtschaft, daß die Bundesregierung der Auffassung ist, „daß die geltenden allgemeinen Datenschutzbestimmungen und die Regelungen im Bereich der Telekommunikation vor dem Hintergrund der neuen technologischen Entwicklung eine Überarbeitung anhand folgender Erfordernisse bedürfen.“

51 JB 1996, 2.2
52 Arbeitspapier „Datenschutzfreundliche Technologien“, abrufbar aus unserem Internetangebot
53 Arbeitspapier „Datenschutzfreundliche Technologien in der Telekommunikation“, abrufbar aus unserem Internetangebot
54 Anlage 2.3.3

Sie beginnt die folgende Aufzählung mit den Sätzen: „Die Benutzung von Multimedia-Diensten muß soweit wie möglich unter Wahrung der Anonymität des Verbrauchers erfolgen können. Soweit personenbezogene Daten verarbeitet und genutzt werden müssen, darf dies nur in dem unbedingt notwendigen Umfang geschehen."

Konsequenterweise verlangen die neuen Bestimmungen des Teledienstedatenschutzgesetzes (TDDSG) und des Mediendienste-Staatsvertrags, daß Anbieter von Tele- und Mediendiensten den Nutzern die Inanspruchnahme und Bezahlung entweder vollständig anonym oder unter Verwendung von Pseudonymen ermöglichen sollen, wenn dies technisch möglich und zumutbar ist[55].

Mit komplexen kryptographischen Verfahren lassen sich die Anforderungen an Anonymität bzw. Pseudonymität gewährende Systeme umsetzen. So geht z. B. das Konzept des *Identity Protectors*[56] von der Idee aus, daß sich informationstechnische Systeme, die nicht vollständig anonym betrieben werden können, so in Einzelprozesse zerlegen lassen, daß der Personenbezug nur in den wenigsten Einzelprozessen unabdingbar ist. Mit den genannten Methoden und Verfahren lassen sich die Bereiche, die die Identität benötigen, von jenen trennen, die mit Pseudonymen auskommen. Aufgabe des Identity Protectors ist es, für diese strikte Trennung zu sorgen und die Pseudonymisierung bzw. Depseudonymisierung bei der Prozeßkommunikation zwischen den getrennten Bereichen unter genau bestimmten Bedingungen durchzuführen.

Die Anwendung solcher Verfahren ist prinzipiell in allen informationstechnischen Systemen denkbar, derzeit konzentriert sich die Diskussion jedoch auf

- den bereits erwähnten *Medienbereich:* Hier geht es speziell um den Schutz der Daten der Mediennutzer, die bei der Inanspruchnahme der elektronischen Informations- und Kommunikationsdienste entstehen, ohne daß sie zwingend für Abrechnungszwecke gebraucht werden, zumal auch anonyme Zahlungsverfahren ermöglicht werden können;
- den *elektronischen Zahlungsverkehr:* Die Anonymität der Bargeldzahlung soll auch im elektronischen Zahlungsverkehr möglich gemacht werden, nachdem scheck- und kreditkartengestützte Zahlungsverfahren die Gefahr des „gläsernen Verbrauchers" aufkommen ließen. Dabei werden zwei Richtungen verfolgt: Im kartengestützten Zahlungsverkehr ruhen die Hoffnungen der Datenschützer auf den vorausbezahlten elektronischen Geldbörsen[57] und bei netzorientierten Zahlungsverfahren auf virtuellen digitalen „Münzen", die mit komplexen kryptographischen Verfahren anonyme Zahlungen gewährleisten, ohne andere Sicherheitsaspekte (Betrugssicherheit, Währungssicherheit) aus dem Auge zu verlieren;
- die Datenkommunikation im *Gesundheitswesen:* Viele der in der Datenkommunikation im Gesundheitswesen verfolgten Ziele lassen sich mit anonymen oder pseudonymen Verfahren verwirklichen: Krankheitsregister (z. B. Krebsregister), Qualitätssicherung, epidemiologische Datenbanken. Ansonsten ist sicherzustellen, daß der Personenbezug medizinischer Daten nur dort besteht, wo es für die Behandlung des Patienten erforderlich ist, also beim behandelnden Arzt;
- die *Telekommunikation:* Die Identität von Sendern und Empfängern bei der Telekommunikation kann beim Einsatz geeigneter Verfahren und Techniken Dritten gegenüber vertraulich bleiben. Auch bei der Entgeltabrechnung läßt sich die Speicherung von Verbindungsdaten zu Abrechnungszwecken je nach Art der Abrechnung und Tarifierung vermeiden oder zumindest minimieren;
- den Bereich *Transport und Verkehr:* Kartengestützte Zahlungssysteme werden vermehrt bei Verkehrsmitteln (Bahn, öffentlicher Personennahverkehr) eingesetzt, bei denen die oben erwähnten datenschutzfreundlichen Ansätze (vor allem elektronische Geldbörsen) in Einsatz kommen können. Hinzu kommen Planungen zu Autobahn- oder City-Mautsystemen, die so zu gestalten sind, daß individuelle Be-

Der Senat ist der festen Überzeugung, daß eine wünschenswerte Entwicklung hin zum „Elektronischen Ticketing" nur mit Blick auf Wahrung und Förderung der Persönlichkeitsrechte erreicht werden kann. Hierzu zählt vorrangig die Berücksichtigung der Rechte des Datenschutzes.

Das mit dem Datenschutzbeauftragten abgestimmte Verfahren bei der „Elektronischen Geldbörse" der BVG (bargeldloser Kauf von Fahrausweisen mittels wiederaufladbarer anonymer Mikroprozessor-Chipkarte) schließt – im Unterschied zu kontenbezogenen Zahlungssystemen wie z. B. die Eurocheque-Karte – individuelle „Bewegungsprofile" aus. Diese datenschutzfreundlichen

55 §§ 4 Abs. 1 TDDSG, 13 Abs. 1 Mediendienste-Staatsvertrag; vgl. unten 3.3
56 John Borking: Der Identity Protector, Datenschutz und Datensicherheit (DuD) 11/96, S. 654 ff.
57 vgl. unten 3.4

wegungsprofile ausgeschlossen sind. Das gleiche Ziel ist bei der Realisierung von Verkehrsleit-, Standortbestimmungs- und Flottenmanagementsystemen anzustreben.

Ansätze gelten auch für den geplanten „elektronischen Fahrschein“.

Beim zur Zeit laufenden Verbundprojekt „Elektronisches Ticketing im öffentlichen Personennahverkehr in Berlin-Brandenburg“ mit der BVG als Projektführer werden nach Aussagen der zuständigen Fachabteilungen der BVG und des VBB Verkehrsverbundes Berlin-Brandenburg datenschutzrechtliche Aspekte berücksichtigt. Mit dem geplanten kartengestützten Zahlungssystem für den öffentlichen Personennahverkehr wird es – ebenso wie bei der „elektronischen Geldbörse“ – nicht möglich sein, das Fahrverhalten („Bewegungsprofil“) von Einzelpersonen nachzuvollziehen.

Mit einer flächendeckenden Einführung eines elektronischen Ticketingsystems im ÖPNV Berlin-Brandenburg ist nach gegenwärtigem Stand nicht vor Ende 2001 zu rechnen. Zunächst sind u. a. noch zwei Pilotversuche in 1999/2000 durchzuführen. Erst nach Abschluß und Auswertung dieser Tests wird über das weitere Verfahren zu entscheiden sein.

Bei der Realisierung von Verkehrsleit-, Standortbestimmungs- und Flottenmanagementsystemen werden datenschutzrechtliche Aspekte angemessen berücksichtigt.

Die Einführung von Autobahn- oder Citymautgebühren ist nicht geplant.

**2.3 Datenverarbeitung in Berlin**

Der Wandel der Gesellschaft zur „*Informationsgesellschaft*“ ist eine Entwicklung, der sich gerade Berlin nicht entziehen kann. Nicht nur die bestehenden Strukturen, sondern vor allem auch die neuen Aufgaben als Bundeshauptstadt und die künftig sicherlich immer bedeutender werdende Rolle als Mittler von Waren- und Dienstleistungstransfers in den osteuropäischen Raum erzeugen einen starken Druck zur umfassenden Nutzung informations- und kommunikationstechnischer Ressourcen. Dies betrifft die Berliner Privatwirtschaft ebenso wie die öffentliche Verwaltung.

Hinzu kommt, daß in unserer Stadt sowohl Forschung und Entwicklung als auch die Produktion auf dem Gebiet der *Elektrotechnik* im allgemeinen und der *Telekommunikationstechnik* im besonderen traditionell stark verankert sind. Die Medien- und Kommunikationsbranche boomt, es wird geschätzt, daß es in Berlin mindestens 6000 Unternehmen mit über 70 000 Beschäftigten in diesem Sektor gibt. Jedes Unternehmen und jede Verwaltung hat ganze Organisationseinheiten, die sich mit der Informationstechnik befassen.

Das *digitalisierte Berliner Telekommunikationsnetz* hat inzwischen über 2 Millionen Teilnehmer, das Breitband-Kabelnetz erreicht fast drei Viertel der Bevölkerung; im Zusammenhang mit dem Regierungsumzug nach Berlin wird ein ATM-Breitband-Übertragungsnetz aufgebaut, dessen Bedeutung weit über die unmittelbare Nutzung durch die Bundesregierung reichen wird. Der Aufbau dieser Infrastruktur wird Telekommunikationstechnik in den nächsten Jahren gerade in Berlin auch in die Haushalte bringen und dort früher als anderswo zu Konsequenzen im Alltag führen.

Zusammen mit der Berliner Wirtschaft hat der Senat im Sommer vergangenen Jahres die ressortübergreifende *Landesinitiative* „Der Berliner Weg in die Informationsgesellschaft“ begründet, die sich dem Wandel „offensiv stellen“ und für die ganze Stadt nachhaltige Problemlösungen entwickeln will. Die einbezogenen Projekte betreffen die Wirtschaftsförderung insbesondere auf dem Gebiet der Entwicklung von Hard- und Software, die Förderung der Informatik in Hochschulen und Schulen, die Entwicklung von Projekten zu Verkehr und Umwelt sowie die Verwaltungsreform.

Die Senatsverwaltung für Wirtschaft und Betriebe hat uns mitgeteilt, daß man der „festen Überzeugung sei, daß eine wünschenswerte Entwicklung hin zur Informationsgesellschaft nur mit Blick auf Wahrung und Förderung der Persönlichkeitsrechte erreicht werden kann“. Dies schließe eine „angemessene Berücksichtigung der Datenschutzrechte“ ein. Wir werden darauf drängen, daß diese – recht zurückhaltende – Aussage bei der Entwicklung der einzelnen Projekte auch umgesetzt wird.

**Organisation des IT-Einsatzes in der Berliner Verwaltung**

Auch wenn die Zuständigkeit des Berliner Datenschutzbeauftragten sich seit August 1995 auch auf private Unternehmen erstreckt, kann eine Übersicht über aktuelle Entwicklungen in der Berliner DV-Szene nur für die öffentliche Verwaltung gegeben werden, da es für private Unternehmen keine generelle Informationspflicht über neue IT-Anwendungen gibt.

In den öffentlichen Stellen Berlins werden alljährlich dreistellige Millionensummen in die Informationstechnik investiert. Daran ändert auch die Knappheit der öffentlichen Haushalte nichts. Im Gegenteil: Ein wesentlicher Bestandteil der Verwaltungsreform ist der verstärkte Einsatz von Informationstechnik, um Personaleinsparungen zu ermöglichen, Verwaltungsabläufe zu straffen, die Beratungskompetenz und damit den Kontakt zum Bürger zu verbessern sowie die Arbeitsumgebungen der Mitarbeiter der öffentlichen Stellen modernen Standards anzupassen.

Es ist klar, daß ein so intensiver Einsatz von Informationstechnik der Koordination im Lande bedarf, um Doppelarbeit und Insellösungen zu vermeiden, um in Sammelausschreibungen günstigere Preise zu erzielen und um – wo notwendig und zulässig – die Interoperabilität der Verfahren zu ermöglichen.

Dennoch hat sich die Verwaltung – federführend ist die Senatsverwaltung für Inneres – in den letzten Jahren schwer getan, verbindliche Regelungen zu schaffen und ein koordiniertes Vorgehen sicherzustellen.

Inzwischen sind die Bemühungen um Koordination der Informationstechnik verstärkt worden und haben zu ersten organisatorischen Konsequenzen geführt:

Ende 1996 wurde ein *IT-Koordinations- und Beratungsausschuß* (IT-KAB) eingerichtet, dem IT-Manager der Hauptverwaltungen, der Großverfahren, der nachgeordneten Behörden und der Bezirke angehören, in beratender Funktion auch der Berliner Datenschutzbeauftragte. Der IT-KAB soll zu den Fragen des IT-Einsatzes beraten und Stellung nehmen, wenn sie aus strategischer oder grundsätzlicher Sicht von behördenübergreifender Bedeutung sind, speziell bei gleichartigen oder ähnlichen Fachaufgaben, die in verschiedenen Behörden wahrgenommen werden, bei durchgängigen Querschnittsaufgaben wie z. B. Personal- und Haushaltswesen, bei IT-spezifischen Querschnittsaufgaben, zu denen auch die informationstechnische Sicherheit und die Aus- und Fortbildung gehören, bei der Nutzung spezifischer Infrastruktureinrichtungen (z. B. das MAN), bei Richtlinien, die in organisatorischer und technischer Hinsicht das behördenübergreifende Zusammenwirken regeln, sowie bei Grundsätzen des IT-Einsatzes in vielerlei Hinsicht, u.a. auch zu Datenschutz und Datensicherheit.

Erste Zwischenergebnisse wurden mit den Entwürfen von Leitlinien zur IT-Strategie des Landes Berlin, der Richtlinie für die *Organisation* des IT-Einsatzes in der Berliner Verwaltung (IT-Organisationsrichtlinie), der Richtlinie für die *Planung und Durchführung* von IT-Projekten in der Berliner Verwaltung (IT-Projektrichtlinie) und des Rahmenkonzepts zur Gewährleistung der notwendigen *Sicherheit* beim IT-Einsatz in der Berliner Verwaltung (IT-Sicherheitsrahmenkonzept) vorgelegt. Die Organisationsrichtlinie wurde vom IT-KAB bereits verabschiedet und soll im ersten Quartal 1998 vom Senat in Kraft gesetzt werden.

Die Geschäftsführung des IT-KAB hat ein inzwischen neu geschaffenes Referat der Service-Abteilung der Senatsverwaltung übernommen. Die offenen Fragen – so auch die Weiterentwicklung des IT-Sicherheitsrahmenkonzepts – sollen in Arbeitsgruppen weiterentwickelt werden.

Die Ausführungen beschreiben und begrüßen die eingeleiteten Maßnahmen zu einer stärkeren Koordinierung. Die Darstellung entspricht im wesentlichen den Tatsachen und bedarf keiner weiteren Kommentierung.

**Vom Landesamt zum Landesbetrieb – die Umwandlung des LIT**

Bereits im Jahresbericht 1994[58] hatten wir mit datenschutzbezogenen Argumenten die Absicht begrüßt, dem Landesamt für Informationstechnik (LIT) einen anderen öffentlich-rechtlichen

58 JB 1994, 2.3

Status zu geben, damit es den Anforderungen eines zentralen IT-Dienstleisters für die Berliner Verwaltung flexibler nachkommen kann. Diese Umwandlung in einen *Betrieb* gemäß § 26 Landeshaushaltsordnung (LHO), der seine eigenen Einnahmen zu erwirtschaften hat, wurde mit Wirkung zum 1. Januar 1998 vollzogen.

Dies erfolgte gegen das Votum des Rechnungshofes von Berlin, der erhebliche Zweifel an der Konkurrenzfähigkeit des geplanten Landesbetriebes äußerte und empfahl, zunächst nur die Verwaltungsreform im LIT konsequent umzusetzen, das Amt zu einem arbeitsfähigen Leistungs- und Verantwortungszentrum im Sinne der Verwaltungsreform zu entwickeln und eine Kosten- und Leistungsrechnung einzuführen.

Die Senatsverwaltung für Inneres wies das Votum des Rechnungshofes jedoch zurück und folgte der Stellungnahme des LIT, in der die Vorhaltungen des Rechnungshofes ebenfalls im wesentlichen zurückgewiesen wurden.

Der Haushaltstitel für das LIT wurde im Haushalt 1998 gestrichen und die Mittel auf die bisherigen Großkunden aus der Verwaltung mit dem Zweck verteilt, davon die Dienstleistungen des LIT zu bezahlen. Für die Dauer von zwei Jahren müssen diese Verwaltungen die Leistungen des LIT abnehmen, danach muß es auf den Wettbewerb mit anderen IT-Dienstleistern eingestellt sein und sich darin bewähren. Die Umwandlung führt dazu, daß die politische Steuerung des LIT und seine Orientierung an den Interessen des Landes in Zukunft entfällt. Statt dessen erfolgt eine Orientierung an den Interessen der Kunden des LIT. Dies können jetzt auch private Kunden sein.

Diese Aussage ist nur begrenzt richtig, da die politische Steuerung durch Rahmensetzung des Senats – der LIT ist noch Teil der Verwaltung – weiterhin gegeben ist.

Die Arbeitsfelder des LIT sind wie folgt umrissen:

- Betrieb proprietärer Mainframes und Netze sowie Druckservices,
- Betrieb des Berliner Landesnetzes,
- Vermarktung der vom Land nicht genutzten Netzressourcen gegenüber Dritten,
- Dienstleistungen bei IT-Beschaffungen,
- Consulting und Projektierungen,
- Schulung.

Von besonderer Bedeutung für den Datenschutz ist die Einrichtung der „*Dienste Netzsicherheit*“ im Geschäftsbereich „Kommunikations-, Informations- und Sicherheits-Services (KISS)“, die Beratungsdienstleistungen bei Sicherheitsverlusten, zum Schutz vor Computerviren oder zur Verschlüsselung zur Verfügung stellen, aber auch selbst Aufträge etwa zur Erstellung von Risikoanalysen übernehmen.

**Berliner Verwaltungsnetz – MAN**

Bereits im Jahresbericht 1996[59] stellten wir fest, daß die zunehmende Nutzung des Berliner Verwaltungsnetzes (Metropolitan Area Network – MAN) verstärkt Sicherheitsprobleme aufwarf. Nachdem im vergangenen Jahr der Umsetzung des Datenschutz- und Datensicherheitskonzeptes für das MAN nicht immer die notwendige Priorität eingeräumt wurde, hatte sich dies zunächst entscheidend geändert. Der im letzten Jahr ins Leben gerufene Arbeitskreis „*Netzsicherheit*“ im Landesamt für Informationstechnik, der einen koordinierten Informationsaustausch im Bereich der Netzsicherheit im gesamten Berliner Landesnetz erreichen sollte, leistete erfolgreiche Arbeit. Die regelmäßigen Treffen und die erarbeiteten Papiere halfen, das Sicherheitsniveau im Landesnetz zu verbessern. In Folge der Umstrukturierung im LIT wurde dieser Arbeitskreis leider aufgelöst. Dies sollte jedoch nicht dazu führen, daß der sehr wichtige Informationsaustausch nicht mehr im bisherigen Umfang stattfindet. Leider mußten wir jedoch feststellen, daß der Informationsfluß in signifikanter Weise unterbrochen wurde.

Ein wesentlicher Schwerpunkt war und ist die sichere Anbindung des Berliner Verwaltungsnetzes an das Internet. Aus der Verwaltung wurden vermehrt Anforderungen an das LIT heran-

Der Berliner Datenschutzbeauftragte war als assoziiertes Mitglied im Arbeitskreis Netzsicherheit (AKS) des LIT vertreten und damit für die Dauer seines Wirkens bis August 1997 über alle Entwicklungen informiert. Die am 26. Mai 1997 gebildete Arbeitsgruppe Kommunikations-, Informations- und Netzsicherheitsdienste (KISS), die mit der Betriebsbildung des LIT in den jetzigen Fachbereich KISS überging, hatte das Ziel, die Verbindlichkeit der Ergebnisse und ihrer Umsetzung im LIT zu gewähr-

59 JB 1994, 4.8.1

getragen, die Nutzung der Dienste des Internet endlich auch den Berliner Behörden zu ermöglichen. Zur Vorbereitung der Internet-Anbindung wurde eine Testumgebung geschaffen, die im wesentlichen das MAN nachbildete. Hier wurden drei verschiedene Firewall-Systeme getestet, um eine Möglichkeit zu schaffen, das System auszuwählen, welches den hohen Anforderungen am besten gerecht wird. Anschließend wurde mit dem *Aufbau eines Grenznetzes* begonnen. Dieses Grenznetz stellt den Übergang zum Internet dar und kann als ein weiteres Subnetz mit speziellen (Abgrenzungs-) Aufgaben am MAN betrachtet werden.

Das Grenznetz soll im wesentlichen zwei Aufgaben erfüllen: Zum einen soll es den gesicherten Übergang zwischen dem MAN und dem Internet oder anderen Fremdnetzen realisieren und damit eine sichere Kommunikation zwischen dem Verwaltungsnetz und dem Internet ermöglichen. Zum anderen sollen Informationsserver eingebunden werden, die Informationen von allgemeinem Interesse zum Abruf zur Verfügung stellen. Dies bedeutet, daß Berliner Verwaltungen eigene Informationsangebote (WWW-Angebote) in das Internet einstellen können, ohne daß externe Internet-Nutzer auf das Verwaltungsnetz zugreifen müssen.

Dieses Konzept ist aus Datenschutz- und Datensicherheitsgründen sehr zu begrüßen. Das mit diesem Grenznetz gebildete Firewall-System kann jedoch nur die Grundlage für die Sicherheit im dahinterliegenden Verwaltungsnetz bilden. Da einerseits die Anforderungen an die Nutzung von Internet-Diensten innerhalb der Berliner Verwaltung sehr unterschiedlich sind und andererseits vor allem auch der Schutz der an das Verwaltungsnetz angeschlossenen Subnetze untereinander gewährleistet sein muß, müssen verstärkt Sicherheitsmechanismen in den einzelnen Verwaltungs-Subnetzen entwickelt und realisiert werden[60].

Erste Schritte in Richtung eines *informationstechnischen Sicherheitskonzepts für die Berliner Verwaltung* wurden mit der Entwicklung von Datenschutz- und Datensicherheitskonzepten für das MAN und der ISDN-Vernetzung der Berliner Verwaltung sowie verfahrenspezifischer Konzepte getan. Weitere sehr wichtige Schritte sind die oben bereits erwähnte Entwicklung eines Sicherheitsrahmenkonzeptes durch den IT-KAB und eines Sicherheitskonzeptes für Backbone-Netzdienste durch das LIT.

Das *Sicherheitsrahmenkonzept* soll die Mindest- und Rahmenbedingungen zur Gewährleistung der IT-Sicherheit aus verfahrens-, behörden- und standortübergreifender Sicht festlegen und ist bei der Erstellung weiterer spezifischer Konzepte zu beachten.

Das *Sicherheitskonzept für Backbone-Dienste* beschreibt die Verantwortungsverteilung beim sicheren Betrieb von Verfahren und Services über das Backbone-Netz des Berliner Verwaltungsnetzes und unterscheidet dabei die einzelnen Rollen für Anwender, Verfahrensverantwortliche und Infrastrukturbetreiber. Dieses Konzept verdeutlicht, daß die Sicherheit nicht an einer einzigen Stelle festzumachen ist, sondern von allen beteiligten Institutionen zusammen erbracht werden muß. Grundlagen sind in jedem Fall die Sicherheitskonzepte der einzelnen Behörden und Verfahren. Die beim Anschluß an das MAN auftretenden zusätzlichen Gefahren – insbesondere vor dem Hintergrund des Anschlusses des MAN an das Internet – werden dargestellt und können als Leitfaden für die Erstellung oder Vervollständigung der behörden- oder verfahrensbezogenen Sicherheitskonzepte verwendet werden. Die Erfahrung der letzten Jahre hat jedoch gezeigt, daß die Erarbeitung von Konzepten allein nicht ausreicht. Der relativ zügigen Umsetzung der in den Konzepten erarbeiteten Maßnahmen kommt jetzt besondere Bedeutung zu.

Leider mußten wir auch diesmal wieder feststellen, daß die Erfahrung nicht trügt und die Realisierung risikoerzeugender Verwaltungsverfahren – hier die *Internet-Anbindung* des Berliner Landesnetzes – schneller erfolgt als die Erarbeitung und Umsetzung der dazugehörigen Datenschutz- und Datensicherheitskonzepte. Die positive Bewertung der schrittweisen Erprobung und Einführung der Internet-Anbindung des MAN muß daher relativiert werden. Wie bereits oben erwähnt, wurde der gerade in diesem Bereich sehr wichtige Informationsfluß durch die Umstrukturierung des LIT stark gestört. So wurde bereits im Oktober 1997 die bisherige Trennung des Verwaltungsnetzes vom Internet leisten (Der AKS war keine Linienstruktur des LIT und seine Ergebnisse hatten empfehlenden Charakter). Der AKS war aber bereits offen für die Mitarbeit anderer Verwaltungen, sodaß eine Weiterführung des Arbeitskreises wünschenswert war. Dazu wurde im August 1997 mit der Innenverwaltung vereinbart, daß dieser Arbeitskreis künftig als Arbeitsgremium auf der Ebene des jetzigen IT-Koordinierungsausschusses Berlin (ITKAB) angesiedelt wird. Das LIT würde darin durch einen KISS-Mitarbeiter vertreten sein. Die Unterbrechung des Informationsflusses zum Berliner Datenschutzbeauftragten bedauern wir, können aber heute im Zusammenhang mit der Überarbeitung und darauffolgenden Umsetzung des IT-Sicherheitsrahmenkonzeptes feststellen, daß sich der ITKAB nun dieser Aufgabe annimmt.

Diese Feststellung können wir so nicht teilen.

Die Anbindung des Grenznetzes des Berliner Verwaltungsnetzes an das Internet im LIT erfolgte im Einklang mit den dazu erarbeiteten Sicherheits- und Betriebskonzepten in einer mehrmonatigen und stufenweisen Erprobung. Diese Vorgehensweise wird im Bericht des Berliner Datenschutzbeauftragten auch positiv gewürdigt.

Es erhielten und erhalten vom LIT nur diejenigen Verwaltungen Zugang zum Grenznetz, die sich in einer Servicevereinbarung verbindlich und nachweisbar erklären, über entsprechende lokale Sicherheitskonzepte zu verfügen. Im Bedarfsfall unterstützt KISS auch die Verwaltung bei der Erstellung und Umsetzung dieser Konzepte.

60 Gestaffeltes Firewall-System, JB 1995, 4.1

| Bericht des Berliner Datenschutzbeauftragten | Stellungnahme des Senats |
|---|---|

durch Inbetriebnahme des *Grenznetzes* und Freischaltung für mehrere Bezirksämter und Senatsverwaltungen aufgehoben. Daß wir diesen aus datenschutzrechtlicher und sicherheitstechnischer Sicht sehr wichtigen Sachverhalt erst aus dem vom LIT veröffentlichten IT-Nachrichtenmagazin „Splitter“ erfahren haben, kann nicht mit organisatorischen Problemen bei der Umstrukturierung oder einer schnellen Marktpositionierung des LIT in seiner neuen Betriebsform begründet werden. Bevor eine Öffnung des MAN zum Internet realisiert wird, hätten einerseits die Erfüllung der Vorgaben aus den existierenden Datenschutz- und Datensicherheitskonzepten von einer zentralen Stelle überprüft und andererseits behörden- und verfahrensspezifische Konzepte erarbeitet oder vervollständigt werden müssen.

Darüber hinaus ist festzustellen, daß durch lokale Proxy-Server, die vom LIT auf den LAZ-Rechnern eingerichtet und administriert werden, eine wesentliche technische Sicherheitsmaßnahme für die lokale Domäne bereits als Dienst angeboten und realisiert wird. Diese Technologie war Bestandteil der Erprobungsstufe 2 der Grenznetzdienste und wurde im LIT im August 1997 erfolgreich abgeschlossen. Gleichzeitig wurde durch Überarbeitung und Anpassung der Arbeitsanweisung 2/97 zur Nutzung der Online-Dienste im LIT der organisatorisch-rechtliche Rahmen für die Nutzung dieser Grenznetzdienste geschaffen. Dieses auf dem Sicherheitskonzept des LIT für die Dienste des MAN beruhende Paket von technischen und organisatorischen Maßnahmen zur Netzsicherheit wurde und wird den Verwaltungen zur Anpassung und Nachnutzung angeboten und auch genutzt.

Ein weiterer wichtiger Aspekt ist die ständige Anpassung der Datenschutz- und Sicherheitskonzepte an neue Risiken und Gefahren. Analog der Virenschutzproblematik, die darin besteht, daß im Normallfall nur bekannte Viren erkannt und beseitigt werden können, neu auftretende jedoch erst in einer neuen Version der Virenscanner beachtet werden können, treten im Kommunikationsbereich ständig neue „Sicherheitslöcher“ auf, die von findigen „Hackern“ ausgenutzt werden. Daher muß der ständigen Beobachtung und Aktualisierung der Maßnahmen besondere Beachtung zukommen.

Die im Bericht angesprochene zentrale Überprüfungsstelle kann nicht vom LIT geschaffen werden, sondern ist auf der Ebene der Innenverwaltung/ITKAB einzurichten.

Ergänzend kann bemerkt werden, daß sich das Sicherheitsbewußtsein der Verwaltungen aus Sicht des LIT deutlich verbessert hat. Das kommt nicht zuletzt darin zum Ausdruck, daß sie vor dem Zugang zum Grenznetz eigene Sicherheitsmaßnahmen planen, mit dem LIT abstimmen und durchführen (z. B. eigene Firewall-Systeme).

Ein weiteres wichtiges Ziel muß die ständige Qualifikation der Netzwerk-, System- und insbesondere *Firewall-Administratoren* sein. Gerade im Bereich eines komplexen, gestaffelten Firewall-Systems bestimmt die fachliche Kompetenz der beteiligten Administratoren erheblich das Maß der möglichen Sicherheit mit.

Diese Anforderung ist bereits im Betriebskonzept Grenznetzdienste fixiert und wurde und wird durch spezielle Schulungen im Sicherheits- und Netzbereich realisiert.

Eine wesentliche Anforderung der Verwaltung ist die Möglichkeit, von außen auf das Verwaltungsnetz zugreifen zu können, zum Beispiel zum Zwecke der *Telearbeit* oder der *Fernadministration.* Die Erfüllung dieser Anforderungen stellt jedoch ein erhebliches Sicherheitsproblem dar, da hierfür auch die Kommunikation von unsicheren externen Netzen in das Verwaltungsnetz hinein möglich sein muß. Es muß daher unbedingt geprüft werden, inwieweit gesicherte Kommunikationspfade für einzelne spezielle Anforderungen geschaffen werden können. Jedoch auch bei Nutzung von solchen sicheren Kommunikationspfaden (sog. Tunneling-Verfahren) bleibt ein nicht unerhebliches Restrisiko bestehen.

Diese Forderung kann vom LIT nur unterstrichen werden. Die dazu von KISS angebotenen Dienste realisieren verschlüsselte Tunnel, derzeit unter Verwendung von ssh. In Vorbereitung sind Tunnel unter SSL. Gleichzeitig mit diesen Diensten werden Leistungen zur Sicherheitsvalidierung im LAN/WAN/Host-Bereich angeboten, die die sichere lokale Umgebung der Tunnelenden überprüfen.

Für den Anschluß des Verwaltungsnetzes an unsichere externe Netze, z. B. das Internet, muß weiterhin unverändert festgestellt werden, daß dieser nur dann vertretbar ist, wenn er einerseits auf die zwingend erforderlichen Kommunikationsbedürfnisse beschränkt wird und andererseits die Gefahren durch technische und organisatorische Maßnahmen beherrscht werden können und auch die Bereitschaft besteht, die dafür notwendigen Investitionen zu tragen. Eine hundertprozentige Sicherheit gegen Angriffe aus dem Internet kann jedoch auch bei Beachtung sämtlicher Maßnahmen nicht erzielt werden.

**Exemplarische IT-Projekte der Berliner Verwaltung**

Die Automatisierung einzelner Verwaltungsbereiche schreitet weiter fort, alte Systeme werden zunehmend durch neue ersetzt. Beispiele sind die folgenden Verfahren, denen wir besondere Aufmerksamkeit gewidmet haben.

Das Projekt „*Integrierte Personalverwaltungverfahren – IPV*“[61] befindet sich in diversen Bezirksämtern in der Erprobung. Für das Pilotbezirksamt Köpenick wurde ein Konzept zur Umsetzung der Datenschutz- und Datensicherungsmaßnahmen erarbeitet, zu dem wir nur in bezug auf einige Detailfragen Verbesserungen empfohlen haben. Für die Datenübertragung im MAN sind Verschlüsselungsverfahren vorgesehen, die den anerkannten Standards entsprechen. Offen bleibt jedoch noch, inwieweit unseren Empfehlungen bisher gefolgt wurde und die vereinbarte Verschlüsselung durchgängig zum Einsatz kommt.

Hinsichtlich des Schutzbedarfs im MAN und der lokalen Netze wurde bereits Ende 1997 eine Testumgebung zur Datenverschlüsselung unter Beteiligung der Firma SUN Microsystems geschaffen.

Der Praxistest soll aufzeigen, inwieweit alle Anwenderanforderungen abgedeckt werden können bzw. ob Restzweifel bestehen bleiben. Als kryptologische Verschlüsselungs-Verfahren werden Standards, wie DES, Triple DES und RSA, eingesetzt.

In Kürze sollen erste Ergebnisse zu den in den Bezirken installierten Piloten vorliegen. Nach Vorliegen der Ergebnisse wird das Projekt IPV umgehend den Einsatz der getesteten Verschlüsselungssoftware planen und diese dann auch einsetzen.

61 JB 1996, 4.4.1

| Bericht des Berliner Datenschutzbeauftragten | Stellungnahme des Senats |
|---|---|
| Das *„Berliner Automatisierte Sozialhilfe-Interaktions-System – BASIS“*, zu dem wir seit 1991 berichten, ist inzwischen in allen Bezirken eingeführt worden. Inzwischen ist bereits die Entwicklung eines Nachfolgeverfahrens BASIS II (auch unter der Bezeichnung BASIS 3000) bei einem Konsortium aus zwei Firmen auf der Grundlage eines umfassenden Pflichtenheftes in Auftrag gegeben worden, welches im Jahr 2000 eingeführt werden soll. Auch aus datenschutzrechtlicher Sicht werden dabei Erfahrungen mit Schwachstellen umzusetzen sein, die sich aus dem praktischen Betrieb des BASIS I-Verfahrens ergeben haben. | |
| Die Neukonzeption des *Automatisierten Haushaltswesens*[62] erfolgte mit dem Programmsystem PROFISKAL und ist mittlerweile in der Berliner Verwaltung weitgehend eingeführt worden. | Mit Stand 1. April 1998 sind 20 Bezirksverwaltungen, die Senatsverwaltung für Finanzen (als Pilotanwender für die Hauptverwaltung), das Abgeordnetenhaus von Berlin sowie Teile der Senatsverwaltungen für Inneres und Bauen, Wohnen, Verkehr an PROFISKAL angeschlossen. Die fehlenden Bezirke Tiergarten, Mitte und Hellersdorf werden noch in diesem Jahr den Echtbetrieb aufnehmen; die übrigen Teile der Hauptverwaltung werden bis spätestens zum 3. Quartal 1999 das Verfahren übernommen haben. |
| Im Bereich der Polizei wird bereits seit Jahren an der Nachfolge des veralteten Informationssystems Verbrechensbekämpfung (ISVB) gearbeitet. Zum Projekt *„Polizeiliches Landessystem zur Information, Kommunikation und Sachbearbeitung – POLIKS“*, welches dieses leisten soll, liegt jedoch bisher noch kein Feinkonzept vor. Das Projekt wird in Zusammenarbeit mit Brandenburg durchgeführt. | Zwischenzeitlich bemühen sich Brandenburg und Berlin um eine Entwicklungspartnerschaft mit der Polizei Sachsens. |
| Mit dem Projekt *DIBA – Datenerfassung in Berliner Abschnitten* – soll die Informationstechnik die tagtägliche formulargestützte Routinearbeit in den Berliner Polizei-Abschnitten und – unter dem Begriff DIBA-mobil – mit dem Einsatz mobiler IT-Systeme auch in den Funkstreifenwagen unterstützen. Das Verfahren wurde bereits 1994 in einem Abschnitt erprobt und soll jetzt eine wesentliche Grundlage für das neue Polizeikonzept „Berliner Modell“ bilden. Technische Schwierigkeiten haben Anfang 1998 zu beträchtlichem öffentlichem Aufsehen geführt, eine datenschutzrechtliche Überprüfung ist eingeleitet. | DiBA steht für „Datenverarbeitung in Berliner Abschnitten“. Das Sicherheitskonzept für das Teilprojekt DiBA-mobil (Formularschrank) liegt dem Berliner Datenschutzbeauftragten inzwischen vor. |
| Mit dem Projekt *BIDAVIS/FABIS – Bilddaten-Verarbeitungs- und Informationssystem/Fingerabdruck-Verarbeitungs- und Informationssystem* soll bei der Polizei die erkennungsdienstliche Behandlung modernisiert und deren Ergebnisse schneller und effektiver den ermittelnden Stellen zur Verfügung gestellt werden. | Dieses Projekt befindet sich in der Realisierungsphase für die Stufe 1 – BIDAVIS, sie wird noch in diesem Jahr in Betrieb genommen. |
| Die langjährigen Bemühungen zur Entwicklung eines neuen *IT-Verfahrens zur Abwicklung von Verkehrsordnungswidrigkeiten (BOWI II)* sind eingestellt worden, da das komplexe Verfahren von der mit der Umsetzung des Konzepts betrauten Firma nicht realisiert werden konnte. Nun wird ein privater Dienstleister gesucht, der das Verfahren im Rahmen einer „Public Private Partnership“ übernehmen soll. Die mit einem solchen Outsourcing in Verbindung stehenden datenschutzrechtlichen Fragen sind jedoch noch ungelöst. | Der Senat weist darauf hin, daß die Bestrebungen zur Einführung des Dialogverfahrens und der elektronischen Aktenhaltung unter Vernichtung der Originalakten bei der Berliner Bußgeldbehörde wieder aufgenommen wurden und umgesetzt werden sollen.<br>Die sich in diesem Zusammenhang ergebenden datenschutzrechtlichen Fragen sind in der Tat noch ungelöst; eine Umsetzung wird nur erfolgen, wenn die datenschutzrechtlichen Belange gewahrt sind. Die Klärung erfolgt durch und mit den zuständigen Verwaltungen sowie den Bundesministerien für Verkehr und Justiz sowie den anderen Bundesländern. |

## 3. Schwerpunkte im Berichtsjahr

### 3.1 Der Bürger im Netz der Sozialdatenverarbeitung

Im Mittelpunkt der öffentlichen Debatten über den Datenschutz in Berlin stand im vergangenen Jahr die Frage, ob der Datenschutz der Aufdeckung des Mißbrauchs von Sozialleistungen im Weg steht und ob nicht durch vermehrte Datenflüsse und eine Lockerung der einschlägigen Bestimmungen Abhilfe geschaffen werden könnte. Es ist zwar verständlich, daß in Zeiten leerer öffentlicher Kassen und hoher Arbeitslosigkeit verstärkt über eine Verhinderung des Mißbrauchs von Sozialleistungen durch intensivere staatliche Kontrollen nachgedacht wird. Hintergrund für diese Überlegungen ist allerdings weniger verläßliches

62 JB 1994, 4.4

Datenmaterial über den Umfang des Sozialleistungsmißbrauchs als vielmehr die teilweise reißerische Berichterstattung in den Medien über spektakuläre Einzelfälle (z. B. „Halbe Million abgezockt – Berlins größter Sozialbetrüger“).

Auch der *Bericht*, den der Senat dem Abgeordnetenhaus über *Maßnahmen gegen Leistungsmißbrauch*[63] vorgelegt hat, enthält kein Datenmaterial über eine Zunahme des Mißbrauchs von Sozialleistungen, er geht aber davon aus, daß Mißbrauch in erheblichem Umfang stattfindet. Der Bericht wirft grundlegende Fragen der *Informationsverarbeitung im Sozialstaat* auf, mit denen wir uns eingehend auseinandergesetzt haben.

Gerade der Sozialstaat muß bestrebt sein, eine mißbräuchliche Inanspruchnahme seiner Leistungen soweit wie möglich auszuschließen. Um dem Sozialleistungsmißbrauch effektiver begegnen zu können, hat vor allem der Bundesgesetzgeber in den vergangenen Jahren ein beträchtliches Arsenal von Befugnissen zum Datenabgleich geschaffen, das erst zum Teil auch in der Praxis umgesetzt worden ist. Dafür ist allerdings nicht der Datenschutz verantwortlich, sondern in erster Linie das zuständige Bundesministerium, das mehr als vier Jahre benötigt hat, um die entsprechenden bundesgesetzlichen Regelungen durch die notwendige Rechtsverordnung im Sozialhilfebereich zu ergänzen. Diese *Rechtsverordnung zum Abgleich von Sozialhilfedaten* ist am 1. Januar 1998 in Kraft getreten[64].

Jede Maßnahme zur Verhinderung von Leistungsmißbrauch hat sich an den gesetzlichen Rahmenbedingungen, insbesondere am seit 1976 bundesgesetzlich garantierten *Sozialgeheimnis*, zu orientieren. Dieses besondere Amtsgeheimnis, dessen Verletzung ebenso wie die ärztliche und anwaltliche Schweigepflicht, das Steuer- und das Statistikgeheimnis mit Strafe bedroht ist, hat gerade im Sozialstaat eine besondere Bedeutung. Wer – häufig ohne eigenes Verschulden – auf staatliche Unterstützung angewiesen ist und Sozialleistungen beantragt, muß in besonders weitgehendem Maße Informationen aus seinem persönlichen Leben preisgeben, damit die Sozialleistungsträger seine Berechtigung überprüfen können. Er ist zur Offenbarung dieser Daten im Sinne einer Obliegenheit verpflichtet. Faktisch unterliegt er einem *Offenbarungszwang*, weil er ohne staatliche Unterstützung kein menschenwürdiges Leben führen kann. Der Gesetzgeber hat deshalb gewissermaßen als Kompensation für eine weitgehende Offenlegungspflicht bezüglich der persönlichen Lebensumstände des Antragstellers eine gesteigerte Geheimhaltungspflicht des Sozialleistungsträgers in Form des Sozialgeheimnisses angeordnet. Nur wenn der hilfebedürftige Bürger sicher sein kann, daß seine Angaben vertraulich behandelt werden, wird er bereit sein, der Behörde Einblick in seine persönliche Lebenssituation zu ermöglichen. Das Sozialgeheimnis beruht daher unmittelbar auf dem *Verfassungsgebot*, die Menschenwürde und das Persönlichkeitsrecht hilfebedürftiger Bürger zu achten (Art. 1 und 2 Grundgesetz). Es ist zugleich wesentliche Voraussetzung dafür, daß die Sozialleistungsträger ihre Aufgaben erfüllen können.

Jede Erweiterung der Möglichkeiten zum Abgleich und zur Überprüfung von Informationen über Sozialleistungsempfänger ist deshalb an diesen verfassungsrechtlichen Grundsätzen zu messen. Schon die gegenwärtig vorhandenen gesetzlichen Möglichkeiten zum Datenabgleich und zur Vernetzung zwischen unterschiedlichen Sozialleistungsträgern und anderen Behörden drohen, das Sozialgeheimnis zunehmend auszuhöhlen. Eine vollständige Registrierung aller Sozialleistungsempfänger unabhängig von konkreten Anhaltspunkten für einen Leistungsmißbrauch z. B. in zentralen Dateien auf Landes- oder gar Bundesebene wäre mit dem Grundgesetz nicht vereinbar.

Schon seit 1995 hatte die *Konferenz der Arbeits- und Sozialminister der Länder (ASMK)* eine Arbeitsgruppe damit beauftragt zu prüfen, ob und in welchem Umfang im Bereich der Sozialleistungen „Verbesserungen“ des Datenaustausches notwendig seien. Die Vorschläge der Arbeitsgruppe haben die Datenschutzbeauftragten des Bundes und der Länder zu einer Entschließung[65] veranlaßt, in der gravierende Bedenken gegen eine pauschale Erweiterung des Datenaustausches geltend gemacht werden. An die

63 Drs 13/1622
64 BGBl. 1998 I, S. 103
65 Anlage 2.2

Stelle des bisher vorgesehenen abgestuften Verfahrens der Datenerhebung beim Antragsteller oder Empfänger von Sozialleistungen und unter bestimmten Voraussetzungen auch bei Dritten sollen Verfahren der Datenerhebung insbesondere durch automatisierten Datenabgleich treten, die schwerwiegend in die Rechte der Betroffenen eingreifen, ohne daß geprüft wird, ob weniger weitreichende Eingriffe in das Persönlichkeitsrecht der Betroffenen zum gleichen Erfolg führen können. Die Datenschutzbeauftragten sind nicht prinzipiell gegen Erweiterungen des Datenaustausches, befürworten aber die Einführung von Verfahren des automatisierten Datenabgleichs nur bei Anhaltspunkten für Mißbrauchsfälle in nennenswertem Umfang. Zugleich müssen neue Datenabgleichsverfahren hinsichtlich ihrer *Wirkung* bewertet werden, um Aufwand und Nutzen zueinander in das verfassungsrechtlich gebotene Verhältnis zu setzen. Insbesondere dürfen anlaßunabhängige Mißbrauchskontrollen nur in ganz begrenzten und konkretisierten Ausnahmefällen zugelassen werden. Pauschale und undifferenzierte Datenerhebungen ohne Beteiligung des Betroffenen und ohne Anlaß sind grundsätzlich abzulehnen. Eine pauschale Auskunftsverpflichtung Dritter (z. B. der Banken und Lebensversicherungen), wie sie von der ASMK-Arbeitsgruppe vorgeschlagen wurde, kann dazu führen, daß der Sozialleistungsträger von vornherein hinter dem Rücken des Betroffenen sofort an Banken oder Lebensversicherungen herantritt und den Betroffenen damit in zweifacher Hinsicht desavouiert: Die Tatsache, daß Sozialleistungen beantragt sind, wird offenbart und mit dem Eindruck verknüpft, der Antragsteller habe seine Vermögensverhältnisse verheimlicht. Es muß bei dem *Grundsatz* bleiben, daß der Sozialleistungsträger in erster Linie *den Betroffenen selbst zu befragen* hat und erst dann unmittelbare Anfragen an Dritte richten darf, wenn die Ermittlungen unter Mitwirkung des Betroffenen ergebnislos geblieben sind und Anhaltspunkte dafür bestehen, daß dieser Informationen zurückgehalten hat.

Die Datenschutzbeauftragten haben betont, daß sie sich nicht gegen einzelne Veränderungen der Datenverarbeitung im Sozialleistungsbereich wenden, soweit sie tatsächlich erforderlich und verhältnismäßig sind, und sie haben ihre Gesprächsbereitschaft dazu erklärt. Dieses Gesprächsangebot ist von der Arbeits- und Sozialministerkonferenz im Oktober 1997 aufgegriffen worden, die die Bundesregierung gebeten hat, die erforderlichen Schritte zur Realisierung eines Datenaustausches in die Wege zu leiten und dabei das Gesprächsangebot der Datenschutzbeauftragten zu berücksichtigen.

Seit Juni 1993 enthält das *Bundessozialhilfegesetz* (BSHG) die Befugnis für einen Datenabgleich zwischen der Bundesanstalt für Arbeit, den Rentenversicherungsträgern, den Unfallversicherungsträgern, den Sozialhilfeträgern und bestimmten öffentlichen Stellen des Landes Berlin wie dem Landeseinwohneramt, den Standesämtern, den Wohnungsämtern, den Energie- und Versorgungsbetrieben und der Kraftfahrzeug-Zulassungsstelle. Bezüglich des Datenabgleichs unter den beteiligten Sozialleistungsträgern konnte diese Befugnis bisher nicht ausgeschöpft werden, weil die entsprechende Rechtsverordnung erst Anfang 1998 in Kraft getreten ist. Für den bezirksübergreifenden Datenabgleich zwischen den Sozialämtern im Rahmen des *Berliner Automatisierten Sozialhilfe-Interaktions-Systems (BASIS)* wurde auf unsere Empfehlung hin das Ausführungsgesetz zum Bundessozialhilfegesetz um eine entsprechende Befugnis ergänzt[66]. Diese Regelung machte auch den *Datenabgleich zwischen den Berliner Sozialämtern* von der noch ausstehenden Rechtsverordnung des Bundes zu § 117 BSHG abhängig. Diese – inzwischen in Kraft getretene – Rechtsverordnung enthält allerdings keinerlei Vorschriften, die sinnvollerweise auf den Datenabgleich innerhalb Berlins anzuwenden wären. Insbesondere sieht die Bundesverordnung nicht die Schaffung einer „*Kopfstelle*“ im Land Berlin vor, die der Senat zunächst für erforderlich gehalten hatte. „Kopfstelle“ für den Datenabgleich nach § 117 Abs. 1 und 2 BSHG ist vielmehr bundeseinheitlich die Datenstelle der Rentenversicherungsträger in Würzburg. Die Einrichtung einer „Kopfstelle“ oder einer *Berliner „Sozialhilfe-Zentralkartei“* ist auch nicht erforderlich, um das vom Abgeordnetenhaus angestrebte Ziel zu erreichen, nämlich festzustellen, ob Bürger von mehr als einem Berliner Sozialamt Sozialhilfe empfangen.

66 JB 1994, 4.11

| Bericht des Berliner Datenschutzbeauftragten | Stellungnahme des Senats |
|---|---|
| Wir haben uns deshalb mit der Senatsverwaltung für Gesundheit und Soziales grundsätzlich darauf verständigt, daß der jetzt im Rahmen der Einführung des neuen Verfahrens BASIS II geplante Datenabgleich zwischen den Sozialämtern in Berlin so realisiert werden soll, daß der Landesbetrieb für Informationstechnik auf einem hierzu gewidmeten Server im *Auftrag der Bezirksämter* logisch getrennte Dateien der Sozialhilfeempfänger führt und auf Anfrage eines Bezirksamts jeweils einen Abgleich mit den Dateien der 22 anderen Bezirke durchführt. Der Abgleich soll im Auftrag der Bezirksämter stattfinden, eine Nutzung über den Abgleich hinaus ist nur auf einzelne Weisung des jeweils zuständigen Bezirksamts zulässig. Der *Landesbetrieb für Informationstechnik* wird damit nicht zu einer eigenen datenverarbeitenden Stelle dieser sensiblen Sozialdaten. Datenschutzrechtlich verantwortlich für „ihre" Sozialhilfedateien bleiben die Bezirke. Auch die Weiterleitung der nach dem Bundessozialhilfegesetz in den bundesweiten Datenabgleich einzubeziehenden Datensätze an die „Kopfstelle" in Würzburg oder ein Abgleich von Daten mit anderen Berliner Behörden oder Versorgungsunternehmen nach § 117 Abs. 3 BSHG würde jeweils dateiweise im Auftrag der Bezirksämter durch den Landesbetrieb für Informationstechnik durchgeführt. | Für BASIS II sind die Ausführungen im Bericht korrekt, dieser Abgleich befindet sich zur Zeit allerdings erst in Vorbereitung/ Erprobung im Rahmen des technischen Piloten für BASIS II. |
| Wie jeder Datenabgleich bedarf auch der bezirksübergreifende Abgleich von Sozialhilfedaten einer besonderen Rechtsgrundlage. Die Senatsverwaltung für Gesundheit erarbeitet deshalb gegenwärtig den Entwurf einer Neufassung des Ausführungsgesetzes zum Bundessozialhilfegesetz und einer entsprechenden Rechtsverordnung. Dazu haben wir bereits detaillierte Empfehlungen gegeben. | Für die Aufgabe „Bundesweiter Automatisierter Datenabgleich Sozialhilfe" fungiert der LIT als „Zentrale Landesstelle" im Auftrag der Geschäftsstelle BASIS für das Land Berlin.<br>Das heißt, daß von max. 47 Bezirksstellen (23 LAZ-Servern) Anfragedateien – zur Zeit aus dem Verfahren BASIS I – übernommen und diese nach Verdichtung als ein Datenbestand an den VDR Würzburg übersandt werden. Im Ergebnis des Abgleichs werden eine Ergebnisdatei und gegebenenfalls eine Fehlerdatei vom VDR Würzburg an den LIT übersandt, hier dann separiert und an die ursprünglichen Absender elektronisch verteilt. Die Technologie der Schnittstelle VDR Würzburg – LIT ist durch die Kopfstelle in Würzburg vorgegeben und durch die Sozialhilfedatenabgleichsverordnung – SozhiDAV vom 21. Januar 1998 geregelt. |
| Der bundesrechtlich vorgesehene Datenabgleich betrifft ausschließlich Personen, die bereits Sozialhilfe beziehen, nicht jedoch auf *Antragsteller* vor dem erstmaligen Sozialhilfebezug. Es besteht Einvernehmen mit der Senatsverwaltung für Gesundheit und Soziales, daß Antragsteller erst nach einer entsprechenden Gesetzesänderung in den bundesweiten Datenabgleich einbezogen werden dürfen[67]. Demgegenüber haben wir einem weitergehenden bezirksübergreifenden Datenabgleich auf landesrechtlicher Grundlage innerhalb Berlins zugestimmt, in den auch Antragsteller einbezogen werden. Allerdings wird auch bei der Durchführung dieses Datenabgleichs der *Grundsatz der Verhältnismäßigkeit* zu beachten sein, wie der Senat in seinem Bericht über Maßnahmen gegen Leistungsmißbrauch zu Recht hervorgehoben hat[68] . Der Abgleich von Sozialdaten darf nicht routinemäßig und ohne *Prüfung der Erforderlichkeit* bei einzelnen Hilfeempfängern oder Gruppen von Hilfeempfängern stattfinden. | Datenschutztechnisch sieht diese eine kryptographierte Übertragung der Daten vor, die Verschlüsselung erfolgt im Public-key-Verfahren. Darüber hinaus werden dem VDR nur anonymisierte Aktenzeichen im Datensatz übergeben, die dort keinen Rückschluß auf das originale Aktenzeichen zulassen.<br>Die Übertragung von und nach den LAZ-Servern der Bezirksstellen erfolgt ebenfalls verschlüsselt. Eine detaillierte Risikoanalyse für diese Datenübertragung wird derzeit im LIT erarbeitet. |
| In den bezirksübergreifenden Datenabgleich sollen auch die *Daten von Asylbewerbern* einbezogen werden, soweit sie Leistungen nach dem Asylbewerberleistungsgesetz des Bundes beantragen. Dies ist auf Grund einer Änderung der bundesrechtlichen Grundlagen möglich. Auch hier wird an ergänzenden Ausführungsbestimmungen des Landes Berlin gearbeitet.<br>Allerdings weist der Senat in seinem Bericht zu Recht darauf hin, daß dieser regelmäßige automatisierte Datenabgleich nicht zur Erkennung gefälschter Personaldokumente führt (II.3, S. 7 des Berichts). Leistungserschleichungen durch sogenannte Mehrfachidentitäten lassen sich nach Überzeugung des Senats nur durch erkennungsdienstliche Maßnahmen verhindern. | |
| Bereits jetzt ist die *erkennungsdienstliche Behandlung von Asylbewerbern* bundesrechtlich vorgeschrieben (§ 16 Abs. 1 Asylverfahrensgesetz – AsylVfG). Die Datenschutzbeauftragten des Bundes und der Länder haben sich schon 1992 gegen dieses Verfahren gewandt[69], da eine erkennungsdienstliche Behandlung von Asylbewerbern, deren Identität bereits zweifelsfrei feststeht, sowie die nahezu unbeschränkte Nutzung der Ergebnisse der erkennungsdienstlichen Behandlung zu Zwecken der Strafverfolgung (§ 16 Abs. 5 AsylVfG) mit dem Menschenbild des Grundgesetzes und der Europäischen Menschenrechtskonvention kaum vereinbar sind. Dies gilt in gleicher Weise für die Überlegungen, künftig alle Bürgerkriegsflüchtlinge erkennungsdienstlich zu behandeln und das Ausländergesetz entsprechend zu ändern. | Es ist richtig, daß der Bundesgesetzgeber im Ausländer- und Asylverfahrensrecht Regelungen geschaffen hat, die die erkennungsdienstliche Behandlung ermöglichen oder für bestimmte Personengruppen zwingend vorschreiben. Überholt ist dagegen die Behauptung, es bestünden „Überlegungen künftig alle Bürgerkriegsflüchtlinge erkennungsdienstlich zu behandeln und das Ausländergesetz entsprechend zu ändern". In diesem Punkt berücksichtigt der Bericht vom 31. Dezember 1997 nicht die seit 1. November 1997 geltende Rechtslage.<br>Der Gesetzgeber hat mit der Änderung des Ausländergesetzes vom 29. Oktober 1997 (BGBl. I, 2584) den § 41 a in das Ausländergesetz eingefügt. Danach ist die Identität eines Ausländers aus einem Kriegs- oder Bürgerkriegsgebiet, der das 14. Lebensjahr vollendet hat, durch erkennungsdienstliche Maßnahmen zu sichern, sofern ihm eine Aufenthaltsbefugnis nach § 32 oder § 32 a oder eine Duldung nach § 54 erteilt wird oder seine Zurückweisung oder Abschiebung in Betracht kommt. |

67 Mitteilung – zur Kenntnisnahme – über Maßnahmen gegen Leistungsmißbrauch, Drs 13/1622, S. 5
68 Drs 13/1622, S. 5
69 JB 1992, Anlage 2.3; siehe auch JB 1996, 3.1

| Bericht des Berliner Datenschutzbeauftragten | Stellungnahme des Senats |
|---|---|

Überdies weist der Senat selbst zutreffend darauf hin, daß eine flächendeckende erkennungsdienstliche Behandlung dieser Personenkreise allein zur Unterbindung des Unterstützungsbetrugs durch Mehrfachidentitäten nicht ausreicht, wenn nicht alle Sozialämter untereinander und mit einer zentralen Fingerabdruckdatei z. B. des Bundeskriminalamts vernetzt sind.

Ein Sozialstaat, in dem jedem Antragsteller und Bezieher von Sozialleistungen, sei er Ausländer oder Deutscher, eine mögliche Betrugsabsicht unterstellt wird und deshalb seine Angaben zusammen mit einer sonst nur in strafrechtlichen Ermittlungsverfahren üblichen Form der Identitätsfeststellung in einer zentralen Datei auf Landes- oder Bundesebene gespeichert würden, wäre nicht mehr der Sozialstaat des Grundgesetzes.

Im Zusammenhang mit dem Sozialleistungsmißbrauch wird bereits seit Jahren die *Forderung der Polizei*, aber auch der *Ausländerbehörde* und anderer Behörden diskutiert, vom Sozialamt eine Mitteilung zu erhalten, wenn Personen, die einer Straftat verdächtig sind, sich im Sozialamt aufhalten oder dort demnächst erscheinen. Im Bericht des Senats über die Entwicklung des Datenschutzes („Gibt es ein Spannungsfeld zwischen informationellem Selbstbestimmungsrecht und schutzwürdigen Belangen der Allgemeinheit?“)[70] wird sogar die Behauptung aufgestellt, der besondere Schutz der Sozialdaten erschwere Strafermittlungen, aber auch die Verhütung von Straftaten in der Praxis erheblich. Konkrete Fälle, die diese Behauptung stützen könnten, nennt der Bericht allerdings nicht.

Das Sozialgeheimnis gilt nicht ausnahmslos. Der Bundesgesetzgeber hat bereits 1976 detaillierte und präzise Regelungen darüber erlassen, in welchen Fällen und unter welchen Voraussetzungen Sozialdaten von den Sozialleistungsträgern unter anderem auch zur Unterbindung des Unterstützungsbetrugs oder für andere Strafverfolgungsmaßnahmen übermittelt werden dürfen (vgl. insbesondere §§ 69 Abs.1 Nr. 1, 2; 73 Sozialgesetzbuch – SGB X). Diese Regelungen sind geeignet, dem Leistungsmißbrauch wirksam zu begegnen. Der Senat teilt diese Auffassung nicht und hat die bezirklichen Sozialämter dazu verpflichtet, auch über das bundesrechtlich zulässige Maß hinaus Sozialdaten zu übermitteln.

Dabei geht es nicht um ein Problem des Leistungsmißbrauchs. Dieser wird von den Sozialämtern bereits bekämpft, die technischen und rechtlichen Möglichkeiten dazu werden – wie oben ausgeführt – ständig erweitert. Bei dem strittigen Komplex geht es dagegen um die grundsätzliche Frage, unter welchen Voraussetzungen die Sozialämter Mitteilungen über Deutsche und Ausländer nach außen geben dürfen, die wegen *anderer* Straftaten gesucht werden. Diese beiden Fragenkomplexe werden in der öffentlichen Diskussion zu häufig vermengt.

In zwei *Gemeinsamen Rundschreiben vom 2. Januar 1997 und 14. Februar 1997*[71] haben die Senatsverwaltungen für Gesundheit und Soziales, für Schule, Jugend und Sport sowie für Inneres die Bezirksämter aufgefordert, den gegenwärtigen Aufenthalt und den *nächsten Vorsprachetermin eines Hilfeempfängers* im Sozialamt der Polizei, den Staatsanwaltschaften und Gerichten, den Ordnungsbehörden und den Justizvollzugsanstalten mitzuteilen, wenn der Betroffene einer Straftat beschuldigt oder deswegen bereits verurteilt ist und gegen ihn ein Haftbefehl vorliegt. Bei Ausländern, die sich illegal in der Bundesrepublik aufhalten oder gegen eine räumliche Beschränkung verstoßen, soll die Ausländerbehörde generell informiert werden. Hinsichtlich der Meldepflicht gegenüber der Ausländerbehörde sind die Bezirke darüber hinaus in einer Allgemeinen Anweisung des Senats verpflichtet worden, entsprechend dem Rundschreiben zu verfahren.

Beide Rundschreiben und die Allgemeine Anweisung stehen *im Gegensatz zu geltendem Bundesrecht.* Das Sozialgesetzbuch (§ 68 Abs. 1 SGB X) legt einen abschließenden Katalog von Informationen über Sozialhilfeempfänger bzw. -antragsteller fest, die ohne richterliche Anordnung an die genannten Behörden übermittelt werden dürfen. Der momentane oder wiederkehrende Aufenthalt im Sozialamt gehört nicht dazu. Die Auslegung des Senats, der den momentanen oder zukünftigen Aufenthaltsort mit dem im Gesetz genannten Begriff der „Anschrift“ gleichsetzt,

Nach der Begründung des Gesetzes soll die erkennungsdienstliche Behandlung vor allem der Vermeidung von Mißbrauch, insbesondere von mehrfachem Leistungsbezug, dienen. Entgegen den Ausführungen des Datenschutzbeauftragten sind die genannten Vorschriften zur Vermeidung von Mißbrauch auch geeignet und verhältnismäßig.

Es liegt in der Natur der Sache, daß Flüchtlinge häufig über keine Ausweisdokumente verfügen. Nur wenn die gesamte Gruppe von Flüchtlingen erkennungsdienstlich behandelt wird, sind Mehrfachantragsteller, die bei verschiedenen Ausländerbehörden vortragen, ohne Dokumente geflohen zu sein, und mit den dort ausgestellten fälschungssicheren Dokumenten bei verschiedenen Sozialleistungsträgern Leistungen beantragen, durch die Ausländerbehörden zu erkennen.

Nach Auffassung des Senats findet die Mitteilung des momentanen sowie des wiederkehrenden Aufenthalts in einer Sozialbehörde in § 68 Abs. 1 SGB X und § 71 Abs. 2 SGB X i. V. m. § 76 Abs. 2 AuslG eine ausreichende Rechtsgrundlage, ohne daß es einer richterlichen Anordnung nach § 73 Abs. 1 und 3 SGB X bedarf.

Wenngleich das zitierte Urteil des Kammergerichts, auf das sich die Rechtsauffassung des Senats im wesentlichen gründet, vor der Entscheidung des Bundesverfassungsgerichts zur Volkszählung ergangen ist, so hält die Präsidentin des Kammergerichts doch nach wie vor an der darin vorgenommenen Auslegung des Begriffs „Anschrift“ im Sinne des momentanen Aufenthalts in § 68 Abs. 1 SGB X fest. Nach Auffassung des Senats ist aber auch der wiederkehrende Aufenthalt ein – zukünftig – momentaner Aufenthalt.

Die Senatsverwaltung für Justiz, die bei der Erarbeitung der Gemeinsamen Rundschreiben vom 2. Januar 1997 (entspricht der Allgemeinen Anweisung vom 13. Mai 1997) und vom 14. Februar 1997 beratend zur Seite stand, hat zu dem Vorschlag des Berliner Datenschutzbeauftragten, im Formular für die Anordnung eines Haftbefehls durch den Richter eine gesonderte Rubrik für die Anordnung der Übermittlung von Sozialdaten nach § 73 SGB X vorzusehen, die gerichtliche und staatsanwaltliche Praxis befragt. Im Rahmen dieser Befragung hat die Präsidentin des Kammergerichts darauf hingewiesen, daß angesichts der Rechtsprechung des Kammergerichts derjenige, der sich an eine von den o. g.

70 Drs Nr. 13/1148 und 13/1423
71 Beide Rundschreiben im Dienstblatt Teil IV, S. 19 ff.

überschreitet die Grenzen des Gesetzeswortlauts. Zwar hat das Berliner Kammergericht in einem Urteil vom 26. Mai 1983[72], also vor der Entscheidung des Bundesverfassungsgerichts zur Volkszählung, in einem besonderen Einzelfall die Auffassung vertreten, daß der momentane Aufenthalt als „Minus“ im Begriff der „Anschrift“ enthalten sei. Der Berliner Datenschutzbeauftragte hält diese Entscheidung auf Grund der besonderen Umstände des Einzelfalls nicht für verallgemeinerungsfähig und bekräftigt seine Rechtsauffassung, daß die Mitteilung des Umstands, daß ein von der Polizei gesuchter Sozialhilfeempfänger sich im Sozialamt aufhält, nur unter den im Sozialgesetzbuch formulierten Voraussetzungen zulässig ist: Die Übermittlung dieser vom Sozialgeheimnis geschützten Information muß zur Durchführung eines Strafverfahrens wegen eines Verbrechens oder einer sonstigen Straftat von erheblicher Bedeutung erforderlich sein, *und sie muß vom Richter angeordnet sein* (§ 73 Abs. 1 und 3 SGB X). Auf Grund der Entscheidung des Kammergerichts sieht der Berliner Datenschutzbeauftragte allerdings davon ab, entsprechende Meldungen über den momentanen Aufenthaltsort einer gesuchten Person an die Polizei förmlich zu beanstanden.

Dagegen kann die *Übermittlung des nächsten Vorsprachetermins* eines gesuchten Sozialhilfeempfängers an die Polizei ohne richterliche Anordnung nicht hingenommen werden. Der bundesrechtliche *Richtervorbehalt* wird durch das vom Senat den Bezirksämtern vorgeschriebene Verfahren, bereits bei Vorliegen eines Haftbefehls gegen die gesuchte Person deren nächsten Vorsprachetermin bekanntzugeben, umgangen. Das gilt auch für die besonderen Übermittlungen, die der Senat den Sozialämtern bei Ausländern vorgeschrieben hat. Der über § 71 Abs. 2 S. 1 Nr. 2 SGB X anwendbare § 76 Abs. 2 Ausländergesetz (AuslG) sieht keine Übermittlungsbefugnis für den nächsten Vorsprachetermin vor. Der Bundesgesetzgeber hat für den Fall, daß es nicht um ein sozialrechtlich relevantes Strafverfahren geht (z. B. wegen Unterstützungsbetrugs), die Entscheidung über eine Übermittlung von Sozialdaten für Zwecke eines Strafverfahrens mit guten Gründen daran geknüpft, daß ein Richter die Frage beurteilt, inwieweit diese Sozialdaten tatsächlich zur Durchführung des Strafverfahrens erforderlich sind. Diese Beurteilung hält der Senat offensichtlich für überflüssig; er will statt dessen den Sicherheitsbehörden ermöglichen, „auf dem kurzen Dienstweg“ diese vom Sozialgeheimnis geschützte Information zu erhalten.

Der Berliner Datenschutzbeauftragte hat zu der kontrovers diskutierten Frage, unter welchen Bedingungen Mitarbeiter der Sozialämter anderen Behörden und insbesondere der Polizei davon Mitteilung machen dürfen, daß sich eine gesuchte Person im Sozialamt zum Empfang von Sozialleistungen aufhält, einen *praktikablen Vorschlag* gemacht, der den Richtervorbehalt berücksichtigt, allerdings bisher in der Praxis nicht umgesetzt wurde. Der Datenschutzbeauftragte hat bereits vor Jahren angeregt, daß im Formular für die Anordnung eines Haftbefehls durch den Richter eine gesonderte Rubrik für die Anordnung der Übermittlung von Sozialdaten nach § 73 SGB X vorgesehen werden sollte. Auf diese Weise würden sowohl die Staatsanwaltschaft bereits bei der Beantragung eines Haftbefehls als auch der Richter bei der Entscheidung über diesen Antrag mit der Frage konfrontiert, ob die Übermittlung von Sozialdaten erforderlich sein könnte.

Mit seiner Auffassung, daß die Übermittlung des nächsten Vorsprachetermins ohne richterliche Anordnung und unabhängig von der Schwere der Straftat zu beanstanden ist, steht der Berliner Datenschutzbeauftragte keineswegs allein. Auch der Bayerische Landesbeauftragte für den Datenschutz, der im Berichtsjahr den Vorsitz in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder führte, hat entsprechende Verwaltungsvorschriften der Bayerischen Staatsregierung, in denen die Übermittlung des nächsten Vorsprachetermins angeordnet wurde, als datenschutzwidrig beanstandet. Nach Auffassung des Bayerischen Landesbeauftragten, die wir teilen, wird dadurch eine völlig neue Dimension der Einbeziehung von Sozialämtern in polizeiliche Fahndungen eröffnet.

Es ist vor dem Hintergrund des Sozialgeheimnisses weder akzeptabel noch erforderlich, daß die *Sozialämter* gewissermaßen *zum verlängerten Arm der Polizei* gemacht werden. Der Bundes-

Rundschreiben und Anweisungen abweichende Regelung hält, dem Vorwurf der (versuchten) Strafvereitelung ausgesetzt sein könnte.

Die Senatsverwaltung für Justiz hat im Einvernehmen mit der Präsidentin des Kammergerichts von einer Annahme des Vorschlags des Berliner Datenschutzbeauftragten abgeraten. Der Senat folgt dieser Empfehlung.

Aus Sicht des Senats sind die schutzwürdigen Belange der Betroffenen in ausreichendem Maße berücksichtigt. Im Rundschreiben zur Übermittlung von Sozialdaten gem. §§ 68 ff. SGB X ist geregelt, daß Sozialdaten nicht übermittelt werden dürfen, wenn Grund zur Annahme besteht, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden. Bei der Prüfung der schutzwürdigen Belange des Betroffenen – dabei kann es sich um persönliche, soziale oder wirtschaftliche Gründe handeln – ist auf den Einzelfall abzustellen. Allein das Interesse, von der Strafverfolgung verschont zu bleiben, ist nicht schutzwürdig.

In der Allgemeinen Anweisung über die Übermittlung von Sozialdaten an die Berliner Ausländerbehörde gem. § 71 Abs. 2 SGB X i. V. m. § 76 Abs. 2 AuslG wird die Übermittlungspflicht ebenfalls durch die Beachtung der schutzwürdigen Belange eingeschränkt. Allerdings ist die Fortsetzung des unrechtmäßigen Aufenthalts nicht schutzwürdig. Soweit der Ausländer aus persönlichen oder tatsächlichen Gründen nicht abgeschoben werden kann, insofern also schutzwürdig ist, prüft dies die Ausländerbehörde gem. §§ 51 bis 55 AuslG. Liegen solche Gründe vor, wird eine Duldung erteilt, und es liegt kein unrechtmäßiger Aufenthalt vor.

Des weiteren ist die praktische Bedeutung der Allgemeinen Anweisung im Bereich des Ausländerrechts im Gegensatz zur Behauptung des Berliner Datenschutzbeauftragten sehr wohl erheblich. Zwischenzeitlich wird die allgemeine Anweisung mit Ausnahme der Bezirke Charlottenburg, Friedrichshain, Kreuzberg, Lichtenberg, Pankow und Treptow von allen Bezirksämtern umgesetzt. Auf Grund dessen wurden der Ausländerbehörde in einer Vielzahl von Fällen der unerlaubte Aufenthalt von Ausländern, die bei den Sozialämtern vorsprechen, mitgeteilt. So ergab die Auswertung einer ausländerbehördlichen Statistik, daß zwischen Juli 1997 und Februar 1998 1 346 Datensätze übermittelt wurden. Soweit die Daten aus den sechs oben genannten Bezirken stammten, wurde in der Regel der nächste Vorsprachetermin nicht angegeben. Dennoch konnten auf Grund der Datenübermittlung in 12 Fällen die Abschiebungen bereits vollzogen und in 82 weiteren Fällen auf Grund der erfolgten Datenübermittlung aufenthaltsbeendende Maßnahmen eingeleitet werden. Darüber hinaus ist abzusehen, daß die Ausländerbehörde in einer Vielzahl von Fällen zum gegebenen Zeitpunkt, d. h. beispielshalber nach Bestätigung der Betroffenen zur Rückführung oder nach Abschluß noch anhängiger Klageverfahren, auf die übermittelten Daten zurückgreifen wird, um die gebotene Abschiebung durchzuführen.

Die Rechtslage soll durch bundesgesetzliche Änderung des § 68 SGB X (im Rahmen des Ersten Gesetzes zur Änderung des Medizinproduktegesetzes, BR-Drucks. 247/98) klargestellt werden. Eine entsprechende Gesetzesinitiative hat das Bundesministerium für Gesundheit noch in dieser Legislaturperiode bereits initiiert. Die abschließende Beratung im Gesundheitsausschuß des Bundestages findet voraussichtlich am 27. Mai 1998 statt. Die Beratung im Bundesrat wird voraussichtlich im Juni 1998 erfolgen.

72 (3) Ss 314/82 (10/83), Juristische Rundschau 1985, 24 ff.

gesetzgeber hat angemessene und ausreichende Regeln über die Weitergabe von Sozialdaten zum Zweck der Strafverfolgung getroffen, die in der Praxis umgesetzt werden sollten.

Der Berliner Datenschutzbeauftragte hat seine Rechtsauffassung im Vorfeld des Erlasses der Rundschreiben vom Januar und Februar 1997 wiederholt und nachhaltig gegenüber den beteiligten Senatsverwaltungen geltend gemacht, ohne daß diese berücksichtigt worden wäre. Nach dem Erlaß des Gemeinsamen Rundschreibens vom Januar 1997 über die Übermittlung von Sozialdaten an die Ausländerbehörde haben wir die Bezirksämter über unsere Rechtsauffassung informiert und angekündigt, daß jede darüber hinausgehende Übermittlung von Sozialdaten, insbesondere die Bekanntgabe des nächsten Vorsprachetermins, zu beanstanden ist. Wir haben außerdem auf die mögliche Strafbarkeit einer solchen Informationsweitergabe nach dem Sozialgesetzbuch (§ 85 SGB X) hingewiesen. Dies hat der Senat in der irrigen Annahme kritisiert, der Berliner Datenschutzbeauftragte sei darauf beschränkt, sich an die Landesregierung oder das Abgeordnetenhaus zu wenden, wenn seine Empfehlungen in Rundschreiben des Senats nicht berücksichtigt werden[73]. Richtig ist vielmehr, daß die Sozial- und Jugendämter der Bezirke die Verantwortung für die Zulässigkeit der Übermittlung von Sozialdaten tragen und der Berliner Datenschutzbeauftragte etwaige Beanstandungen bei unzulässigen Datenübermittlungen an die Bezirksämter zu richten (§ 26 Abs. 1 Nr. 2 BlnDSG) oder über die Rechtslage zu informieren und zu beraten hat (§ 24 Abs. 1 BlnDSG). Es gehört zu unseren Aufgaben, die datenverarbeitenden Stellen auf mögliche Datenschutzverstöße und sein Beanstandungsrecht (bei nicht unerheblichen Verstößen ist er sogar zur Beanstandung verpflichtet) sowie mögliche strafrechtliche Folgen bei unzulässiger Datenverarbeitung hinzuweisen.

Durch die Rundschreiben und Anweisungen werden die Bezirksämter zu einer Verfahrensweise veranlaßt, die mit der Fürsorgepflicht gegenüber ihren Bediensteten nur schwer zu vereinbaren ist, da sie diese der Gefahr strafrechtlicher Ermittlungen aussetzen.

Die praktische Bedeutung solcher Fälle dürfte jedenfalls im Bereich des Ausländerrechts sehr begrenzt sein, denn nach Angaben der Sozialämter kommt es äußerst selten vor, daß ein Ausländer, der sich illegal in der Bundesrepublik aufhält, zum Sozialamt geht, um seinen – bestehenden – Anspruch auf Hilfe zum Lebensunterhalt geltend zu machen.

### 3.2 „Spannungsbericht“

Auf Antrag der Fraktionen der CDU und der SPD[74] hat das Abgeordnetenhaus am 10. April 1997 beschlossen, daß der Senat einen Bericht erstellen und mit einer Stellungnahme des Datenschutzbeauftragten versehen soll, in dem insbesondere für den Bereich der Kriminalitätsbekämpfung dargestellt wird, ob und ggf. in welchen Fällen ein *Spannungsfeld zwischen Datenschutz und schutzwürdigen Belangen der Allgemeinheit* besteht und welche Schlußfolgerungen daraus zu ziehen sind.

Der Bericht des Senats beginnt mit dem zutreffenden Hinweis, daß der Schutz des informationellen Selbstbestimmungsrechts der Bürger nach dem Grundgesetz und der Verfassung von Berlin *grundrechtliche Qualität* hat. Die im Beschluß des Abgeordnetenhauses zum Ausdruck gebrachte Antithese („Spannungsfeld“) zwischen Datenschutz und schutzwürdigen Belangen der Allgemeinheit ist insofern irreführend, als hierdurch der Eindruck erweckt wird, der Datenschutz gehöre nicht zu den schutzwürdigen Interessen der Allgemeinheit. Der Senat weist zu Recht darauf hin, daß die Gesetze, die dem Schutz der personenbezogenen Daten des Einzelnen dienen, gerade auch im öffentlichen Interesse erlassen worden sind.

Aus verfassungsrechtlicher Sicht ist hier zu ergänzen, daß das Bundesverfassungsgericht den *Datenschutzbeauftragten* in Bund und Ländern eine wichtige Funktion im Interesse eines vorgezogenen Rechtsschutzes für die Bürger zugewiesen hat, von

73 Mitteilung – zur Kenntnisnahme – über Maßnahmen gegen Leistungsmißbrauch, Drs 13/1622, S. 4

74 Drs 13/1148; Drs 13/1423 mit geändertem Vorlagedatum für den Bericht

deren Erfüllung der effektive Schutz des Rechts auf informationelle Selbstbestimmung abhängt[75] und ohne die bestimmte staatliche Überwachungsmaßnahmen verfassungsrechtlich nicht hingenommen werden könnten[76]. Dem trägt die Verfassung von Berlin in Art. 47 Rechnung.

Zu Recht weist auch die Senatsverwaltung für Justiz in dem Bericht darauf hin, daß trotz der hohen Präferenz der Strafverfolgung innerhalb der staatlichen Zielstellungen, die von niemandem (auch dem Datenschutzbeauftragten nicht) angezweifelt wird, der Datenschutz keineswegs prinzipiell gegenüber den *Strafverfolgungsinteressen* zurückzutreten hat. Der Gesetzgeber hat in einer Vielzahl von Regelungen gerade auch im Strafprozeßrecht den Ermittlungsbehörden und auch den Gerichten die Erhebung von Informationen (etwa Geständnissen) oder die Verwendung rechtswidrig erlangter Informationen untersagt und damit ein Informationsdefizit bewußt in Kauf genommen. Niemand (auch nicht die Polizei) hat diesen Informationsverzicht bisher prinzipiell kritisiert. Auch das Datenschutzrecht ist als Konkretisierung des grundgesetzlichen Rechts auf informationelle Selbstbestimmung grundlegend für rechtsstaatliches Handeln[77].

Zutreffend ist die Aussage in dem Bericht, daß das Recht auf informationelle Selbstbestimmung nicht *uneingeschränkt* gewährleistet ist. Der Betroffene darf aber nur dann übergangen werden, wenn ein überwiegendes Allgemeininteresse eine Verarbeitung seiner Daten rechtfertigt. Der Eingriff in das informationelle Selbstbestimmungsrecht ist somit keine beliebig überwindbare Barriere. Erst eine sorgfältige *Abwägung der Verarbeitungsinteressen* der Allgemeinheit gegen das Recht auf informationelle Selbstbestimmung kann ergeben, inwieweit das Allgemeininteresse überwiegt und deshalb Vorrang verdient. Eine derartige Abwägung lassen die Ausführungen des Teils des Berichts zur Polizei – im Gegensatz zu anderen Teilen – nicht erkennen. Die Interessen der Polizei werden einseitig in den Vordergrund gestellt. Der Mangel an Bereitschaft, den Stellenwert des informationellen Selbstbestimmungsrechts anzuerkennen, wird auch durch den polemischen Stil dieses Berichtsteils deutlich, der sich insoweit von anderen Teilen des Berichts abhebt, die überwiegend von einer sachlichen Interessenabwägung und Ausdrucksform gekennzeichnet sind. Es liegt auf der Hand, daß bei einer Verwaltung, die bewußt auf die Konfrontation mit dem Berliner Datenschutzbeauftragten setzt, die Suche nach ausgewogenen Lösungen für beide Seiten mühsam, aufwendig und im Ergebnis für die Interessen des Bürgers meistens erfolglos ist.

Datenschutzrechtliche Regelungen müssen auch bei der Strafverfolgung und der vorbeugenden Straftatenbekämpfung zum Schutz des Persönlichkeitsrechts *Grenzen* setzen. Diese Wirkung teilen die Datenschutzvorschriften mit vielen Verfahrensregelungen der StPO. In einem Rechtsstaat kann nicht jede „*kriminaltaktische Notwendigkeit*“ Grundrechtseingriffe rechtfertigen. Der Zweck heiligt nicht die Mittel.

Im Mittelpunkt der Argumentation in dem Berichtsteil „Polizei“ stehen Erörterungen, die zunächst mit dem Datenschutz nichts zu tun haben, sondern auf eine grundsätzliche *Neuorientierung* des Polizeirechts abzielen. Sind die herkömmlichen Bestimmungen des Rechts der Strafverfolgung und der Gefahrenabwehr darauf ausgerichtet, daß Eingriffe durch die Polizei zureichende tatsächliche Anhaltspunkte für das Vorliegen einer Straftat (§ 152 StPO) bzw. eine konkrete Gefahr voraussetzen, tendieren die Sicherheitsbehörden seit Jahren dahin, diese Beschränkungen zu sprengen und sich Eingriffsbefugnisse weit im Vorfeld dieser Voraussetzungen zu verschaffen[78]. Die Forderung im Bericht, der Polizei müßten Befugnisse zustehen, damit sie „den zureichenden Anfangsverdacht aktiv gewinnen“ kann, bringt dies auf geradezu überdeutliche Weise zum Ausdruck.

Der 1992 in das ASOG eingeführte Begriff der „*vorbeugenden Straftatenbekämpfung*“ stellte einen wichtigen Schritt in diese Richtung dar. Wer für Gefahren „vorsorgt“, die er im einzelnen noch gar nicht kennt, die weder personell noch situativ einge-

Die Einschätzung, der zweite Teil (Polizei) des Senatsberichts über Entwicklung des Datenschutzes (Drs Nr. 13/2267) sei durch polemischen Stil und bewußte Konfrontation mit dem Berliner Datenschutzbeauftragten geprägt, können wir nicht teilen. In dem Berichtsteil über die Polizei geht es darum, dem Abgeordnetenhaus von Berlin vor Augen zu führen, in welchem Bereich datenschutzrechtliche Vorschriften Auswirkungen auf die polizeiliche Aufgabenerfüllung haben und zu welchen Folgen dies führen kann.

Eine Rechtsgüterabwägung zwischen Recht auf informationeller Selbstbestimmung und anderen Interessen der Allgemeinheit hat in vielen Bereichen der Gesetzgeber bereits betroffen. Selbstverständlich sind gesetzliche Regelungen für die Polizei verbindlich. Das schließt aber nicht aus, mit der Darstellung der praktischen Auswirkungen gesetzlicher Regelungen auch den Wunsch zu verbinden, einzelne Regelungen zu modifizieren. Dies hat mit Polemik oder bewußter Suche nach Konfrontation nichts zu tun, sondern dient dazu, dem Berliner Abgeordnetenhaus eine möglichst breite Informationsbasis für künftige Entscheidungen zu geben.

Die „vorbeugende Bekämpfung von Straftaten“ gehörte schon immer – auch ohne ausdrücklich im Gesetz erwähnt gewesen zu sein – zu den Aufgaben der Polizei. Sie hat sich noch nie darauf beschränkt, erst zu reagieren, wenn ihr Straftaten bekannt werden. Aufgabe der im Jahr 1848 gegründeten Berliner Schutzmannschaft war es, Gefahren, insbesondere krimineller Art, zu verhüten. Die Berliner Kriminalpolizei führte seit der Mitte des 19. Jahrhunderts sog. „fliegende Patrouillen“ durch, deren Aufgabe es war, kriminalistische Ermittlungen zu unterstützen.

75 BVerfGE 65,1 ff., 46
76 BVerfGE 67, 157 ff., 185
77 vgl. auch Art. 33 Verfassung von Berlin
78 JB 1996, 4.1.1

grenzt sind, der handelt ohne Anknüpfung an den polizeilichen Gefahrenbegriff. Bezogen auf eine potentielle Straftat heißt dies, es liegt noch nicht einmal ein Anfangsverdacht vor, wie er in § 152 Abs. 2 StPO vorausgesetzt wird. Die bei jedem Delikt zu stellenden Fragen „Wer? Wo? Wann? Was? Wie?“ sind noch offen. Datenschutzrechtlich betrachtet hat diese Neuorientierung gravierende Konsequenzen für die informationelle Selbstbestimmung. Läßt die herkömmliche Aufgabenbestimmung der Polizei Informationseingriffe nur bei Vorliegen einer konkreten Gefahr oder eines Verdachts, daß eine Straftat begangen wurde, zu, wurden schon mit dem ASOG auch für die Informationsverarbeitung Befugnisse weit im Vorfeld geschaffen. In dem Berichtsteil „Polizei“ werden noch weitergehende Befugnisse gefordert.

Läßt man Eingriffe in das Recht auf informationelle Selbstbestimmung zum Zweck der vorbeugenden Straftatenbekämpfung zu, müssen die Eingriffsvoraussetzungen deshalb so klar und präzise wie möglich benannt werden. Unsere Prüfungen haben gezeigt, daß die Regelungen des ASOG diese Anforderungen nicht immer hinreichend erfüllen. Das ASOG enthält viele Normen mit wortreichen Scheintatbestandlichkeiten, wie z. B. die Floskel, daß eine Maßnahme zulässig sei, wenn zu einem potentiell Tatverdächtigen „eine Verbindung besteht, die erwarten läßt, daß die Maßnahme zur vorbeugenden Bekämpfung der Straftat beitragen wird“ (§ 25 Abs. 2 Nr. 2 ASOG).

In dieser Situation sind datenschutzrechtliche Hemmnisse keine unangemessene Behinderung polizeilicher Arbeit; sie sind vielmehr Garant dafür, daß auch vor dem Hintergrund konturenloser Befugnisnormen ein *Mindestmaß an informationeller Selbstbestimmung* gewährleistet bleibt.

Die im Berichtsteil „Polizei“ aufgeführten Einzelfälle für fehlende Befugnisse belegen nicht das Bild, das von den angeblichen Behinderungen der Polizeiarbeit durch Datenschutzbestimmungen gezeichnet wird. Die Beispielsfälle beruhen auf fehlerhaften Interpretationen der gesetzlichen Regelungen, die die gewünschten Eingriffe bereits zulassen, übersehen andere datenschutzgerechte Lösungen, die teilweise schon vor Jahren vom Berliner Datenschutzbeauftragten vorgeschlagen wurden, oder betreffen Vorhaben, die dem Berliner Datenschutzbeauftragen nicht bekanntgemacht wurden und gegen die deshalb auch keine datenschutzrechtlichen Einwendungen erhoben wurden. Soweit überhaupt Fälle aufgeführt werden, in denen gesetzliche Regelungen der Polizei Grenzen setzen, ist die Entscheidung des Gesetzgebers, der sich mit den Belangen der Strafverfolgungsbehörden intensiv auseinandergesetzt hat und – z. B. im Sozialdatenschutz – angemessene Lösungen vorsieht, zu akzeptieren. Auf die unbegründete Kritik der Polizei am Sozialgeheimnis wird an anderer Stelle dieses Berichts[79] näher eingegangen.

Der Berliner Datenschutzbeauftragte ist in der *Ausübung seines Amtes unabhängig* und nur dem Gesetz unterworfen (§ 22 Abs. 2 BlnDSG). Der in dem Bericht erhobene Vorwurf, der Datenschutzbeauftragte greife bei seinen Prüfungen tief in rechtliche und fachliche Beurteilungskompetenzen der Polizei, der Staatsanwaltschaft, der Fachaufsichtsbehörde und der Gerichte ein, stellt nicht nur diese Unabhängigkeit in Frage, sondern liegt auch neben der Sache.

Bei der Kontrolle von Datenerhebungen, Speicherungen und Übermittlungen muß der Berliner Datenschutzbeauftragte das Vorliegen der Eingriffsvoraussetzungen prüfen. Wenn die Normen weitgehend aus *Generalklauseln* bestehen und die Erforderlichkeit einzige Eingriffsvoraussetzung ist, muß sich die Prüfung auf das Vorliegen dieser Voraussetzungen konzentrieren. Ausführungen der Polizei und Staatsanwaltschaft sowie deren Fachaufsichtsbehörden zu kriminaltaktischen Notwendigkeiten werden hierbei berücksichtigt. Es ist widersprüchlich, wenn auf der einen Seite immer konturenlosere Eingriffsvoraussetzungen gefordert werden, bei denen die Grenze des Zulässigen die Verhältnismäßigkeit der Maßnahme ist, und auf der anderen Seite beklagt wird, daß der Datenschutzbeauftragte ebendies prüft. Das Problem könnte entschärft werden, wenn das ASOG präzisere Voraussetzungen für bestimmte Eingriffe in das Persönlichkeitsrecht vorsehen würde.

79 vgl. unten 3.4

Gleiche Ziele verfolgte der bereits 1896 als besondere Organisationseinheit der Berliner Polizei eingerichtete Erkennungsdienst. Um die Jahrhundertwende wurden eine Fotosammlung zur Identifizierung von Personen („Verbrecheralbum“) und weitere Karteien zur vorbeugenden Bekämpfung von Straftaten angelegt (Dr. Dietmar Peitsch, Vorbeugende Bekämpfung von Straftaten und Vorbereitung auf die Gefahrenabwehr als Aufgaben der Polizei und ihre Beschreibung in den Novellierungsentwürfen des Polizei- und Strafverfahrensrechts, Die Polizei, Heft 9/1990, S. 213 ff.).

Daraus ergibt sich, daß der Sache nach die vorbeugende Bekämpfung von Straftaten bzw. die Vorsorge für die künftige Verfolgung von Straftaten keineswegs eine neue Aufgabe für die Polizei ist, die erst mit dem ASOG von 1992 geschaffen wurde. Richtig ist allerdings, daß vor dem Hintergrund neuer, moderner Formen der Kriminalität der kriminalstrategische Ansatz, Straftaten zu verhüten und kriminelle Strukturen zu erkennen und zu zerschlagen, immer mehr an Bedeutung gewinnt. Eine rein reaktive Kriminalitätsbekämpfung kann bei Erscheinungsformen wie z. B. organisierter oder terroristischer Kriminalität nicht greifen. Wirksames polizeiliches Handeln zum Schutz potentieller Opfer und zum Schutz der Allgemeinheit muß hier schon ansetzen, bevor sich eine Gefahr dergestalt konkretisiert hat, daß eine Straftat unmittelbar bevorsteht.

Die Unabhängigkeit des Berliner Datenschutzbeauftragten ist gesetzlich gewährleistet und wird vom Senat nicht in Frage gestellt. Es wurde lediglich darauf hingewiesen, daß sich der Datenschutzbeauftragte bei seinen Prüfungen nicht auf die Frage einer mißbräuchlichen Verwendung von Daten beschränkt, sondern mindestens ebenso häufig prüft, ob Daten überhaupt erhoben, d. h. Ermittlungen geführt werden durften. Letzteres ist bei Strafermittlungen Aufgabe der sachleitungsbefugten Staatsanwaltschaft und bei Maßnahmen zur Gefahrenabwehr Aufgabe der Polizei bzw. deren Aufsichtsbehörde. Zusätzlich unterliegen polizeiliche Maßnahmen der gerichtlichen Kontrolle. Die Aussage, daß Prüfungen des Berliner Datenschutzbeauftragten in die rechtliche und fachliche Beurteilungskompetenz der Polizei, der Staatsanwaltschaft, der Fachaufsichtsbehörden und der Gerichte eingreifen, belegt insbesondere ein in dem Senatsbericht geschildertes Beispiel, in dem der Datenschutzbeauftragte polizeiliche Verfahrensweisen beanstandete, die von der Staatsanwaltschaft I bei dem Landgericht Berlin für rechtlich unbedenklich gehalten wurden. Im übrigen wird hierzu auf 3.1.2 des „Spannungsberichtes“ Bezug genommen.

| Bericht des Berliner Datenschutzbeauftragten | Stellungnahme des Senats |
|---|---|

Es wird in dem Berichtsteil „Polizei“ der Eindruck erweckt, als würde der Berliner Datenschutzbeauftragte untersagen, daß strafrechtliche Ermittlungen überhaupt geführt werden. Das ist falsch und noch nie erfolgt, was auch die im Bericht aufgeführten Beispiele belegen. Allerdings ist es Aufgabe des Datenschutzbeauftragten zu prüfen, wie mit personenbezogenen Daten bei Ermittlungen umgegangen wird und ob die Voraussetzungen für den Einsatz von Ermittlungsmethoden, die teilweise tief ins Persönlichkeitsrecht eingreifen, vorlagen.

In dem Bericht wird erneut beklagt, daß der Berliner Datenschutzbeauftragte sich dafür einsetzt, daß die Polizei Betroffenen auch *Einsicht in die zu ihrer Person vorhandenen Akten* gewährt. Das Recht der Bürger auf Zugang zu ihren Akten ist von elementarer Bedeutung. Das Bundesverfassungsgericht hat dies im Volkszählungsurteil besonders hervorgehoben: „Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer, was, wann und bei welcher Gelegenheit über sie weiß“[80]. Vor diesem Hindergrund ist nicht verständlich, daß der Polizeipräsident den Bürgern grundsätzlich keine Einsichtnahme mehr in die zu ihrer Person geführten Kriminalakten gewährt und sich auf die zwangsläufig nicht so aussagekräftige Auskunft über den Akteninhalt beschränkt. Die Auskunft über den Inhalt der Akte ist nur eine allgemeingehaltene Inhaltsangabe. Um vollständig Kenntnis über die Informationen zu erhalten, welche die Polizei besitzt, muß der Bürger auf seinem Einsichtsrecht bestehen.

Die dem Wortlaut nach anscheinend unverbindliche Kann-Vorschrift in § 50 Abs. 6 ASOG nutzt die Polizei als Möglichkeit, die Einsichtnahme grundsätzlich zu verweigern mit der dem Charakter des Einsichtsrechts hohnsprechenden Begründung, das Einsichtsrecht des ASOG sei nur als Möglichkeit zur Arbeitserleichterung gedacht. Dem Betroffenen ist vielmehr im Rahmen der Ausübung pflichtgemäßen Ermessens Akteneinsicht zu gewähren. Es ist in jedem Einzelfall zu prüfen, ob die Gewährung von Akteneinsicht möglich ist. Dabei ist zu berücksichtigen, daß es für den Betroffenen ein fundamentaler Unterschied ist, ob ihm der Inhalt seiner Akte nur geschildert wird oder ob er Gelegenheit hat, die Akte selbst einzusehen. Die Begründung des Referentenentwurfs zum ASOG, der von den Regierungsfraktionen im Abgeordnetenhaus eingebracht wurde, belegt, daß nicht die „Arbeitserleichterung“ das Motiv für die einschränkende Regelung zur Akteneinsicht war. Vielmehr sollte verhindert werden, daß durch ein vorzeitiges Bekanntwerden von Informationen polizeiliche Aufgaben unterlaufen werden könnten.

Im Berichtsteil „Polizei“ wird auch der Verwaltungsaufwand für die *Benachrichtigungen der Betroffenen* über die Speicherung ihrer Daten in einer automatisierten Datei der Polizei nach § 43 Abs. 3 ASOG beklagt und in Frage gestellt, ob der Aufwand noch in einem vertretbaren Verhältnis zu dem datenschutzrechtlichen Nutzen stehe. Die Regelung weicht bereits von der in § 16 Abs. 2 BlnDSG normierten weitgehenden Unterrichtungspflicht zu Lasten des Persönlichkeitsrechts der Bürger ab. Nach dem BlnDSG ist bei jeder automatisierten Verarbeitung von Daten der Betroffene hiervon zu unterrichten. Bei der Polizei besteht die Unterrichtungspflicht nur bei länger als fünf Jahre andauernden Speicherungen in automatisierten Dateien. Damit ist die Polizei gegenüber den anderen Berliner Verwaltungen bereits erheblich privilegiert. Nicht akzeptabel wäre, die Unterrichtung in diesem sensiblen Bereich vollkommen entfallen zu lassen, da die Betroffenen z. B. bei Verfahrenseinstellungen ohne vorherige Vernehmung gerade nichts von ihrer polizeilichen Registrierung wissen. Zudem ist den Betroffenen oft nicht bewußt, daß und wie lange sie bei der Polizei in automatischen Dateien registriert werden.

Die Begründung des von den Koalitionsfraktionen übernommenen Entwurfs für das novellierte ASOG führt zutreffend aus: „Die Vorschrift dient dem Schutz des Bürgers gegen langfristige Speicherungen in automatisierten Dateien, die wegen der schnellen Suchfähigkeit und der besonderen Zusammenführungsmöglichkeiten der Daten stärkere Eingriffsqualität haben als langfristige Speicherungen in nichtautomatisierten Dateien und

Es ist erneut darauf hinzuweisen, daß es ein vom Berliner Datenschutzbeauftragten reklamiertes Recht auf Akteneinsicht gegenüber Ordnungsbehörden und der Polizei nicht gibt.

Das allgemeine Datenschutzrecht enthält in § 16 Abs. 4 des Berliner Datenschutzgesetzes in der Tat einen Anspruch des Betroffenen auf Akteneinsicht. Der Gesetzgeber hat aber in § 51 ASOG den § 16 BlnDSG für unanwendbar bei der Erfüllung der Aufgaben nach dem ASOG erklärt. Der allgemeine datenschutzrechtliche Akteneinsichtsanspruch gilt also nicht gegenüber der Polizei. Statt dessen hat der Gesetzgeber in § 50 Abs. 1 ASOG einen Anspruch der betroffenen Person auf Auskunft über gespeicherte Daten geregelt. Das macht deutlich, daß er bewußt von dem allgemeinen Grundsatz der Akteneinsicht abweichen wollte. Dementsprechend gibt § 50 Abs. 6 ASOG der Polizei auch nur die Möglichkeit, statt einer Auskunft auch Akteneinsicht zu gewähren. Die Ausgestaltung des § 50 Abs. 6 ASOG als „Kann-Vorschrift“ zeigt, daß damit gerade kein Akteneinsichtsrecht des Betroffenen geschaffen werden sollte. Ob die Behörde Auskunft erteilt oder Einsicht gewährt, liegt danach in deren Ermessen.

Wegen der Besonderheiten insbesondere der polizeilichen Aufgabenerfüllung verbietet es sich auch, dem Betroffenen ein gesetzliches Recht auf Akteneinsicht zu gewähren. Der Inhalt von Kriminalakten, die auf der Grundlage von § 42 Abs. 1 ASOG geführt werden, ist anderer Natur als der Akteninhalt in Bereichen der allgemeinen Verwaltung. In fast jeder Kriminalakte sind Daten oder Informationen enthalten, auf deren Mitteilung der Betroffene keinen Anspruch hat. Dabei handelt es sich nicht nur um Daten über andere Personen, sondern auch um Informationen über polizeiliche Arbeitsabläufe und Ermittlungsmethoden oder andere behördliche Maßnahmen oder Vorgehensweisen. Gerade bei Kriminalakten besteht die Gefahr, daß sich ein Betroffener in Kenntnis solcher Informationen auf polizeiliche Maßnahmen einstellen und diese unterlaufen könnte. Andererseits verbietet es sich aus arbeitsökonomischen und auch aus kriminaltaktischen Gründen, Kriminalakten durch Umkopieren, Schwärzen oder das Einlegen von Leerblättern so „aufzubereiten“, daß sie nur noch die zur Kenntnisnahme des Betroffenen bestimmten Informationen enthalten und zur Einsichtnahme geeignet sind.

Aus dieser Rechtslage ist aber nicht abzuleiten, daß die Polizei grundsätzlich keine Akteneinsicht gewährt. Zwar rechtfertigen in der Mehrzahl der Fälle kriminaltaktische oder arbeitsökonomische Gründe die Entscheidung, Aktenauskunft zu erteilen. Sofern solche Gründe nicht vorliegen und Akteneinsicht beantragt wurde, gewährt die Polizei aber auch diese Akteneinsicht.

Es bestehen Zweifel, ob die Frage der Akteneinsicht von großer praktischer Bedeutung ist. Zwar werden Anträge auf Akteneinsicht beim Polizeipräsidenten in Berlin nicht gesondert statistisch erfaßt. Der Senatsverwaltung für Inneres ist aber noch nie ein Widerspruch oder eine Beschwerde einer betroffenen Person wegen Verweigerung von Akteneinsicht vorgelegt worden.

80 BVerfGE 65, 1 ff., 43

Akten. Es ist zu erwarten, daß die Benachrichtigungspflicht zur besonders gründlichen Prüfung der Notwendigkeit langfristiger Speicherungen führen wird.“ Dem ist nichts hinzuzufügen.

In dem Berichtsteil „Polizei“ wird der Eindruck vermittelt, als seien zu viele Mitarbeiter durch den Datenschutz gebunden. Die Angaben zu der Zahl der *Mitarbeiter, die mit Datenschutzbelangen* befaßt sind, sind nicht aussagekräftig, widersprüchlich und zum Teil irreführend. Ungeachtet dessen erscheinen 47 Mitarbeiter, die sich (unter anderem!) mit Datenschutz befassen, bei 3,5 Millionen im ISVB registrierten Personen nicht zu hoch.

Unverständlich ist, warum im Berichtsteil „Polizei“ auch die Wahrnehmung des vom Bundesverfassungsgericht geforderten Auskunftsrechtes durch die Betroffenen als „Spannungsfeld zwischen Datenschutz und schutzwürdigen Belangen der Allgemeinheit“ hervorgehoben wird. Es liegt auch im öffentlichen Interesse – nämlich im Interesse einer funktionierenden Demokratie –, daß Bürger erfahren können, was über ihre Person bei öffentlichen Stellen gespeichert ist. Die Zunahme der Anträge auf Auskunft und Löschung von Daten[81] spiegelt den Bedarf wieder und ist aus datenschutzrechtlicher Sicht zu begrüßen. Sie zeigt, daß immer mehr Betroffene von ihren Rechten Gebrauch machen. Von den vielfältigen Gesetzen zum Datenschutz, die inzwischen geschaffen worden sind, können die Bürger nur profitieren, wenn sie selbst ihre Rechte wahrnehmen. Aus diesem Grund stellt der Berliner Datenschutzbeauftragte seit 1982 das *Datenscheckheft* mit Musterschreiben als Hilfsmittel zur Geltendmachung der Datenschutzrechte bei verschiedenen öffentlichen und privaten Stellen zur Verfügung.

Auch die Kostenträchtigkeit technisch-organisatorischer Maßnahmen wird beklagt und mit den unterschiedlichen Regelungen des Berliner und des Bundesdatenschutzgesetzes begründet. Nach dem BlnDSG haben sich die Maßnahmen nach dem jeweiligen Stand der Technik zu richten (§ 5 Abs. 1 Satz 2), nach dem BDSG sind Maßnahmen nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (§ 9 Satz 2 BDSG). Die faktischen Unterschiede sind höchst marginal.

Auch für die Polizei gilt, daß die *Kosten für technisch-organisatorische Maßnahmen* des Datenschutzes nicht nur der Wahrung der informationellen Selbstbestimmung der Bürger dienen, sondern auch der Qualität der Aufgabenerfüllung der Behörde. Der Bruch der Vertraulichkeit der in polizeilichen Informationssystemen gespeicherten Daten und Zweifel an der Verläßlichkeit der dort gespeicherten Daten und eingesetzten Systeme sind nicht nur aus Gründen des Datenschutzes zu verhindern, vielmehr gehört die Gewährungsleistung informationstechnischer Sicherheit zu den primären Gestaltungszielen moderner IT-Verfahren. Die Kosten dafür können nicht dem Datenschutz allein zugerechnet werden, auch dann nicht, wenn er davon profitiert. Es ist daher auch höchst irreführend, wenn man die Kosten für die IT-Sicherheit und den Datenschutz in bezug zu den Gesamtkosten eines Systems setzt. Kein Automobilhersteller, kein Autofahrer käme auf den Gedanken, dem Gesetzgeber oder dem TÜV durch den Vergleich mit den Gesamtkosten eines Fahrzeugs die Kosten für Bremsen und Sicherheitssysteme vorzuhalten.

Überflüssigerweise kostenträchtig sind technisch-organisatorische Maßnahmen zur Sicherstellung des Datenschutzes und der IT-Sicherheit auf jeden Fall dann, wenn sie als gleichrangiges Gestaltungsziel nicht anerkannt werden, sondern bei der Verfahrenskonzeption zunächst unberücksichtigt bleiben und erst im Rahmen der Nachbesserung eingefügt werden. Da Nachbesserungen in der Regelung nicht die gleiche Wirksamkeit erreichen wie Maßnahmen, die bei der Planung der Verfahren bereits berücksichtigt wurden, kann eine angemessene Sicherheit nur mit Mehraufwand erreicht werden.

Auch bei dem Berichtsteil *„Verfassungsschutz“* ist die Tendenz zu beobachten, Beschränkungen für Eingriffe in das Recht auf informationelle Selbstbestimmung, trotz der noch über das ASOG hinausgehenden Privilegierung der Interessen des Verfassungsschutzes, weiter abzubauen.

81 vgl. unten 4.1.1

Gestrichen werden sollen die Regelungen zur Dokumentation von Datenübermittlungen, zur – ohnehin nur begrenzten – Begründungspflicht bei der Ablehnung von Auskunftsanträgen, zur Löschungspflicht für nicht erforderliche personenbezogene Daten, die durch nachrichtendienstliche Mittel erlangt wurden und zu festen Löschungsfristen. In diesem Berichtsteil wird vielfach gefordert, die Normen des Gesetzes über das Landesamt für Verfassungsschutz den Regelungen des Bundesverfassungsschutzgesetzes anzupassen. Es ist bedauerlich, daß bei dieser Auflistung nicht auch Regelungen aufgeführt wurden, die die Datenschutzsituation der Betroffenen gegenüber dem Landesgesetz verbessern.

Die Berichtsteile der *anderen Verwaltungen* weisen überwiegend auf Fälle hin, die in den Jahresberichten des Berliner Datenschutzbeauftragen erwähnt sind und z. T. in Ausschüssen des Abgeordnetenhauses intensiv beraten wurden. In weiteren Teilen – z. B. im Berichtsteil „Justiz“ – wird aus den Beispielsfällen erkennbar, daß angemessene Lösungen für datenschutzrelevante Sachverhalte gefunden werden können und daß dort die Tätigkeit des Berliner Datenschutzbeauftragten als notwendig und hilfreich anerkannt wird.

### 3. 3 Datenschutz bei Telediensten

Die *private und geschäftliche Nutzung von Online-Diensten* und insbesondere des Internets nimmt auch in Deutschland stark zu. Diese Entwicklung dürfte durch die Liberalisierung des Sprachtelefonmarktes und die damit verbundene Kostensenkung für den Nutzer weiter an Fahrt gewinnen. Für diesen Bereich sind das am 1. August 1997 in Kraft getretene Bundesgesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste *(Informations- und Kommunikationsdienste-Gesetz)*[82] und der zeitgleich in Kraft getretene *Mediendienste-Staatsvertrag der Länder*[83] von erheblicher praktischer Bedeutung. An den Vorarbeiten zu beiden Regelungswerken waren wir beteiligt[84].

Voraussichtlich wird der wirtschaftlich bedeutsamere und größere Teil der Aktivitäten im Online-Bereich dabei dem Bundesrecht unterliegen, das die Teledienste in den ersten beiden Artikeln des Informations- und Kommunikationsdienste-Gesetzes regelt. Das *Teledienstegesetz* (TDG) gilt für „alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt“ (§ 2 Abs. 1 TDG). Dazu zählen insbesondere

- Angebote im Bereich der Individualkommunikation (beispielsweise Telebanking, Datenübertragung),
- Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (Datendienste, z. B. Verkehrs-, Wetter-, Umwelt- und Börsendaten, Verbreitung von Informationen über Waren- und Dienstleistungsangebote),
- Angebote zur Nutzung des Internets oder weiterer Netze,
- Angebote zur Nutzung von Telespielen sowie
- Angebote von Waren- und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit.

Bei den Vorschriften des *Teledienstedatenschutzgesetzes* (TDDSG) ist besonders die Verpflichtung der Diensteanbieter hervorzuheben, die Gestaltung und Auswahl technischer Einrichtungen für Teledienste an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen (§ 3 Abs. 4 TDDSG). Ferner hat der Diensteanbieter dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 4 Abs. 1 TDDSG). Die Erstellung von Nutzungsprofilen ist nur bei Verwendung von Pseudonymen zulässig. Unter einem Pseudonym erfaßte Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden (§ 4 Abs. 4 TDDSG).

82 BGBl. I, S. 1870
83 GVBl. S. 361; vgl. dazu im einzelnen 4.7.4
84 JB 1996, 4.7.1

Damit hat der Gesetzgeber der technisch ohne weiteres möglichen Erstellung von personenbezogenen *Nutzerprofilen z. B. über Einkaufsgewohnheiten* wirksam vorgebeugt. Wer sich auf dem virtuellen Marktplatz umsieht, soll wie auf einem realen Marktplatz nicht gezwungen werden, (elektronische) Spuren zu hinterlassen. Diese Regelungen sind aus Datenschutzsicht insbesondere deswegen positiv zu bewerten, weil sie erstmals auch Vorgaben hinsichtlich der technischen Gestaltung der verwendeten Systeme unter dem Gesichtspunkt des Datenschutzes machen.

Der Gesetzentwurf enthielt noch eine Verpflichtung der Teledienstеanbieter zur *Übermittlung von Kundendaten an Sicherheitsbehörden.* Er sah die Erteilung von Auskünften über Daten zur Begründung, inhaltlichen Ausgestaltung oder Änderung der Vertragsverhältnisse (Bestandsdaten) insbesondere an die Polizei und die Nachrichtendienste vor. Diese pauschale Bestimmung[85] wurde im Bundestag gestrichen, nachdem die 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung derartig weitgehende Übermittlungsvorschriften[86] abgelehnt hatte. Auch der Bundesrat, der zunächst noch eine Befugnis für Anbieter zur spontanen Übermittlung derartiger Daten an die Sicherheitsbehörden einführen wollte, hat diese Forderung später fallengelassen. Das ist insofern zu begrüßen, als das geltende Recht hinreichende Zugriffsbefugnisse für Polizei und Strafverfolgungsbehörden bereithält. Entsprechende Zugriffsbefugnisse für Nachrichtendienste auf private Datenbestände sind unserer Rechtsordnung dagegen fremd. Mit der Streichung der Verpflichtung zur Übermittlung von Kundendaten an die Sicherheitsbehörden hat der Bundesgesetzgeber auch eine wichtige Angleichung der Datenschutzbestimmungen für Tele- und Mediendienste vollzogen. Der Mediendienste-Staatsvertrag sah eine derartige Verpflichtung nämlich von vornherein nicht vor.

Nur in einem weiteren Punkt bleibt eine Differenz zwischen den ansonsten nahezu wortgleichen Datenschutzbestimmungen für Multimedia-Dienste im Bundes- und Landesrecht bestehen: Ein *„Datenschutz-Audit“* sieht das Teledienstedatenschutzgesetz im Gegensatz zum Mediendienste-Staatsvertrag nicht vor[87]. Diese Differenz ist allerdings in der Praxis wenig bedeutsam, weil auch der Mediendienste-Staatsvertrag keinen entsprechenden Anbieter zur Durchführung eines Datenschutz-Audits verpflichtet. Umgekehrt verbietet das Bundesrecht keinem Unternehmen, das Teledienste anbieten will, sich ein entsprechendes *Gütesiegel für datenschutzfreundliche Gestaltung* seines Angebots auf freiwilliger Basis ausstellen zu lassen. Allerdings fehlt es bisher an einer dem Umwelt-Bereich vergleichbaren Struktur von zugelassenen, d. h. auf Zuverlässigkeit geprüften Sachverständigen, die derartige Gütesiegel ausstellen könnten. Dennoch halten wir die Initiative der Deutschen Telekom AG, alle entsprechenden Anbieter von Tele- und Mediendiensten, Telekommunikationsdiensten und Inhalten zu einem Arbeitskreis *„Datenschutz-Audit Multimedia“* einzuladen, für begrüßenswert. Wir waren bei der Konstituierung dieses Arbeitskreises vertreten und werden uns an den Gesprächen weiter beteiligen.

Der Deutsche Bundestag hat bei der Verabschiedung des Informations- und Kommunikationsdienste-Gesetzes in einer Entschließung[88] festgestellt, daß die Regelung des Teledienstedatenschutzgesetzes sich durch *vier Kernelemente,* nämlich den *Systemdatenschutz,* das Prinzip der *Datenvermeidung,* die Sicherung der *Anonymität* und die Möglichkeit zur *elektronischen Einwilligung,* auszeichnet. Das Parlament hat die Bundesregierung aufgefordert, im Rahmen einer Evaluierung zu prüfen, wie sich durch die neuen gesetzlichen Regelungen die Akzeptanz der Multimedia-Dienste bei Nutzern und Unternehmen entwickelt und inwieweit ggf. Vorschriften auch unter Berücksichtigung europäischer Überlegungen zu ändern sind, um die Entwicklung neuer Dienste zu fördern. Auch an diesem *Evaluierungsprozeß* werden wir uns beteiligen.

Wenngleich die neue Multimedia-Gesetzgebung in vielen Punkten eine Vorreiterrolle zur Weiterentwicklung des Datenschutzrechts übernommen hat, stellt sich in der Praxis eine Reihe

85 JB 1996, 4.7.1
86 vgl. Anlage 2.2.3
87 vgl. JB 1996, 4.7.1
88 BT-Drs 13/7935

schwieriger *Abgrenzungsprobleme.* Diese betreffen weniger die horizontale Abgrenzung zwischen Tele- und Mediendiensten, weil für beide Dienstearten weitgehend identische datenschutzrechtliche Anforderungen gelten. Sie betreffen vielmehr die vertikale Geltung verschiedener Regelungsmaterien für das konkrete Angebot eines Online-Dienstes. Dies läßt sich am Beispiel des Homebanking anschaulich machen: Beim *Homebanking (Telebanking)* handelt es sich um einen Teledienst nach § 2 Abs. 1 TDG, auf dessen Anbieter das Teledienstedatenschutzgesetz jedenfalls insoweit Anwendung findet, als personenbezogene Daten gerade im Zusammenhang mit der Nutzung des Teledienstes entstehen. Zugleich findet aber auf das mit Hilfe des Teledienstes begründete oder ausgestaltete Vertragsverhältnis (Kontokorrentverhältnis) mit der Bank das Bundesdatenschutzgesetz Anwendung, das zum Teil noch abweichende Regelungen vom Teledienstedatenschutzgesetz enthält. Schließlich liegt der Nutzung des Teledienstes stets eine Übermittlung mittels Telekommunikation zugrunde. Im Verhältnis zum Anbieter dieses Telekommunikationsdienstes finden das Telekommunikationsgesetz und die (novellierungsbedürftige) Telekommunikationsdienstunternehmen-Datenschutzverordnung Anwendung. Diese komplizierte Rechtslage, die auch eine teilweise Aufspaltung der Datenschutzkontrolle zur Folge hat, führt naturgemäß zu Schwierigkeiten in der Praxis, die nur durch eine rasche Abstimmung zwischen den beteiligten Aufsichtsbehörden zur Einordnung und Bewertung neuer Multimedia-Dienste zu lösen sind. Diese Abstimmung mit den obersten Aufsichtsbehörden der Länder, den Landesbeauftragten für den Datenschutz, den Rundfunkdatenschutzbeauftragten und dem für den Telekommunikationsbereich zuständigen Bundesbeauftragten für den Datenschutz haben wir im vergangenen Jahr weiter vorangetrieben und hoffen, auf diese Weise im laufenden Jahr zu einem *Grundgerüst gemeinsamer Positionen* bei der Anwendung und Durchsetzung des neuen *„Online-Rechts“* zu gelangen. Nur auf diese Weise werden die zweifellos auch in Zukunft auftretenden praktischen Probleme mit dieser Gesetzgebung angemessen zu lösen sein.

Das Problem der Kontrolle und Verfolgung strafbarer Angebote im Internet hat bereits vor dem Inkrafttreten einer entsprechenden Regelung zur Verantwortung von Diensteanbietern im Teledienstegesetz die Europäische Kommission und den Rat beschäftigt. In einem gleichzeitig veröffentlichten *Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in audiovisuellen Diensten und Informationsdiensten*[89] und einer *Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen über rechtswidrige und schädliche Inhalte im Internet*[90] hat die Kommission Vorschläge zur Lösung der angesprochenen Probleme gemacht. Der Telekommunikations-Ministerrat hat am 28. November 1996 eine *Entschließung über rechtswidrige und schädliche Inhalte im Internet* gefaßt, die diese Vorschläge in allgemeiner Form aufgreift. Wir haben eine Stellungnahme der Datenschutzbeauftragten der Europäischen Union vom 28. Februar 1997 zu diesen Dokumenten[91] koordiniert. Darin wird betont, daß die Tatsache, daß im Bereich der Online-Dienste jeder Nutzer zu einem potentiellen Anbieter von Informationen werden kann, nicht dazu führen darf, daß die Verantwortung für rechtswidrige oder nur schädigende (aber nicht strafbare) Inhalte generell vom Urheber dieser Information auf den Nutzer verlagert oder erstreckt wird. Der Umstand, daß das Internet oder andere (zukünftige) Netze in gewissem Umfang dazu genutzt werden, illegale Inhalte zu verbreiten, sollte nicht dazu führen, daß das Internet in *ein nahtloses Netz der Überwachung* verwandelt wird, in dem der gesamte Netzverkehr beobachtet wird, um rechtswidrige Verhaltensweisen aufzuspüren. Das gilt um so mehr, als moderne Techniken der Kommunikation im Internet und des Auffindens von Informationen (Offline-Browser) dazu führen können, daß dem einzelnen PC-Nutzer Material auf seinen Rechner geladen wird, von dem er keine Kenntnis hat oder mit dessen Inhalt er nicht einverstanden ist. Die Datenschutzbeauftragten haben die Entschließung des Rates vom November 1996 begrüßt, in der dieser die Europäische Kommission auffordert, die Erforschung von technischen Verfahren, insbesondere der *Filter-Software* und der *Bewertung,* zu unter-

89 KOM (96) 483 endg.
90 KOM (96) 487
91 Anlage 3.1

stützen und zur datenschutzfreundlichen Gestaltung der Technik beizutragen. Die Datenschutzbeauftragten haben außerdem angeregt, einen ihrer Vertreter in eine mögliche Arbeitsgruppe einzubeziehen, die diese Fragen im Zusammenhang mit dem Datenschutz und dem Schutz der Privatsphäre erörtern könnte. Das Land Berlin hat sich auf unseren Vorschlag hin im Ausschuß der Regionen dafür eingesetzt, daß diese Gesichtspunkte auch in die Stellungnahme dieses Gremiums zum Grünbuch der Kommission einfließen. Dies wurde von den Vertretern der anderen Regionen allerdings mit knapper Mehrheit abgelehnt.

Inzwischen setzt sich vor allem unter dem Eindruck der Entscheidung des US-Supreme Court zu einem gesetzlichen Verbot von unanständigem (nicht strafbarem) Material im Internet[92] die Auffassung durch, daß die Probleme des Jugendschutzes und der Kontrolle von rassistischem Informationsmaterial im Internet sich nur durch eine Kombination von mehreren Maßnahmen werden lösen lassen. So hat die Europäische Kommission im November 1997 einen Aktionsplan zur Förderung der sicheren Nutzung des Internets vorgestellt. Darin wird die Förderung der Selbstkontrolle der Anbieter auf der Grundlage bestehender Verhaltenskodizes angekündigt. Maßnahmen zur Entwicklung von Filter- und Bewertungssystemen insbesondere zum Schutz von Kindern und Jugendlichen sollen ergriffen werden. Neben einer stärkeren Information von Eltern und Lehrern hinsichtlich der Gefahren im Internet und der schon bestehenden Möglichkeiten zur Begrenzung der Nutzung auf bestimmte Inhalte sollen auch die Anwendung bestehenden Rechts und die Entwicklung neuer Gesetze im Bereich des Internets auf europäischer und internationaler Ebene koordiniert werden. Hierzu hat auch das Abgeordnetenhaus den Senat aufgefordert, sich auf Bundesebene für eine verstärkte internationale Kooperation und eine Harmonisierung der Rechtsgrundlagen gegen Kinderpornographie einzusetzen[93].

Während im Rundfunkbereich nicht ohne Mitwirkung der Zuschauer bzw. Zuhörer registriert werden kann, wer welche Programme gesehen oder gehört hat, ist die Nutzung von Online-Diensten prinzipiell registrierbar, ohne daß der Nutzer dies bisher beeinflussen könnte. Teledienstedatenschutzgesetz und Mediendienste-Staatsvertrag verpflichten in Deutschland niedergelassene Anbieter, unter bestimmten Voraussetzungen auch anonyme Nutzungs- und Bezahlungsmöglichkeiten zu eröffnen. Auch nach Auffassung des Europäischen Parlaments sollten bei der Bekämpfung von schädigenden und illegalen Inhalten die im Rundfunksektor gemachten Erfahrungen und das dort erreichte Schutzniveau als Richtschnur angesehen werden[94]. Das bedeutet zugleich, daß der im Rundfunksektor erreichte Datenschutzstandard auch bei den Tele- und Mediendiensten erhalten bleiben sollte.

Angesichts der Schwierigkeiten einer Harmonisierung rechtlicher Regeln und ihrer Durchsetzung im Internet auf internationaler Ebene ist es verständlich und auch zu begrüßen, daß verstärkt über *technische Verfahren zur Kontrolle und Bekämpfung von illegalen Angeboten* nachgedacht wird. Im Bereich des Jugendschutzes hat das World Wide Web-Konsortium, das faktische Standards für den wichtigsten Internetdienst, das World Wide Web, entwickelt, die *Platform for Internet Content Selection (PICS)* erarbeitet, mit deren Hilfe pornographische Angebote (insbesondere Bildmaterial) aus dem Internet gefiltert und ihr Abruf durch Kinder durch eine entsprechende Einstellung des heimischen PC zumindest erschwert werden kann. Ein Informationsangebot im Internet (z. B. eine *Website*) kann aber nicht nur wegen ihres Inhalts, sondern auch wegen der Verwendung von personenbezogenen Daten der Nutzer dieses Angebots gegen rechtliche Regelungen verstoßen. Aus diesem Grund liegt es nahe, über den Einsatz von Filtertechnologien auch zur Verbesserung des Datenschutzes im Internet nachzudenken. Zu diesem Zweck hat das Word Wide Web-Konsortium das Projekt *„Platform for Privacy Preferences“ (P3P)* begonnen, bei dem Vorschläge für eine Änderung der Architektur des World Wide Web gemacht werden sollen, die eine *datenschutzfreundliche Nutzung dieses wichtigsten*

Bei der Jugendministerkonferenz im Juni 1997 wurde beschlossen, daß die Länder zur Unterstützung der Behörden bei der Umsetzung der Regelungen zum Jugendschutz im Mediendienste-Staatsvertrag (§ 18 Abs. 1) eine länderübergreifende Stelle errichten.

Die Länder sind diesem Beschluß nachgekommen und haben für diesen Teil die federführenden Aufgaben Rheinland-Pfalz übertragen.

Die länderübergreifende Stelle der Obersten Landesjugendbehörden ist seit Oktober 1997 etabliert. Zum 15. Oktober 1997 wurden Räume angemietet (Anschrift: Bahnstraße 8, 65205 Wiesbaden).

Die hauptamtliche Stelle der Beauftragten wurde mit einer Medienpädagogin, die Halbtagsstelle auf der Grundlage eines Honorarvertrages mit einem Verwaltungsjuristen besetzt. Beide Stellen sind entsprechend der vorläufigen Ländervereinbarung bis 31. Dezember 1998 befristet. Bis dahin muß die Entscheidung über die Weiterführung der länderübergreifenden Stelle und deren Organisationsstruktur getroffen werden.

Diese länderübergreifende Stelle mit der Bezeichnung „jugendschutz.net, Beauftragten der Obersten Landesbehörden für Jugendschutz in den Mediendiensten“ versteht sich ihrem Selbstverständnis nach als eine Selbstkontrolle („Insbesondere bemüht sich ’jugendschutz.net’, unmittelbar die Anbieter zu beraten, um zu erreichen, daß bei problematischen Angeboten sie selbst Veränderungen oder Sperrungen vornehmen.“ – Presseinformation des Ministeriums für Kultur, Jugend, Familie und Frauen, Rheinland-Pfalz vom 26. Januar 1998), zumal auch geplant war, daß die Internet-Anbieter sich an der Finanzierung beteiligen. Dies ist bisher nicht erfolgt.

Nordrhein-Westfalen und Bayern möchten für diese Stelle einen Staatsvertrag, damit sie hoheitliche Befugnisse erhält.

92 Reno v. ACLU Supreme Court of the USA Nr. 69-511 v. 26. Juni 1997

93 Anträge der Fraktionen der SPD und der CDU, Drs 13/890 und 891, beschlossen im Plenum des Abgeordnetenhauses am 25. September 1997

94 Entschließung des Europäischen Parlaments zum Grünbuch der Kommission über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen und den Informationsdiensten vom 24. Oktober 1997, BR-Drs 901/97

*Internet-Dienstes* ermöglicht. Das Projekt, an dem wir uns beratend beteiligen, könnte den Nutzer besser als bisher in die Lage versetzen, seine Interessen und Rechte bei der Nutzung des Internets zu schützen.

Grundsätzlich müssen technische Verfahren zur Verbesserung des Datenschutzes stets in einem Regelungsrahmen eingebettet sein, der ein Mindestmaß an Datenschutz gewährleistet. Es wird auch in Zukunft nicht den *„Datenschutzknopf"* am Computer geben, mit dessen Drücken man alle Datenschutzprobleme lösen kann. Ebensowenig sind rechtliche Regelungen – die im internationalen Rahmen ohnehin nur langfristig zu erreichen sind – ein Patentrezept zur Lösung der Datenschutzprobleme im Internet. Technik, Recht, vertragliche Vereinbarungen und Verhaltenskodizes sollten miteinander kombiniert werden, um die notwendigen Lösungen zu erreichen. Datenschutzfreundliche Technik und Datenschutzrecht werden beide wirkungslos bleiben, wenn ihre Umsetzung nicht von einer *unabhängigen Aufsichtsinstanz* überwacht wird.

Mit der Verabschiedung des *Signaturgesetzes*[95] und der *Signaturverordnung*[96] ist eine weitere wichtige Voraussetzung für die Nutzung weltweiter Datennetze wie des Internets zum Abschluß von Rechtsgeschäften und anderen kommerziellen Zwecken geschaffen worden. Das Signaturgesetz und die dazu erlassene Rechtsverordnung regeln ausschließlich die Verwendung von Verschlüsselungsverfahren zur Erstellung einer *digitalen Signatur (elektronischen Unterschrift)*, mit der sich der Absender einer elektronischen Nachricht beweissicher authentifizieren kann. Das Gesetz regelt nicht die Verschlüsselung von Nachrichteninhalten, die Gegenstand der anhaltenden *Kryptodebatte* ist[97]. Sowohl unverschlüsselte Nachrichten (im Klartext) als auch verschlüsselte Nachrichten können elektronisch unterschrieben werden. Ihr Absender kann anschließend dem Empfänger gegenüber nicht mehr bestreiten, daß die Nachricht von ihm stammt. Bevor eine digitale Signatur allerdings als beweiskräftig gelten kann, müssen bestimmte Voraussetzungen erfüllt sein. Wer Nachrichten digital unterschreiben will, muß sich zuvor unter Offenlegung seiner Identität von einer *Zertifizierungsstelle (Trust Center)* einen öffentlichen Signaturschlüssel durch ein entsprechendes Zertifikat zuordnen lassen. Dieser Signaturschlüssel wird anschließend veröffentlicht und ist z. B. im World Wide Web abrufbar. Auf diese Weise kann sich jedermann von der Gültigkeit einer fremden Signatur überzeugen, wenn er eine Nachricht erhält, die mit dem geheimen privaten Schlüssel des Absenders signiert worden ist[98]. Aus datenschutzrechtlicher Sicht ist entscheidend, daß niemand auf die Verwendung eines einzigen öffentlichen Signaturschlüssels beschränkt ist, der sonst leicht die Funktion eines *globalen Personenkennzeichens* erhalten könnte. Vielmehr läßt das Signaturgesetz die Vergabe von Attribut-Zertifikaten zu, so daß jemand mehrere öffentliche Schlüssel je nach der Rolle verwenden kann, in der er die entsprechende Nachricht versendet (z. B. geschäftlich oder privat). Außerdem kann der Inhaber eines Signaturschlüssels sich ein Zertifikat ausstellen lassen, in dem statt seines Namens ein unverwechselbares *Pseudonym* aufgenommen wird. Darin ist eine wichtige Ergänzung zur Verpflichtung von Tele- und Mediendiensteanbietern zu sehen, die pseudonyme Nutzung und Bezahlung ihrer Angebote zu ermöglichen. Wichtig ist schließlich, daß es keine zentrale Zertifizierungsstelle geben wird, bei der alle Inhaber von Signaturschlüsseln registriert sind. Vielmehr werden in erster Linie private Betreiber von Trust Centern die Zertifizierung von Signaturschlüsseln als Dienstleistung anbieten. Jeder Interessent kann sich an das Trust Center wenden, das er für das vertrauenswürdigste hält. Allerdings entstehen bei allen diesen Zertifizierungsstellen sensible Sammlungen von personenbezogenen Daten; deshalb ist es zu begrüßen, daß der Bundesgesetzgeber den Ausichtsbehörden nach dem Bundesdatenschutzgesetz die Überprüfung dieser Trust Center auch dann ermöglicht hat, wenn Anhaltspunkte für eine Verletzung von Datenschutzvorschriften nicht vorliegen.

95 BGBl. 1997 I, 1870
96 BGBl. 1997 I, 2498
97 JB 1996, 3.4
98 Einzelheiten zu diesem asymmetrischen Verschlüsselungsverfahren in JB 1996, 3.4

### 3.4 Bankautomation

Man könnte meinen, die Zeit, in der Waren und Dienstleistungen mit Bargeld bezahlt wurden, geht ihrem Ende entgegen. Begriffe wie *Point of Sale, elektronische Geldbörse, Cybercash und Cybermoney, Homebanking und Electronic Commerce* haben sich gerade im vergangenen Jahr immer nachhaltiger in den Medien verbreitet, sie spiegeln einen weltweiten Trend wieder, der unaufhaltsam zu sein scheint. Mit immer mannigfaltigeren Innovationen versuchen Geldinstitute und Handel dem Rationalisierungsdruck hinsichtlich der Abwicklung des Zahlungsverkehrs zu begegnen. Für den Bürger wird es zusehend schwieriger, den Fluß seiner persönlichen Daten nachzuvollziehen, wenn er sich darauf einläßt bzw. mangels anderer Alternativen sogar darauf einlassen muß, seine Geldgeschäfte mittels elektronischer Medien abzuwickeln.

Insbesondere die Anonymität, wie sie bei Barzahlungen noch weitestgehend gewahrt ist, wird bei der Nutzung des elektronischen Zahlungsverkehrs einer nicht zu vernachlässigenden Gefährdung ausgesetzt. Hier bedarf es schon eines erheblichen Vertrauensvorschusses des Bürgers hinsichtlich der Redlichkeit der mit der Automation des Zahlungsverkehrs befaßten Institutionen. Hinzu kommen noch die Risiken, die sich allein daraus ergeben, daß bei der Komplexität der Systeme wohl keine der beteiligten Stellen eine absolute Garantie dazu abgeben kann, gegen eine mißbräuchliche Nutzung ihrer Systeme gefeit zu sein (auch wenn dies immer wieder behauptet wird).

Da die Gewährleistung einer ordnungsgemäßen Verarbeitung personenbezogener Daten zu den Grundanliegen der Datenschutzgesetze (§ 19 Abs. 1 BlnDSG, § 18 Abs. 2 BDSG) gehört, sind auch Probleme, die dem ersten Anschein nach eher dem Verbraucherschutz zuzuordnen wären, datenschutzrechtlich relevant.

Bei *kartengestützten Zahlungsverfahren* sind entsprechend der Liquiditätswirkung auf den Kartennutzer drei Varianten zu unterscheiden: Während bei *Kreditkarten* eine Kontenbelastung erst nach einer längeren Zeitspanne wirksam wird, erfolgt die Abbuchung des Zahlbetrages bei *Debitkarten* sehr zeitnah. Die dritte Kartenart, die *Wertkarte*, belastet die Liquidität ihres Nutzers hingegen bereits vor deren Einsatz im Zahlungsverkehr, da der dort gespeicherte Geldbetrag entweder durch Barzahlung oder durch eine unmittelbare Kontenbelastung beim „Aufladen“ realisiert wird. Bereits beim *Beantragen bzw. Erwerb dieser Karten* besteht ein sehr differenziertes Niveau bei der Offenbarung personenbezogener Daten. Während bei *Kreditkarten* (hochpreisige Güter, höheres Einkommen) eine ganze Reihe sensibler Daten beim Antragsteller selbst oder bei anderen Institutionen (z. B. bei der SCHUFA – Schutzgemeinschaft für allgemeine Kreditsicherung) erhoben werden, kann eine derartige Datenerhebung beim Erwerber von *Wertkarten* (z. B. Telefonkarten) ganz entfallen.

#### Kreditkarten

Bei der *Nutzung von Kreditkarten* sind immer noch folgende wesentliche Schwachstellen zu beobachten:

*Gestohlene Karten* sind bis zur Sperrung durch den Karteninhaber z. B. zur Bezahlung von Waren und Dienstleistungen weiterhin einsetzbar, da bei dieser Nutzungsart keine Authentifizierung des Karteninhabers durch die Eingabe der PIN (Persönliche Identifikations-Nummer/Geheimnummer) üblich ist. Arbeitet eine Akzeptanzstelle sogar noch nach dem „Ritsch-ratsch-Verfahren“, d. h. ohne Online-Prüfung bei dem jeweiligen Rechenzentrum, verhindert selbst eine unmittelbar nach dem bemerkten Verlust eingeleitete Sperrung der Karte nicht deren Mißbrauch.

Mit vergleichsweise geringem technischem Aufwand sind die auf den *Magnetstreifen* gespeicherten Kartendaten kopierbar, wodurch kriminellen Tätern Totalfälschungen der Karten erleichtert werden. Da die Originalkarte weiterhin im Besitz des Inhabers bleibt, fällt ein Mißbrauch mit dem Duplikat möglicherweise erst bei der Abrechnung auf. Im Gegensatz zu ec-Karten weisen Kreditkarten keinen als schwer fälschbar geltenden *„MM“-Code* auf, der in Geldautomaten zur Echtheitsprüfung herangezogen wird.

Zur Reduzierung von Risiken wurden einige technische und organisatorische Maßnahmen durchgesetzt bzw. angekündigt:

Der Algorithmus zur Ermittlung neuer Kartennummern wurde dahingehend verändert, daß die sequentielle Vergabe dieser Nummern verhindert wird. (Dieser Umstand wurde zuvor ebenfalls zur Kartenfälschung genutzt.) Paßfotos auf der Karte scheinen sich allmählich durchzusetzen.

Auf die Zustellung der *Kreditkarten* per Post wird entweder ganz verzichtet – die Übergabe der Karte erfolgt persönlich am Bankschalter – oder die Karte wird erst nach Empfangsbestätigung sowohl der Karte als auch der getrennt versandten bzw. persönlich übergebenen zugehörigen PIN freigegeben.

Bei der Benutzung von *Kreditkarten* an POS-Terminals (Point of Sale – Verkaufsstelle), die zur Autorisierung der Zahlungstransaktionen online mit dem jeweiligen Rechenzentrum verbunden sind, werden Plausibilitätsprüfungen durchgeführt. So kann beispielsweise anhand der dort gespeicherten Informationen zum bisherigen Konsumverhalten – Kaufbeträge nie über 500 DM und monatlich weniger als insgesamt 5 000 DM – bei einem aktuell geforderten Betrag von 10 000 DM eine zusätzliche Identitätsprüfung des Kartennutzers veranlaßt werden, bevor der Zahlungsvorgang akzeptiert wird. Die gleiche Wirkung kann auch eine Prüfung hinsichtlich der räumlichen Entfernung der POS-Standorte innerhalb eines kurzen Zeitintervalls haben.

Seit einiger Zeit vermehren sich die Ankündigungen der Anbieter von *Kreditkartensystemen* zur schrittweisen Ablösung der unsicheren Magnetstreifen durch Chips, die eine wesentlich höhere Fälschungssicherheit aufweisen.

**Debitkarten**

Ein klassisches Beispiel für eine *Debitkarte* ist die „ec-Karte“. Diente sie anfangs seit Einführung von Euroschecks 1968 lediglich als Schecksicherungskarte und später zur Bereitstellung von Bargeld an Geldausgabeautomaten, kamen im Laufe der Zeit weitere Funktionen hinsichtlich des bargeldlosen Zahlungsverkehrs hinzu. Eine wesentliche Etappe dieser Entwicklung stellte die Inbetriebnahme des „electronic-cash-Systems“ (ec-Karte + PIN) im Jahre 1990 dar. Neben diesem Zahlsystem entstand 1992 auf Druck des Handels ein Online-Lastschrift-Verfahren, das als „*POZ-System*“ (Point Of Sale ohne Zahlungsgarantie) bezeichnet wird, und bei dem auf die Eingabe der PIN verzichtet wird. Statt dessen gibt der Karteninhaber dem Händler per Unterschrift (Vergleich mit der Unterschrift auf der Karte) auf einem Beleg zum einen eine Lastschrifteinzugsermächtigung, zum anderen eine Einwilligung zur Adreßmitteilung durch sein Geldinstitut an den Händler bei Ablehnung einer Lastschrift.

Auch die PIN stellt ein risikobehaftetes Authentifikationsmittel dar. Die *PIN-Berechnung* aus einigen im Magnetstreifen der ec-Karte gespeicherten Daten (die PIN selbst ist dort nicht gespeichert!) zum Abgleich mit der eingegebenen PIN erfolgt – auch im Ausland – grundsätzlich online im mit dem jeweiligen Endgerät verbundenen Rechenzentrum. Sollte diese Verbindung unterbrochen sein, besteht lediglich die Möglichkeit einer limitierten Bargeldauszahlung (Offline-Prüfung). Der dem PIN-Verfahren zugrundeliegende Algorithmus basierte bisher auf einer Verschlüsselung von Kartendaten mit geheimen Schlüsseln von 56 Bit Länge.

Aus dem Ergebnis der Verschlüsselung werden die vierstelligen PINs in einer Weise berechnet, die dazu führt, daß die PINs zwar alle Werte zwischen 1000 und 9999 annehmen können, innerhalb dieses Zahlenbereichs jedoch keine Gleichverteilung auftritt. Vielmehr gibt es bestimmte PINs, die fast zehnmal häufiger auftreten, als es bei der Gleichverteilung der Fall wäre.

Dieser Umstand und die Warnung der Experten zur Sicherheit des *Verschlüsselungsverfahrens* haben erstmals zu einem rechtskräftigen Urteil[99] geführt, in dem u. a. festgestellt wird, daß „davon ausgegangen werden muß, daß ein Täter auch ohne Mitwirkung des Karteninhabers Kenntnis von der PIN entweder durch Ausprobieren oder durch Entschlüsselung anhand der auf der Karte abgespeicherten Daten erlangt hat“. Diese von den Kreditinstituten nach wie vor heftig bestrittene Feststellung bedeutet, daß ein Kreditinstitut nicht mehr so selbstverständlich von

99 Oberlandesgericht Hamm vom 17. März 1997, 31 U 72/96

einem Betrugsversuch oder von grober Fahrlässigkeit des Kunden ausgehen kann, wenn dieser angibt, daß mit einer ihm abhanden gekommenen Karte Geld von seinem Konto abgehoben wurde.

Die meisten Kreditinstitute – leider noch nicht die Berliner Sparkasse – haben inzwischen begonnen, ihren Kunden eine neue PIN zuzuweisen und die Berechnungs- und Verifizierungsverfahren so zu verändern, daß die beschriebenen Schwächen beseitigt wurden. Das bisherige Verschlüsselungsverfahren wurde durch eine andere Version ersetzt, die doppelt so lange Schlüssel verlangt und somit nach heutigem Kenntnisstand als absolut sicher gelten kann.

Es bleibt das Problem, daß die vierstellige PIN immer noch ausgeforscht werden kann, wenn sie an Geldautomaten oder an *ec-cash-Terminals* vor den Augen Dritter eingegeben wird. Den damit verbundenen Risiken könnte man dadurch entgegenwirken, daß man dem Kunden die Möglichkeit eröffnet, die PIN ohne weiteres ändern zu können, wenn er den Eindruck hat, sie könnte ausgespäht worden sein. Das neue Verfahren enthält die Option, daß dem Kunden jederzeit die Möglichkeit eröffnet wird, die PIN beliebig zu wählen. Hier bestünde jedoch die Gefahr, daß Kunden sich leicht zu merkende, damit aber auch leicht zu erratende PINs wählen. Ein wirklich manipulationssicheres Authentifizierungsverfahren dürfte erst mit *biometrischen Verfahren* (z. B. Fingerabdruckverfahren) möglich sein, die jedoch bisher noch keinen hinreichenden Entwicklungsstand erreicht haben.

**Wertkarten**

Seit einiger Zeit werden von einigen Geldinstituten (bei der Berliner Sparkasse generell, bei anderen nur auf ausdrücklichen Wunsch) ec-Karten ausgegeben, in deren Kartenkörper ein Chip implantiert ist. Die mit diesem Chip verbundene Funktionalität entspricht dem einer *Wertkarte*, die auch als „elektronische Geldbörse“ bezeichnet wird. Im Gegensatz zum Magnetstreifen, bei dem die darauf gespeicherten Daten mit vergleichsweise einfachen technischen Mitteln ausgelesen und verändert werden können, ist der Chip als ein eigenständiger „intelligenter“ Minicomputer anzusehen. Hier können sowohl Daten als auch Programme geschützt gespeichert werden. Bei der Berliner Sparkasse und anderen Anbietern firmiert diese elektronische Geldbörse unter dem Begriff *„GeldKarte“*, während sie als Gemeinschaftsprodukt der Deutschen Bahn AG, der Deutschen Telekom AG und des Verbandes Deutscher Verkehrsunternehmen als *„PayCard“* zunächst in bestimmten Regionen (Berlin zählt derzeit noch nicht dazu) erprobt wird.

Allen gemeinsam ist die grundsätzliche Zweckbestimmung: der Einsatz zur Bezahlung von Waren und Dienstleistungen im Niedrigpreisbereich, ohne daß an den Erwerber dieser Karte Bonitätsansprüche gestellt werden müßten. Aus datenschutzrechtlicher Sicht gibt es zwei sich gravierend voneinander unterscheidende Modifikationen der elektronischen Geldbörse. Zum einen kann die Karte so beschaffen sein, daß ihr Gebrauch völlig unabhängig von personenbezogenen Daten – mithin anonym – erfolgen kann, zum anderen ist ihre Nutzung an ein Konto des Karteninhabers gebunden. Im ersten Fall spricht man von einer *„Weißen Karte“*. Was diese Kartenart von einer vergleichbaren Telefonkarte (bei der nach dem Verbrauch des auf der Karte gespeicherten Guthabens allenfalls noch ein gewisser Sammlerwert zu verzeichnen ist) unterscheidet, ist die *Mehrfachnutzung durch Wiederaufladen* mit Bargeld. Während die PayCard in dieser Variante angeboten wird und konzeptionell auch bei der GeldKarte der Kreditinstitute vorgesehen ist, favorisiert die Berliner Sparkasse eindeutig die kontengebundene GeldKarte, bei der auf die Nutzung personenbezogener Daten nicht verzichtet werden kann.

Beim Ladevorgang (z. B. an einem mit dem GeldKarten-Logo gekennzeichneten Geldautomaten) wird zunächst die Echtheit der Karte geprüft. Die zur Authentifizierung des Kartenbesitzers notwendige Eingabe der PIN wird durch den Chip kontrolliert, ehe die durch ein Kryptogramm gesicherten Ladedaten (u. a. Betrag, Informationen zum kartenausgebenden Institut und verschlüsselte Daten zum Kartenkonto) zur jeweiligen Ladezentrale gesendet werden. Sind alle übermittelten Daten korrekt, werden

die Kontodaten entschlüsselt und am zur GeldKarte gehörenden Konto geprüft, ob der Ladebetrag autorisiert, d. h. freigegeben werden kann. Bei positivem Prüfungsergebnis wird dieser Betrag vom Konto des Kartenbesitzers abgebucht und einem „Börsenverrechnungskonto“ (BVK – reines Saldenkonto ohne Bezug auf die konkrete Geldkarte und das damit verknüpfte Kundenkonto) gutgeschrieben. Die wiederum durch ein Kryptogramm gesicherte Ladeantwort wird an das Terminal zurückgesendet; nach Prüfung der Integrität und Authenzität der Daten durch den GeldKarten-Chip wird der aktuelle Saldo der Börse um den Ladebetrag erhöht. Bei erfolgreichem Abschluß des Ladevorgangs werden die dabei relevanten Daten (u. a. Kartennummer und Ladebetrag, nicht aber die Kontonummer) an die *„Kartenevidenzzentrale“* (KEZ – registriert alle Lade- und Entlade- bzw. Bezahlvorgänge zu einer Geldkarte) übermittelt. Beim Laden der Geldkarte wird demzufolge der entsprechende „Schattensaldo“ um den jeweiligen Ladebetrag erhöht.

Wird die so gefüllte Börse – es ist von einem Maximalbetrag von 400 DM auszugehen – anschließend zum Bezahlen (ohne Eingabe der PIN!) genutzt, ergibt sich in der Regel der folgende Ablauf: Am Display des Händlers wird der Kaufbetrag angezeigt, vom Kunden bestätigt und dessen GeldKarte in das Händlerterminal eingeführt. Da auf dem Chip u. U. verschiedene Zahlungsfunktionen („Börsenapplikationen“), bezogen auf bestimmte Händler- oder Dienstleistungsanbietergruppen, vorgesehen sein können, wird durch das Händlerterminal die diesem konkreten Fall entsprechende Variante ausgewählt und die Kartenidentifikationsdaten einschließlich des aktuellen Börsensaldos übernommen. Nach Prüfung der übernommenen Daten hinsichtlich ihrer Plausibilität wird die Abbuchung des Kaufbetrags veranlaßt. Auf dem GeldKarten-Chip wird der aktuelle Betrag der Börse um den Kaufbetrag reduziert und der Kaufvorgang einschließlich der händlerspezifischen Daten gespeichert. Der Datensatz, der den Zahlvorgang widerspiegelt, wird im Händlerterminal abgespeichert, wobei er zum Schutz vor Manipulationen mit einem Zertifikat versehen wird. Dem Karteninhaber wird abschließend die ordnungsgemäße Beendigung der Kauftransaktion und der auf seiner Karte verbliebene Restsaldo angezeigt. Die im Händlerterminal gespeicherten Datensätze werden dann regelmäßig an die *„Händlerevidenzzentrale“* (HEZ) zur Verrechnung weitergeleitet. Die auf die GeldKarte bezogenen Transaktionsdaten werden von der HEZ an die KEZ übermittelt, um den dort geführten Schattensaldo der betroffenen GeldKarte zu aktualisieren. Die händlerbezogenen Transaktionsdaten werden von der HEZ über einen Datenträgeraustausch zum einen als Gutschrift der Händlerbank zugeleitet und zum anderen als summarische Sammellastschrift dem jeweiligen Börsenverrechnungskonto zur Aktualisierung dessen Saldos übermittelt.

Dem Karteninhaber soll zur persönlichen Kontrolle des Guthabens auf seiner GeldKarte ein einfaches und preiswertes Lesegerät zur Verfügung gestellt werden. Bei Reklamationen sind grundsätzlich zwei Bearbeitungsvarianten (Chip lesbar / Chip defekt) zu unterscheiden. Bei lesbarem Chip werden über ein *Bankenleseterminal* die auf der GeldKarte gespeicherten (maximal 3) letzten Ladevorgänge, die ebenfalls dort gespeicherten (maximal 15) letzten Zahlvorgänge (sie enthalten jeweils Angaben zum Zeitpunkt der Zahlung, zur Banken- bzw. Händlerterminal-Identifikation und den Betrag) sowie der Kartensaldo zur Klärung der vermuteten bzw. tatsächlichen Unstimmigkeiten angezeigt. Falls der Chip defekt ist, muß sich der Karteninhaber etwas gedulden, da dann auf den bei der KEZ gespeicherten Schattensaldo zurückgegriffen werden muß. Wegen der unterschiedlichen Händlereinreichungsfristen können diese Daten frühestens nach 15 Tagen unter Angabe der Kartennummer abgerufen werden. Nach Rückmeldung (sie beinhaltet den Kartensaldo und den Buchungstag) kann dann das noch vorhandene Guthaben bar ausgezahlt oder dem Konto des Karteninhabers gutgeschrieben werden. Die Möglichkeit zur Barauszahlung bzw. Kontengutschrift des Restguthabens besteht.

Da die GeldKarte ohne Eingabe der PIN zum Bezahlen genutzt werden kann und auch eine Unterschrift entbehrlich ist, kann jeder, der in den Besitz dieser Karte gelangt, das auf ihrem Chip noch gespeicherte Restguthaben verbrauchen. Insoweit wäre der Verlust einer kontounabhängigen GeldKarte mit dem Verlust eines Portemonnaies gleichzusetzen.

Die Risiken hinsichtlich der Erstellung von *individualisierbaren Konsumprofilen* bei der Nutzung einer kontogebundenen GeldKarte sind gering. Nur beim eigenen Kreditinstitut ist über Karten- und Kontonummer der Inhaber der GeldKarte ermittelbar. Nachvollziehbar sind dort jedoch nur die Ladevorgänge. Das Börsenverrechnungskonto wird nur als Saldenkonto ohne individuellen Karten- bzw. Händlerbezug geführt. Selbst anläßlich der Reklamationsbearbeitung bei defektem Chip erhält die Bank von der KEZ lediglich Informationen zum Kartensaldo und zum Buchungstag. Beim Händler werden sowohl die kartenbezogenen Einzeltransaktionen als auch die Summendatensätze durch ein Kryptogramm gesichert, um den Risiken hinsichtlich der Einreichung gefälschter bzw. verfälschter Umsätze sowie der Mehrfacheinreichung von Umsätzen zu begegnen. Auch ein automatisierter Zugriff auf die Kundendaten ist am Händlerterminal nicht möglich.

Als eine mögliche Schwachstelle könnten die Evidenzzentralen (KEZ und HEZ) angesehen werden, da dort sowohl händler- als auch kartenbezogene Informationen verfügbar sind. Jedoch ist auch hier der Kundenbezug nicht herstellbar, da die Kette Kartennummer-Kontonummer-Karteninhaber bereits bei der Kartennummer unterbrochen wird. Selbst die Reklamationsbearbeitung erfolgt bei den Kreditinstituten allein über ihre Bankleitzahl und die Nummer der GeldKarte.

Eine umfassende Nutzung der GeldKarte in Berlin ist derzeit noch nicht möglich, da es noch an der dazu notwendigen Infrastruktur fehlt. Zum einen gibt es erst eine geringe Anzahl von Akzeptanzstellen, bei denen die GeldKarte zum Bezahlen genutzt werden könnte, zum anderen fehlt es auch noch an Ladestationen in den Filialen der Kreditinstitute. So will die Berliner Sparkasse bis zum Februar 1998 ca. 50 % ihrer Filialen entsprechend ausgestattet haben. Inwieweit die GeldKarte auch an institutsfremden Terminals aufgeladen werden kann und welche Zusatzkosten dadurch entstehen können, muß abgewartet werden.

**Homebanking**

Die rasante technische Entwicklung und die damit verbundene weite Verbreitung von PCs – gerade auch im privaten Bereich – unterstützt eine andere Strategie der Geldinstitute, ihren Zahlungsverkehr noch umfassender zu rationalisieren: die direkte Abwicklung finanzieller Geschäfte aus dem unmittelbaren Umfeld ihrer Kunden heraus. Die sich aus der Nutzung von offenen Kommunikationsnetzen (Telefonnetz, Internet) ergebenden Vorteile für beide Seiten befördern diesen Trend nachhaltig. Einerseits erspart sich der Kunde den Gang zur nächstgelegenen Filiale seiner Bank und macht sich zudem unabhängig von deren Öffnungszeiten, andererseits können die Kreditinstitute ihr Personal reduzieren, ganze Filialen schließen oder sogar ganz auf den Aufbau eines Filialnetzes verzichten (Direktbanken) und somit erhebliche Kosteneinsparungen erzielen.

Als eine Variante dieser Transaktionsabwicklung hat sich das Homebanking über den Netzzugang *T-Online* der Deutschen Telekom AG durchgesetzt (ursprünglich *Btx* bzw. *Datex-J*). So hat sich die Zahl der Homebanker im zurückliegenden Jahr nahezu verdoppelt. Wer über einen PC und einen Telefonanschluß verfügt, benötigt lediglich noch ein Modem (bei analogem Telefonanschluß) bzw. eine ISDN-Karte sowie eine mehr oder weniger komfortable Zugangssoftware für seinen Computer, um sich bei seiner Bank als Online-Kunde anzumelden. Als Dankeschön für die Kooperationsbereitschaft werden die letztgenannten Hilfsmittel sogar häufig zum „Nulltarif“ zur Verfügung gestellt. Über die mit dieser Art der Kontoführung verbundenen Risiken wird der potentielle „Homebanker“ allerdings in den seltensten Fällen umfassend informiert. Die Hinweise beschränken sich in der Regel darauf, daß er für eine sichere Verwahrung der neben der Kontonummer für den Zahlungsverkehr notwendigen geheimzuhaltenden Daten zu sorgen hat. Dazu gehört zum einen das für den T-Online-Zugang benötigte persönliche Paßwort, das zunächst als Einstiegspaßwort vom Netzanbieter vorgegeben wird und nach der ersten Anmeldung zu ändern ist. Zum anderen sind die von der Bank auf dem Postweg zugestellte PIN (im allgemeinen fünfstellig) und die Liste mit den *Transaktionsnummern* (TAN, im allgemeinen sechsstellig) so zu hinterlegen, daß Unbefugten der Zugriff verwehrt wird. T-Online-Paßwort und Bank-

PIN sollten möglichst nur im Gedächtnis des Nutzers hinterlegt sein, um das Mißbrauchsrisiko (z. B. für den Fall eines Wohnungseinbruchs) so gering wie möglich zu halten.

Kann man sich auf diese Weise vor einem direkten Zugang zum Konto über den eigenen PC noch recht gut schützen, erweist sich das zur Datenkommunikation genutzte Telefonnetz als ein weiteres bedeutsames *Risiko.* Mit verhältnismäßig geringem technischem Aufwand kann der Datenaustausch zwischen dem Kunden und seiner Bank gezielt „abgehört" und aufgezeichnet werden (z. B. an den oftmals leicht zugänglichen Telefonverteilerkästen von Wohnanlagen). Da nach dem bisherigen Homebanking-Verfahren auch die sicherheitsrelevanten Daten unverschlüsselt über das Netz transportiert werden, kann ein solcher Täter Kenntnis von den Zugangsdaten erhalten und diese anschließend am eigenen PC nutzen, um sich zunächst über die Bonität des jeweiligen Homebankers zu informieren. Mit der PIN allein ist der *Online-Bankraub* nämlich noch nicht zu bewerkstelligen. Der Zugriff auf das Konto nach der Eingabe der PIN beschränkt sich im wesentlichen auf „lesende" Funktionen. Zum Veranlassen (Autorisieren) von Überweisungen, Einrichten von Daueraufträgen und zur Anforderung von ec-Scheck-Vordrucken werden zudem die TANs benötigt. Da diese unmittelbar nach einmaliger Verwendung verfallen, nützt die Aufzeichnung einer solchen Transaktion dem Angreifer zunächst nicht viel, es sei denn, er ist auf irgendeine Weise an die TAN-Liste gelangt und kann so die nächstgültige TAN ermitteln und für illegale Aktivitäten einsetzen.

Mit größerem technischem Aufwand und entsprechendem Know-how kann der „Online-Räuber" beim Anzapfen der Telefonleitung mittels eines speziellen Programms *(Watchdog)* die interessanten Transaktionen herausfiltern und in seinem Sinne modifizieren (sog. „Man in the Middle Attack"), bevor sie weitergeleitet werden. Eine weitere Bedrohung kann sich dann ergeben, wenn im Netz angebotene Software ungeprüft auf den eigenen PC geladen wird und sich dadurch unbemerkt ein Virus einschleicht, der nach gezieltem Ausforschen der PC-Speicher bei der nächsten Online-Verbindung die für einen erfolgreichen Zugriff auf das Konto notwendigen Daten über das Netz dem potentiellen Angreifer zustellt.

Der Homebanker sollte also tunlichst darauf verzichten, seine geheimen Daten auf seinem PC zu speichern. Das bedeutet insbesondere auch, auf die von einigen Homebanking-Softwareprodukten angebotenen, den automatisierten Zugang zum Konto ermöglichenden Anmeldeprozeduren zu verzichten und Paßwort, PIN und TAN bei jeder Online-Sitzung über die Tastatur einzugeben. Hier sollte zur eigenen Sicherheit die Bequemlichkeit nachrangig sein. Wenn sich auch der T-Online-Geschäftsführer dafür verbürgt, daß es seit den Btx-Anfängen keinen echten Kriminalfall gegeben hat, scheint das Risikobewußtsein bei den Kreditinstituten doch so gewachsen zu sein[100], daß ernsthaft nach Möglichkeiten gesucht wurde, das Homebanking sicherer zu gestalten. Die wichtigsten Verbände der deutschen Kreditwirtschaft haben sich 1997 darauf verständigt, ihren Kunden die Abwicklung von Bankgeschäften via Homebanking multibankfähig und gesichert zu ermöglichen. Dazu hat man sich auf die Bereitstellung eines offenen Standards zur Datenübertragung und Dialogabsicherung geeinigt: das *Homebanking Computer Interface* (HBCI). Diese Schnittstelle bei der Datenübertragung sieht vor, alle Nachrichten vom Kunden zur Bank mit einer digitalen Signatur (elektronische Unterschrift) zu versehen und diese Nachrichten standardisiert mit dem *Triple-DES-Verfahren* zu verschlüsseln. Dabei wird angestrebt, an den PC ein Chipkarten-Lesegerät anzuschließen und mit Hilfe einer speziellen Chipkarte, deren intelligenter Chip die Realisierung aller Sicherheitsfunktionen übernimmt, den Datenaustausch auf eine gesicherte Basis zu stellen. Allerdings werden bei dieser Methode die geheimzuhaltenden Daten zumindest noch auf dem Weg von der Tastatur zum PC ungeschützt transferiert. Um die Übertragung der Finanztransaktionen für heimliche Lauscher uninteressant zu machen, nutzt beispielsweise die Sparda-Bank Hamburg bereits seit Juli 1996 eine Hardwarekomponente, den *MeCHIP,* um den Datentransfer durch Verschlüsselung und elektronische Unterschrift zu sichern. Ein nicht zu unterschätzender Vorteil dieser

100 siehe FAZ v. 16. Dezember 1997, S. T 6: „17 Jahre Homebanking ohne Panne"

Technologie besteht darin, daß dieses Sicherheitsmodul direkt an die Tastatur angeschlossen wird und demzufolge unverschlüsselte Daten noch nicht einmal in den Arbeitsspeicher des PCs gelangen können.

Nicht alle Kreditinstitute sind jedoch in der Lage, die Sicherheit ihrer Online-Banking-Produkte mit der notwendigen Souveränität plausibel zu machen: Als die Berliner Verwaltungsakademie uns um Hinweise bat, ob die Durchführung ihrer Haushaltsgeschäfte mit Hilfe der Software ModernCash der *Deutschen Postbank AG* über T-Online datenschutzrechtlich zulässig und sicher sei, baten wir das Kreditinstitut routinemäßig um die Überlassung von Informationen, die uns eine datenschutzrechtliche Beurteilung erlauben würden.

Der Rest war eine Farce: Eine erste E-Mail-Anfrage wurde höflich bestätigt und an den ModernCash-Experten weitergeleitet. Dieser bot über das gleiche Medium ein Gespräch an und benannte seine Kontaktadresse und Telefonnummer. Nachdem zwei Monate später diverse telefonische Kontaktversuche gescheitert waren, wandten wir uns schriftlich an den Experten. Da dies ohne Antwort blieb, versuchten wir es zwei Monate später per Telefax. Ein weiterer Versuch per E-Mail blieb ebenfalls ohne Antwort. Fünf Monate nach einer vertröstenden Zwischennachricht an die Verwaltungsakademie erfolgte dann ein erneuter schriftlicher Versuch, die Blockade der Postbank zu durchbrechen. Endlich kam dann ein telefonischer Kontakt mit dem Experten zustande, der zwar abwehrend reagierte, dennoch die Übersendung des Materials binnen zwei Wochen versprach[101].

Über die Sicherheit des Postbank-Verfahrens darf man also weiter spekulieren. Wir haben der Verwaltungsakademie deshalb mitgeteilt, daß wir unter diesen Umständen empfehlen, von der Nutzung der Postbank-Software abzusehen.

**Digitales Geld**

Im als „Netz der Netze“ bezeichneten Internet setzt sich immer mehr eine Form der unmittelbaren Bezahlung von Waren und Dienstleistungen durch, die am ehesten noch mit der Wertkartentechnologie (siehe GeldKarte) vergleichbar ist: *elektronisches/digitales Geld*. Ein derartiges Zahlungssystem basiert auf *virtuellen Geldmünzen/Banknoten*, die durch kryptographische Verfahren gegen Fälschungen gesichert im PC gespeichert und auf elektronischem Weg übertragen werden können. Um sich vor einem Betrug durch mehrfach eingereichte, identische Banknoten zu schützen, versieht das ausgebende Kreditinstitut ihre „Geldscheine“ mit einer Seriennummer, die bei Einlösung von der Empfängerbank gespeichert wird und so durch Abgleich mit den zuvor eingegangenen Banknoten unzulässige Duplikate erkennbar macht. Die emittierten Geldscheine werden zudem mit einer digitalen Signatur der Ausgabebank versehen, wobei ein spezielles Verfahren, die „blinde Signatur“, den Käufer der Geldscheine unkenntlich macht. Beim Bezahlen mit einer solchen Banknote kann wiederum der Empfänger (z. B. ein Händler) des Geldes diese Signatur auf Echtheit überprüfen, ohne die ausgebende Bank konsultieren zu müssen. Der Versuch, die Banknote mehrfach zum Bezahlen zu benutzen bzw. vom Händler mehrfach einlösen zu wollen, führt durch ein ausgeklügeltes Verschlüsselungssystem zur Überführung des Betrügers, obwohl weder der Händler noch die Bank die auf dem Geldschein verschlüsselt vorhandenen, jedoch „zerbrochenen“ personenbezogenen Daten des Kunden entziffern kann (sog. „secret splitting“). So ist gewährleistet, daß die Anonymität des Nutzers von digitalem Geld lediglich im Falle eines Mißbrauchs aufgehoben werden kann. Auf Grund dessen kann auch das datenschutzrechtlich bedeutsame Risiko der Erstellung von Nutzungsprofilen, das bei den zuvor beschriebenen elektronischen Zahlungsverfahren mehr oder minder vorhanden ist, weitestgehend ausgeschlossen werden. Ob dieses Verfahren auch gegen kriminelle Mißbrauchsattacken gefeit ist, mag bei der Struktur des Internets allerdings bezweifelt werden.

101 Wenige Tage vor Redaktionsschluß erreichte uns ein entschuldigendes Fax mit ersten Informationen und einem Gesprächsangebot

# 4. Aus den einzelnen Arbeitsgebieten

## 4.1 Sicherheit

### 4.1.1 Polizei

Mit dem am 1. August 1997 in Kraft getretenen *Bundeskriminalamtgesetz* (BKAG)[102] ist endlich eine bereichsspezifische Rechtsgrundlage für die polizeiliche Informationsverarbeitung auf Bundesebene – insbesondere für die Übermittlungen der Landespolizeien an das BKA – geschaffen worden. Die erwartete Verlagerung von datenschutzrechtlichen Kompetenzen[103] zu Lasten der Länder auf den Bund ist nunmehr festgeschrieben.

Nach der Ratifikation des Übereinkommens vom 26. Juli 1995 über den Aufbau einer europäischen Zentralstelle für den unterstützenden Informationsaustausch zwischen den Mitgliedstaaten und für die Analyse von bestimmten schwerwiegenden Formen der internationalen Kriminalität (Europolkonvention)[104] wurden im vergangenen Jahr nunmehr auch das Europol-Gesetz und das Europol-Auslegungs-Protokoll-Gesetz[105] verabschiedet.

Mit dem *Europol-Gesetz* wird die Konvention in nationales Recht umgesetzt. Im einzelnen regelt das Gesetz die

- Ziele und Aufgaben von Europol;
- Stellung und Aufgaben der nationalen Stellen, mit denen Europol verbunden ist, einschließlich der Aufgaben der von jedem Mitgliedstaat zu entsendenden nationalen Verbindungsbeamten;
- Ausgestaltung des bei Europol einzurichtenden Datenverarbeitungssystems und der Zugriffsmöglichkeiten durch die Mitgliedstaaten sowie die nationalen Verbindungsbeamten;
- datenschutzrechtlichen Anforderungen an den Umgang mit den bei Europol befindlichen und von Europol weiterzuleitenden Daten;
- Regelung der Haftung und der gerichtlichen Kontrolle von Handlungen von Europol und die
- institutionellen Fragen, die im Zusammenhang mit der Errichtung einer gemeinsamen Behörde aller EU-Mitgliedstaaten erforderlich sind.

Das *Europol-Auslegungs-Protokoll-Gesetz* regelt die Vorab-Entscheidungskompetenz des Europäischen Gerichtshofes in Fällen, in denen bei Verfahren vor nationalen Gerichten entscheidungsrelevante Fragen der Auslegung des Europol-Übereinkommens auftreten. Durch die Einbeziehung des Europäischen Gerichtshofes soll eine einheitliche Auslegung des Europol-Übereinkommens in den Mitgliedstaaten der Europäischen Union sichergestellt werden.

Auf der Grundlage des Europol-Übereinkommens ist von den Mitgliedstaaten der Europäischen Union ferner ein Protokoll über die Vorrechte und Immunitäten für Europol, die Mitglieder der Organe und die Bediensteten von Europol unterzeichnet worden, dessen Umsetzung mit dem *Europol-Immunitäten-Protokoll-Gesetz* erfolgen soll.

Folgende verfassungsrechtliche Bedenken der Datenschutzbeauftragten sind unberücksichtigt geblieben:

- Die rechtliche Konstruktion als zwischenstaatliche Einrichtung läßt eine unmittelbare Kontrolle des Europäischen Parlamentes nicht zu.
- Die Mitarbeiter von Europol sollen für Straftaten – dazu zählen auch Datenschutzverstöße –, die sie im Amt begehen, nicht zur Rechenschaft gezogen werden.
- Bürger laufen Gefahr, in das Datennetz dieser Behörde zu geraten. Es geht nicht nur um die Erfassung der Daten von Straftätern, sondern auch von Zeugen oder Opfern.
- Das fundamentale Recht des Betroffenen im Datenschutzrecht – der Auskunftsanspruch – wird verkürzt. Der Auskunftsantrag kann ohne Begründung zurückgewiesen werden.

102 BGBl. I, S. 1650
103 JB 1996, 4.1.1
104 BGBl. 1997 II, 2150
105 BGBl. 1997 II, 2170

Die Verkürzung des Rechtsschutzes der Bürger ist damit gerechtfertigt worden, daß Europol bisher keine „exekutiven Befugnisse“ habe. Dabei wird verkannt, daß jede Verwendung personenbezogener Daten zu massiven Eingriffen in Grundrechte der Betroffenen führt.

**Errichtungsanordnung für AFIS**

Bei dem Bundeskriminalamt (BKA) wird die Datei AFIS geführt, die dazu dient, über einen *daktyloskopischen* Vergleich Personen und unbekannte Tote zu identifizieren. Zudem können mit der Datei über einen daktyloskopischen Vergleich von Tatortfingerspuren und in der Datei erfaßten Fingerabdruckdaten Spurenverursacher identifiziert werden. Die nicht identifizierten Tatortfingerspuren können in einem gesonderten Bestand gespeichert und untereinander abgeglichen werden, um Tatzusammenhänge zu erkennen. AFIS wird bei dem BKA als Zentraldatei geführt. Die Länder liefern dazu elektronische Daten zum Zweck der Spurenauswertung an oder fragen diese ab. Insoweit handelt es sich um eine Verbundanwendung mit der Folge, daß die Länder der Errichtungsanordnung zustimmen müssen.

Bei der Errichtungsanordnung, deren Entwurf uns die Senatsverwaltung für Inneres vor der erteilten Zustimmung nicht zur Kenntnis gegeben hat, haben wir neben einigen noch klärungsbedürftigen Punkten folgende Mängel festgestellt:

Die *bereichsspezifischen Regelungen* über erkennungsdienstliche Sammlungen und Verbundanwendungen des neuen BKAG wurden nicht berücksichtigt. Nach § 34 Abs. 1 Nr. 3 BKAG ist der *Personenkreis* konkret festzulegen, über den die Daten gespeichert werden. Diesen Anforderungen genügt ein allgemeiner Hinweis auf „daktyloskopierte Personen, soweit nach der Zweckbestimmung der Daten deren Speicherung zulässig ist“ nicht. In AFIS sollen neben den Fingerabdrücken, die nach Polizeirecht und Strafprozeßordnung erhoben wurden, auch die nach dem *Ausländergesetz* (AuslG) und dem *Asylverfahrensgesetz* (AsylVfG) erhobenen Daten gespeichert werden. § 78 Abs. 2 AuslG und § 16 Abs. 4 AsylVfG schreiben – zusätzlich zu der besonderen Kennzeichnung der Daten – eine von anderen erkennungsdienstlichen Unterlagen getrennte Aufbewahrung vor. Das Bundesministerium des Innern hat in seinem Entwurf der allgemeinen Verwaltungsvorschriften zum AuslG vorgesehen, daß mit der getrennten Aufbewahrung der Unterlagen (getrennte Behältnisse, Räume, Dateien und besondere Zugangsberechtigungen) sicherzustellen ist, daß sie nur für ausländerrechtliche Zwecke genutzt werden können. Der Entwurf der Errichtungsanordnung entsprach nicht diesen gesetzlichen Vorgaben. Die Innenressorts anderer Länder haben die Zustimmung zu der Errichtungsanordnung nicht so schnell erteilt, sondern vielmehr gegenüber dem Bundesminister des Innern Bedenken angemeldet.

Obwohl es sich bei den in der Datei AFIS gespeicherten Daten auch um Daten handelt, für deren Speicherung Berliner Stellen verantwortlich sind, weigerte sich die Senatsverwaltung für Inneres, uns zu beteiligen.

Das Zustimmungsverfahren ist inzwischen gescheitert. Das Bundesministerium des Innern hat eingeräumt, daß das Konzept problematisch ist, die logisch getrennten und damit eigenständigen Datenbesände von AFIS-Fahndung und AFIS-Asyl zusammenzuführen. Das BKA ist gebeten worden, getrennte Ermittlungsanordnungen zu erstellen, die dann erneut in das Zustimmungsverfahren gegeben werden. Wir erwarten, daß wir diesmal von der Senatsverwaltung für Inneres beteiligt werden.

**Besondere polizeiliche Ermittlungsmethoden**

Obwohl die polizeilichen Ermittlungsmethoden mit Änderung der Polizeigesetze der Länder[106], mit dem Verbrechensbekämpfungsgesetz und dem Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) um eine Reihe tief in das Persönlichkeitsrecht eingreifender Überwachungsmöglichkeiten ergänzt wurden, halten die Diskussionen um die Einführung weiterer Eingriffsbefugnisse wie den *Großen Lauschangriff* und neuerdings den „*Spähangriff*“ (heimliche Bildaufnahmen in Wohnungen) unvermindert an.

Der Senat ist der Auffassung, daß die vom Berliner Datenschutzbeauftragten an der Errichtungsanordnung für die Datei AFIS bemängelten Punkte in die datenschutzrechtliche Verantwortung des Bundeskriminalamts fallen und gegebenenfalls vom Bundesdatenschutzbeauftragten zu überprüfen sind.

Bei der Datei AFIS handelt es sich um eine Zentraldatei, die das Bundeskriminalamt nach § 8 Abs. 6 BKAG führt. Nur soweit Daten durch die Landeskriminalämter auf Stromwegen zum Zwecke der Spurenauswertung angeliefert oder abgefragt werden, handelt es sich um eine Verbundanwendung im Sinne des § 11 Abs. 2 BKAG.

Die datenschutzrechtliche Verantwortung für Zentraldateien trägt das Bundeskriminalamt, das insoweit der datenschutzrechtlichen Kontrolle des Bundesbeauftragten für den Datenschutz unterliegt. Da sich die Einwendungen des Berliner Datenschutzbeauftragten gegen die Errichtungsanordnung nur auf Bereiche erstrecken, die außerhalb der Verbundanwendung und damit auch außerhalb unserer fachaufsichtlichen Kompetenzen lagen, haben wir von einer inhaltlichen Stellungnahme abgesehen.

Allerdings enthält § 12 Abs. 2 BKAG für Verbundanwendungen im Rahmen des polizeilichen Informationssystems (§ 11 Abs. 2 BKAG) eine Sonderregelung dahingehend, daß die datenschutzrechtliche Verantwortung für die bei der Zentralstelle gespeicherten Daten namentlich für die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit oder Aktualität der Daten den Stellen obliegt, die die Daten unmittelbar eingeben. Die Verantwortung für die Zulässigkeit eines Abrufs trägt die abrufende Stelle. Im übrigen bleibt aber auch bei solchen Dateien die datenschutzrechtliche Verantwortung des Bundeskriminalamts bestehen. Dementsprechend erstreckt sich die Prüfungskompetenz der Landesbeauftragten für den Datenschutz nach § 12 Abs. 3 BKAG auf die von den Ländern eingegebenen Datensätze. Im übrigen obliegt dem Bundesbeauftragten für den Datenschutz die Datenschutzkontrolle.

Die Errichtung von Dateien des polizeilichen Informationssystems (Verbundanwendungen) bedarf der Zustimmung der zuständigen Innenministerien und Senatsinnenverwaltungen der Länder (§ 34 Abs. 2 BKAG). Allerdings ist nach § 34 Abs. 1 BKAG auch in diesen Fällen vor Erlaß einer Errichtungsanordnung der Bundesbeauftragte für den Datenschutz anzuhören. Auf Grund dieser klaren gesetzlichen Regelung und der nach § 12 Abs. 3 BKAG beschränkten Prüfkompetenz der Landesbeauftragten für den Datenschutz auf die von den Ländern in das polizeiliche Informationssystem eingegebenen Datensätze gehen wir davon aus, daß es nicht im Aufgabenbereich des Berliner Datenschutzbeauftragten liegt, zu generell-abstrakten Regelungen in einer Errichtungsanordnung des Bundeskriminalamts Stellung zu nehmen. Die ohne Zweifel notwendige datenschutzrechtliche Kontrolle ist bei Errichtungsanordnungen des Bundeskriminalamts durch den Bundesbeauftragten für den Datenschutz gewährleistet.

106 In Berlin durch die Neufassung des ASOG am 26. April 1992, GVBl. 1992, S. 119, zuletzt geändert durch Gesetz vom 19. Juli 1994, GVBl. S. 241

Bevor weitere Ermittlungsbefugnisse eingeführt werden, müssen zunächst einmal über die Auswirkungen des vorhandenen Instrumentariums Erfahrungen gesammelt werden und diese einer Erfolgungskontrolle unterzogen werden[107]. Dies ist dringend geboten, da der Einsatz der besonderen Ermittlungsmethoden zur vorbeugenden Straftatenbekämpfung in den Jahren 1994 bis 1996 kontinuierlich zugenommen hat, ohne daß etwas über die Eingriffsintensität und den Erfolg der Maßnahmen bekannt ist.

So hat der verdeckte Einsatz technischer Mittel (heimliche Bildaufnahmen und heimliches Abhören außerhalb von Wohnungen, § 25 Abs. 1 Nr. 2 ASOG) von insgesamt 18 auf 43 Anordnungen zugenommen. Der Einsatz von V-Personen (§ 26 Abs. 1 Nr. 1 ASOG), stieg von 24 auf 56 Anordnungen. Der verdeckte Einsatz technischer Mittel in oder aus Wohn- und Nebenräumen sowie Arbeits-, Betriebs- und Geschäftsräumen, also der „Große Lauschangriff“ zur Gefahrenabwehr (§ 25 Abs. 4 ASOG) stieg von einer Anordnung im Jahre 1994 auf vier Anordnungen im Jahre 1996.

Welche Erfolge diese Maßnahmen bei der Bekämpfung der Kriminalität erbracht haben und inwieweit dabei das informationelle Selbstbestimmungsrecht der Betroffenen eingeschränkt wurde, sollte jährlich in einem öffentlichen Bericht gegenüber dem Abgeordnetenhaus dargelegt werden, um die parlamentarische Kontrolle zu verbessern und mehr Transparenz in diesem Bereich zu erhalten.

Den Lauschangriff im Jahre 1994 haben wir überprüft, das Verfahren war bemerkenswert.

> *Ein Anbieter äußerte bei der Polizei die Befürchtung, daß bei einem in einem Lokal vereinbarten Gespräch mit Vertretern der Verwaltung entweder später die Behauptung eines Korruptionsversuches aufgestellt oder er mit der Forderung eines Schmiergeldes konfrontiert werden könnte.*

Für die Staatsanwaltschaft kam ein Ermittlungsverfahren nicht in Betracht. Darüber hinaus wäre eine Maßnahme nach § 100 c StPO unzulässig gewesen, weil das Delikt nicht zu den Katalogstraftaten des § 100 a StPO zählte. Die Staatsanwaltschaft hat die Polizei allerdings darauf aufmerksam gemacht, daß sie eine Maßnahme nach § 25 Abs. 4 ASOG in eigener Zuständigkeit durchführen könne. Danach kann die Polizei in oder aus Wohn- und Nebenräumen Daten nur erheben, wenn das zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerläßlich ist. Die Einschränkung gilt nicht für *Arbeits-, Betriebs- und Geschäftsräume* sowie andere Räume, die der Öffentlichkeit zugänglich sind oder zugänglich waren und den Anwesenden zum weiteren Aufenthalt zur Verfügung stehen, wenn der Lauschangriff während der Arbeits-, Geschäfts- oder Aufenthaltszeit erfolgt.

Maßnahmen nach § 25 Abs. 4 ASOG dürfen – außer bei Gefahr im Verzug – nur durch den Richter angeordnet werden. Das Amtsgericht Tiergarten hat den Antrag der Polizei mit der Begründung abgelehnt, daß keine Straftat von erheblicher Bedeutung vorliegt. Die sofortige Beschwerde des Polizeipräsidenten hat das Landgericht zurückgewiesen. Erst nach einer weiteren Beschwerde hat das Kammergericht diese Beschlüsse aufgehoben und die Sache an das Amtgericht zurückverwiesen, weil es die Auslegung des Begriffes „Straftaten von erheblicher Bedeutung“ nicht teilte. Da in der Zwischenzeit der Zeitpunkt eines Gespräches abgelaufen war, beantragte die Polizei für ein weiteres, in einem Lokal vereinbartes Gespräch erneut bei dem Amtsgericht Tiergarten den Lauschangriff. Das wurde abermals abgelehnt mit der Begründung, daß Sinn und Zweck der gesetzlichen Regelungen des ASOG auf die Gefahrenabwehr und die vorbeugende Straftatenbekämpfung zielen. Durch das Abhören bzw. Aufzeichnen des Gespräches würden jedoch keine Straftaten bekämpft oder verhindert, sondern lediglich dokumentiert. Dies sei nicht Aufgabe und Sinn der Regelung. Auf Grund der sofortigen Beschwerde der Polizei hat letztlich das Landgericht den Einsatz der technischen Mittel angeordnet.

Bei der geschilderten Maßnahme handelt es sich um den ersten Fall seit der Neufassung des ASOG im Jahre 1992, in dem die Befugnisnormen des § 25 Abs. 4 ASOG zur Anwendung kam. Somit waren auch die Berliner Gerichte erstmals mit dieser Rechtsmaterie befaßt, was möglicherweise zur uneinheitlichen Einschätzung des Falls beigetragen hat.

Eingeleitet wurden die polizeilichen Maßnahmen durch die Anzeige eines freien Unternehmers bei einer kriminalpolizeilichen Ermittlungsstelle, der aussagte, durch Vertreter einer Berliner Behörde aufgefordert worden zu sein, Verhandlungen über einen möglichen Geschäftsabschluß nach Dienstschluß in einem Lokal zu führen, da man ein solches Gespräch nicht in einem Büro führen könne. Ferner wurde der Geschäftsmann angehalten, nur allein, ohne Begleitperson zu erscheinen. Das Ziel der konspirativen Verhandlungen blieb im Dunkeln.

Bereits im ersten einleitenden Bericht der Ermittlungsdienststelle wurde abschließend festgehalten, daß die Beantragung eines richterlichen Beschlusses zum Einsatz technischer Mittel gemäß § 25 Abs. 1 Nr. 2 ASOG angestrebt werde. Eine Maßnahme nach 100 c StPO wurde in diesem Bericht nicht erörtert. Am Folgetag wurde die ASOG-Maßnahme schriftlich beantragt und durch einen Richter des Amtsgerichtes zurückgewiesen, da nach Auffassung des Gerichts keine Straftat von erheblicher Bedeutung in Frage stand.

Gegen diesen Beschluß wurde durch die Polizei schriftlich Beschwerde eingelegt. Unter anderem wurde die durch dem Amtsrichter gezogene Analogie zu den §§ 138 StGB und 100 a StPO hinsichtlich der Definition einer Straftat von erheblicher Bedeutung beanstandet, da im § 17 Abs. 4 ASOG selbst Ordnungswidrigkeiten unter bestimmten Voraussetzungen den Straftaten von erheblicher Bedeutung gleichgestellt werden. Diese Beschwerde wurde durch die Zivilkammer des Landgerichts zurückgewiesen, da die Auffassung des Amtsgerichts geteilt wurde. Gegen diesen Beschluß wurde durch die Polizei unter Hinweis darauf, daß Eingriffe nach § 25 ASOG auch unter den Voraussetzungen des § 17 Abs. 3 ASOG möglich sind, weitere Beschwerde erhoben. Das Landgericht hielt am angefochtenen Beschluß fest.

107 vgl. Entschließung der Datenschutzkonferenz, JB 1994, Anlage 2.9

Wie bedenklich der Lauschangriff bei derart vagen Eingriffsvoraussetzungen ist, belegen die *widersprüchlichen Entscheidungen* der Gerichte eindrucksvoll. Der fehlende Straftatenkatalog und die schwammige Voraussetzung, daß lediglich Tatsachen vorliegen müssen, die die Annahme rechtfertigen, daß eine Straftat von erheblicher Bedeutung begangen wird, führen zu einer erheblichen Rechtsunsicherheit für Betroffene.

Im vorliegenden Fall konnte nicht einmal ein Erfolg den Eingriff rechtfertigen. Die Auswertung der Bänder ergab keine Anhaltspunkte für eine Straftat. Die Mitarbeiter der Verwaltung haben vielmehr sogar die Übernahme der Zeche abgelehnt. Bei dem Gespräch wurden lediglich die Positionen in einem Rechtsstreit in anderer Sache ausgetauscht.

Durch Beschluß des Kammergerichts schließlich wurden die Beschlüsse der Vorinstanzen aufgehoben und der Argumentation der Polizei gefolgt, insbesondere hinsichtlich der Legaldefinition der Straftat von erheblicher Bedeutung. Die Vorschriften der §§ 100 a und 100 c StPO stehen nach Auffassung des Kammergerichts der Gesetzesauslegung des § 17 Abs. 3 ASOG nicht entgegen, weil die StPO-Regelung nicht abschließend sei und der Gesetzgeber bei der Regelung der Gefahrenabwehr durch die Polizei weitergehende Tatbestände als die strafprozessualen einbeziehen kann.

Die Darstellung dieses Sachverhaltes im Jahresbericht macht deutlich, wie wenig den Datenschutzbauftragten die Rechtsauffassung des Kammergerichts beeindruckt. Die vom Datenschutzbeauftragten gewählte Darstellung läßt auch nicht erkennen, daß in einem besonders sensiblen Fall von Korruptionsverdacht der lange Rechtsweg (mit der Konsequenz, daß die Verabredung mit dem Verdächtigen immer wieder hinausgeschoben werden mußte) für die Ermittlungen nicht gerade förderlich war.

Die vier Fälle aus dem Jahr 1996 hätten wir gern in unsere Prüfung einbezogen; leider haben sich die Entscheidungsträger im Landeskriminalamt mit unserem Wunsch nach Akteneinsicht sehr schwer getan. Es war – trotz der wiederholt geäußerten Bitte im Laufe des Jahres 1997 – nicht möglich, uns die Unterlagen zur Verfügung zu stellen.

Welche *praktischen Schwierigkeiten mit dem Lauschangriff* verbunden sind, zeigt eine Entscheidung des Bundesgerichtshofs aus dem vergangenen Jahr[108].

Der BGH hat das *heimliche und verdeckte Öffnen des Kfz zum Zweck des Einbaus einer Abhöreinrichtung* für zulässig erklärt. Er weist zwar darauf hin, daß es an einer ausdrücklichen gesetzlichen Bestimmung, ob und wie weit zur Durchführung des Abhörens vorbereitende oder begleitende Maßnahmen, die in sonstige Rechte des Betroffenen oder Dritter eingreifen, zulässig sind, fehlt, sieht jedoch in § 100 c Abs. 1 Nr. 2 StPO eine konkludente Ermächtigung durch den Gesetzgeber für Vorbereitungs- und Begleitmaßnahmen, die mit dem Abhören typischerweise verbunden sind. Nicht zulässig wäre danach jedoch das Verbringen des Pkw in eine Werkstatt, ohne daß der Eigentümer zugestimmt hat, da dies keine typische Vorbereitungsmaßnahme für das Abhören sei. Es handelt sich zudem bei dem Entzug des Fahrzeuges nicht mehr um einen geringfügigen Eingriff in die Rechte des Betroffenen. Dagegen stellt das bloße Öffnen des Fahrzeuges nach Auffassung des BGH nur einen geringfügigen Eingriff in den Rechtskreis des Betroffenen dar, der diesem zugemutet werden kann.

Auf eine entsprechende Anfrage des Berliner Datenschutzbeauftragten wurde diesem mit Schreiben des Polizeipräsidenten in Berlin vom 10. Oktober 1997 mitgeteilt, daß im Jahr 1996 der verdeckte Einsatz technischer Mittel in oder aus Wohn- und Nebenräumen sowie Arbeits-, Betriebs- und Geschäftsräumen gemäß § 25 Abs. 4 ASOG viermal angeordnet wurde. Mit Schreiben vom 11. November 1997 bat der Berliner Datenschutzbeauftragte um Einsicht in sämtliche bei der Polizei geführten Unterlagen. Da die Unterlagen zu den oben genannten Maßnahmen nicht zentral geführt werden, sondern je nach Einsatzlage unterschiedliche Dienststellen betroffen sind, mußte zunächst eingehend recherchiert werden, wo zu den jeweiligen Fällen Akten abgelegt sind, um eine umfassende Einsichtnahme zu ermöglichen.

Am 29. Januar 1998 führte der Berliner Datenschutzbeauftragte seine Einsichtnahme durch. Ein Bericht des Berliner Datenschutzbeauftragten mit dem Ergebnis seiner Überprüfung ist dem Polizeipräsidenten in Berlin bisher nicht zur Stellungnahme zugegangen.

**Der abgehörte Anwalt in der Wahllichtbildvorlage**

*Ein Strafverteidiger stellte bei der Einsicht in die Ermittlungsakte des Beschuldigten fest, daß sein eigenes Lichtbild Dritten anläßlich einer zeugenschaftlichen Vernehmung in einer Wahllichtbildvorlage gezeigt wurde. Das Landeskriminalamt hatte vermerkt, daß es sich um die Lichtbilder von ermittelten möglichen Tatverdächtigen handelt.*

Was war geschehen? Auf Grund mehrerer Beschlüsse des Amtsgerichts Tiergarten wurde das Telefon des Beschuldigten abgehört. Unter den Protokollen waren fünf Wortprotokolle von Anrufen des Beschuldigten bei seinem Verteidiger. Daraufhin hat das Landeskriminalamt (LKA) das Lichtbild des Verteidigers aus dem Personalausweisantrag bei der Meldebehörde angefordert, weil er für verdächtig gehalten wurde.

Die Gespräche des Verteidigers wurden überwacht, obwohl bekannt war, daß dieser den Gesprächspartner, gegen den die Telefonüberwachung angeordnet worden war, im zugrundeliegenden Verfahren anwaltlich vertritt. § 148 Strafprozeßordnung (StPO) garantiert demgegenüber den freien, unüberwachten mündlichen – und damit auch telefonischen – Verkehr zwischen Verteidiger und Beschuldigtem. Diese Bestimmung schränkt § 100 a StPO hinsichtlich der Überwachung von Verteidigergesprächen ein. Daraus folgt, daß Gespräche zwischen Verteidiger

108 1 BGs 88/97

und Beschuldigtem nicht überwacht werden dürfen. Der *Europäische Gerichtshof* für Menschenrechte bezeichnet die vertrauliche Kommunikation zwischen Verteidiger und Beschuldigtem auch als Menschenrecht[109].

Bereits die *Aufzeichnung von Gesprächen zwischen Verteidiger und Beschuldigtem* auf Bändern ist unzulässig, da die bloße Datenerhebung und -speicherung eine Überwachung des Verteidigergespräches darstellt. Die Senatsverwaltung für Justiz hatte uns allerdings in einem anderen Zusammenhang bereits mitgeteilt, daß die derzeitig vorhandene Technik das Unterdrücken der eingehenden Verteidigergespräche nicht zuläßt. Die Entwicklungskosten für ein derartiges Verfahren seien nicht absehbar. Auch ein alleiniges Mithören durch Polizeibeamte sei nicht durchführbar und auch rechtlich problematisch. Die Arbeitsbänder würden in der Regel zunächst von der Polizei ausgewertet. Die Prüfung der Verwertbarkeit erfolge allein durch den zuständigen Staatsanwalt. Wenn schon bei der Aufzeichnung der Gespräche Verteidigergespräche nicht unterdrückt werden können, habe allerdings eine Niederschrift eines Verteidigergespräches bei der Auswertung des Arbeitsbandes zu unterbleiben. Nur so würde das Überwachungsverbot des § 148 StPO umgesetzt.

Die Staatsanwaltschaft, die erst durch unsere Prüfaktivitäten von dem Vorgang Kenntnis erlangt hat, teilt ebenfalls unsere Auffassung, daß Gespräche des Beschuldigten mit seinem Verteidiger nicht überwacht werden dürfen und – sofern es die technische Ausstattung bei der Telefonüberwachungsaufzeichnung nicht zuläßt, die Aufnahme derartiger Gespräche von Anfang an zu verhindern – von diesen Gesprächen zumindest keine Arbeitskopien und Abschriften gefertigt werden dürfen. Dennoch erstellte Aufzeichnungen müßten vernichtet werden.

Zu den Hintergründen der Wahllichtbildvorlage haben wir folgendes festgestellt:

Die Polizei hat Gespräche aus der Telefonüberwachung in einem Parallelverfahren ohne vorherige Rücksprache mit der Staatsanwaltschaft verwertet. Die Verwertung war zwar grundsätzlich zulässig, nicht jedoch die Verwertung der unzulässigerweise gespeicherten Verteidigergespräche. Weil die Polizei die Gesprächspartner des Beschuldigten offenbar als potentielle Mittäter angesehen hatte, wurde auch das Lichtbild des Verteidigers bei dem Landeseinwohneramt aus seinem Personalausweisantrag beschafft und dieses im Rahmen der Wahllichtbildvorlage verwandt. Die Polizei wollte bei der Beschaffung des Lichtbildes nicht gewußt haben, daß es sich um den Verteidiger des Beschuldigten gehandelt hat. Das ist sowohl nach unserer als auch der Auffassung der Staatsanwaltschaft nur schwer nachzuvollziehen, da die Informationen über den Verteidiger von dem Mitarbeiter der Polizei stammten, der dort das Parallelverfahren bearbeitete, in dem der Rechtsanwalt ebenfalls den Beschuldigten vertrat. Die Staatsanwaltschaft hat zusätzlich darauf hingewiesen, daß die bloße Tatsache, daß jemand zum Bekanntenkreis eines Beschuldigten zählt, noch niemanden automatisch verdächtig mache. Irgendwelche Indizien, die auf den Verteidiger als möglichen Tatbeteiligten hingewiesen hätten, habe es nicht gegeben. Die Staatsanwaltschaft hätte daher keinen Anlaß gesehen, irgendwelche Ermittlungen in dieser Richtung zu führen.

Nach alledem war die Aufnahme des Lichtbildes des Verteidigers in eine Wahllichtbildvorlage unzulässig. Auch diese Auffassung wird von der Staatsanwaltschaft geteilt.

**Durchführung der Telefonüberwachung**

Die Durchführung von Telefonüberwachungsmaßnahmen war auch Gegenstand einer Amtsprüfung bei Staatsanwaltschaft und Polizei an Hand einer kleinen Stichprobenauswahl. Wenn auch im Großen und Ganzen kein Anlaß für eine Beanstandung vorgefunden wurde, traten doch über die beschriebenen Probleme beim Abhören von Anwälten hinaus eine Reihe von Mängeln zu Tage, die Gegenstand von Erörterungen mit Staatsanwaltschaft und Polizei sind.

Der umfangreiche Bericht des Berliner Datenschutzbeauftragten ist der Staatsanwaltschaft zunächst zur Stellungnahme übersandt worden. Der Senat bittet um Verständnis dafür, daß vor Eingang der Stellungnahme eine Äußerung zu den Einzelpunkten nicht erfolgen kann.

109 EGMR, Urt. v. 28. November 1991, NJW 92, 3090

Eine wesentliche Voraussetzung für die Rechtmäßigkeit der Telefonüberwachung ist das in § 100 b Abs. 5 StPO festgelegte Verbot der Zweckentfremdung von Daten, die aus der Maßnahme stammen. Wir stellten fest, daß es in Einzelfällen für erforderlich gehalten wird, auch aus kriminaltaktischen Erwägungen Erkenntnisse zur *vorbeugenden Straftatenbekämpfung* festzuhalten. Damit ist eine unzulässige Durchbrechung der Zweckbestimmung verbunden. Durch die Telefonüberwachung erlangte Unterlagen dürfen nur zur Strafverfolgung genutzt und von der Polizei nicht in die Kriminalakte des Betroffenen aufgenommen werden.

Nach § 101 Abs. 1 StPO sind die Beteiligten zu *benachrichtigen*, sobald dies ohne Gefährdung des Untersuchungszwecks, der öffentlichen Sicherheit, von Leib und Leben einer Person sowie der weiteren Verwendung eines eingesetzten nicht offen ermittelnden Beamten geschehen kann. Um welche Personen es sich bei den Beteiligten handelt, hat der Gesetzgeber in dem Wortlaut der Regelung offen gelassen. Beteiligte sind der Beschuldigte und in den Fällen des § 100 a Satz 2 StPO die Personen, gegen die sich die Maßnahme richtet, also die Anschlußinhaber. Problematisch ist die Frage, wer zu benachrichtigen ist, wenn bei Überwachungsmaßnahmen – wie häufig bei Mobiltelefonen der Fall – der Anschlußinhaber nicht identisch mit dem tatsächlichen Nutzer des Telefons ist. Sofern sich bei einer Telefonüberwachungsmaßnahme herausstellt, daß Anschlußinhaber und Nutzer eines Anschlusses nicht personenidentisch sind, ist die tatsächlich abgehörte Person als Beteiligter anzusehen und von der Telefonüberwachungsmaßnahme zu unterrichten. Bis auf einen Fall wurden die Beteiligten von der Staatsanwaltschaft unterrichtet oder waren Gründe, aus denen die Unterrichtung unterbleiben konnte, dokumentiert. In diesem Fall ergab sich aus der Akte lediglich, daß die Benachrichtigung der Beteiligten beabsichtigt war.

Die durch die Telefonüberwachungsmaßnahmen erlangten Unterlagen sind unverzüglich unter Aufsicht der Staatsanwaltschaft zu *vernichten*, sobald sie zur Strafverfolgung nicht mehr erforderlich sind (§ 100 b Abs. 6 StPO). Über die Vernichtung ist eine Niederschrift anzufertigen. Hierzu zählen nicht nur die Tonträger selbst, sondern auch die Protokolle der Tonbandaufzeichnungen sowie Aktenvermerke. Unzulässig ist, Kopien der Unterlagen in einem Aktenretent bei der Polizei zurückzuhalten.

Bei *Zufallsfunden*, die bei der Telefonüberwachung gewonnen worden sind, ist zu klären, ob ein Verwertungsverbot vorliegt. Bei anderen als in der richterlichen Anordnung bezeichneten Katalogtaten nach § 100 a StPO ist die Verwertung gegen den Beschuldigten oder einen Teilnehmer zulässig. Zufallsfunde zu Nicht-Katalogtaten dürfen dagegen nicht unmittelbar zum Beweis und damit auch nicht zum Vorhalt genutzt werden. Zulässig ist nach der Rechtsprechung nur eine mittelbare Verwertung des Zufallsfundes in der Weise, daß auf Grund der erlangten Erkenntnisse Ermittlungen durchgeführt werden mit dem Ziel, andere Erkenntnisse zu gewinnen. Zufallsmaterialien, bei denen ein Verwertungsverbot besteht, sind unverzüglich zu vernichten und die Tonbänder, auf denen die Aufzeichnung erfolgt ist, zu löschen[110].

In einem Fall fiel eine Zufallserkenntnis an, die keine Katalogstraftat betrifft. Gleichwohl hat die Polizei Gesprächsprotokolle an eine andere Polizeidienststelle zur Weiterermittlung übersandt. Zulässig wäre nur die Mitteilung gewesen, daß der Verdacht auf ein bestimmtes Delikt besteht. Diese Mitteilung reicht als Ermittlungsansatz aus.

Die Staatsanwaltschaft ist verpflichtet, die *unverzügliche Vernichtung* der nicht (mehr) benötigten Telefonüberwachungsprotokolle und Aufzeichnungsbänder zu prüfen. Allerdings wird die Staatsanwaltschaft nicht immer vom LKA darüber informiert, ob tatsächlich auch Wortprotokolle von den aufgezeichneten Gesprächen gefertigt worden sind. Überhaupt gibt es Mängel bei der Unverzüglichkeit der Umsetzung: Zwei bis drei Monate sind nicht ungewöhnlich, aber auch Zeiträume von über einem Jahr nach Erreichung des Ziels der Maßnahme wurden festgestellt. Wir sind der Auffassung, daß ein Zeitraum von mehr als einem Monat den Begriff der Unverzüglichkeit nicht mehr erfüllt.

110 OLG Koblenz Beschluß v. 21. Dezember 1993 – 3vas 25/93 – in 94, S. 284

Die Prüfung hat ergeben, daß die Entscheidung über die Protokollierung und Auswertung der Gespräche stark vom Ermessen des einzelnen polizeilichen Sachbearbeiters abhängt. Angesichts des massiven Eingriffs in die Grundrechte der Beschuldigten und unbeteiligter Dritter sollte die Durchführung von Telefonüberwachungsmaßnahmen verbindlich, einheitlich und transparent in einer Geschäftsanweisung geregelt werden. Hierfür haben wir eine Reihe von konkreten Vorschlägen gemacht.

Ein erheblicher Mangel lag darin, daß uns die Polizei nicht nach § 24 Abs. 3 Satz 3 BlnDSG über die Anschaffung einer *digitalen Abhöranlage* vorab informiert hatte, wie dies in einem anderen Bundesland der Fall war. Datenschutzrechtliche Belange wie die Unterdrückbarkeit der Aufzeichnung von Verteidigergesprächen hätten so berücksichtigt werden können.

**Datenerhebung bei polizeilichen Ermittlungen**

*Anläßlich der Ermittlungen wegen einer Vergewaltigung bat das Landeskriminalamt das Virchow-Klinikum schriftlich um Übersendung der Untersuchungsbefunde des Opfers. Eine Person, die autorisiert ist, das Schreiben zu öffnen, war nicht benannt. Sowohl der Name, Geburtstag, Geburtsort und Wohnort des Beschuldigten als auch der Name des minderjährigen Opfers waren dem Schreiben zu entnehmen. Um den tatsächlichen Adressaten innerhalb des Krankenhauses zu ermitteln, wurde der Brief von der Poststelle geöffnet und irrtümlich an eine Abteilung weitergeleitet, die mit dem Vorgang gar nichts zu tun hat. Wie viele weitere Stellen bzw. Personen in dem Krankenhaus noch von dem Inhalt des Schreibens Kenntnis nehmen konnten, ist nicht bekannt.*

Das Schreiben wurde in der beschriebenen Form in der Erwartung übersandt, daß der behandelnde Arzt innerhalb des Krankenhauses schneller ausfindig gemacht werden könne, als dies durch Ermittlungen der Polizei der Fall wäre.

Die *Übermittlung von Daten zur Person des Beschuldigten* an das Virchow-Klinikum war unzulässig. Die Beamten des Polizeidienstes haben Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten (§ 163 StPO). Es gilt der Grundsatz, daß das Ermittlungsverfahren frei gestaltet werden kann. Dennoch hat sowohl die Staatsanwaltschaft als auch die Polizei den Grundsatz der Verhältnismäßigkeit zu berücksichtigen. Die Weitergabe personenbezogener Daten an Dritte hat bei Sexualdelikten eine erheblich diskriminierende Wirkung für die Betroffenen, insbesondere den Beschuldigten, wenn sich der Tatverdacht nicht bestätigen sollte. Die Übermittlung von Angaben zum vermutlichen Tathergang einschließlich des Namens, Geburtsdatums und -ortes, Wohnortes, der Straße und Hausnummer des mutmaßlichen Täters ist bei der Anforderung von Untersuchungsbefunden des Opfers nicht erforderlich und damit unverhältnismäßig.

Hier kam erschwerend hinzu, daß durch die *fehlerhafte Adressierung* und die fehlende Benennung der zuständigen Abteilung im Virchow-Klinikum bzw. des dortigen behandelnden Arztes unbefugte Dritte vom Inhalt des Briefes Kenntnis nehmen mußten. Bei der Verarbeitung personenbezogener Daten sind Maßnahmen zu treffen, die den Zugriff Unbefugter beim Transport verhindern (§ 5 Abs. 2 BlnDSG). Das Vorgehen der Polizei war ein eklatanter Verstoß gegen diesen datenschutzrechtlichen Grundsatz. Die erforderlichen Angaben für eine korrekte Adressierung des Schreibens an den behandelnden Arzt oder an die Fachabteilung, die für derartige Untersuchungen zuständig ist, wären durch eine telefonische Rücksprache mit dem Virchow-Klinikum oder eine Nachfrage bei den Erziehungsberechtigten des Opfers in Erfahrung zu bringen gewesen.

*Eine Petentin beschwerte sich über eine Mitarbeiterin der Polizei, die anläßlich eines gegen sie geführten Ermittlungsverfahrens bei einer beliebig aus dem Telefonbuch herausgesuchten Firma der Branche, in der die Petentin tätig ist, unter Nennung des Namens der Petentin allgemeine Erkundigungen einzog.*

Eine derartige, am Zufallsprinzip orientierte Ermittlung des Arbeitgebers einer Beschuldigten ist unverhältnismäßig. Durch das zufällige Heraussuchen von Telefonnummern von Unternehmen der Branche, in der die Beschuldigte tätig ist, und die anschließende telefonische Befragung der unbekannten Ge-

sprächsteilnehmer zur Person der Petentin wurden Dritte darüber unterrichtet, daß ein Ermittlungsverfahren gegen diese geführt wird. Eine Erforderlichkeit für die Offenbarung dieser sensiblen personenbezogenen Daten bestand nicht.

*Der Polizeipräsident in Berlin wurde von der Kreisordnungsbehörde des Landkreises Ostvorpommern im Zusammenhang mit einem Antrag einer Berlinerin auf Erteilung einer Gaststättenerlaubnis um Stellungnahme über den Leumund der Antragstellerin und deren Ehegatten gebeten sowie um Mitteilung, ob dort Versagungsgründe bekannt sind. Daraufhin hat der zuständige Kontaktbereichsbeamte die Nachbarn der Antragstellerin und ihres Ehemannes nach deren Lebensumständen befragt.*

Die Erhebungsbefugnis des Berliner Beamten, der in Amtshilfe für den Landkreis tätig wurde, richtet sich nach den Befugnissen dieser Stelle selbst.

Gemäß § 2 Abs. 1 Gaststättengesetz (GaststättenG) hat der Antragsteller einen Rechtsanspruch auf Erteilung der Erlaubnis, soweit dem nicht Versagungsgründe entgegenstehen. Die Versagungsgründe sind abschließend in § 4 GaststättenG aufgeführt. Die Erlaubnis ist vor allem zu versagen, wenn der Antragsteller unzuverlässig ist. Unzuverlässig ist, wer nicht die Gewähr dafür bietet, daß er sein Gewerbe in Zukunft ordnungsgemäß betreiben wird. Grundlage für diese Prognose kann nur das bisherige Verhalten des Betroffenen unter Würdigung aller mit seiner Person zusammenhängenden Umstände sein. Zur Beurteilung der Zulässigkeit darf die zuständige Stelle gemäß § 11 Abs. 1 Gewerbeordnung (GewO) (auf dessen Anwendbarkeit § 31 GaststättenG verweist) die erforderlichen personenbezogenen Daten des Antragstellers und solcher Personen, auf die es für die Entscheidung ankommt, erheben. Neben Daten zur Identifizierung der Person und zum beruflichen Werdegang können auch *Angaben zum Leumund* z. B. in strafrechtlicher oder finanzieller Hinsicht erforderlich sein. Auch hier gilt der Grundsatz der Datenerhebung bei dem Betroffenen (§ 11 Abs. 2 Satz 1 GewO). Bei anderen Personen oder Stellen dürfen die Daten ohne Mitwirkung des Betroffenen nur erhoben werden (vgl. § 11 Abs. 2 Satz 2 GewO), wenn die Entscheidung eine Erhebung bei Dritten erforderlich macht – was dann der Fall ist, wenn der Betroffene über den fraglichen Sachverhalt keine Angaben macht, die Information verweigert oder der Verdacht besteht, daß er falsche Informationen gegeben hat – oder wenn die Erhebung beim Betroffenen einen unverhältnismäßig hohen Aufwand erfordern würde. Darüber hinaus ist zwischen dem Interesse der zuständigen Behörde an der Erhebung ohne Mitwirkung des Betroffenen und dessen möglicherweise entgegenstehendem Interesse eine Abwägung vorzunehmen.

Im geschilderten Fall war eine Datenerhebung bei Dritten nicht erforderlich. Weder die zuständige Ordnungsbehörde in Ostvorpommern (Auftraggeber) noch der Kontaktbereichsbeamte der Berliner Polizei (Auftragnehmer) hätte die Befragung der Nachbarn durchführen dürfen.

**Videoaufzeichnungen anläßlich einer Kundgebung**

*Anläßlich einer genehmigten Kundgebung zum Thema „Abschaffung des Zwangseinkaufssystems und Wiedereinführung von Bargeldleistungen für Flüchtlinge und Asylbewerber" wurden von der Polizei Videoaufzeichnungen der Versammlungsteilnehmer gefertigt.*

Die Videoaufzeichnung deckt – mehrfach unterbrochen – den Zeitraum der Kundgebung und damit in Zusammenhang stehender Ereignisse ab. Die akustische Qualität ist schlecht, der Ton während der gesamten Länge des Filmes unverständlich. Es handelt sich vorwiegend um Gruppenaufnahmen der Veranstaltungsteilnehmer, wobei einzelne Personen durchaus identifizierbar sind. Im Hintergrund ist bei einigen Aufnahmen ein Fahrzeug erkennbar. Von diesem sollen laut Mitteilung der Polizei über Lautsprecher strafrechtlich relevante Redebeiträge verbreitet worden sein. Der Videoaufzeichnung ist dazu allerdings kein Hinweis zu entnehmen. Auf dem Rückweg von der Versammlung wurde das Fahrzeug, aus dem während der Versammlung über einen Lautsprecher Redebeiträge erfolgten, von der Polizei angehalten, zur Feststellung der Personalien der Insassen unter Anwendung von unmittelbarem Zwang geöffnet, die Insassen

Die in Rede stehenden Videoaufzeichnungen anläßlich des polizeilichen Einsatzes fanden bekanntlich im Anschluß an die Kundgebung des Flüchtlingsrats statt. Sie dienten der Beweissicherung, um die Identität der Insassen des Fahrzeugs festzustellen, aus dem zuvor während der Veranstaltung Redebeiträge mit beleidigendem Inhalt ausgestrahlt worden waren.

Entgegen der Annahme des Berliner Datenschutzbeauftragten handelte es sich hierbei nicht um Maßnahmen auf der Grundlage des Versammlungsrechts, die auf die Vorschrift des § 12 a des Versammlungsgesetzes zu stützen gewesen wären. Nach den auch uns überzeugenden Darlegungen der Polizeibehörde handelte es sich vielmehr um eine Maßnahme zum Zweck der Durchführung des Strafverfahrens. Als Rechtsgrundlage für die Videoaufzeichnungen kam mithin nur die Vorschrift des § 81 b 1. Alternative StPO in Betracht mit der Folge, daß auch die weitere Aufbewahrung der angefertigten Aufzeichnungen nach § 81 b 2. Alternative StPO zu beurteilen war.

§ 81 b StPO bestimmt, daß erkennungsdienstliche Maßnahmen auch gegen den Willen eines Beschuldigten vorgenommen werden dürfen. Gegen den Willen bedeutet nicht, daß ein entgegen-

wurden herausgeholt und dem polizeilichen Einsatzfahrzeug zugeführt. Dabei soll es zu Widerstandshandlungen gegen Mitarbeiter der Polizei gekommen sein. Die Aktion wurde, für die Betroffenen nicht erkennbar, aus dem Inneren des Einsatzfahrzeuges heraus aufgezeichnet.

Die Polizei darf gemäß § 12 a Versammlungsgesetz (VersG) Bild- und Tonaufnahmen von Teilnehmern bei oder im Zusammenhang mit öffentlichen Versammlungen – z. B. bei der An- und Abfahrt – anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß von ihnen eine erhebliche Gefahr für die öffentliche Sicherheit und Ordnung ausgeht. Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Nach Beendigung der öffentlichen Versammlung oder der damit im Zusammenhang stehenden Ereignisse sind die Unterlagen unverzüglich zu vernichten. Die Vernichtung kann gemäß § 12 a Abs. 2 Nr. 1 VersG unterbleiben, wenn die Daten zur Verfolgung von Straftaten, die von Teilnehmern begangen wurden, benötigt werden.

Die Voraussetzungen für die Datenerhebung und weitere Speicherung nach § 12 a VersG waren nicht erfüllt. Wir haben empfohlen, das Videomaterial – Originalaufnahme und Kopien – unverzüglich zu vernichten. Die Polizei ist dieser Empfehlung nicht gefolgt. Die Filme werden weiter aufbewahrt, weil man es zur Verfolgung von Straftaten für erforderlich hält. Überrascht hat die Begründung, die uns von der Polizei dafür mitgeteilt wurde. Danach wurde ein versammlungsrechtlicher Bezug für die Aufnahmen auf dem Rückweg von der Versammlung abgestritten und die *Videomaßnahme als erkennungsdienstliche Behandlung* erklärt, die auf § 81 b 1. Alternative StPO gestützt werden könne. Dabei wird verkannt, daß erkennungsdienstliche Behandlungen offen zu erfolgen haben. Im vorliegenden Fall wurden die Aufnahmen jedoch aus dem Innenraum eines Einsatzfahrzeuges für die Betroffenen nicht erkennbar – also verdeckt – gefertigt. Ohne Wissen des Betroffenen dürfen derartige Bildaufzeichnungen in Ermittlungsverfahren nur hergestellt werden, wenn die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise weniger erfolgversprechend oder erschwert wäre (§ 100 c Abs. 1 Nr. 1 StPO). Diese Voraussetzungen lagen nicht vor. Bemerkenswert ist in diesem Zusammenhang auch, nach welchen Kriterien die Polizei die *Abgrenzung zwischen verdeckten und offenen Maßnahmen* vornimmt. Für die Polizei kommt es anscheinend „auf die Heimlichkeit, insbesondere auf die Vertarnung polizeilichen Handelns“ an. Dies sei nicht gegeben, wenn „Einsatzkräfte aus ihrem Einsatzfahrzeug, das von jedermann als polizeiliches erkennbar war, videographierten und nichts taten, um ihre Zugehörigkeit zur Polizei zu verschleiern“.

Der heimlichen Erhebung personenbezogener Daten durch technische Mittel wären nach dieser Auffassung – abgesehen von dem immer zu beachtenden Erforderlichkeitsgrundsatz – kaum noch Grenzen gesetzt.

**Auskunft an Betroffene**

*Im Zusammenhang mit ihrem Antrag auf Auskunft über die bei dem Polizeipräsidenten in Berlin zu ihrer Person gespeicherten Daten wurde eine Petentin gebeten, Angaben zum Zeitpunkt, Ort und Anlaß einer möglichen Erfassung zu machen. Nur so könnten weitere dezentrale oder fachbezogene Datenspeicherungen überprüft werden.*

Ein Antragsteller wird auf Auskunft um *weitere Angaben zum Zeitpunkt, Ort und Anlaß einer möglichen polizeilichen Erfassung* gebeten, wenn sein Antrag auf eine umfassende Auskunft gerichtet ist und in den kriminalpolizeilichen Datensammlungen, bei denen der Name des Betroffenen als Suchkriterium dient, kein weiterer Datenbestand festgestellt werden konnte. In diesen Fällen ist nicht auszuschließen, daß der Antragsteller dennoch in Unterlagen der Polizei erfaßt ist. So werden z. B. über alle polizeilichen Einsätze Berichte gefertigt und zum großen Teil dezentral – sortiert nach Zeit, Ort und Anlaß des Einsatzes – in Tagebüchern zu Dokumentationszwecken für einen Zeitraum von zwei Jahren aufbewahrt. Eine Recherche nur nach den Personalien eines Auskunftssuchenden ist in diesen Datensammlungen nicht möglich. Nur durch die genannten zusätzlichen Angaben ist es mit vertretbarem Aufwand möglich, eventuell vorhandene Daten

stehender Wille ausdrücklich kundgegeben werden muß. Da der Gesetzgeber die Durchführung der erkennungsdienstlichen Behandlung ausdrücklich auch gegen den Willen des Betroffenen zuläßt, ist ein solcher Eingriff auch dann erlaubt, wenn der Betroffene aus unterschiedlichen Gründen einen solchen Willen nicht bekunden kann, weil er die Maßnahme nicht erkennt oder erkennen kann, eine sofortige Durchführung jedoch notwendig ist, um deren Erfolg nicht zu gefährden.

Zu diskutieren wäre allerdings die Frage nach einer nachträglichen Benachrichtigung des Betroffenen von der Tatsache der durchgeführten Maßnahme, um diesem die Möglichkeit zu geben, von seinem Recht auf informationelle Selbstbestimmung Gebrauch zu machen. Im vorliegenden Fall ist diesem Anliegen im Rahmen der Überprüfung des Vorgangs durch den Berliner Datenschutzbeauftragten Rechnung getragen worden. Auf die im jeweiligen Einzelfall zu treffende Abgrenzung zwischen verdeckten und offenen Maßnahmen kommt es daher nicht an.

zur Person des Auskunftsbegehrenden festzustellen. Das Verfahren entspricht den Bestimmungen des § 50 Abs. 1 Satz 2 ASOG und ist datenschutzrechtlich nicht zu beanstanden.

Interessante Angaben zum Auskunftsanspruch gegenüber der Polizei enthält die Antwort auf eine Kleine Anfrage[111]. Folgende Zahlen wurden vorgelegt:

| 1991 | 1992 | 1993 | 1994 | 1995 | 1996 | 1997 |
|---|---|---|---|---|---|---|
| 133 Anträge | 82 Anträge | 456 Anträge | 232 Anträge | 241 Anträge | 261 Anträge | 182 Anträge |

Die durchschnittliche Bearbeitungsdauer eines Datenauskunftsantrages betrug im ersten Halbjahr 1997 etwa drei Monate.

**Fristenberechnung bei der vorbeugenden Straftatenbekämpfung**

*Bei der Speicherung von Daten eines Betroffenen zur vorbeugenden Straftatenbekämpfung gemäß § 42 Abs. 3 ASOG ist es Praxis des Polizeipräsidenten in Berlin, daß die Prüffrist für die Aufbewahrung der Daten bzw. Unterlagen schematisch nach dem Zeitpunkt des zuletzt gespeicherten Datensatzes berechnet wird. Für bereits vorhandene Datenspeicherungen verlängert sich die Prüffrist – unabhängig von der Art der Daten – entsprechend. Eine Einzelfallprüfung zur Erforderlichkeit einer weiteren Speicherung dieses Altdatenbestandes über den ursprünglich festgesetzten Zeitpunkt hinaus findet nicht statt.*

Durch diese *schematische Anwendung der Prüffristen* kann eine unvertretbare *„Fristenspirale“* in Gang gesetzt werden. Im Ergebnis führt dies in vielen Fällen dazu, daß die zur Person gespeicherten Datensätze über Tatvorwürfe Auskunft geben, für die allein die übliche Speicherfrist schon verstrichen wäre. Besonders problematisch werden kann dieser Automatismus, wenn kurz vor Ablauf der Speicherfrist für das erste Delikt ein weiteres aus einem anderen Deliktsbereich hinzukommt oder wenn es nur um ein Bagatelldelikt geht.

Gemäß § 48 Abs. 4 Satz 3 ASOG beginnt der Fristenlauf regelmäßig mit dem letzten Anlaß für eine Datenspeicherung. Die von der Polizei geübte Praxis der Fristenberechnung steht im Widerspruch zu dieser Bestimmung. Durch die Verwendung des Begriffes „regelmäßig“ hat der Gesetzgeber klargestellt, daß beim Hinzutreten von Datenspeicherungen die Erforderlichkeit einer weiteren Speicherung bereits vorhandener Daten nicht schematisch vorausgesetzt werden darf, sondern in jedem Einzelfall zu prüfen ist.

Grundsätzlich sind personenbezogene Daten nach § 48 Abs. 2 Nr. 2 ASOG zu löschen, wenn ihre Kenntnis zur Erfüllung der Aufgaben der speichernden Stelle nicht mehr erforderlich ist. Ob die weitere Speicherung erforderlich ist, ist entweder bei der nach bestimmten Fristen vorzunehmenden Überprüfung oder aber aus Anlaß einer Einzelfallbearbeitung festzustellen.

Die Dauer der Prüffristen hat der Gesetzgeber und – auf der Grundlage der Verordnungsermächtigung in § 48 Abs. 4 ASOG – der Senat im Sinne einer verallgemeinernden Interessenabwägung schematisch festgelegt. Der Fristenlauf beginnt nach § 48 Abs. 4 Satz 3 ASOG und § 4 Abs. 1 Satz 3 der Prüffristenverordnung regelmäßig mit dem letzten Anlaß für eine Datenspeicherung. Jeder neue Speicheranlaß unterbricht also den Fristenlauf und setzt die Prüffrist erneut in Gang.

Mit dieser Regelung haben der Gesetzgeber und der Verordnungsgeber erkennbar die langjährigen bewährten Regelungen der Nr. 5 der Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KPS-Richtlinien) übernommen. Deshalb bestehen keine Bedenken, wenn die Polizei insbesondere auch bei der Fristenberechnung an der langjährigen Praxis festhält, die auf Nr. 5.5 der KPS-Richtlinien beruhte.

Im Einzelfall könnte allerdings die Situation eintreten, daß der letzte Speicheranlaß keinen Einfluß auf die Fristenberechnung hat. Wenn z. B. der letzte Speicheranlaß ein Fall von geringer Bedeutung ist, kann die für diesen Anlaß an sich festzulegende Frist kürzer sein als eine bereits laufende. In diesem Fall ist der spätere Prüfungstermin der bereits laufenden Frist maßgeblich.

Die Prüffrist läuft für alle in einer Datei über einen Betroffenen gespeicherten Daten einheitlich. § 48 Abs. 2 ASOG spricht allgemein von in Dateien gespeicherten personenbezogenen Daten und stellt nicht auf die unterschiedlichen Speicheranlässe ab. Daraus ergibt sich, daß die Vergabe unterschiedlicher Prüffristen zu verschiedenen Speicheranlässen von Gesetzes wegen nicht geboten ist.

Unabhängig von der Dauer der Prüffristen ist allerdings stets zu erwägen, ob die Speicherung von Daten zu einem neuen Anlaß überhaupt erforderlich ist. Dabei sind die bekannten, aus der Rechtsprechung des Bundesverwaltungsgerichts abgeleiteten Grundsätze entscheidend. Ein Anlaß, zu dem mangels Erforderlichkeit keine Daten gespeichert werden, kann auch nicht eine laufende Prüffrist unterbrechen und neu in Gang setzen. In diesem Fall läuft die bereits festgesetzte Frist weiter.

Die Prüfung, ob eine weitere Speicherung bereits vorhandener Daten noch erforderlich ist – sei es nach Ablauf der Prüffrist oder anläßlich einer Einzelfallbearbeitung – muß sich dann auf jedes einzelne zu einer Person gespeicherte Datum beziehen, so daß gegebenenfalls ein Teil der Daten zu bereinigen und ein anderer Teil weiterzuspeichern ist.

111 Antwort des Senats auf die Kleine Anfrage Nr. 13/2768 vom 7. Oktober 1997, ergänzt um den letzten Stand v. 1997

### 4.1.2 Verfassungsschutz

**Sicherheitsüberprüfungen**

Seit Jahren ist das Fehlen hinreichender Rechtsvorschriften für die Durchführung der Sicherheitsüberprüfungen der bedeutendste Mangel der Berliner Gebetzgebung. Es ist deshalb zu begrüßen, daß das Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Land Berlin *(Berliner Sicherheitsüberprüfungsgesetz* – BSÜG –) vom Senat im März 1997 im Abgeordnetenhaus eingebracht und dort beraten wurde[112]. Es wird Anfang 1998 in Kraft treten. Das Gesetz regelt den personellen Geheim- und Sabotageschutz bei öffentlichen und nichtöffentlichen Stellen. Es enthält Bestimmungen über die Voraussetzungen und das Verfahren der Sicherheitsüberprüfung von Mitarbeitern, die Beschreibung der Sachverhalte, die ein Sicherheitsrisiko begründen, den Umfang der zu erhebenden Daten, die Nutzung der erlangten Daten für andere Zwecke, die Wiederholungsprüfungen und die Auskunftsrechte des Betroffenen.

Über die von uns bereits gegenüber der Innenverwaltung vorgebrachten, aber nicht akzeptierten Empfehlungen[113], hinaus wurden in den Beratungen im Unterausschuß „Datenschutz“ des Abgeordnetenhauses weitere Verbesserungen erzielt:

Es soll genauer angegeben werden, welche Voraussetzungen vorliegen müssen, damit eine öffentliche Stelle oder ein Privatunternehmen als „*lebens- oder verteidigungswichtig*“ eingestuft werden kann. In einer Rechtsverordnung sind die zu schützenden Arten von Einrichtungen abschließend festzulegen. Damit wird für die Betroffenen transparent, in welchen Bereichen sie einer Sicherheitsüberprüfung unterzogen werden können. Nicht gefolgt wurde unserer Empfehlung, Sicherheitsüberprüfungen nur auf die Bereiche zu beschränken, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß[114].

In den Beratungen des Gesetzentwurfs im Unterausschuß „Datenschutz“ wurde unter Beteiligung des Berliner Datenschutzbeauftragten die im § 2 Nr. 4 BSÜG enthaltene Formulierung festgelegt. Danach sind Einrichtungen lebens- und verteidigungswichtig, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben zahlreicher Menschen zu befürchten oder die für das Funktionieren des Gemeinwesens unverzichtbar sind. Durch diese Definition sind auch solche Einrichtungen erfaßt, deren Ausfall erhebliche Unruhe in großen Teilen der Bevölkerung entstehen lassen und dadurch die öffentliche Ordnung bedrohen würde.

Es wird klargestellt, daß der *Betroffene* auch über die bei der Sicherheitsüberprüfung beabsichtigten *Datenerhebungen*, z. B. bei Dritten, *zu unterrichten* ist.

Gestrichen wurden die *erweiterte Sicherheitsüberprüfung* bei Mitarbeitern, die in Teilen von Behörden tätig sind, die zum Sicherheitsbereich erklärt wurden, die aber selbst keinen Zugang zu Verschlußsachen haben. Hier soll die einfache Sicherheitsüberprüfung genügen.

*Angaben, die den Ehegatten oder Lebenspartner* betreffen, werden künftig bei den Betroffenen selbst erhoben und nicht in einem einheitlichen Sicherheitsfragebogen abgefragt.

Eine beabsichtigte *Beschränkung des Kontrollrechts des Berliner Datenschutzbeauftragten* wurde fallengelassen. Personenbezogene Daten einer Person, der Vertraulichkeit zugesichert worden ist, sind entgegen dem Entwurf zumindest dem Berliner Datenschutzbeauftragten persönlich zu offenbaren. Dies ist auch vorgesehen, wenn die Senatsverwaltung für Inneres im Einzelfall feststellt, daß dies die Sicherheit des Bundes oder eines Landes gebietet.

Der Betroffene erhält einen *Anspruch auf Akteneinsicht.* Das Landesamt für Verfassungsschutz und der Geheimschutzbeauftragte seiner Beschäftigungsstelle haben ihm auf Antrag Einsicht in die Teile der Akten zu gewähren, die Daten zu seiner Person enthalten. Auch soll dem Betroffenen nicht mehr die Mitteilung verweigert werden, woher die über ihn gespeicherten Daten stammen und an welche Stellen sie weitergeleitet wurden, wenn dem nicht Geheimhaltungsinteressen entgegenstehen.

In folgenden Punkten wurde unseren Empfehlungen nicht gefolgt:

Festgehalten wurde an den weitgehenden Möglichkeiten zu *Befragungen Dritter.* Diese sollen bereits möglich sein, „wenn die Erhebung bei dem Betroffenen oder seinem Lebenspartner nicht ausreicht“. Durch diese großzügige Ausdehnung der Befragungen

Der Forderung des Berliner Datenschutzbeauftragten nach dem Zustimmungserfordernis für alle zusätzlichen Befragungen konnte nicht gefolgt werden, weil sonst die Aussagekraft der Sicherheitsüberprüfung nicht mehr gegeben wäre. Auch muß die Vergleichbarkeit der nach dem BSÜG durchgeführten Sicherheitsüberprüfungen mit denen vom Bund und von anderen Ländern durchgeführten Überprüfungen berücksichtigt werden. Die vorliegenden Gesetze des Bundes und anderer Länder gehen generell von der Notwendigkeit der Befragung ohne Zustimmung des Betroffenen aus.

112 Drs 13/1472
113 vgl. JB 1996, 5.1
114 vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995, JB 1995, Anlage 2.2

| Bericht des Berliner Datenschutzbeauftragten | Stellungnahme des Senats |
|---|---|

können die Grenzen zwischen den einzelnen Stufen der Sicherheitsüberprüfung (einfache Sicherheitsüberprüfung, erweiterte Sicherheitsüberprüfung und erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen) zerfließen und die Dreiteiligkeit, mit der dem Grundsatz der Verhältnismäßigkeit Rechnung getragen werden soll, ihrem Sinn nach ins Leere laufen. Der Begriff „geeignete Stellen“ oder „weitere geeignete Auskunftspersonen“ läßt für den Betroffenen offen, welche Befragungen hier konkret vorgenommen werden. Es bleibt dem Landesamt für Verfassungsschutz überlassen, den zu befragenden Personenkreis zu bestimmen. Die Regelung widerspricht der Forderung der Datenschutzkonferenz vom 13. September 1985[115] nach Transparenz des Sicherheitsüberprüfungsverfahrens.

Die Möglichkeit, Daten nicht beim Betroffenen und dessen Ehegatten oder Lebenspartner, sondern ohne deren Zustimmung bei anderen geeigneten Stellen oder Personen zu erheben, besteht nur, um sicherheitserhebliche Erkenntnisse zu verifizieren. Dies ist keineswegs eine großzügige Möglichkeit, um die Befragungen auszudehnen, sondern kann nur in begründeten Einzelfällen angewandt werden. Auch werden mit dieser Regelung nicht die Grenzen zwischen den einzelnen Überprüfungsstufen fließend, da nach § 8 Abs. 1 des Gesetzes eine weitergehende als die ursprünglich vorgesehene Überprüfungsstufe die Unterrichtung des Betroffenen erfordert.

Eine weitere Konkretisierung, welche Personen oder Stellen hiernach befragt werden könnten, ist nicht möglich. Dies ergibt sich aus dem jeweiligen Einzelfall, wird aber vom LfV auch nicht willkürlich festgelegt, da es sich ja um Personen oder Stellen handeln muß, die in Bezug zum Betroffenen stehen und zu konkreten Sachverhalten befragt werden.

Auch die zugelassene *Nutzung der Daten für fast alle Aufgaben des Verfassungsschutzes* ist bedenklich. Damit kann das Landesamt für Verfassungsschutz durch seine Mitwirkung bei der Sicherheitsüberprüfung in den Besitz von Daten gelangen, die es für seine Aufgaben nicht hätte erheben dürfen.

Auch hier handelt es sich um eine im Bund und in den anderen Ländern einheitliche Regelung die aus den vorgenannten Gründen ein Abweichen nicht zuläßt.

An den großzügigen *Datenspeicherungsbefugnissen* des Landesamtes für Verfassungsschutz wurde festgehalten. Es darf nicht nur die Daten des Betroffenen, sondern auch die Daten des Ehegatten oder Lebenspartners in automatisierten Dateien, insbesondere im NADIS, dem bundesweiten Informationssystem der Nachrichtendienste, speichern. Die Möglichkeit, Erkenntnisse, die ein Sicherheitsrisiko begründen, in einer automatisierten Datei zu speichern, soll zwar auf unsere Anregung auf Erkenntnisse über „objektive Sicherheitsrisiken“ beschränkt werden; diese verkürzte Darstellung des Akteninhalts in einer Datei bringt dennoch die Gefahr einer Verfälschung und irreführender Verkürzungen der ursprünglichen Aussage mit sich. Gleichzeitig pflegen sich derartige Darstellungen gegenüber der in den Akten enthaltenen Langfassung zu verselbständigen in der Weise, daß bevorzugt und fast ausschließlich auf die Kurzfassung zurückgegriffen wird.

Die im BSÜG festgeschriebene Datenspeicherungsbefugnis ist für das LfV unabdingbar, um der in § 18 Abs. 1 BSÜG festgeschriebenen Unterrichtung der zuständigen Stelle bei nach Abschluß der Sicherheitsüberprüfung anfallenden Erkenntnissen zeitnah nachkommen zu können. Dies gilt ebenso für die Speicherung im NADIS, wodurch Erkenntnisse anderer Verfassungsschutzbehörden einer sicherheitsüberprüften Person zugeordnet werden können. Die Daten der Ehegatten oder Lebenspartner werden nur bei den erweiterten Sicherheitsüberprüfungen nach den §§ 11 und 12 BSÜG, nicht aber bei der einfachen Sicherheitsüberprüfung nach § 10 BSÜG im NADIS gespeichert.

Zur Speicherungsbefugnis der objektiven Sicherheitsrisiken sind die Befürchtungen des Berliner Datenschutzbeauftragten hinsichtlich einer Verselbständigung und Qualitätsverschlechterung der Daten bzw. Verfälschung und/oder irreführenden Verkürzung der ursprünglichen Aussage unbegründet. Durch diese Datei wird nicht die Heranziehung der Akte entbehrlich. Mit der Datei soll vielmehr erreicht werden, daß bei der Vielzahl von Sicherheitsüberprüfungsakten das LfV im Bedarfsfall im Rahmen einer Querschnittsabfrage schnell auf alle in Frage kommenden Akten zugreifen kann.

**Beobachtung von Gruppierungen innerhalb der PDS**

*Aus der Mitte des Abgeordnetenhauses wurden wir um Überprüfung der Verarbeitung personenbezogener Daten im Zusammenhang mit der Beobachtung von Gruppierungen innerhalb der PDS gebeten.*

Das Landesamt für Verfassungsschutz beobachtet sieben als verfassungsfeindlich eingestufte Gruppierungen innerhalb der PDS, soweit erforderlich auch mit nachrichtendienstlichen Mitteln. Eine Beobachtung der PDS als Gesamtpartei erfolgt nicht.

Die fachliche Schlußfolgerung, daß tatsächliche *Anhaltspunkte für verfassungsfeindliche Bestrebungen* bei den beobachteten Gruppierungen vorliegen, ist nicht vom Berliner Datenschutzbeauftragten zu bewerten. Unsere Prüfung beschränkte sich auf die Frage, ob vor dem Hintergrund der negativen Erfahrungen im Zusammenhang mit der Beobachtung der AL[116] sichergestellt ist, daß keine Daten über Personen erhoben und gespeichert werden, die lediglich im Zusammenhang mit der PDS stehen und keine als verfassungsschutzrelevant eingestuften Aktivitäten im Zusammenhang mit den beobachteten Gruppierungen entfalten.

Die Probleme bei der Trennung der relevanten personenbezogenen Informationen über die beobachteten Gruppierungen von Angaben über sonstige PDS-Mitglieder sind vom Berliner Datenschutzbeauftragten zutreffend dargestellt. Eine Beobachtung von Teilgruppierungen der PDS bei einem völligen Verzicht auf Unterlagen, die auch Informationen zur Gesamtpartei enthalten, ist naturgemäß nicht möglich. Das Landesamt für Verfassungsschutz legt jedoch einen strengen Maßstab an und prüft in jedem Einzelfall die Erforderlichkeit einer Datenspeicherung.

115 JB 1985, Anlage 4
116 JB 1989, 2.2

Datenspeicherungen über Personen allein auf Grund ihrer Tätigkeit in der PDS haben wir bei unseren Stichproben in den Akten nicht festgestellt. Bei den eingesehenen Akten war das Bemühen erkennbar, nur die für die beobachteten Gruppierungen relevanten personenbezogenen Informationen zu sammeln. Die Durchführung dieser Differenzierung ist in der Praxis – angesichts der vielfältigen Aktivitäten der Mitglieder dieser Gruppierungen innerhalb der PDS – jedoch schwierig. So sind Angaben über PDS-Mitglieder oft schwer von diesen Informationen zu trennen. Wir haben einen strengen Maßstab für Datenspeicherungen in diesem Zusammenhang gefordert. Das Landesamt für Verfassungsschutz hat zugesagt, unseren Empfehlungen auf Herausnahme von einigen Unterlagen nachzukommen.

Bei der Beeinflussung einer Partei durch Gruppierungen, die als verfassungsschutzrelevant eingestuft werden, muß sich die Beobachtung des Landesamtes für Verfassungsschutz auf die Personen beschränken, die die als verfassungsschutzrelevant eingestuften Gruppierungen nachhaltig unterstützen.

## 4.2 Ordnung

### 4.2.1 Meldewesen und Wahlen

Bereits 1988[117] haben wir Klarstellungen im *Meldegesetz* angeregt. Seitdem hat uns die Senatsverwaltung für Inneres immer wieder erklärt, daß sie einen Gesetzentwurf vorlegen wird. Das ist bisher nicht geschehen. Auch die Anpassung des Meldegesetzes an die Änderung des Melderechtsrahmengesetzes im Jahr 1994 ist nicht innerhalb der vorgeschriebenen zwei Jahre erfolgt. Um dem Verfahren einen Schub zu geben, haben wir dem Unterausschuß „Datenschutz“ einen Forderungskatalog vorgelegt, der u. a. folgende Punkte umfaßt:

- die klare Abgrenzung der Befugnisse des Landeseinwohneramtes und der Bezirksämter,
- das Recht, dritte Personen nach Meldedaten zu befragen,
- die freiwillige Speicherung von Daten für Notfälle,
- die Protokollierung der Auskünfte,
- die ausdrückliche Einwilligung der Einwohner zur Aufnahme ihrer Daten in CD-ROMs,
- das weitere Verfahren mit den alten Meldekarteikarten aus DDR-Zeiten.

Im Zusammenhang mit der Berliner Verwaltungsreform und der Bezirksgebietsreform sowie einer damit verbundenen Überprüfung der Aufgabenverteilung zwischen Senat und Bezirken steht auch eine umfassende Neustrukturierung melderechtlicher Zuständigkeiten im Land Berlin zur Diskussion. Um eine wiederholte Befassung des Landesgesetzgebers mit Fragen des Melderechts innerhalb eines überschaubaren Zeitraums zu vermeiden, ist beabsichtigt, die vom Berliner Datenschutzbeauftragten angemahnte Anpassung des Meldegesetzes an die 1994 geänderten rahmenrechtlichen Vorgaben mit einer im Land Berlin gegebenenfalls erforderlich werdenden Neuregelung melderechtlicher Zuständigkeiten zu verbinden. Da die hierzu notwendigen Prüfungen jedoch eine erhebliche Vorbereitungszeit erfordern, hat sich die in dieser Legislaturperiode geplante Einbringung eines Entwurfes zur Novellierung des Meldegesetzes verzögert.

Für die Umsetzung des Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes in Landesrecht hat der Bundesgesetzgeber – entgegen der insoweit offenbar vom Berliner Datenschutzbeauftragten vertretenen gegenteiligen Auffassung – keine Frist bestimmt. Die in § 23 Melderechtsrahmengesetz enthaltene zweijährige Anpassungsfrist bezieht sich ausschließlich auf die ursprüngliche Fassung des Melderechtsrahmengesetzes und ist nicht auf die Novelle aus dem Jahr 1994 anzuwenden.

Der Senat erachtet im übrigen die Erörterung von Einzelaspekten, die nach Auffassung des Datenschutzbeauftragten Gegenstand einer melderechtlichen Neuregelung sein sollten, im Unterausschuß „Datenschutz“ vor Einbringung eines entsprechenden Gesetzesentwurfes als wenig sinnvoll.

Die Aufnahme der Volksinitiative sowie des Volksbegehrens und des Volksentscheides zum Erlaß von Gesetzen in die Verfassung von Berlin (Art. 61–63 Verfassung von Berlin) erforderte eine gesetzliche Regelung zu ihrer Durchführung. Mit dem im vergangenen Jahr verabschiedeten Gesetz[118] wird auch das Meldegesetz geändert:

Ein *bezirksübergreifender Zugriff auf die Meldedaten* durch die Bezirke auch mit der Befugnis, Einzeldaten für andere Bezirke zu speichern und zu löschen, wurde geschaffen; weitere melderechtsfremde Daten werden gespeichert; Wahlausschlußgründe werden bei allen Einwohnern registriert.

In den parlamentarischen Beratungen haben wir die Auffassung vertreten, daß die mit dem Entwurf beabsichtigten Änderungen des Meldegesetzes nicht erforderlich sind und bis zur Novellierung des Meldegesetzes zurückgestellt werden können. Damit konnten wir uns nicht durchsetzen.

Das Gesetz über Volksinitiative, Volksbegehren und Volksentscheid wurde mit den in § 45 Abs. 1 des Gesetzes geregelten Änderungen des Meldegesetzes nach eingehender Erörterung und Beratung in den zuständigen parlamentarischen Ausschüssen am 11. Juni 1997 verabschiedet. Der Senat hält eine Stellungnahme zu der vom Berliner Datenschutzbeauftragten vorgetragenen Kritik, mit der er sich bereits im Rahmen der parlamentarischen Beratung nicht durchsetzen konnte, für nicht erforderlich.

117 JB 1988, 4.5
118 Gesetz über Volksinitiative, Volksbegehren und Volksentscheid vom 11. Juni 1997, GVBl. S. 304

Für den *bezirksübergreifenden Zugriff auf das Melderegister* wurde eine Rechtsgrundlage geschaffen, um die Überprüfung der Unterstützungsunterschriften zu erleichtern. Dazu wird nicht nur der Zugriff selbst erlaubt, sondern es ist auch die Befugnis für die Speicherung und Löschung in Datensätzen von Einwohnern anderer Bezirke geschaffen worden.

Die Anträge auf Volksinitiative oder Volksbegehren bedürfen einer bestimmten Zahl von Unterstützungsunterschriften. Jede Unterschrift hat auf einem gesonderten Blatt zu erfolgen. Zur Erleichterung der Überprüfung der Unterschriften werden *alle* Bezirksämter ohne Rücksicht auf die örtliche Zuständigkeit verpflichtet. Es ist nicht ersichtlich, warum die einzelnen Bögen nicht auf die jeweils zuständigen Bezirksämter verteilt werden können. Der zeitliche Mehraufwand ist begrenzt und rechtfertigt derart weitgehende Zugriffs-, Speicherungs- und Löschungsbefugnisse anderer als der datenverarbeitenden Stelle i. S. d. Datenschutzgesetzes nicht. Ein Antrag der Fraktion Bündnis 90/ Die Grünen hat die prinzipiellen melderechtlichen Zuständigkeiten des Wohnbezirkes unangetastet gelassen und entsprach damit unserer Empfehlung, die Zuständigkeitsgrenzen nach dem Meldegesetz aufrechtzuerhalten.

Sowohl das Melderechtsrahmengesetz als auch die Meldegesetze der anderen Länder enthalten zur Vorbereitung und Durchführung von Wahlen lediglich die Befugnis zur Speicherung der Tatsache, daß der Betroffene vom Wahlrecht ausgeschlossen ist. Nach § 2 Abs. 3 Melderechtsrahmengesetz (MRRG) kann durch Landesgesetz bestimmt werden, daß für die Erfüllung von Aufgaben der Länder über den dort enthaltenen Katalog hinaus weitere Daten gespeichert werden. Die Speicherung *zusätzlicher Daten* ist dann unbedenklich, wenn der Landesgesetzgeber eine ausschließlich in der Zuständigkeit des Landes oder seiner Kommunen liegende Aufgabe regelt, die der Bundesgesetzgeber mit seiner Rahmenkompetenz nicht berücksichtigen konnte.

In Berlin durfte bisher schon nach § 2 Abs. 2 Nr. 1 b) Meldegesetz als einzigem Bundesland über die Tatsache hinaus, daß ein Wahlausschlußgrund vorliegt, die *Tatsache einer geleisteten Unterstützungsunterschrift gespeichert* werden. Darüber hinaus wird nun auch noch die Befugnis zur zusätzlichen *Speicherung der Angabe des unterstützten Wahlvorschlages* und dessen Trägers – also beispielsweise eine Partei oder ein Einzelbewerber – geschaffen. Hierbei handelt es sich um ein melderechtsfremdes Datum, das wegen des Festhaltens von politischen Meinungen der Betroffenen äußerst sensibel ist und im übrigen auch in den Verbotskatalog der EU-Richtlinien fällt (Art. 8 EU-RiLi).

Auch bei der *Speicherung von Wahlbewerbungen einschließlich des erlernten und zuletzt ausgeübten Berufes* besteht kein Zusammenhang zum Melderecht. Hier geht es ausschließlich darum, das Melderegister als Speichermedium im Zusammenhang mit der Bekanntmachungspflicht nach § 40 Landeswahlordnung (LWahlO) zu nutzen.

Bisher durfte einheitlich die Tatsache des Ausschlusses vom Wahlrecht – und in einigen Ländern auch von der Wählbarkeit – von deutschen Einwohnern über 17 Jahren gespeichert werden (§ 2 MRRG; § 2 Abs. 2 Nr. 1 a MeldeG). Die Speicherungsbefugnisse werden auf **alle** Einwohner erweitert. Dies hielten wir im Hinblick auf den Regelungsgehalt des Gesetzes nicht für erforderlich. Unterschriftsberechtigt bei der Volksinitiative sind alle volljährigen Personen, die ihre alleinige Wohnung oder ihre Hauptwohnung in Berlin haben. Abstimmungsberechtigt bei Volksinitiativen und Volksentscheiden sind all jene, die zum Abgeordnetenhaus von Berlin wahlberechtigt sind. Das sind nach § 1 Landeswahlgesetz (LWahlG) alle volljährigen Deutschen i. S. d. Grundgesetzes.

Die Befugnis zur Speicherung von Wahlausschlußgründen kann im Hinblick auf künftige Wahlen zu den Bezirksverordnetenversammlungen von Bedeutung sein. Nach § 22 a LWahlG sind zu den Bezirksverordnetenversammlungen unter den gleichen Voraussetzungen wie Deutsche auch Personen, die die Staatsangehörigkeit eines EU-Mitgliedstaates besitzen, wahlberechtigt und wählbar. Zu diesem Zweck ist es erforderlich, daß Wahlausschlußgründe dieses Personenkreises gespeichert werden. Eine Rechtfertigung für die *Speicherung von Wahlausschlußgründen bei Ausländern, die nicht EU-Bürger sind,* ist jedoch nicht erkennbar.

| Bericht des Berliner Datenschutzbeauftragten | Stellungnahme des Senats |
|---|---|

Diese über die Meldegesetze der anderen Länder weit hinausgehenden Regelungen genügen der Senatsverwaltung für Inneres für die Umsetzung des Gesetzes über Volksinitiative, Volksbegehren und Volksentscheid offensichtlich noch immer nicht. Weil auch *wohnsitzlose Personen* abstimmungsberechtigt sind, sollen die Bezirkseinwohnerämter zur Überprüfung von Doppelunterschriften die Möglichkeit erhalten, für diesen Personenkreis Datensätze unter einer fiktiven Anschrift im Melderegister aufzubauen und diese auch zu löschen. Die Meldebehörde hat nach § 1 Abs. 1 MeldeG Daten über die im Geltungsbereich dieses Gesetzes wohnhaften Einwohner und deren Wohnungen zu registrieren, um die für die rechtmäßige Erfüllung der Aufgaben öffentlicher Stellen erforderlichen Grunddaten feststellen und nachweisen zu können. Da wohnsitzlose Personen gerade keine Wohnung haben, mangelt es an dem die Meldepflicht – und somit die Speicherbefugnis – auslösenden Tatbestand des Beziehens einer Wohnung. Eine Speicherung von Daten dieser Personengruppe im Melderegister ist damit unzulässig.

Im Wahlbereich werden die nach wahlrechtlichen Vorschriften bestehenden Möglichkeiten ausgeschöpft, durch Speicherung relevanter Daten den unterschiedlichen Anforderungen bei der Durchführung verschiedener Wahlen und plebiszitärer Verfahren in Berlin gerecht zu werden. Es trifft zwar zu, daß einzelne Daten nicht in direktem Zusammenhang mit dem Melderecht stehen. Es liegt jedoch auf der Hand, daß für die Wahldurchführung vorhandene automatisierte Verfahren genutzt werden, wie es beim Einwohnerdatenbestand und den Programmöglichkeiten der Fall ist, wenn in datenschutzwürdige Belange von Betroffenen nicht eingegriffen wird. Dies ist unseres Erachtens sichergestellt.

Mit dem Prüfprogramm zur Feststellung von Doppelunterschriften sollen z. B. auch keine wohnsitzlosen Personen unter einer Adresse von Amts wegen angemeldet werden. Es handelt sich vielmehr um eine Hilfsdatei, die nach Wegfall des Erfordernisses sofort gelöscht wird.

**Meldestelle nimmt per Knopfdruck der Mutter das Kind**

*Eine Mutter hat bei ihrer Meldestelle einen Reisepaß beantragt. In diesem Paß sollte ihr nichteheliches Kind eingetragen werden, für das sie das Sorgerecht besitzt. Das wurde ihr mit dem Hinweis darauf verweigert, daß im Datensatz des Kindes die geschiedene Frau des Kindesvaters als leibliche Mutter gespeichert sei und es im übrigen keinen Hinweis auf eine Adoption gebe.*

Die Überprüfung des Vorganges hat ergeben, daß die Meldeunterlagen zunächst korrekt geführt wurden. Anläßlich eines erneuten Zuzuges des Kindesvaters wurde die Anmeldung durch die Meldestelle fehlerhaft verarbeitet. Fälschlicherweise wurde die überhaupt nicht nach Berlin mitgezogene Ehefrau des Kindesvaters als Mutter im Melderegister eingegeben. Alle in das Programm eingebauten Fehlermeldungen und Hinweise sind vom Bearbeiter nicht beachtet worden. Die Gründe dafür sind nicht mehr nachvollziehbar. Das Landeseinwohneramt hat sich bei der Mutter entschuldigt und die Mitarbeiter erneut auf äußerste Sorgfalt bei der Eingabe derartiger Vorgänge hingewiesen. Wenigstens sind innerhalb des Zeitraumes der Fehlspeicherung keine Ausweispapiere für das Kind ausgestellt und an nicht antragsberechtigte Personen ausgehändigt worden.

Es handelt sich um einen abgeschlossenen Einzelfall, bei dem anläßlich der Eingabe von Meldedaten ins Melderegister bedauerlicherweise eine fehlerhafte Bearbeitung erfolgte. Der Berliner Datenschutzbeauftragte hat bereits darauf hingewiesen, daß die Mitarbeiter des Landeseinwohneramtes in diesem Zusammenhang erneut auf äußerste Sorgfalt hingewiesen wurden.

**Und immer wieder: Namensverwechslungen**

*Ein Petent, der sich wegen einer Namensverwechslung bei einem Rentenversicherungsträger schon einmal an uns gewandt hatte*[119]*, erhielt dieses Mal vom Wirtschaftsamt Wilmersdorf einen Bußgeldbescheid, der wiederum eine namensgleiche Person mit gleichem Geburtsdatum (nur anderes Jahr) betraf.*

Was war diesmal geschehen? Das Wirtschaftsamt hat zunächst mit Namen, Vornamen und Geburtsdatum beim Bezirkseinwohneramt nachgefragt und die zutreffende Information erhalten, daß die Person unbekannt verzogen sei. Eine weitere Anfrage – diesmal beim Landeseinwohneramt – ergab, daß die gesuchte Person auch von dort nicht zu ermitteln sei. Eine erneute Anfrage beim Bezirkseinwohneramt – nun allerdings ohne das Geburtsdatum – führte zu einer Auskunft über den Petenten.

Nach § 25 MeldeG darf die Meldebehörde Meldedaten an andere Behörden und sonstige öffentliche Stellen übermitteln. Meldebehörde ist nach § 1 Abs. 2 MeldeG das Landeseinwohneramt. Das für die Wohnung zuständige Bezirksamt nimmt als Ausnahme von der Regel für die in § 2 Abs. 2 Nr. 1 (Wahlen), Nr. 2 (Lohnsteuerkarten) und Nr. 4 (Schöffen) MeldeG genannten Daten die Aufgaben der Meldebehörde wahr (§ 1 Abs. 4 MeldeG). Übermittlungen aus dem Melderegister an andere öffentliche Stellen fallen allerdings nicht unter diese Ausnahmeregelung.

Die vom Bezirkseinwohneramt durchgeführten Übermittlungen aus dem Melderegister an das Wirtschaftsamt waren schon dem Grunde nach unzulässig. Hinzu kommt, daß vor der Übermittlung der Daten die Identität der gesuchten Person unzureichend geprüft wurde. Nur mit den Merkmalen Name, Vorname und Geburtstag wird im Datensichtgerät angezeigt, daß zwei

Auf Grund der angeführten melderechtlichen Vorschriften wäre grundsätzlich nur die Meldebehörde zur Auskunftserteilung an das Wirtschaftsamt Wilmersdorf zuständig gewesen. Nach Anlage 5 zu § 3 Nr. 2 DVO-MeldeG sind jedoch die jeweils zuständigen Stellen der Bezirksämter als Empfänger regelmäßiger Datenübermittlungen aus dem Melderegister durch Einrichtung automatisierter Verfahren festgelegt. Wenn aber ein Abruf der bereitzuhaltenden Daten im Online-Verfahren aus technischen Gründen den zuständigen Stellen der Bezirksämter nicht möglich ist, muß ihnen doch zumindest ein Zugriff auf den entsprechenden Datensatz über die in den Bezirkseinwohnerämtern vorhandenen Terminals gestattet sein.

Die Beanstandung im Einzelfall trifft zu, da die bedauerliche Namensverwechselung auf eine ungenügende Prüfung im Einwohner- und Wirtschaftsamt zurückzuführen ist.

119 JB 1994, 3.6

Datensätze vorhanden sind. Ohne weitere Prüfung wurde über die erste – nicht gesuchte – Person Auskunft erteilt. Vom Wirtschaftsamt hätten weitere Daten zur zweifelsfreien Identifikation angefordert werden müssen.

### 4.2.2 Ausländer

**Erst Daten, dann Rückkehr**

*Einer Bitte des Bundesministeriums des Innern folgend, hat die Berliner Ausländerbehörde dem Bundesamt für die Anerkennung von Flüchtlingen (BAFl) umfangreiche personenbezogene Daten von Bürgerkriegsflüchtlingen aus Bosnien-Herzegowina zum Zweck der Förderung von Wiederaufbau- und Rückkehrprojekten der EU übermittelt. Weitergegeben wurden auch Angaben zur Ethnie, die besonders sensibel sind. Betroffen von der Datenübermittlung war eine fünfstellige Personenzahl.*

Die Senatsverwaltung für Inneres vertritt dazu die Auffassung, daß die Datenübermittlungen zur Erfüllung ordnungsbehördlicher Aufgaben der Ausländerbehörde erforderlich waren und insoweit auf § 44 Abs. 2 Nr. 1 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) gestützt werden können.

Das Flüchtlingsproblem hat – darin ist der Senatsverwaltung für Inneres zuzustimmen – nicht nur aufenthaltsrechtliche, sondern insbesondere auch soziale, ökonomische und außenpolitische Komponenten. Maßnahmen, die die freiwillige Rückkehr in die Heimat bei Vermeidung der zwangsweisen Abschiebung unterstützen, sind in jedem Fall zu begrüßen. Finanzielle Anreize – z. B. im Rahmen von *Wiederaufbauprojekten* – fördern die Bereitschaft der Betroffenen zur Rückkehr. Damit im Zusammenhang stehende Tätigkeiten der Ausländerbehörde sind jedoch – entgegen der Auffassung der Senatsverwaltung für Inneres – keine Aufgaben zur Gefahrenabwehr (§ 2 Abs. 1 ASOG). Zuständigkeiten der Ordnungsbehörden werden im einzelnen durch Gesetz bestimmt (§ 2 Abs. 4 Satz 1 ASOG), diejenigen der Ausländerbehörde sind abschließend in § 33 Nr. 4 Gesetz über die Zuständigkeit der Ordnungsbehörden (OrdZG) geregelt. Danach sind der Ausländerbehörde die Ordnungsaufgaben in Angelegenheiten des Aufenthaltsrechtes der Ausländer zugewiesen. Die *Förderung der freiwilligen Rückkehr von Bürgerkriegsflüchtlingen* geht über die aufenthaltsrechtliche Aufgabenstellung der Ausländerbehörde hinaus. Die Übermittlung der Flüchtlingsdaten zu dem genannten Zweck durch die Ausländerbehörde an Dritte – sei es an die Senatsverwaltung für Inneres oder das BAFl – kann nicht auf § 44 Abs. 2 Nr. 1 ASOG gestützt werden. Eine Einwilligung der Betroffenen wurde nicht eingeholt, so daß die Datenübermittlungen unzulässig waren.

Im übrigen konnte die Senatsverwaltung für Inneres nicht darlegen, zu welchem konkreten Zweck die zum Teil sehr sensiblen personenbezogenen Daten im Rahmen der Förderprojekte der EU überhaupt erforderlich sind. Inwieweit es sich überhaupt um eine personengebundene Förderung handelt, wurde uns nicht mitgeteilt. Der Umstand, daß die Daten von nationalen oder internationalen Stellen verlangt werden, ist noch kein Nachweis für deren Erforderlichkeit.

Die Rechtsauffassung des Datenschutzbeauftragten wird nicht geteilt, vielmehr wird § 44 Abs. 2 Nr. 1 ASOG als eine für Datenübermittlungen der genannten Art ausreichende Rechtsgrundlage angesehen.

§ 44 Abs. 2 ASOG ist eine Auffangvorschrift, die zur Anwendung kommt, wenn – wie im konkreten Fall – die Voraussetzungen des § 44 Abs. 1 ASOG nicht vorliegen. Gemäß § 44 Abs. 2 Nr. 1 ASOG können Daten von den Ordnungsbehörden und der Polizei an Behörden und sonstige öffentliche Stellen übermittelt werden, soweit dies „zur Erfüllung ordnungsbehördlicher oder polizeilicher Aufgaben erforderlich ist“.

Die Datenübermittlung diente dem Ziel der Förderung von Wiederaufbau- und Rückkehrprojekten und damit der Verstärkung der Bereitschaft zur freiwilligen Rückkehr bei den bosnischen Kriegsflüchtlingen und so letztendlich der Erfüllung ordnungsbehördlicher Aufgaben.

Der Begriff der „ordnungsbehördlichen Aufgabe“ ist mit Blick auf die Flüchtlinge aus dem ehemaligen Jugoslawien dabei weiter zu interpretieren als lediglich im klassischen polizei- und ordnungsrechtlichen Sinne. Angesichts des komplexen Hintergrundes dieses Flüchtlingsproblems mit seinen vielfältigen nicht nur aufenthaltsrechtlichen, sondern insbesondere auch sozialen, ökonomischen und außenpolitischen Verwobenheiten erschöpft sich die ordnungsbehördliche Tätigkeit nicht nur in der Erteilung von Aufenhaltstiteln und dem Ergreifen aufenthaltsbeendender Zwangsmaßnahmen. Sie steht vielmehr in engem Zusammenhang mit den sozialen und ökonomischen Fragen der Flüchtlingsrückführung. Die Aufgabe der Ausländerbehörden entspricht hier in gewisser Weise der der früheren Flüchtlingsverwaltung mit ihrer Erfassungs- und Steuerungsfunktion. Die von der IMK wie auch dem Senat von Berlin immer wieder in den Vordergrund gestellte freiwillige Flüchtlingsrückkehr bei weitgehender Vermeidung zwangsweiser Abschiebungen ist daher Teil auch der ordnungsbehördlichen Aufgabenstellung. Im Rahmen der Erfüllung dieser Zielsetzung hat die Ausländerbehörde die notwendigen Daten stellvertretend auch für die übrigen involvierten Behörden erfaßt.

Vor dem Hintergrund dieses erweiterten ordnungsbehördlichen Aufgabenbegriffs war die Datenübermittlung an das Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) eine geeignete und erforderliche Maßnahme. Nach Auskunft des BMI ist die zentrale Datenerfassung beim BAFl mit der Möglichkeit kurzfristigen Abrufs notwendige Voraussetzung für das Einbeziehen der entsprechenden Flüchtlinge in die Planung von Wiederaufbau- und Rückkehrprojekten der EU. Es sei darauf hingewiesen, daß sich die EU massiv um personenbezogene Wiederaufbauhilfe bemüht. Entsprechende Datenübermittlung ist ferner ein wesentlich geringerer Grundrechtseingriff als die Alternative zwangsweiser Durchsetzung der Ausreisepflicht.

Es sei ferner darauf hingewiesen, daß der Bundesbeauftragte für den Datenschutz mit Schreiben vom 19. November 1996 an die Landesbeauftragten für Datenschutz zur Prüfung der Frage der Förderwürdigkeit und zur Durchführung der Fördermaßnahmen im Rahmen von Wiederaufbauprojekten die Erforderlichkeit der Angaben personenbezogener Daten bejaht hat.

Das Einholen der individuellen Einwilligung zur Datenübermittlung war angesichts der fünfstelligen Zahl der betroffenen Personen aus organisatorischen Gründen nicht möglich.

Die Datenübermittlung an das BAFl wurde im übrigen nicht durch die Ausländerbehörde, sondern durch die Senatsverwaltung für Inneres vorgenommen. Die vorgeschaltete Übermittlung durch die Ausländerbehörde an die genannte Senatsverwaltung erfolgte im Zuge fachaufsichtlicher Prozesse.

| Bericht des Berliner Datenschutzbeauftragten | Stellungnahme des Senats |
|---|---|

**Ausländische Gäste**

*Der Gastgeber eines ausländischen Besuchers hat sich zu verpflichten, für alle Kosten – einschließlich der Versorgung im Krankheits- oder Pflegefall – aufzukommen, die durch den Besuch seines ausländischen Gastes verursacht werden (§ 84 AuslG). Hierfür kommt ein bundeseinheitliches Formular zur Anwendung, mit dem umfangreiche Daten der Betroffenen erhoben werden.*

Die Ausländerbehörde ist berechtigt, die Daten zu erheben, die notwendig sind, um die Rechtsverbindlichkeit der *Verpflichtungserklärung* sicherzustellen bzw. um überprüfen zu können, ob der Erklärende in der Lage ist, der eingegangenen Verpflichtung nachzukommen (§ 75 Abs. 1 AuslG). Erforderlich ist in jedem Fall die Erhebung und Verarbeitung von Daten zur Identität des Gastgebers und des Gastes (Name, Vorname, Geburtsdatum, -ort, Anschriften und Paßdaten). Ohne diese Daten wäre die Abgabe einer verbindlichen Verpflichtungserklärung nicht möglich. Dagegen sind die geforderten Angaben zum Beruf bzw. Arbeitgeber des Gastgebers, zur Größe seiner Wohnung und ob er diese als Mieter oder Eigentümer bewohnt, für den genannten Zweck nicht erforderlich.

Um überprüfen zu können, ob der Gastgeber wirtschaftlich in der Lage ist, der von ihm eingegangenen Haftungsverpflichtung nachzukommen, sind in begrenztem Umfang Angaben über die *Einkommens- und Vermögensverhältnisse* notwendig. Ausreichend ist, wenn der Erklärende glaubhaft macht, daß sein Einkommen eine bestimmte Höhe übersteigt. Dabei ist es dem Gastgeber freizustellen, in welcher Weise (z. B. neutraler Einkommensnachweis, Bürgschaft) er dies darlegt.

Bei der datenschutzrechtlichen Bewertung des Formulars „Verpflichtungserklärung“ ist auch zu bedenken, daß alle in dem Vordruck enthaltenen Angaben nicht nur bei der örtlichen Ausländerbehörde bleiben; der eingeladene Ausländer erhält ebenfalls eine Ausfertigung und damit Kenntnis vom Beruf des Einladenden, von dessen Arbeitgeber und der Höhe seines Einkommens. Inwieweit diese Angaben beim ausländischen Gast nur zur Erlangung eines Visums verwendet werden, entzieht sich der Kontrolle des Einladenden.

Die Senatsverwaltung für Inneres hat uns dazu mitgeteilt, daß die Berliner Ausländerbehörde in Visaverfahren, in denen ihr Einvernehmen (§ 11 Abs. 1 Durchführungsverordnung zum Ausländergesetz) nicht erforderlich ist, derzeit weder Verpflichtungserklärungen nach § 84 AuslG entgegennimmt noch Bonitätsprüfungen anstellt.

Wir haben empfohlen, die „Verpflichtungserklärung“ in der vorliegenden Form in Berlin auch künftig nicht zu verwenden.

Der Berliner Datenschutzbeauftragte weist in seinem Bericht selbst darauf hin, daß der für Verpflichtungserklärungen nach § 84 AuslG vorgesehene bundeseinheitliche Vordruck in Berlin bislang nicht verwendet wird.

Die Verwendung des Vordrucks zur Datenerhebung für die Prüfung, ob der Erklärende wirtschaftlich zur Übernahme von Unterhaltsverpflichtungen überhaupt in der Lage ist, setzt aus Sicht des Senats die Klärung verschiedener inhaltlicher und organisatorischer Fragen voraus. Es ist zur Zeit nicht abzusehen, wann die bundesweite Meinungsbildung hierzu abgeschlossen sein wird.

**Traumatisierung in der Ausländerakte**

*Unter bestimmten Voraussetzungen sind Kriegsflüchtlinge aus Bosnien-Herzegowina von einer Rückführung in ihre Heimat ausgenommen, wenn sie sich als traumatisierte Personen in Deutschland in ärztlicher Behandlung befinden. Die Betroffenen haben dies durch entsprechende Nachweise – z. B. ärztliche Atteste – zu belegen. In Einzelfällen kommt es vor, daß die Betroffenen die ärztlichen Gutachten direkt an die Ausländerbehörde übersenden. Das Original wird mit einer kurzen Darstellung des Sachverhaltes an die Senatsverwaltung für Gesundheit und Soziales zur Begutachtung bzw. Überprüfung übersandt. Eine Kopie bleibt in der Ausländerakte.*

Gegen dieses Verfahren bestehen erhebliche datenschutzrechliche Bedenken. Die Gutachten unterliegen der *ärztlichen Schweigepflicht.* Eine Bewertung bzw. Überprüfung aus fachlicher Sicht kann nur durch einen Arzt vorgenommen werden. Zudem ist davon auszugehen, daß die Unterlagen regelmäßig erheblich mehr Angaben über die Traumatisierung und ihre Ursachen enthalten, als für die ausländerrechtliche Entscheidung erforderlich ist. Das Verfahren zum Umgang mit diesen Unterlagen wurde zwischen der Senatsverwaltung für Inneres und der Senatsverwaltung für Gesundheit und Soziales abgestimmt. Danach sollen die ärztlichen Atteste und Gutachten vom Ausstellenden verschlossen direkt an die Senatsverwaltung für Gesundheit und Soziales übersandt werden. Dort werden die Unterlagen unter fachlichen

Die Kritik ist unbegründet. Da mit dem Attest ein Abschiebungshindernis geltend gemacht wird, ist die Ausländerbehörde berechtigt und verpflichtet, eine Kopie des Attestes zur Ausländerakte zu nehmen. § 75 Abs. 1 und 2 AuslG läßt die Erhebung solcher Daten durch die Ausländerbehörde ausdrücklich zu. Im übrigen sei darauf hingewiesen, daß die Einbindung der Senatsverwaltung für Gesundheit und Soziales keinesfalls ein zwingendes Verfahren ist, sondern auf einer individuellen Absprache zwischen dieser Verwaltung und der Senatsverwaltung für Inneres beruht. Ohne diese Sonderregelung bliebe die Senatsverwaltung für Gesundheit und Soziales völlig außerhalb des Beurteilungsvorganges.

Dementsprechend werden die Atteste auch nicht nur in Einzelfällen an die Ausländerbehörde übersandt, sondern sind ihr stets im Original vorzulegen, von wo sie dann an die Senatsverwaltung für Gesundheit und Soziales weitergeleitet werden. Dies entspricht dem Regelungsgehalt von § 70 Abs. 1 AuslG, wonach es Ausländern obliegt, ihm günstige Umstände unverzüglich gegenüber der Ausländerbehörde geltend zu machen und die zur Überprüfung erforderlichen Nachweise beizubringen.

Gesichtspunkten auf ihre Plausibilität überprüft. Die Ausländerbehörde erhält eine Eingangsbestätigung. Die Unterlagen bleiben bei der Senatsverwaltung für Gesundheit und Soziales unter Verschluß. Nichtärztliches Personal erhält keinen Einblick in die medizinischen Daten. Nach Beendigung der Prüfung wird der Ausländerbehörde eine Stellungnahme in Kurzform mit Plausibilitätsbegründung übersandt, die zur Ausländerakte genommen wird.

Dieses Verfahren sollte in den Fällen eine entsprechende Anwendung finden, in denen der Betroffene die Unterlagen direkt der Ausländerbehörde überreicht. Die Unterlagen sind umgehend verschlossen an die Senatsverwaltung für Gesundheit und Soziales weiterzuleiten. Ein Verbleib von Kopien der medizinischen Unterlagen in der Ausländerakte ist für die ausländerrechtlichen Entscheidungen der Ausländerbehörde nicht erforderlich und damit unzulässig (vgl. § 75 AuslG).

**Großzügige Fahndung nach Ausländern**

Im letzten Jahresbericht[120] haben wir kritisiert, daß Ausländer im INPOL-Fahndungsbestand gespeichert wurden, obwohl Abschiebungshindernisse bestanden.

Der Senat hat eine Löschung der Daten dieser Personen abgelehnt, da der Zweck der Ausschreibung zur Festnahme nicht entfalle, wenn die Abschiebung in den Heimatstaat vorübergehend nicht mehr erreicht werden kann, weil dieser Staat seine Bürger ohne ein Rückführungsabkommen nicht aufnimmt[121].

Nach einer Entscheidung des Bundesverwaltungsgerichtes vom 25. September 1997[122] müssen ausreisepflichtige Bürgerkriegsflüchtlinge aus Ex-Jugoslawien und Vietnamesen, die nicht abgeschoben werden können, weil sie von ihren Heimatländern nicht aufgenommen werden, nun eine Duldung erhalten.

Nach dieser Entscheidung sind auch Konsequenzen für die Registrierung von ca. 40 000 Personen im *INPOL-Fahndungsbestand* und im *Schengener Informationssystem* zu ziehen. Die Daten von Personen, die in diesen Fahndungsbeständen gespeichert sind, obwohl die Abschiebung in ihre Heimatländer nicht möglich ist, sind umgehend zu löschen.

Wie bereits in der Stellungnahme zum Bericht des Berliner Datenschutzbeauftragten für das Jahr 1996 dargelegt, ist entgegen den Ausführungen des Berliner Datenschutzbeauftragten der Umgang der Berliner Ausländerbehörde mit dem polizeilichen Fahndungsbestand weder was die Ausschreibung zur Festnahme noch die Löschung dieser Daten angeht, zu beanstanden.

Die Ausschreibung zur Festnahme durch die Berliner Ausländerbehörde erfolgt, wenn ein Ausländer

- ausgewiesen worden und nach Ablauf der Ausreisefrist untergetaucht ist,
- als abgelehnter Asylbewerber nach Ablauf der Ausreisefrist untergetaucht ist und in beiden Fällen, die Abschiebung auch möglich ist oder
- ein Ausländer abgeschoben wurde.

Sie hat den Zweck,

a) die Abschiebung in den Heimatstaat oder einen dritten Staat zu ermöglichen,

b) behördlich auf den Straftatbestand des illegalen Aufenthalts reagieren zu können und

c) das bestehende Einreise- und Aufenthaltsverbot auch nach Verlassen des Bundesgebiets durchsetzen zu können.

In der Vergangenheit waren bezüglich dieser Verfahrenspraxis aus datenschutzrechtlicher Sicht Bedenken erhoben worden. Es wurde zum Teil die Auffassung vertreten, hier fehle es an einer Rechtsgrundlage. Der Gesetzgeber hat mit der Änderung des Ausländergesetzes vom 29. Oktober 1997 (BGBl. I, 2584) Klarheit geschaffen. § 42 Absatz 7 Ausländergesetz stellt nunmehr klar, daß ein Ausländer zum Zwecke der Aufenthaltsbeendigung in den Fahndungsmitteln der Polizei zur Aufenthaltsermittlung und zur Festnahme ausgeschrieben werden kann, wenn sein Aufenthalt unbekannt ist. Im Fall eines Einreiseverbotes gemäß § 8 Absatz 2 Satz 1 des Ausländergesetzes kann er zum Zweck der Einreiseverhinderung außerdem zur Zurückweisung und für den Fall des Antreffens im Bundesgebiet zur Festnahme ausgeschrieben werden.

Spricht ein wegen unbekannten Aufenthalts zur Festnahme ausgeschriebener Ausländer bei der Ausländerbehörde vor, und hat einen Anspruch auf Duldung, so wird die Ausschreibung selbstverständlich gelöscht. So wurde und wird bundesweit unabhängig von der zitierten Rechtsprechung des Bundesverwaltungsgerichts verfahren. Festnahmeersuchen von Personen, die weiterhin unbekannten Aufenthalts sind, werden dagegen nicht gelöscht. Im übrigen sei angemerkt, daß Abschiebungen in die Nachfolgestaaten der Sozialistischen und Föderativen Republik Jugoslawien und nach Vietnam sehr wohl möglich sind.

120 JB 1996, 4.2.3
121 Stellungnahme des Senats zum Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1996, Abghs.-Drs 13/1721, zu Ziff. 4.2.3
122 1 C 3.97, 1 C 10.97, 1 C-11.97

### 4.2.3 Straßenverkehr

Das Gesetz zur Änderung des *Straßenverkehrsgesetzes* und anderer Gesetze ist Ende 1997 verabschiedet worden. Über den jeweiligen Stand des Gesetzgebungsverfahrens und die wesentlichen datenschutzrelevanten Änderungen hatten wir mehrfach berichtet[123].

Als wesentliche Neuerungen sind die Regelungen über die *Vernichtung von Unterlagen* zu nennen. Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse sind nach spätestens zehn Jahren zu vernichten, es sei denn, die Unterlagen stehen im Zusammenhang mit einer Eintragung im Verkehrszentralregister oder im Zentralen Fahrerlaubnisregister. Unterlagen in „Altakten“ müssen erst dann vernichtet werden, wenn die Fahrerlaubnisbehörde aus anderem Anlaß mit dem Vorgang befaßt ist. Fünfzehn Jahre nach Inkrafttreten des Gesetzes sollen alle Akten „auf Vernichtenswertes“ überprüft sein. Neuerdings unterliegen Urteile oder Entscheidungen wegen einer Ordnungswidrigkeit nach Ablauf der für das Verkehrszentralregister geltenden Tilgungsfrist einem gesetzlichen *Verwertungsverbot*, die bisher unbefristete Verwertungsmöglichkeit nach § 52 Bundeszentralregistergesetz wurde abgeschafft. Damit dürfen die Tat und die Entscheidung dem Betroffenen nach der Tilgung im Verkehrszentralregister im Verfahren über die Erteilung oder Entziehung einer Fahrerlaubnis nicht mehr vorgehalten werden. Neu eingeführt wird beim Kraftfahrt-Bundesamt (neben dem Zentralen Fahrzeugregister und dem Verkehrszentralregister) das *Zentrale Fahrerlaubnisregister*, in dem alle Fahrerlaubnisinhaber gespeichert sind. Die örtlichen Fahrerlaubnisregister dürfen nur noch bis spätestens Ende 2005 geführt werden. Aufgenommen wurde auch eine Bestimmung, die der Polizei die Weitergabe derjenigen Informationen an die Fahrerlaubnisbehörde gestattet, die auf *nicht nur vorübergehende Mängel hinsichtlich der Eignung* einer Person zum Führen von Kraftfahrzeugen schließen lassen. Damit wird klargestellt, daß nicht jede Eignungsbedenken begründende Tatsache (wie z. B. der bloße Besitz von Drogen oder Alkohol) mitgeteilt werden soll, sondern nur diejenige, die den Verdacht auf eine andauernde Ungeeignetheit nahelegt.

Die neue Gesetzgebung bestätigt in weiten Teilen die Auffassungen, die wir in der Vergangenheit gegenüber der Berliner Führerscheinstelle bei der Auslegung des Begriffs der Erforderlichkeit vertreten haben[124].

Die Zeit bis zum Inkrafttreten des Gesetzes soll den beteiligten Stellen Gelegenheit geben, sich auf die neuen Regelungen einzustellen. Wir werden uns, wie schon zuvor, weiterhin dafür einsetzen, daß angesichts der Vielzahl der bei der Führerscheinstelle geführten Akten bereits jetzt mit der Umsetzung der Bestimmungen über die Vernichtungsfristen begonnen und nicht erst bis zum Inkrafttreten des Gesetzes gewartet wird.

#### Darf die Zulassungsstelle Dossiers anlegen?

*Die Zulassungsstelle legte außerhalb der üblichen Vorgangsverwaltung einen Sammelvorgang wegen zulassungsrechtlicher Auffälligkeiten im Zusammenhang mit mehreren 10 000 Ausnahmegenehmigungen gemäß § 50 Abs. 8 Straßenverkehrszulassungsordnung (StVZO) (Abblendlichtbündelung von Scheinwerfern) des zuständigen Landesamtes in Mecklenburg-Vorpommern an. Dabei wurden umfangreiche Ermittlungen wie Anforderungen von Gewerbeanzeigen und Handelsregisterauszügen angestellt und Schriftwechsel mit den Ermittlungsbehörden geführt.*

Dieser Vorgang entstand aus einem umfangreichen Schriftwechsel mit der Senatsverwaltung für Verkehr und Betriebe und zwischen der Senatsverwaltung und den anderen Länderministerien, der überwiegend sachorientiert, also weitestgehend ohne Personenbezug, geführt wurde. Erst später – als sich immer deutlicher herausstellte, daß Firmen einer bestimmten Person beteiligt waren – hat das Landeseinwohneramt eigene Ermittlungen durchgeführt.

Das Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze ist zwar am 19. Dezember 1997 beschlossen worden, jedoch noch nicht verkündet. Der Senat erwartet die Verkündung demnächst und das Inkrafttreten zum 1. Januar 1999.

123 JB 1996, 4.2.4, JB 1995, 5.12, JB 1994, 4.13, JB 1993, 4.11
124 vgl. vor allem unseren Prüfbericht im JB 1996, 4.2.4

Die Durchführung dieser umfangreichen personenbezogenen Übermittlungen sowie die Speicherung dieser Daten waren unzulässig. Das Landeseinwohneramt hat als untere Verwaltungsbehörde nach der StVZO alle ordnungsbehördlichen Entscheidungen zu treffen, z. B. den Antrag abzulehnen und ein Fahrzeug nicht zuzulassen, wenn die Voraussetzungen für eine Zulassung nicht vorliegen (§ 33 Nr. 11 a Ordnungsaufgabenzuständigkeitengesetz). Sofern die Zulassungsstelle bei der ordnungsgemäßen Aufgabenerfüllung Anhaltspunkte für das Vorliegen einer Straftat feststellt, kann es die Strafverfolgungsbehörden einschalten, die ihrerseits dann die erforderlichen *Ermittlungen* durchzuführen haben. Der Verdacht einer Steuerstraftat ist nach § 116 Abgabenordnung (AO) der Finanzbehörde mitzuteilen.

Der Inhalt des geprüften Vorganges ging weit über das hinaus, was für die ordnungsbehördliche Maßnahme benötigt wird. Es wurden vielmehr eigene Ermittlungen angestellt, die den Strafverfolgungsbehörden obliegen (beispielsweise Anforderung von Kopien der Gewerbeanmeldung oder von Handelsregisterauszügen).

Sowohl nach § 14 Abs. 6 der Gewerbeordnung als auch nach dem zum Zeitpunkt der Übermittlung anwendbaren § 44 Abs. 1 ASOG ist die Übermittlung von Daten aus Gewerbeanmeldungen zulässig, soweit dies zur Erfüllung ordnungsbehördlicher Aufgaben erforderlich ist. Das ist hier nicht der Fall: Diese Ermittlungen und Feststellungen zählen nicht mehr zu den Aufgaben der Zulassungsstelle. Demzufolge fehlt auch eine Speicherungsbefugnis nach § 42 Abs. 1 ASOG. Gleiches gilt hinsichtlich der Anforderung von Handelsregisterauszügen.

Die Zulassungsstelle ist unseren Empfehlungen gefolgt und hat die nicht erforderlichen Unterlagen vernichtet. Soweit Schriftstücke noch benötigt wurden, sind sie zum jeweiligen Einzelvorgang genommen worden. Der Hauptordner wird als Grundsatzvorgang ohne Personenbezug weitergeführt.

Da der Berliner Datenschutzbeauftragte an dieser Stelle selbst davon ausgeht, daß die Angelegenheit erledigt ist und dies auch in einem Schreiben gegenüber der Zulassungsstelle des Landeseinwohneramt zum Ausdruck gebracht hat, verzichtet der Senat auf weitere Ausführungen.

### 4.2.4 Wirtschaftsverwaltung

**Datenlöschung in Gewerbeakten**

*Ein Bürger beschwerte sich darüber, daß sich in seiner Gewerbeakte noch ein Auszug aus dem Bundeszentralregister befinde, aus dem hervorgehe, daß er 1986 wegen Verstoßes gegen das Betäubungsmittelgesetz verurteilt worden sei, obwohl die Eintragung 1992 beim Bundeszentralregister getilgt worden sei. Auch eine Kopie des Urteils befand sich in der Gewerbeakte.*

Nach § 51 Abs. 1 Bundeszentralregistergesetz (BZRG) dürfen die Tat und die Verurteilung dem Betroffenen im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden, wenn die Eintragung im Bundeszentralregister getilgt ist. Eine fortdauernde Vorhaltung des Führungszeugnisses und des Strafurteils ist nach den enggefaßten Ausnahmen des Bundeszentralregistergesetzes möglich, wenn etwa die Zulassung des Betroffenen zu einem Gewerbe sonst zu einer erheblichen *Gefährdung der Allgemeinheit* führen würde; das gleiche gilt, wenn der Betroffene die Aufhebung einer die Ausübung eines Gewerbes untersagenden Entscheidung beantragt. Das BZRG geht in den die Allgemeinheit gefährdenden Fällen davon aus, daß eine Verurteilung auch nach Ablauf der Tilgungsfrist verwertet werden kann.

In dem konkreten Fall räumte das Gewerbeamt ein, daß weder der Zentralregisterauszug noch das Urteil zur Erfüllung der Aufgaben des Gewerbeamtes benötigt würden. Es bestehe aber eine Pflicht der Behörde zur vollständigen Aktenführung, die einer nachträglichen Entfernung von Informationen entgegenstehe, wenn diese rechtmäßig dorthin gelangt seien. Wegen des Grundsatzes der Vollständigkeit der Akten würde das Gewerbeamt hinsichtlich der Bundeszentralregisterauszüge auch keine Fristenkontrolle im Hinblick auf die *Tilgungsfrist* des BZRG und das daraus folgende *Verwertungsverbot* durchführen.

Wir haben die Senatsverwaltung für Wirtschaft darauf hingewiesen, daß ein *Grundsatz der Vollständigkeit* der Akte, der das informationelle Selbstbestimmungsrecht (ein Grundrecht) aushebelt, nicht existiert. Gemäß § 11 Abs. 6 Gewerbeordnung in Verbindung mit § 17 Abs. 3 Satz 1 Berliner Datenschutzgesetz

Der beanstandete Einzelfall berührt Grundfragen der Gewerbeaktenführung.

Nach § 11 Abs. 1 GewO darf die zuständige öffentliche Stelle personenbezogene Daten des Gewerbetreibenden und solcher Personen, auf die es für die Entscheidung ankommt, erheben, soweit die Daten zur Beurteilung der Zuverlässigkeit und der übrigen Berufszulassungskriterien bei der Durchführung gewerberechtlicher Vorschriften erforderlich sind.

Die zuständige Behörde darf daher im Rahmen ihrer Aufgabenerfüllung insbesondere Bundeszentralregisterauszüge und gegebenenfalls Strafurteile anfordern und zu den Akten nehmen soweit dies für die zu treffende Entscheidung erforderlich ist.

Für persönliche Daten, die im Laufe des Verwaltungsverfahrens gespeichert wurden, kann jedoch auf Sonderbestimmungen wie beispielsweise § 20 BDSG und auch § 17 Abs. 6 BlnDSG, die dem Grundsatz der Aktenvollständigkeit Rechnung tragen, verwiesen werden.

Das damit deutlich herausgestellte Erfordernis, den gesamten entscheidungsrelevanten Akteninhalt zur Verfügung zu haben, ist auch sinnvoll. Das Verwertungsverbot aus § 51 BZRG kann nicht dazu führen, daß es der zuständigen Behörde unmöglich gemacht wird, einem Betroffenen nach Eintritt des Verwertungsverbotes zu beweisen, daß eine ihn betreffende frühere Entscheidung rechtmäßig war.

Das Verwertungsverbot in § 51 Abs. 1 BZRG bezweckt den Schutz des Betroffenen für die Zukunft, soll aber nicht die unter Umständen auch in seinem Interesse liegende Nachvollziehbarkeit früherer Entscheidungen gefährden bzw. unmöglich machen.

Demnach ist eine Löschung von personenbezogenen Daten in Gewerbeakten nur dann vorzunehmen, wenn der gesamte Akteninhalt zur Aufgabenerfüllung nicht mehr erforderlich ist. Dies ist bei Gewerbeakten in der Regel erst dann der Fall, wenn feststeht, daß der Betroffene in gewerberechtlicher Hinsicht nicht mehr in

sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die datenverarbeitende Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Bei der Frage, welche personenbezogenen Daten zur rechtmäßigen Aufgabenerfüllung erforderlich sind, sind die Vorschriften des BZRG zu berücksichtigen. Da im vorliegenden Fall die Eintragung im Bundeszentralregister für die gewerberechtliche Bearbeitung der Akte ohne Bedeutung ist, ist die Kenntnis der Straftat für die Aufgabenerfüllung des Gewerbeamtes nicht erforderlich, so daß die Vernichtung des Führungszeugnisses und der Kopie des Urteils erfolgen muß.

Erscheinung tritt und die Akten ihre die Gesetzmäßigkeit der Verwaltung sichernde Dokumentationsfunktion nicht mehr zu erfüllen haben (BVerwG NVwZ 1988, S. 621 f).

### 4.2.5 Veterinäraufsicht

**Der Hund und sein gespeichertes „Frauchen“**

*Das Veterinär- und Lebensmittelaufsichtsamt hatte einer Charlottenburger Hundebesitzerin auf Grund wiederholter Bißvorfälle die Auflage erteilt, die Hunde in der Öffentlichkeit nur an einer kurzen, reißsicheren Leine zu führen. Kopien des Antwortschreibens auf den Antrag auf Aufhebung der Entscheidung (Auflage) sind an ein Veterinäramt und ein Ordnungsamt in einem anderen Bundesland – wo sich die Hundehalterin häufig mit ihren Hunden aufhält – gesandt worden. Darüber hinaus wurden Stellungnahmen des zuständigen Polizeiabschnittes und der Eltern des zuletzt gebissenen Kindes angefordert. Die Akte enthielt darüber hinaus eine Übersicht der Bißvorfälle seit 1977 (auch von anderen Hunden).*

Nicht alle Hunde wurden zu einem angesetzten Termin vorgeführt. Sie befanden sich zu diesem Zeitpunkt in dem anderen Bundesland. Daher wurde ein weiterer Termin dort bei dem Veterinäramt notwendig. Zur umfassenden Beurteilung der Hunde muß diese Behörde sowohl den aktuellen Sachverhalt als auch die Vorgeschichte kennen. Die *Datenübermittlung* war zur Aufgabenerfüllung des *Veterinäramtes* erforderlich und somit rechtmäßig (§ 44 Abs. 1 ASOG). Die Weitergabe an das Ordnungsamt war ebenfalls zulässig. Der Aufenthalt der Hunde begründet im Hinblick auf die von dem Tier ausgehende Gefahr die dortige örtliche Zuständigkeit.

Durch die *Anfrage bei dem Polizeiabschnitt* sollte in Erfahrung gebracht werden, ob dort Erkenntnisse über aktuelle Auffälligkeiten der Hunde vorliegen. Diese Anfrage ist nicht erforderlich (§ 18 Abs. 1, § 44 Abs. 1 ASOG) und damit unzulässig. Die Polizei übermittelt der zuständigen Ordnungsbehörde ohnehin alle relevanten Bißvorfälle (§ 4 i. V. m. § 42 Abs. 2 Nr. 1 ASOG). Sofern der Kontaktbereichsbeamte bei seinem Rundgang feststellt, daß von einem Hund eine Gefahr ausgeht, hat er dies der zuständigen Ordnungsbehörde mitzuteilen, die ihrerseits die erforderlichen Maßnahmen zu treffen hat. Die Polizei darf die erhobenen Daten nur solange in Akten oder Dateien speichern, soweit das zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist. Sie hat hier keine eigene Zuständigkeit und wird im Rahmen des § 4 ASOG nur hilfsweise für die Ordnungsbehörden tätig. Für darüber hinausgehende Speicherungen bleibt kein Raum.

Mit der *Stellungnahme der Eltern des zuletzt gebissenen Kindes* sollte eine Einschätzung des aktuellen Verhaltens der Hunde gewonnen und in Erfahrung gebracht werden, wie die seinerzeit Betroffenen eine Aufhebung des Leinenzwanges beurteilen. Nach § 18 Abs. 1 ASOG können die Ordnungsbehörden personenbezogene Daten erheben, wenn dies zur Abwehr einer Gefahr erforderlich ist. Die Eltern hätten als Zeugen nur Aussagen zu einem Vorfall machen können, der gut 22 Monate zurücklag. Da von ihnen weder zu erwarten war, daß sie eine korrekte Einschätzung der von den Hunden aktuell ausgehenden Gefahr hätten geben können, noch diese Einschätzung maßgeblich für den Erlaß eines Verwaltungsaktes gewesen wäre – dies ist die Aufgabe des Veterinär- und Lebensmittelaufsichtsamtes – beschränkt sich der Wert solcher Stellungnahmen lediglich auf die Beschreibung eigener Reaktionen und Gefühle sowie der Folgen des damaligen Bißvorfalles. Hieraus lassen sich jedoch keine Rückschlüsse auf das momentane Verhalten der Hunde ziehen. Die Datenerhebung bei den Eltern des zuletzt gebissenen Kindes war demzufolge nicht erforderlich.

Im Rahmen der Fachaufsicht war der Vorgang Gegenstand sowohl von Gesprächen mit dem betroffenen Veterinär- und Lebensmittelaufsichtsamt als auch in Dienstversammlungen mit den Leitern der Veterinär- und Lebensmittelaufsichtsämter der Berliner Bezirke. Die dabei abgesprochene Vorgehensweise ist außerdem mit dem Berliner Datenschutzbeauftragten abgestimmt worden. Danach sollen folgende Prüffristen den Veterinär- und Lebensmittelaufsichtsämtern als Entscheidungshilfe dienen:

1. Warnung nach Vorfall ohne Gefährdung von Menschen (Hund beißt Hund): 6 Monate
2. Leinenzwang und/oder Maulkorbzwang, Weggabe des Hundes: 3 Jahre
3. sofortige Tötung des Hundes: 3 Jahre
4. Weggabe des Hundes und Haltungsverbot: 5 Jahre
5. Sofortige Tötung des Hundes und Haltungsverbot: 10 Jahre

Sollte im Einzelfall eine längere Prüfzeit erforderlich werden, so ist diese mit einer nachvollziehbaren Begründung aktenkundig zu machen.

Soweit der Berliner Datenschutzbeauftragte davon ausgeht, daß die Aufbewahrungsfristen nach Bekanntwerden des Todes oder Verlustes (z. B. Weggabe) des Hundes gegenstandslos werden, liegt offenbar ein Mißverständnis vor. Der Berliner Datenschutzbeauftragte hat inzwischen erkannt, daß z. B. bei sofortiger Tötung des Hundes eine Prüffrist von drei Jahren anzusetzen ist. Es kann nichts anderes gelten, wenn der Hund weggegeben wurde. Die Verantwortlichkeit für die Gefahrenfälle liegt beim Halter und nicht beim Hund.

Soweit in den Fällen Nr. 3, 4 und 5 die Unzuverlässigkeit des Halters besonders entscheidend ist, muß für den Fall der Rückholung des Hundes bzw. einer Ersatzbeschaffung der Datenzugriff möglich bleiben. In solchen Fällen ist nach der Lebenswirklichkeit von einer fortbestehenden (konkreten) Gefahr auszugehen.

Die Veterinär- und Lebensmittelaufsichtsämter werden im übrigen sicherstellen, daß eine Weitergabe von Daten und unzulässige Anfragen nicht erfolgen.

Die in *Akten* gespeicherten Daten sind nach § 48 Abs. 3 ASOG spätestens *zu vernichten,* wenn die gesamte Akte zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgabe nicht mehr erforderlich ist. Bei Daten, die in personenbezogenen Akten gespeichert sind, ist nach Ablauf bestimmter Fristen zu prüfen, ob die Speicherung der Daten zur Aufgabenerfüllung erforderlich ist. Die Fristen dürfen regelmäßig bei Erwachsenen zehn Jahre nicht überschreiten, wobei nach dem Zweck der Speicherung sowie der Art und Bedeutung des Anlasses zu unterscheiden ist. Hier ist – mit Ausnahme besonders schwerer Fälle, in denen ein Haltungsverbot und die Abgabe oder sofortige Tötung des Hundes angeordnet werden muß – eine Prüffrist von höchstens drei Jahren angemessen. Wenn der Hund innerhalb dieses Zeitraumes nicht mehr auffällig gewesen ist, ist eine weitere Speicherung nicht erforderlich. Die Frist beginnt mit dem letzten Anlaß der Speicherung (§ 48 Abs. 4 ASOG). Die Akten sind ferner nach Bekanntwerden des Todes oder des Verlustes (z. B. Weggabe) des Hundes zu vernichten. Das Veterinär- und Lebensmittelaufsichtsamt ist zur Überprüfung gesetzlich verpflichtet. Hier sind entsprechende organisatorische Maßnahmen zu treffen.

## 4.3 Justiz und Finanzen

### 4.3.1 Justiz

Mitte 1997 haben Bundestag und Bundesrat nun endlich das Justizmitteilungsgesetz (JuMiG)[125] beschlossen. Das Artikelgesetz wird am 1. Juni 1998 in Kraft treten. Bis zu diesem Zeitpunkt sollen die Verwaltungsvorschriften über Mitteilungen in Straf- und Zivilsachen von den Justizverwaltungen des Bundes und der Länder überarbeitet und dabei den Regelungen des JuMiG angepaßt werden. In Berlin kann damit die provisorische Regelung des Ausführungsgesetzes zum Gerichtsverfassungsgesetz (AGGVG), nach der bundeseinheitliche Verwaltungsvorschriften in Berlin Gesetzeskraft hatten (§ 29 Abs. 2 AGGVG), durch eine haltbare Bestimmung abgelöst werden.

Durch das JuMiG wird erstmals in Form eines Gesetzes geregelt, in welchen Fällen personenbezogene *Mitteilungen der Justizbehörden über staatsanwaltschaftliche und gerichtliche Verfahren* an andere öffentliche Stellen zulässig sind. Nicht aufgenommen worden ist in das Gesetz die Pflicht zur *Benachrichtung des Betroffenen* über die Datenübermittlungen von Amts wegen. Nur in den Fällen, in denen der Betroffene bei Mitteilungen in Strafsachen nicht zugleich der Beschuldigte oder in Zivilsachen nicht zugleich Partei oder Beteiligter ist, sieht das Gesetz eine Unterrichtung über den Inhalt und den Empfänger der Daten von Amts wegen vor. In allen übrigen Fällen wird dem Betroffenen nur auf Antrag Auskunft erteilt.

Das Gesetz enthält auch überraschende Regelungen. So verbirgt sich hinter dem geänderten § 125 Beamtenrechtsrahmengesetz auch eine Verwendungsbefugnis für nach dem JuMiG übermittelte Daten für die Wahrnehmung der Aufgaben nach dem Sicherheitsüberprüfungsgesetz (SÜG) oder einem entsprechenden Landesgesetz. Es lohnt sich also, dieses Gesetz sorgfältig zu lesen.

Im letzten Jahresbericht[126] hatten wir darüber berichtet, daß die Bundesregierung noch Ende des Jahres 1996 einen eigenen Entwurf eines Strafverfahrensgesetzes vorgelegt hatte. Die Konferenz der Datenschutzbeauftragten hat daraufhin am 17./18. April 1997 eine Entschließung zu den Beratungen zum Strafverfahrensänderungsgesetz (StVÄG) 1996 gefaßt, in der noch einmal wesentliche Kritikpunkte an dem Gesetzentwurf vorgestellt wurden[127]. Erst Anfang 1998 lagen die Äußerung des Bundesrates und die Gegenäußerung der Bundesregierung vor[128]. Es ist zu befürchten, daß das Gesetzgebungsverfahren in dieser Legislaturperiode nicht mehr zu einem Abschluß kommen wird und im Justizbereich immer noch ohne ausreichende datenschutzrechtliche Regelungen gearbeitet werden muß.

Der Senat begrüßt, daß das Justizmitteilungsgesetz nach einer langen gesetzgeberischen Vorlaufzeit 1997 endlich verabschiedet werden konnte. Die vom Berliner Datenschutzbeauftragten angesprochenen Punkte waren Gegenstand intensiver Beratungen im Bundesrat und Bundestag, in die die Stellungnahmen der Datenschutzbeauftragten jeweils Eingang gefunden haben. Gleiches gilt für die Neufassung der „Anordnung über Mitteilungen in Strafsachen (MiStra)“, die derzeit auf Grund des Justizmitteilungsgesetzes ländereinheitlich neu gefaßt und zum 1. Juni 1998 in Kraft gesetzt wird.

Der Entwurf zu einem Strafverfahrensänderungsgesetz 1996 (StVÄG 1996), der eine Vielzahl datenschutzrechtlicher Detailregelungen für das Strafverfahren enthält, befindet sich noch in den Beratungen im Bundestag. Die Justizminister der Länder haben wiederholt den Bundestag aufgefordert, diese Entwürfe vorrangig zu behandeln, um den teilweise nicht hinnehmbaren Zustand der Rechtsunsicherheit für die Strafverfolgungspraxis, aber auch für die Betroffenen, zu beenden. Der Senat teilt die Sorge des Berliner Datenschutzbeauftragten, daß eine kurzfristige Verabschiedung des Entwurfs nicht möglich sein wird.

125 BGBl. 1997, I, S. 1430; vgl. auch JB 1995, 5.7; JB 96, 4.3.1
126 JB 1996, 4.3.1
127 Anlage 2.1.1
128 BT-Drs 13/9718

**Elektronisch überwachter Hausarrest – eine neue Form des Strafvollzuges**

Die Senatsverwaltung für Justiz hat eine Gesetzesvorlage für eine Bundesratsinitiative des Landes Berlin zur Änderung des Strafvollzugsgesetzes vorgelegt[129], mit der durch die Einführung eines § 11 a in das Strafvollzugsgesetz die Erprobung des elektronisch überwachten Hausarrestes im Strafvollzug in Deutschland ermöglicht werden soll. Voraussetzung soll die Einwilligung des Strafgefangenen sowie seiner Haushaltsangehörigen sein.

Nähere Vorgaben werden nicht gemacht. So stünde die ganze bislang vor allem in den USA, aber unter anderem auch in Schweden (mit angeblich gutem) und Großbritannien (mit katastrophalem Ergebnis) praktizierte bzw. erprobte Palette technischer Umsetzungen zur Disposition: die *aktive Variante,* bei der ein an Hand- oder Fußgelenk angebrachter Sender *Signale an ein Zusatzgerät am Telefon* aussendet, das mit einem entsprechenden Rechner im Justizvollzug verbunden ist und übermittelt, ob der Gefangene einen bestimmten Radius verläßt oder – bei entsprechender Ausgestaltung – in welcher Entfernung er sich vom Telefon befindet; die *passive Variante,* bei der sich der Gefangene auf *Abruf* melden muß – was den Vorteil hat, daß zusätzliche Daten abgerufen werden können (diskutiert werden nicht nur Identifizierungsdaten, sondern etwa auch die digitalisierten Ergebnisse von Alkoholtests) –; *„watch-patrol"-Systeme,* die mit *Radiowellen* oder *Mobilfunk* arbeiten und – im Gegensatz zu den vorherigen Verfahren – auch eine Kontrolle unterwegs oder am Arbeitsplatz ermöglichen. Daß das ganze auch auf Privatunternehmen „outgesourced" werden könnte, versteht sich inzwischen fast schon von selbst (in Großbritannien war man schon so vorgegangen). Das justizpolitische und kriminologische Für und Wider ist in den letzten Jahren mehrfach diskutiert worden. Zumindest in der Literatur überwiegen klar die ablehnenden Stimmen.

Basis aller Verfahren ist die Erhebung von Daten aus der Privatwohnung, sei es der Minimalinformation, daß der Wohnbereich verlassen wurde, sei es der Angabe des jeweils genau bestimmbaren Aufenthaltsorts in der Wohnung. Dies müssen durchaus nicht nur Daten des Gefangenen, sondern können gleichzeitig auch *Daten anderer Haushaltsmitglieder* sein (weswegen u. a. auch deren Einwilligung eingeholt werden soll). Bei watch-patrol-Systemen kommen entsprechende Bewegungsdaten auch außerhalb der Wohnung hinzu. Ungeachtet der Frage, ob die Speicherung dieser Daten gesetzlich zugelassen würde, wäre damit zumindest technisch die Erstellung der entsprechenden Bewegungsprofile möglich. Wiederum würde eine riskante Informationsinfrastruktur geschaffen. Ob als Grundlage für die Erhebung derartiger Daten die – in der Regel unter sozialen Zwängen abgegebene – Einwilligung ausreichen kann, ist (auch vor dem Hintergrund der Unverletzlichkeit der Wohnung und dem damit einhergehenden Verbot der Erhebung von Daten aus der Wohnung) zu bezweifeln. Diese Frage stellt sich dann verschärft, wenn zusätzliche Daten erhoben werden – etwa über regelmäßig zu Hause durchzuführende *Alkoholtests.*

Probleme anderer Art wirft der Umstand auf, daß sich die Verfahren des Telefons oder anderer Telekommunikationsmittel bedienen müssen, die derzeit noch unter den bekannten Unsicherheitsrisiken leiden. Mangelnder Abhörschutz, die Möglichkeit der Manipulation (auch durch den Gefangenen selbst) oder Authentifikationsprobleme machen einen hohen Aufwand für die Informationssicherheit erforderlich, der die Kostenvorteile in Frage stellen kann.

Auf abstrakterer Ebene stellt sich die Frage, ob das Überstülpen eines elektronischen Käfigs den Menschen nicht „zum Objekt eines technischen Überwachungsapparates"[130] macht und damit auf unverhältnismäßige Weise in seine unabdingbaren Freiheitsrechte eingreift. Das unaufhaltsame Vordringen der Informationstechnik macht es zunehmend erforderlich, Grenzen der Digitalisierung zu markieren, zumal wenn der Staat als Hoheitsträger oder gar wie hier als Strafvollstrecker auftritt. Die in den USA angeblich ernsthaft diskutierte Idee, die Elektronische Fessel dahingehend weiterzuentwickeln, daß beim virtuellen Berühren der Käfigstäbe das Sendegerät nach Art eines elektrischen

Der Rechtsausschuß des Bundesrates hat in seiner Sitzung am 12. November 1997 beschlossen, die Bundesratsinitiative des Landes Berlin zur Erprobung des elektronisch überwachten Hausarrestes zu vertagen. Dies erfolgt, um klärungsbedürftige Fragen, die im Zusammenhang mit der Erprobung des elektronisch überwachten Hausarrestes entstanden sind, im Rahmen einer länderübergreifenden Arbeitsgruppe klären zu lassen. Diese hat – unter Federführung durch das Land Berlin – inzwischen ihre Arbeit aufgenommen.

Es wurde Einvernehmen darüber erzielt, daß die Thematik der Arbeitsgruppe nicht allein auf der Grundlage der Gesetzesinitiative des Landes Berlin, die eine vollzugliche Lösung vorsieht, diskutiert werden soll, sondern daß die gesamte Bandbreite der in Betracht kommenden Anwendungsbereiche des elektronisch überwachten Hausarrestes Gegenstand der Erörterung sein soll. Arbeitsergebnisse sollen noch im Laufe des Jahres 1998 vorliegen.

Im Hinblick darauf, daß bei diesem Sachstand eine Erprobung des elektronisch überwachten Hausarrestes jedenfalls im Jahr 1998 nicht zu erwarten war, sind die insoweit im Entwurf des Haushaltsplans 1998 vorgesehenen Mittel von 200 000,– DM für eine anderweitige Verwendung bestimmt worden.

Die Senatsverwaltung für Justiz wird die Ausführungen im Jahresbericht 1997 zum elektronisch überwachten Hausarrest den anderen Landesjustizverwaltungen zur Kenntnisnahme übermitteln.

129 BR-Drs 698/97
130 so zuletzt der ehemalige Generalstaatsanwalt Ostendorf in: ZRP 97, 473 ff.

Weidezauns Stromschläge austeilt, zeigt, welche Weiterungen ins Blickfeld geraten, wenn man alle Grenzen ignoriert. Der Schritt zum gleichzeitig empfangenden und sendenden Televisor Orwells zur Überwachung des Bürgers scheint dann gar nicht mehr so groß.

Mit einer baldigen Entscheidung über den Gesetzentwurf wird in Berlin derzeit offenbar nicht gerechnet. Die ursprünglich für 1998 für die Einführung der elektronischen Fußfessel vorgesehenen Haushaltsmittel in Höhe von fast DM 500 000,– sind gestrichen worden.

**Korruptionsbekämpfung**

Im Jahresbericht 1996[131] hatten wir über die Planung der Senatsverwaltung für Justiz berichtet, ein Gesetz über die Einrichtung einer *Zentralen Erfassungs- und Koordinierungsstelle* zur Vorbeugung gegen Korruption zu schaffen. Gegen die Vorstellungen der Senatsverwaltung für Justiz bestanden erhebliche datenschutzrechtliche Bedenken.

In diesem Jahr hat die Senatsverwaltung für Justiz den Gesetzentwurf auf Grund zahlreicher Einwände verschiedener Stellen nochmals überarbeitet, dabei jedoch nur wenigen datenschutzrechtlichen Gesichtspunkten Rechnung getragen. Wir mußten die Senatsverwaltung daher darauf hinweisen, daß unsere Hauptkritikpunkte nach wie vor bestehen. Auch in der letzten, uns bekannten Fassung enthält der Gesetzentwurf keine klare Abgrenzung der Befugnisse der geplanten Koordinierungsgruppe von der Tätigkeit der Polizei zur vorbeugenden Verbrechensbekämpfung sowie der Tätigkeit der Staatsanwaltschaft bei der Einleitung eines Ermittlungsverfahrens.

Immer mehr andere Bundesländer haben im übrigen die Bekämpfung der Korruption im öffentlichen Dienst auf eine Sondergruppe bei den jeweiligen Staatsanwaltschaften übertragen – eine rechtstaatlich klare Lösung, die wir auch aus Sicht des Datenschutzes nur unterstützen können. Nach dem überraschenden Wechsel an der Spitze der Senatsverwaltung für Justiz wird das Projekt in dieser Form nicht mehr weiterverfolgt.

**Verbesserungen im Strafvollzug**

In unserem Jahresbericht 1995[132] hatten wir über unsere Querschnittsprüfung in der *größten Berliner Justizvollzugsanstalt*, der JVA Tegel, berichtet. In der Zwischenzeit haben mit Mitarbeitern der JVA Tegel und der Senatsverwaltung für Justiz zahlreiche Besprechungen zur Abarbeitung der bei der Querschnittsprüfung festgestellten Probleme stattgefunden. Bei diesen Besprechungen, aber auch bei der Bearbeitung von Eingaben, die die JVA Tegel betrafen, haben wir festgestellt, daß die Aufgeschlossenheit der Mitarbeiter gegenüber datenschutzrechtlichen Fragen und der Wille, Lösungen für diese Probleme zu finden, in eindrucksvoller Weise gestiegen ist. Dies zeigt sich auch darin, daß die Mitarbeiter der JVA Tegel im Rahmen der Verwaltungsreform einen Fortbildungsbedarf in datenschutzrechtlichen Fragen angemeldet haben, dem die Anstaltsleitung nachkommt. Ein praktisches Beispiel für die Aufgeschlossenheit der Mitarbeiter ist die Suche nach einer Alternative zu offenen Tafeln, die in den Gefangenen zugänglichen Räumen hängen und Gefangenendaten enthalten. Aus Althölzern wurde eine Falttafel konstruiert, die anstelle der offenen Tafeln aufgehängt werden kann. Die Werkstätten der Anstalt werden von dem Prototypen nach und nach Nachbauten anfertigen. Damit kann das datenschutzrechtliche Problem der unzulässigen Offenbarung von Gefangenendaten an Dritte in doppelter Hinsicht gut gelöst werden.

Die folgenden Verbesserungen konnten in der Zwischenzeit auf Grund unserer Gespräche mit der JVA Tegel und der Senatsverwaltung für Justiz erreicht werden:

- Alle Berliner Justizvollzugsanstalten haben inzwischen ein internes Dateienregister erstellt.

Der Datenschutzbericht 1997 enthält in diesem Bereich eine kurze Aufzählung datenschutzrechtlicher Probleme, die zwischenzeitlich einvernehmlich gelöst worden sind.

Die Senatsverwaltung für Justiz wird sich auch künftig im Gespräch mit ihren Mitarbeitern bemühen, Verständnis und Sensibilität für datenschutzrechtliche Belange zu wecken.

Die im Bericht angeführten Aufbewahrungsfristen personenbezogener Daten sollen – neben anderen bereichsspezifischen Regelungen über den Schutz und die Verwendung personenbezogener Daten – in einem neu zu fassenden § 184 des Strafvollzugsgesetzes geregelt werden.

131 JB 1996, 4.3.1
132 JB 1995, 3.5

- Lichtbilder von Gefangenen, die zu erkennungsdienstlichen Zwecken gefertigt worden sind, werden in Zukunft nur noch in der Vollzugsgeschäftsstelle und in den Teilanstalten (dort entweder in der Zentrale oder im Hausbüro) gesammelt werden. Das Fotostudio der JVA Tegel ist aufgelöst worden.
- Bei Entlassung eines Gefangenen in die Freiheit erfolgt eine Vernichtung aller zu erkennungsdienstlichen Zwecken gefertigten Lichtbilder in der JVA Tegel von Amts wegen.
- Die Anzahl der Stellen, die wöchentlich eine aktuelle Liste mit den Namen der Gefangenen erhalten, die der organisierten Kriminalität zugerechnet werden oder bei denen eine besondere Fluchtgefahr besteht, wurde um 25 Stellen verringert.

Die Mitarbeiter der JVA Tegel beschäftigen sich zur Zeit mit der Frage, wie lange die personenbezogenen Unterlagen, die auch Gefangenendaten enthalten, tatsächlich für ihre Aufgabenerfüllung benötigt werden. Das Thema der Aufbewahrungsfristen wird eines der nächsten Themen in unseren Gesprächsrunden sein.

**Nun doch noch: Ein Merkblatt zu datenschutzrechtlichen Fragen nach Ehescheidung**

Im Jahresbericht 1995[133] hatten wir über ein datenschutzrechtliches Problem bei *Ehescheidungsverbundurteilen* berichtet. Nach dem Ausspruch der Scheidung erhalten die geschiedenen Eheleute ein Urteil, das in seinem Urteilstenor die einzelnen Entscheidungen des Gerichtes – wie beispielsweise den Scheidungsausspruch, die Entscheidung über die elterliche Sorge oder über den Versorgungsausgleich – enthält. Da nach der Scheidung zahlreiche Behörden und sonstige Stellen die Vorlage des Scheidungsurteils verlangen, für ihre Aufgabenerfüllung aber nur einen einzelnen Entscheidungsausspruch aus dem Urteilstenor benötigen, hatten wir bei der Senatsverwaltung für Justiz angeregt, den Parteien nach der Scheidung ein Merkblatt zuzusenden, das auf die Möglichkeit verweist, sich für die verschiedenen Vorlagezwecke des Scheidungsurteils entsprechende Auszüge aus dem Scheidungstenor fertigen zu lassen.

Nachdem die Senatsverwaltung für Justiz ein solches *Merkblatt* zunächst nicht für erforderlich hielt, hat sie nun auf Grund einer entsprechenden Empfehlung des Unterausschusses „Datenschutz“ des Abgeordnetenhauses die Versendung eines entsprechenden Merkblattes zusammen mit dem Scheidungsurteil bei den Gerichten angeordnet. Damit wird es den Parteien nach einer Ehescheidung wesentlich erleichtert, ihre Datenschutzrechte wahrzunehmen.

Ein Merkblatt für Bürger, das auf Datenschutzrechte hinweist, ist auch eine Form der Bürgerfreundlichkeit.

Es wird bestätigt, daß die Versendung des Merkblatts angeordnet worden ist. Nicht geteilt werden kann die Einschätzung, daß es sich dabei um eine sinnvolle Form der Bürgerfreundlichkeit handelt.

Vielmehr wird die Einschätzung der gerichtlichen Praxis geteilt, daß die Verteilung von jährlich knapp 19 000 Merkblättern nur im Bereich des Familiengerichts Tempelhof-Kreuzberg in der Summe ein personeller und materieller Mehraufwand ist, der in keinem Verhältnis zum Nutzen für die Bürger steht.

**Übermittlung einer vollständigen Urteilsabschrift an eine Behörde**

*Ein Berliner Amtsgericht übermittelte an die für die Führung des Wählerverzeichnisses zuständige Abteilung der Senatsverwaltung für Inneres eine vollständige beglaubigte Abschrift eines strafrechtlichen Urteils des Landgerichtes Berlin. In dem Urteil war die Unterbringung des Beschuldigten in einem psychiatrischen Krankenhaus angeordnet worden. Es enthielt eine detaillierte Schilderung der Lebensgeschichte des Betroffenen sowie seiner Taten, deretwegen das Gericht die Unterbringung in einem psychiatrischen Krankenhaus angeordnet hatte. Darüber hinaus waren gutachterliche Beurteilungen über den Betroffenen, die Namen des Opfers und der Zeugen in dem Urteil enthalten.*

Die Übersendung einer vollständigen Urteilsabschrift an die für das Wählerverzeichnis zuständige Verwaltungsbehörde stellt einen Verstoß gegen § 29 Abs. 2 AGGVG i. V. m. den Nrn. 12 a Abs. 2 und 8, Abs. 4 der Mitteilungen in Strafsachen (MiStra) dar, da die Übersendung einer vollständigen Urteilsabschrift für die Aufgabenerfüllung der Verwaltungsbehörde nicht erforderlich war. Die sich aus den MiStra ergebende Mitteilungspflicht bezieht sich nur auf die Tatsache, daß eine Unterbringung in

Die zuständigen Mitarbeiter des Amtsgerichts sind auf die Beanstandung des Berliner Datenschutzbeauftragten hingewiesen und auf die Einhaltung der datenschutzrechtlichen Bestimmungen hingewiesen worden. Dem Senat ist nicht bekannt, daß es erneut zu einem vergleichbaren Verstoß gegen datenschutzrechtliche Vorschriften gekommen ist. Es handelt sich um einen bedauerlichen Einzelfall.

133 JB 1995, 5.7

einem psychiatrischen Krankenhaus angeordnet worden ist. Alle anderen Daten sind für die Arbeit der Senatsverwaltung für Inneres ohne Belang. Wir haben deshalb gegenüber der Senatsverwaltung für Justiz eine Beanstandung ausgesprochen. Die Senatsverwaltung sieht in der Übersendung der vollständigen Urteilsabschrift ebenfalls einen Verstoß gegen datenschutzrechtliche Vorschriften. Sie geht von einem Einzelfall aus. Es bleibt zu hoffen, daß sie recht hat.

Bei jeder Datenübermittlung nach MiStra ist die Erforderlichkeit der Daten für den Empfänger vorab zu prüfen.

### 4.3.2 Finanzen

Seit vielen Jahren[134] fordern die Datenschutzbeauftragten des Bundes und der Länder die Aufnahme datenschutzrechtlicher Bestimmungen in die Abgabenordnung (AO). Auch dieses Berichtsjahr ist abgelaufen, ohne daß sich das Bundesministerium der Finanzen und die Landesfinanzverwaltungen inhaltlich weiterführend mit den Vorschlägen der Datenschutzbeauftragten befaßt hätten. Die Diskussion ist festgefahren, da die Finanzverwaltungen sie unter dem Gesichtspunkt führen, daß das Steuerrecht bereits eine umfassende, alles abdeckende Datenschutzvorschrift enthalte, nämlich die Regelung des Steuergeheimnisses. Dabei setzen sich die Behörden leider nicht mit den Vorgaben des Bundesverfassungsgerichtes im Volkszählungsurteil auseinander. Der Reformstau betrifft also nicht nur die Neuordnung des Einkommensteuerrechts, sondern auch die Berücksichtigung der informationellen Selbstbestimmung durch die Finanzverwaltung.

Zunächst geht der Senat davon aus, daß die Vorschläge der Datenschutzseite zur Aufnahme datenschutzrechtlicher Regelungen in die Abgabenordnung in den entsprechenden bundeseinheitlichen Gremien stets unter kritischer Hinterfragung des eigenen Standpunktes objektiv beraten werden.

Im übrigen hält die Finanzverwaltung an ihrer Auffassung fest, derzufolge das Steuerrecht bereits umfassende, alles abdeckende Datenschutzvorschriften in Gestalt des Steuergeheimnisses (§ 30 Abgabenordnung) enthält.

Die Bemerkungen des Berliner Datenschutzbeauftragten über einen angenommenen Reformstau beim steuerlichen Verfahrensrecht sind deshalb nicht richtig. Es wird darauf hingewiesen, daß in dem zitierten Volkszählungsurteil ausdrücklich festgestellt wird, daß die Sicherungsvorkehrungen der Abgabenordnung zum informationellen Selbstbestimmungsrecht in die verfassungsrechtlich gebotene Richtung weisen.

**Mitteilungsblatt der Steuerberaterkammer als Pranger**

*Ein Bürger machte uns darauf aufmerksam, daß die Steuerberaterkammer in ihrem Mitteilungsblatt regelmäßig die Namen und Adressen von Personen veröffentlicht, die strafbewehrte Unterlassungserklärungen gegenüber der Kammer haben abgeben müssen, oder gegen die eine einstweilige Verfügung wegen wettbewerbswidrigen Handelns ergangen ist, die verurteilt worden sind wegen Mißbrauchs von Titeln oder die nach einem Beschluß des Landgerichtes noch eine strafbewehrte Unterlassungserklärung abgegeben haben. Das Mitteilungsblatt der Steuerberaterkammer wird nicht nur von Kammermitgliedern gelesen, es liegt auch in öffentlich zugänglichen Bibliotheken aus.*

Zur Rechtfertigung wurden die verschiedensten Rechtsgrundlagen herangezogen. So zum Beispiel § 23 Abs. 2 des Gesetzes gegen den unlauteren Wettbewerb (UWG), der eine gerichtliche Anordnung voraussetzt oder § 76 Abs. 1 Steuerberatergesetz, der die Interessenwahrnehmung der Kammer für ihre Mitglieder festschreibt. Diese Bestimmungen sind so allgemein, daß sie eine derart eingreifende Maßnahme nicht stützen können.

Die *Veröffentlichung personenbezogener Daten* beurteilt sich vielmehr nach § 13 BlnDSG, da sie eine Datenübermittlung einer öffentlichen Stelle an Personen außerhalb des öffentlichen Bereiches darstellt. Die Kammermitglieder, die Adressaten des Mitteilungsblattes sind, sind gegenüber der Körperschaft Dritte, so daß eine Datenübermittlung an Dritte vorliegt. Voraussetzung für die Zulässigkeit einer Datenübermittlung an Dritte ist eine ausdrückliche Rechtsvorschrift, die diese erlaubt (oder aber die Einwilligung des Betroffenen). Eine derartige Rechtsvorschrift gibt es aber nicht. Der von der Steuerberaterkammer herangezogene § 76 Abs. 1 StberG stellt nur eine Aufgabenbeschreibung dar. § 23 Abs. 2 UWG lag nicht vor, denn in keinem Fall hatte ein Gericht die Veröffentlichung der zivilrechtlichen Entscheidung auf Antrag des Klägers im Urteil wegen eines Wettbewerbsverstoßes angeordnet. Strafrechtliche Urteile wegen Mißbrauchs von Titeln, in denen auch eine Veröffentlichung des Urteils verkündet worden wäre, sind uns ebenfalls nicht bekannt.

Die Steuerberaterkammer teilte inzwischen mit, sie werde bei der derzeitigen Rechtslage keine solchen Veröffentlichungen mehr vornehmen.

Da die Steuerberaterkammer sich der Auffassung des Berliner Datenschutzbeauftragten angeschlossen hat, hält der Senat eine Stellungnahme für entbehrlich.

134 JB 1996, 1.1

**Falsche Angabe zum Auftraggeber**

*Ein Erbin erhielt in einer seit langem beim Amt zur Regelung offener Vermögensfragen (AROV) anhängigen Vermögensrückübertragungsangelegenheit „aus heiterem Himmel" von einer Beratungsgesellschaft ein Schreiben, wonach diese „gemäß beigefügter Vollmacht des Landesamtes zur Regelung offener Vermögensfragen (LAROV Berlin) beauftragt" sei, „Recherchen zur Feststellung von Eigentumsveränderungen und Rechtsnachfolgen an restitutionsbelasteten Grundstücken" durchzuführen.*

Die der Beratungsgesellschaft erteilte *Vollmacht* ermächtigte nur zur Recherche bei Vermessungs- und Grundstücksämtern (nicht aber bei Privaten) und resultierte aus einem zwischen dem LAROV und der Beratungsgesellschaft geschlossenen Vertrag. Die Beratungsgesellschaft ist im vorliegenden Fall jedoch nicht für das LAROV tätig geworden, sondern tatsächlich für verschiedene Wohnungsbaugesellschaften. Diese haben nämlich an der Beschleunigung der Rückübertragungsverfahren (wegen der ihnen nach dem Gesetz zur Regelung offener Vermögensfragen zustehenden Verfügungsberechtigung) ein nicht unerhebliches Eigeninteresse. Deswegen haben sie die Durchführung von Recherchen zur Feststellung von Eigentumsveränderungen und Rechtsnachfolgen durch die Beratungsgesellschaft veranlaßt. Die so gewonnenen Erkenntnisse wurden dem jeweils zuständigen AROV übersandt. Sie sind also weder bei der Beratungsgesellschaft noch bei der jeweiligen Wohnungsbaugesellschaft gespeichert worden. Durch die Verwendung der Vollmacht ist allerdings bei den Befragten der Eindruck erweckt worden, daß das LAROV (als – den für die Entscheidungen in Restitutionsverfahren zuständigen Ämtern zur Regelung offener Vermögensfragen – übergeordnete Behörde) der Auftraggeber für die Recherchetätigkeit sei.

Wir konnten dem LAROV die fehlerhafte Verwendung seiner Vollmacht durch die Beratungsgesellschaft nicht vorwerfen, zumal nicht nachzuweisen war, daß ihm die Verwendung bekannt gewesen ist. Die Verfahrensweise der Beratungsgesellschaft selbst war aber rechtswidrig, weil sie gegen § 28 Abs. 1 Satz 2 BDSG verstoßen hat. Danach müssen personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Davon kann jedoch dann nicht ausgegangen werden, wenn dem Betroffenen durch Vorlage der Vollmacht einer Behörde vorgespiegelt wird, diese sei der „Initiator" für die durch die Beratungsgesellschaft durchzuführende Recherchetätigkeit. Es würde sonst ein Rechtsschein gesetzt, der auch einem der tragenden datenschutzrechtlichen Grundsätze zuwiderläuft, nach dem der Betroffene ein Recht darauf hat zu wissen, wer sich tatsächlich als Auftraggeber hinter derjenigen Stelle verbirgt, die die Erhebung personenbezogener Daten faktisch betreibt. Die Beratungsgesellschaft hatte die Tätigkeit für die Wohnungsbaugesellschaften zwischenzeitlich eingestellt.

Dem LAROV war nicht bekannt, daß die ausgestellte Vollmacht an die Beratungsgesellschaft auch gegenüber Privatpersonen genutzt worden ist. Sie wurde umgehend zurückgefordert, nachdem das LAROV über den vom Berliner Datenschutzbeauftragten dargestellten Sachverhalt informiert worden ist. Die Zusammenarbeit wurde eingestellt.

## 4.4 Sozialordnung

### 4.4.1 Arbeitnehmer und öffentliche Bedienstete

**Fragen nach der DDR-Vergangenheit**

In vier Urteilen vom Juli 1997 hat das Bundesverfassungsgericht die Verfassungsmäßigkeit der Sonderkündigungstatbestände nach dem *Einigungsvertrag* und der damit verbundenen *Überprüfung* für Angehörige des öffentlichen Dienstes der ehemaligen DDR im Grundsatz bestätigt, jedoch die Notwendigkeit der Einzelfallprüfung unterstrichen. Wir haben uns bereits 1990 ausführlich mit der zugrundeliegenden *Fragebogenaktion* auseinandergesetzt[135]. Einem der jetzt ergangenen Urteile lag eine Verfassungsbeschwerde aus Berlin zugrunde, bei der es um die Frage ging, ob ein Stellenbewerber aus der ehemaligen DDR verpflichtet ist, dem Arbeitgeber unbeschränkt Auskunft über frühere Tätigkeiten in SED-Funktionen oder die Zusammenarbeit mit dem Ministerium für Staatssicherheit zu geben.

Das Bundesverfassungsgericht hat klargestellt, daß diese Offenlegungspflicht zeitlich begrenzt ist[136]. Es hat hervorgehoben, daß im Rahmen der Eignungsprüfung im Einzelfall der Zeitfaktor zu

135 JB 1990, 3.5

136 BVerfG vom 8. Juli 1997 BvR 2111/94, 195/95 und 2189/95, EuGRZ 1997, 279, 284

berücksichtigen ist. Sowohl strafrechtliche Verjährungsfristen wie auch Tilgungsfristen des Strafregisterrechts verdeutlichen, daß sich die gesellschaftliche Ächtung von Fehlverhalten mit der Zeit verliert. Auch der Bundesgesetzgeber hat das *Stasi-Unterlagen-Gesetz* inzwischen dahingehend geändert, daß der Bundesbeauftragte für die Stasi-Unterlagen grundsätzlich keine Mitteilungen über den Inhalt von Akten des Ministeriums für Staatssicherheit mehr macht, wenn keine Anhaltspunkte vorhanden sind, daß nach dem 31. Dezember 1975 eine inoffizielle Tätigkeit für den Staatssicherheitsdienst vorgelegen hat[137]. Das Bundesverfassungsgericht hat darüber hinaus einen Zwang zur Offenlegung von Tätigkeiten als Funktionär in der SED oder für das Ministerium für Staatssicherheit als unverhältnismäßigen Eingriff in das allgemeine Persönlichkeitsrecht bezeichnet, soweit derartige Vorgänge vor dem Jahre 1970 abgeschlossen waren. Derartige Vorgänge hätten keine oder nur eine äußerst geringe Bedeutung für den Fortbestand des Arbeitsverhältnisses, und als Indiz für eine mangelnde Eignung taugten sie regelmäßig nicht mehr. Stellenbewerbern sei es deshalb nicht zuzumuten, eine zeitlich unbeschränkte Frage nach entsprechenden Tätigkeiten in vollem Umfang wahrheitsgemäß zu beantworten. Würden Vorgänge aus den Jahren vor 1970 verschwiegen, so dürften Arbeitgeber daraus keine arbeitsrechtlichen Konsequenzen ziehen.

Auch das Gesetz über den *Landesbeauftragten zur Aufarbeitung der Unterlagen des Staatssicherheitsdienstes* der ehemaligen DDR im Land Berlin (LStUG) wurde – neben einer Verlängerung der Geltungsdauer bis zum 30. November 2002 – insoweit geändert, als die Befugnisse des Landesbeauftragten erweitert wurden[138]. Wie bisher berät der Landesbeauftragte die öffentlichen Stellen des Landes. Er kann sich darüber hinaus auf Antrag an Überprüfungsverfahren beratend beteiligen und dabei in die herangezogenen Unterlagen Einsicht nehmen. Er ist außerdem befugt, die Ergebnisse von Überprüfungen von Mitarbeitern und Bewerbern bei den öffentlichen Stellen des Landes einzusehen (§ 1 Abs. 2 LStUG).

Wir haben im Gesetzgebungsverfahren darauf hingewiesen, daß die neue Befugnis des Landesbeauftragten, Ergebnisse von Überprüfungen bei den öffentlichen Stellen des Landes einzusehen, nach dem Gesetzeswortlaut weder durch eine Zweckbindung noch durch den Grundsatz der Erforderlichkeit eingeschränkt ist. Angesichts der hohen Sensibilität der Daten in den Überprüfungsunterlagen haben wir vorgeschlagen, die Einsichtnahme durch den Landesbeauftragten von der *Einwilligung* der Betroffenen abhängig zu machen. Der Gesetzgeber ist dieser Empfehlung nicht gefolgt.

Wir gehen allerdings davon aus, daß die Ausübung der neuen Einsichtsbefugnisse des Landesbeauftragten zwar nicht von der Einwilligung der Betroffenen abhängig ist, wohl aber der Zweckbindung nach dem Bundesgesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (§ 29) und dem verfassungsrechtlichen Grundsatz der Erforderlichkeit unterliegen.

**EU-Mittel Zug um Zug gegen Personaldaten**

*Ein Unternehmen beschwerte sich darüber, daß es als Träger von Förderungsmaßnahmen bei den beschäftigten ABM-Kräften umfangreiche Daten erheben sollte, die per Diskette an eine Servicegesellschaft weiterzuleiten waren. Diese sollte ihrerseits die Daten an ein überregionales Beratungsunternehmen für die Aufbereitung zu Gesamtaussagen übermitteln. Die Daten wurden der Senatsverwaltung für Arbeit, Berufliche Bildung und Frauen übergeben, die letztlich gegenüber der EU-Kommission die gewährten Mittel des Europäischen Sozialfonds (ESF) abzurechnen hatte. Die in einem von dem Beratungsunternehmen entwickelten Teilnehmerregistratursystem (TRS) zusammengefaßten Angaben zur einzelnen ABM-Kraft enthielten neben dem Namen, Vornamen, Geburtsdatum, Geschlecht und der Adresse u. a. Informationen darüber, ob der betroffene Ausländer, behindert, für bestimmte Zeit arbeitslos oder ungeeignet für den Arbeitsmarkt gewesen ist.*

Die zuständige Senatsverwaltung für Arbeit, Berufliche Bildung und Frauen, die auf Grund der Ausreichung von Fördermitteln des Europäischen Sozialfonds (ESF) an AB-Maßnahmeträger gegenüber der EU-Kommission verpflichtet ist, entsprechend Rechnung zu legen, sah sich im vorliegenden Fall, unter Einbeziehung eines beliehenen Unternehmens datenschutzrechtlich einer komplexen Aufgabenlösung gegenüber. Hierbei spielte das von einem Beratungsunternehmen entwickelte Teilnehmerregistratursystem (TRS) eine besondere Rolle. In diesem Zusammenhang trat die Vielschichtigkeit der datenschutzrechtlichen Beurteilung, speziell im Hinblick auf die Verschachtelung mehrerer Stellen, die personenbezogene Daten zu verarbeiten haben, am augenfälligsten zutage.

Da die Senatsverwaltung für Arbeit, Berufliche Bildung und Frauen die Kooperation mit dem Berliner Datenschutzbeauftragten schon rechtzeitig im Vorlauf zum datenschutzrechtlichen Lösungsansatz suchte, konnte auch in diesem Fall eine einvernehmliche Lösung, wie im vorliegenden Datenschutzbericht ausgewiesen, gefunden werden. Die Erfassung der notwendigen ABM- Arbeitnehmerdaten durch den Arbeitgeber bzw. der durch ihn Beauftragten ist insoweit eine zulässige Datenspeicherung, da die Überprüfung, inwieweit die Qualifizierung der ABM-Arbeit-

137 Drittes Änderungsgesetz zum Stasi-Unterlagen-Gesetz vom 20. Dezember 1996, BGBl. I, 2026

138 Erstes Gesetz zur Änderung des Gesetzes über den Landesbeauftragten zur Aufarbeitung der Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik im Land Berlin vom 5. November 1997, GVBl. S. 578

Besonders schwierig war hier die Ermittlung des Sachverhaltes, weil nicht klar war, welche der genannten Stellen welche Daten zur Erfüllung welcher Aufgaben benötigte, insbesondere weil es auch nicht möglich war, die europarechtlichen Bestimmungen hinreichend in Erfahrung zu bringen. Der Fall zeigt aber auch die Komplexität der datenschutzrechtlichen Beurteilung, wenn mehrere Stellen, die personenbezogene Daten verarbeiten, ineinander geschachtelt werden.

Das Erfassen der Arbeitnehmerdaten durch den Arbeitgeber stellt eine zulässige Datenspeicherung dar, weil die Prüfung, ob die Qualifizierung der ABM-Kraft mit den zur Verfügung stehenden Finanzmitteln erfolgreich gefördert worden ist, in den Rahmen der Zweckbestimmung des Vertragsverhältnisses mit dieser Arbeitskraft fällt (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Dasselbe gilt für die (ebenfalls nach dieser Vorschrift zulässige) Weitergabe der Daten an die Servicegesellschaft. Sie ist – wie das Beratungsunternehmen auch – Treuhänder des Landes Berlin und mit der Durchführung der Arbeitsbeschaffungsmaßnahmen für das Land Berlin, vertreten durch die Senatsverwaltung für Arbeit, Berufliche Bildung und Frauen, betraut. Da diese Treuhänder für die Senatsverwaltung die gesamte Funktion und nicht nur reine Datenverarbeitungsschritte wahrnehmen, sind sie jeweils eigenständige datenverarbeitende Stelle, so daß ihre Tätigkeit aus datenschutzrechtlicher Sicht den für sie selbst geltenden Rechtmäßigkeitsanforderungen unterliegt.

Als mit der Wahrnehmung hoheitlicher Aufgaben (nämlich bei der Gewährung von Zuwendungen) nach der Landeshaushaltsordnung beliehene Unternehmen (§ 7 Haushaltsgesetz 1995/1996) gelten diese als öffentliche Stellen. Da die Datenverarbeitung jedoch arbeitsrechtliche Rechtsverhältnisse betrifft, sind anstelle der einschlägigen Bestimmungen des BlnDSG diejenigen des BDSG maßgebend (§ 34 Abs. 2 BlnDSG).

Nach § 13 Abs. 1 BDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Dies ist insoweit der Fall, als ohne die im TRS aufzuführenden Daten die von der Servicegesellschaft und dem Beratungsunternehmen zu veranlassende Vergabe bzw. Abrechnung der ESF-Fördermittel nicht erfolgen kann. Das bedeutet zugleich, daß nur diejenigen Daten erhoben werden dürfen, die für die *jeweilige* Fördermaßnahme (d. h. für die Vergabe und Abrechnung der hierfür vorgesehenen Mittel) erforderlich sind. Da aber alle Daten, die in den einzelnen Förderprogrammen angefallen sind, in einem System vereinheitlicht wurden und die Maßnahmeträger (mangels entgegenstehender Information) häufig all diese Daten (und nicht nur die für das beantragte Förderprogramm erforderlichen) aufgeliefert haben, war diese „undifferenzierte“ Datenerhebung durch die Servicegesellschaften und das Beratungsunternehmen rechtswidrig.

Auch wurde nicht beachtet, daß personenbezogene Daten *beim Betroffenen bzw. mit seiner Mitwirkung* zu erheben sind. Da die Servicegesellschaften und das Beratungsunternehmen selbst nicht mit dem einzelnen Arbeitnehmer in Kontakt treten, müssen sie zumindest dafür sorgen, daß die für sie bestehenden Vorgaben des § 13 Abs. 2 BDSG durch die Maßnahmeträger erfüllt werden. Diese müssen die Mitwirkung der ABM-Kraft veranlassen, sie etwa bei der Eingehung des Arbeitsverhältnisses darüber informieren, daß zur Abwicklung des Vertragsverhältnisses eine Erhebung bestimmter personenbezogener Daten erforderlich ist.

Die weitere Datenübermittlung durch die Servicegesellschaft an das Beratungsunternehmen ist zulässig, weil dieses die Daten zu dem gleichen Zweck (nämlich zur Förderung von ABM-Kräften bzw. zur Vergabe und Abrechnung der Fördermittel) wie die Servicegesellschaft benötigt (§ 12 Abs. 1 Satz 2 BlnDSG), wobei diese Datenübermittlung zur rechtmäßigen Erfüllung der durch die Landeshaushaltsordnung zugewiesenen „Aufgaben bei der Gewährung von Zuwendungen“ erforderlich ist.

**Keine Verwaltungsreform ohne Datenzugriff**

Wesentlicher Bestandteil der Verwaltungsreform ist die Einführung einer *Kosten- und Leistungsrechnung,* die auf der Erhebung von Daten über den Aufwand beruht, der für die Erstellung der

nehmer mit den bereitgestellten finanziellen Mitteln effizient gewesen ist, mit der Zweckbestimmung des zugrunde liegenden Vertragsverhältnisses korrelieren muß. Insbesondere den haushaltsrechtlichen Belangen konnte im Rahmen des beschriebenen vielschichtigen Vertragsverhältnisses Rechnung getragen werden.

Die Aufgabe der einmaligen Zeit- und Mengenstatistik bestand in einer Überprüfung der durch die jeweiligen Beteiligten definierten Produkte bezüglich ihrer Tauglichkeit als Berichts- und

| Bericht des Berliner Datenschutzbeauftragten | Stellungnahme des Senats |
|---|---|
| „Produkte“ der Verwaltung erforderlich ist. In einer einmaligen Zeit- und Mengenstatistik wurde hierfür in den vergangenen Monaten Ausgangsmaterial gesammelt[139]. Nach Abschluß dieser Phase wird nun das Permanentverfahren in der Berliner Verwaltung eingeführt. Grundlage bildet die zwischen dem Hauptpersonalrat und der Senatsverwaltung für Inneres abgeschlossene Dienstvereinbarung vom April 1997. | Steuerungsobjekte. Dabei sollte u.a. festgestellt werden, wie trennscharf die Produktdefinitionen waren und wie sich die Arbeit mit den festgelegten Bezugsgrößen gestaltet. Die Schaffung von Ausgangsmaterial zur Kosten- und Leistungsrechnung war mit der einmaligen Zeit- und Mengenstatistik nicht beabsichtigt und auch nicht zu erreichen. |
| Im Rahmen der Zeitstatistik werden Stellenanteile pro Produkt und Mitarbeiter im Verhältnis zur Sollarbeitszeit erfaßt. Außerdem wird der Anteil der nichtproduktbezogenen Tätigkeiten pro Mitarbeiter – ebenfalls im Verhältnis zur Sollarbeitszeit – ausgewiesen. Diese Daten werden in das *„PRO-FISKAL-Modul zur Leistungserfassung“* (DLE-X) eingegeben. Im Gegensatz zum Testverfahren ist die Angabe eines eindeutigen Identifikationsmerkmals für die Mitarbeiter auf den Meldebelegen vorgesehen. Dies ist für Vollständigkeitskontrollen bei den Meldebelegen und für die Pflege des Datenbestandes erforderlich. Die Zusammenführung der Daten aus der Zeitstatistik und der Mengendaten, deren Zählung anonym erfolgen soll, findet nach dem Buchungsschluß im Kernmodul für die Kostenrechnung (DKR-X) statt, wobei nach Darlegung der Senatsverwaltung für Finanzen auch bei den Daten aus der Zeitstatistik kein Personenbezug mehr vorhanden sein soll. | In der Zeitstatistik werden keine Stellenanteile im Verhältnis zur Sollarbeitszeit erfaßt. Grundsätzlich hält jede Dienstkraft fest, wie sich ihre tatsächliche Arbeitszeit in einem Monat anteilig auf die Produkte verteilt, die von ihr bearbeitet wurden. Die Arbeitszeit, deren Anteile an der tatsächlichen Arbeitszeit nicht eindeutig einem Produkt zugerechnet werden können, wird als nichtproduktbezogene Tätigkeit (npT) erfaßt. Diese Anteile der Arbeitszeit werden dann bewertet und als Kostendatum zu einzelnen Produkten ausgewiesen. |
| Nach Ziffer 4.2 der Dienstvereinbarung sind die erhobenen Daten aus der Zeitstatistik nicht für individuelle *Leistungs- und Verhaltenskontrollen* von Dienstkräften zu verwenden. Zum Verhalten des Mitarbeiters kann anhand der Daten aus der Zeitstatistik nur eine Aussage über die prozentuale Verteilung der monatlichen Sollarbeitszeit auf Produkte und auf nicht produktbezogene Tätigkeiten getroffen werden. Diese Angaben werden über die Meldestelle an den Kostenstellenleiter weitergeleitet und nach der Datenerfassung durch die zuständigen Sachbearbeiter „Kostenrechnung“ vernichtet. | Da lediglich der Anteil an der tatsächlichen Arbeitszeit erfaßt wird, kann über die Verteilung der monatlichen Sollarbeitszeit keine Aussage getroffen werden (vgl. oben). |
| Nach längerem Schriftwechsel zwischen der Senatsverwaltung für Finanzen einerseits und dem Hauptpersonalrat sowie dem Berliner Datenschutzbeauftragten andererseits wurde darüber hinaus festgelegt, daß die Übergabe der Daten von DLE-X nach DKR-X ausschließlich in verdichteter Form vorgenommen wird, da andernfalls in besonders kleinen Verwaltungseinheiten ein Personenbezug herstellbar wäre. Ferner wurden die Zugriffsrechte auf die Daten im Modul DLE-X ausschließlich auf die Sachbearbeitung Kostenrechnung beschränkt. Dies hat zur Folge, daß nur die damit betraute Person an die Beschäftigten zwecks Rückfragen bzw. Vervollständigung von Angaben herantreten kann. | |
| Allerdings kam es bei der Umsetzung dieses Verfahrens zu Irritationen: So beabsichtigte ein Bezirksamt für die Bildung des sogenannten „Identen“ die *Personalnummer* der Mitarbeiterinnen und Mitarbeiter zu verwenden. Dieses Vorhaben stieß auf datenschutzrechtliche Bedenken. | Die Auffassung des Berliner Datenschutzbeauftragten über die Nutzung der Personalnummer als „Ident“ wird vom Senat geteilt. Bei der Zeitstatistik ist deshalb eine andere Lösung gewählt worden, die datenschutzrechtlich unbedenklich ist. |
| Sollen Personaldaten – dazu zählt auch die Personalnummer – in automatisiert geführten Dateien verarbeitet werden, so ist die Erforderlichkeit ihrer Verarbeitung besonders zu prüfen. Das Personalkennzeichen ist für die Personalverwaltung das zentrale Ordnungsmerkmal, dient der besseren Organisation und soll unnötige Suchaktionen verhindern. Die Verwendung dieser Nummer zur Identifizierung des Beschäftigten bei der Durchführung der Zeit- und Mengenstatistik dient nicht dem ursprünglichen Zweck, also weder der Personalverwaltung noch der Personalwirtschaft, und versetzt den Sachbearbeiter „Kostenrechnung“ in die Lage, den Schlüssel für sämtliche die Person des Beschäftigten betreffende höchstpersönliche Daten zu erhalten. Die Nutzung der Personalnummer als „Ident“ ist daher unzulässig. | |
| Hinter der Verwaltungsreform verbirgt sich neben dem Bestreben, die Kostenstrukturen transparenter zu machen, auch die Intention, den wegen der Haushaltslage erforderlichen dramatischen Personalabbau zu effektivieren. Auch hierzu müssen Personaldaten verarbeitet werden. So zum Beispiel mittels eines Fragebogens zur sozialen Lage der Bediensteten. | |

139 JB 1995, 3.6

*Bei einer Senatsverwaltung stellte das Personalreferat mit einem Rundschreiben zur Sozialauswahl für die Ermittlung von Personalüberhang fest, die in dem Fragenkatalog aufgeführten Angaben fielen in das Informationsrecht des jeweiligen Vorgesetzten, es sei denn, daß sich die zu erfragenden Angaben auf Dritte (unterhaltsberechtigte/pflegebedürftige Personen) beziehen. Für diese sei eine Einverständniserklärung mittels eines Formblattes entwickelt worden, in dem die Betroffenen ihr Einverständnis bezüglich der Erhebungsbefugnis des Vorgesetzten erklären können.*

Ein Informationsrecht des Vorgesetzten bezüglich der Auswahlkriterien besteht nicht. Sowohl bei Fragen nach Lebensalter, Beschäftigung beim Land Berlin, Unterhaltsverpflichtungen gegenüber Kindern, Familienstand etc. handelt es sich um Personalaktendaten, zu denen Zugang nur Beschäftigte haben dürfen, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Zu diesem Personenkreis zählt der Vorgesetzte nicht. Den Mangel durch Einholung einer entsprechenden Einwilligungserklärung beheben zu wollen, ist ebenfalls datenschutzrechtlich bedenklich.

Einwilligung setzt Selbstbestimmung und diese wiederum Entscheidungsfreiheit über die vorzunehmenden oder zu unterlassenden Handlungen voraus. Da der Schutz der informationellen Selbstbestimmung die Fremdbestimmung ausschließen soll, muß die Einwilligung freiwillig erteilt werden. Der Betroffene muß, ohne einen Nachteil befürchten zu müssen, die Einwilligung auch verweigern dürfen. Da im vorliegenden Fall zwischen Vorgesetztem und Mitarbeitern regelmäßig ein Über- bzw. Unterordnungsverhältnis besteht, das wiederum zu einem Abhängigkeitsverhältnis führt, ist von einer *Freiwilligkeit der Einwilligung* nicht ohne weiteres auszugehen. Im Ergebnis ist daher festzustellen, daß eine Erhebung bzw. Verarbeitung der Personaldaten zum Zwecke der Sozialauswahl nur von der jeweiligen personalaktenführenden Stelle durchzuführen ist. Die Senatsverwaltung ist unseren Ausführungen im Ergebnis gefolgt.

*Wem es widerfährt, daß seine Stelle abgebaut werden soll und er deshalb in den Personalüberhang aufgenommen wird, muß auch hinsichtlich seiner Daten mit einigen Unannehmlichkeiten rechnen. Im Telefonverzeichnis einer Senatsverwaltung wurden die Bearbeiterzeichen aller Beschäftigten, die zum Personalüberhang des Landes Berlin gehören und somit keine Planstelle mehr haben, mit einem dreistelligen Namenskürzel gekennzeichnet. Auch die Namenstafeln an den Diensträumen wurden mit diesem Kennzeichen versehen.*

Die Zugehörigkeit zum Personalüberhang ist ein Umstand, der die Betroffenen in besonderer Weise diskriminieren kann. Zwar wird das betreffende Personal nicht ausdrücklich als „Überhang“ bezeichnet, doch ist davon auszugehen, daß dieser „Code“ (falls er überhaupt als solcher gedacht war) sehr schnell von den übrigen Mitarbeitern „entschlüsselt“ wird.

Derartige Daten unterliegen auf Grund ihrer hohen Sensibilität einer gesteigerten Geheimhaltungspflicht und sind nur einem begrenzten Personenkreis zugänglich zu machen. Die *Kennzeichnung der Personalüberhangkräfte* auf Namenstafeln und in Telefonverzeichnissen führt jedoch zu einer unnötigen Stigmatisierung und Ausgrenzung der Betroffenen, die durch die bestehende Situation ohnehin beschwert sind. Die Maßnahmen wurden eingestellt.

Die Maßnahme wurde eingestellt. Allerdings hätte sich die betroffene Senatsverwaltung einen etwas sensibleren Umgang mit dem gesamten Vorgang gewünscht. Erst durch die Publizierung des Vorgangs wurde der Personenkreis allgemein entschlüsselt. Gerade weil es sich um gesetzlich geschützte Personalaktendaten handelt, wäre eine interne Klärung hilfreicher gewesen.

Es scheint, als sei das „Outsourcing“[140], also die Privatisierung von Aufgaben, die bislang unangefochtenerweise von der öffentlichen Verwaltung wahrgenommen wurden, das Non-plus-ultra der Verwaltungsreform. Mitunter werden allerdings – auch im wörtlichen Sinne – die zulässigen Grenzen überschritten.

*Der Sender Freies Berlin und eine Berliner Krankenkasse hatten die Pfälzische Pensionsanstalt in Bad Dürkheim „beauftragt“, die Berechnung der Beihilfen gegenwärtigen und früheren Bediensteten des SFB und der Krankenkasse sowie – am Fall der Krankenkasse – der Versorgungsbezüge durchzuführen.* Die

140 vgl. JB 1994, 3.3

*Pfälzische Pensionsanstalt übernahm das Bereitstellen der Antragsformulare, die Entgegennahme der Beihilfeanträge sowie – laut Leistungsbeschreibung – „die Berechnung und Vorbereitung der Beihilfefestsetzung nach den jeweils gültigen landesrechtlichen Beihilfevorschriften" (also in eigener Verantwortung) und die Auszahlung der Beihilfeleistung. Auch sollten sie den Schriftwechsel für notwendige amts- und vertrauensärztliche Begutachtungen durchführen und schließlich zur schriftlichen Unterstützung im Zusammenhang mit Prozessen verpflichtet sein.*

Die *Datenverarbeitung im Auftrag*, die ohne weitere materielle Voraussetzungen zulässig ist (§ 3 BlnDSG), stellt lediglich eine Hilfsfunktion für die Erfüllung der Aufgaben und Geschäftszwecke der datenverarbeitenden Stelle dar. Datenverarbeitung im Auftrag liegt dagegen nicht vor, wenn die ursprüngliche datenverarbeitende Stelle die zugrundeliegenden Aufgaben ganz oder teilweise mit überträgt oder wenn der externe Datenverarbeiter überwiegend eigene Geschäftszwecke verfolgt, indem er über die technische Durchführung der Verarbeitung hinaus mit Hilfe der überlassenen Daten vertragliche Leistungen erbringt[141].

Hier wollten der SFB und die Berliner Krankenkasse beide Funktionen vollständig übertragen, so daß die Pfälzische Pensionsanstalt selbst datenverarbeitende Stelle geworden und die Weitergabe der personenbezogenen Daten von der AOK an sie eine Datenübermittlung wäre. Hierfür ist eine Rechtsgrundlage erforderlich. Denn Personalakten, zu denen auch die Unterlagen über die *Beihilfe* als Teilakte gehören, können ohne Einwilligung der Beamten nur unter engen Voraussetzungen weitergegeben werden, die hier nicht vorliegen. Das gilt erst recht, wenn es sich um die Weitergabe der mit Beihilfeanträgen regelmäßig verbundenen medizinischen Unterlagen handelt. Auch das Einholen einer Einwilligung wäre nicht zulässig, weil bei dienst- oder arbeitsrechtlichen Verhältnissen Zweifel an der Freiwilligkeit einer solchen Einwilligung nie völlig ausgeräumt werden können. Die Einwilligung kann daher nicht als Rechtsgrundlage für eine Übermittlung derart sensibler Personaldaten herangezogen werden. Hinzu kam in diesem Fall, daß die zuständige Rechtsaufsichtsbehörde die Auffassung vertreten hat, daß ein Tätigwerden der Pfälzischen Pensionsanstalt außerhalb der Landesgrenzen von Rheinland-Pfalz unzulässig sei. Wir haben dementsprechend den Sender Freies Berlin und die Krankenkasse aufgefordert, die Vereinbarungen mit der Pfälzischen Pensionsanstalt aufzuheben.

**Wer darf welche Personaldaten kennen?**

In der öffentlichen Verwaltung stellt sich gleichermaßen wie in der Privatwirtschaft die Frage, welchen Stellen in der Organisation welche persönliche Daten der Bediensteten oder Arbeitnehmer zur Verfügung stehen dürfen. Es gilt der Grundsatz, daß Personaldaten geheimzuhalten sind und nur denjenigen Stellen offenbart werden dürfen, die Aufgaben der Personalverwaltung wahrnehmen. In das Beamtenrecht ist dieser Grundsatz vor einiger Zeit ausdrücklich aufgenommen worden (in Berlin in § 56 Abs. 3 Landesbeamtengesetz) – für die anderen Arbeitnehmer gilt er mangels hinreichender, wenn auch dringend erforderlicher gesetzlicher Regelungen, unmittelbar.

Schwierig wird die Abgrenzung des berechtigen Personenkreises immer dann, wenn ein *Fachvorgesetzter* zwar für die Arbeitsabläufe verantwortlich, selbst aber nicht mit der Bearbeitung von Personalangelegenheiten befaßt ist.

*Der Amtsleiter einer bezirklichen Fachabteilung hielt in seinem Amtszimmer eine Personaldaten- bzw. Personalaktendatensammlung über die in seinem Amt beschäftigten Mitarbeiterinnen und Mitarbeiter vor, die sowohl von seinen Vorgängern als auch von ihm selbst angelegt worden war. Die Sammlung betraf einen Zeitraum von ca. 30 Jahren. Sie enthielten, alphabetisch nach den Zunamen der Mitarbeiter sortiert, ausschließlich Personalvorgänge, die entweder beim jeweiligen Amtsleiter entstanden oder ihm in Kopie zur Kenntnis bzw. zur Stellungnahme zugeschickt worden waren. Dabei handelte es sich vornehmlich um Zeiterfassungsbögen, Stellenbesetzungs- und Personalpla-*

141 vgl. unten 4.8.1

*nungsvermerke, Stellungnahmen zur nachträglichen Vergütung von Bereitschaftsdienstzeiten, Abgeltung von Mehrarbeit, Eingruppierungsfragen etc. Darüber hinaus enthielten die Ordner alte Entwürfe von Dienstleistungsberichten, die von der jeweiligen Amtsleitung verfaßt worden waren. Dagegen fanden sich bei dem von uns gesichteten Aktenmaterial keine geheimen Aufzeichnungen oder persönliche Notizen des Amtsleiters über Verhalten, Leistung oder Auftreten der Beschäftigten.*

Es ist – entgegen häufig vertretenen Auffassungen – zulässig, daß Fachvorgesetzte *Nebenakten* führen, wenn dies für die Aufgabenerfüllung erforderlich ist und sie nur Unterlagen enthalten, die sich auch in der Grund- bzw. Teilakten befinden (§ 56 Abs. 2 Satz 3 LBG). Von daher war der Sachverhalt aber nicht zu beanstanden.

Da Personalunterlagen, soweit sie nicht Gegenstand der Personalakte werden, allerdings dann zu vernichten sind, wenn sie für die Aufgabenerledigung im Amt nicht mehr erforderlich sind, haben wir die Vorgehensweise des Amtsleiters bemängelt.

Nunmehr wird in dem betreffenden Bezirksamt den Amtsleitern jeweils am Jahresende im Zuge einer sogenannten Jahresinventur die Durchsicht aller bei ihnen befindlichen Personalunterlagen aufgegeben. Mit einer Speicherung des Zeugnisentwurfs als Grundlage der folgenden Beurteilung waren wir einverstanden. Spätestens nach deren Abgabe muß jedoch der alte Entwurf vernichtet werden. Dem Beispiel dieses Bezirksamts sollten alle anderen Bezirksämter folgen.

*Ein Beschäftigter einer Hochschule hegte den Verdacht, seine Beschäftigungsstelle führe hinter seinem Rücken eine geheime Nebenakte zu seiner Personalakte. In der Tat wurde über den Petenten ein Aktenordner geführt. Dieser Ordner befand sich zwar in einem speziell gesicherten Behältnis, enthielt jedoch Unterlagen, die bereits überprüfte und abgeschlossene Sachvorgänge sowie verschiedene zwischen Arbeitgeber und Petenten geführte Arbeitsgerichtsprozesse betrafen. Ferner stellte sich heraus, daß dieser Vorgang dem Petenten bislang nicht zur Kenntnis gegeben worden war.*

Hier war die Führung einer Nebenakte nicht erforderlich. Die Institutsleitung wurde daher gebeten, die Unterlagen, die für Gerichtsverfahren benötigt werden bzw. wurden, dem Rechtsreferat der Hochschule zur Verfügung zu stellen, die Unterlagen, die bereits abgeschlossene Sachvorgänge betrafen, zu vernichten und dem Petenten auf Wunsch Einsicht in den Ordner zu gewähren.

Auch die später von uns überprüfte Personalakte des Petenten wies etliche Mängel auf. So fanden sich in der Akte noch Hinweise auf eine Dienstrüge, die auf Grund einer Entscheidung des Arbeitsgerichts zurückgenommen werden mußte, sowie der gesamte Schriftwechsel mit dem Petitionsausschuß auf Grund einer Petition des Beschäftigten. Auch diese Unterlagen sind aus den Akten entfernt worden.

Der Grundsatz, daß nur mit der Bearbeitung von Personalangelegenheiten betraute Bedienstete Personaldaten zur Kenntnis erhalten dürfen, gilt auch im Verhältnis zu Bezirksverordnetenversammlungen, wenn diese nicht im Rahmen ihrer Zuständigkeiten in nichtöffentlicher Sitzung über Personalsachen beraten.

Die Frauenvertreterin eines Berliner Bezirksamtes schilderte uns folgenden Sachverhalt:

*In der Sitzung des Ausschusses für Gleichstellung der Bezirksverordnetenversammlung sei im Zusammenhang mit einer Stellenbesetzung eine vom Bürgermeister in Auftrag gegebene Stellungnahme zu einer Mitarbeiterin, die in der Art einer Beurteilung beantwortet worden war, in öffentlicher Sitzung in Kopie an alle Ausschußmitglieder verteilt worden, ohne den Namen der Mitarbeiterin zu schwärzen. Zum anderen seien Einschätzungen von Bewerberinnen um die Stelle der Frauenvertreterin namentlich und ungeschwärzt an die Senatsverwaltung für Inneres geschickt und ebenfalls ungeschwärzt in Kopie an den Ausschuß für Gleichstellung gegeben worden. Wie sich später herausstellte, waren diese Personalunterlagen vom Bezirksbürgermeister nicht irrtümlich, sondern bewußt dem Gleichstellungsausschuß übergeben worden.*

Die Vorgehensweise des Bürgermeisters verstieß gegen datenschutzrechtliche Bestimmungen. Bei den übermittelten Daten handelte es sich um Personalaktendaten von Beschäftigten. Diese sind auch gegenüber der *Bezirksverordnetenversammlung* vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Zugang zu diesen Unterlagen dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist.

Personaldaten sind ebenfalls vertraulich zu behandeln und dürfen nur unter den in § 6 BlnDSG genannten Voraussetzungen verarbeitet werden.

Da keine der genannten Voraussetzungen erfüllt war, wurden die mit diesem Vorgang verbundenen Verstöße gegen die §§ 56 LBG sowie 6 BlnDSG beanstandet.

**Unsensibel mit sensiblen Daten**

Auch soweit es nicht um Angelegenheiten der Personalverwaltung geht, läßt der Umgang mit personenbezogenen Daten am Arbeitsplatz mitunter zu wünschen übrig. Insbesondere wird häufig genug nicht darauf geachtet, daß bei Vorgängen, bei denen der Personenbezug nicht erforderlich ist, eine anonyme Bearbeitung ausreicht.

*Eine Justizangestellte im Protokolldienst berichtete uns, sie habe einen schriftlichen Verbesserungsvorschlag gefertigt und an die Verwaltung im Hause mit dem Zusatz „vertraulich/verschlossen“ gerichtet. Die Verwaltung habe daraufhin diesen Vorschlag kopiert und in ihrem Namen an Kollegen der Petentin verteilt. Auch anläßlich einer Dienstbesprechung sei ihr Name gefallen. Danach sei sie verbalen Angriffen der Kollegen ausgesetzt gewesen. Die Verwaltung rechtfertigte ihr Vorgehen mit dem Hinweis, die Beschäftigte habe in ihrem Schreiben weder ausdrücklich um Anonymität im Zusammenhang mit ihrem Vorschlag gebeten, noch sei das Schreiben als „vertraulich“ gekennzeichnet gewesen.*

Für die Behandlung eines Verbesserungsvorschlages tut der Name des Bediensteten nichts zur Sache. Aus dem Umstand, daß das Schreiben nicht als „vertraulich“ von der Absenderin gekennzeichnet wurde, folgt nicht zwingend, daß die Petentin auf einen solchen Umgang mit ihrem Verbesserungsvorschlag verzichten wollte, zumal der Vorschlag offensichtlich nicht nur den Arbeitsbereich der Petentin, sondern auch anderer Mitarbeiterinnen und Mitarbeiter tangierte und von diesen möglicherweise als belastend empfunden wurde.

Wir haben daher einen datenschutzrechtlichen Mangel festgestellt und empfohlen, derartige Vorgänge grundsätzlich vertraulich zu behandeln, es sei denn, der Beschäftigte wünscht ausdrücklich die Nennung seines Namens.

*Der kaufmännische Angestellte eines größeren Unternehmens berichtete, er habe ein Schreiben von einer Versicherung erhalten, in der ihm eine Direktversicherung durch Gehaltsumwandlung angeboten worden sei. Es handelt sich um eine persönliche Berechnung, die auf der Grundlage seiner Personalnummer, seines Geburtsdatums und seines Diensteintrittsalters erstellt worden war. Auf Vorhalt habe der Personalleiter erklärt, es handele sich hierbei um einen ganz normalen Vorgang. Das Unternehmen habe zum Wohle der Mitarbeiter Daten an einen nicht unternehmensgebundenen Versicherer übermittelt, um jedem seine persönliche Berechnung nach Hause schicken zu können.*

Das Verhalten des Arbeitgebers verstößt gegen das Bundesdatenschutzgesetz. Danach beeinträchtigt die Übermittlung von Informationen, die sich auf arbeitsrechtliche Verhältnisse beziehen, in jedem Fall schutzwürdige Interessen der betroffenen Arbeitnehmer (es sei denn, der Arbeitnehmer hat eingewilligt).

*Der behördliche Datenschutzbeauftragte einer Anstalt des öffentlichen Rechts fragte an, ob der Grund der Abwesenheit vom Arbeitsplatz (Krankheit, Urlaub, Sitzung, Dienstreise) allen Mitarbeitern mittels PC bekanntgemacht werden darf.*

Ein datenschutzrechtlicher Mangel liegt im Gegensatz zu der Auffassung des Berliner Datenschutzbeauftragten nicht vor. Es ist schon zweifelhaft, ob der Direktor des Amtsgerichts den Namen der Petentin „verwendet“ hat. Denn sie selbst hat ihn mit dem Verbesserungsvorschlag verbunden. Ihr Name war auch ein von dem Vorschlag nicht zu trennender Bestandteil. Denn nach den im Berichtszeitraum geltenden Grundsätzen über das Vorschlagswesen in der Berliner Verwaltung – Vorschlagsgrundsätze (VorschlGr.) vom 27. Juli 1982 (DBl. I/1982 S. 106/DBl. I Nr. 8 vom 6. Juli 1990) – , waren für die Vorschläge Prämien ausgelobt, die an die Einreicher ausgezahlt wurden. Dazu ist naturgemäß der Name erforderlich.

Der *Abwesenheitsgrund* ist ein personenbezogenes Datum, das nach dem Grundsatz der Erforderlichkeit nur dem engeren Mitarbeiterkreis, bei dem ein dienstliches Interesse vorhanden ist, mitgeteilt werden darf. Die Einschränkung auf den gewünschten Personenkreis läßt sich durch entsprechende Zugriffsrechte auf dieses Datum technisch bewerkstelligen.

**Paßwortschutz nicht gegenüber Arbeitgeber?**

Auch die Frage, welche Angaben der Arbeitgeber vom Arbeitnehmer während des Arbeitsverhältnisses verlangen kann, ist mitunter problematisch.

> *Zunehmend werden wir von Arbeitgebern und Dienstvorgesetzten gefragt, ob es zulässig sei, Mitarbeiterinnen und Mitarbeitern das persönliche Paßwort abzufordern, wenn der Verdacht besteht, daß diese den dienstlichen PC für private Zwecke mißbrauchen.*

*Paßwörter* werden vergeben, um eine eindeutige Zuordnung zwischen Benutzer und System herzustellen. Damit werden mehrere Zwecke verfolgt, z. B. Zugangssicherung, Zugangsprotokollierung, Authentifikation bei Veränderungen. Wird dieses Paßwort an einen Dritten herausgegeben, unabhängig um welche Person es sich dabei handelt (Arbeitgeber, Kollege, Systemverwalter), kann nicht mehr nachvollzogen werden, wer Aktivitäten am System vorgenommen hat. Aktionen könnten den Mitarbeitern nicht mehr zugeordnet werden, eine personenbezogene Protokollierung, etwa zur Umsetzung der datenschutzrechtlich vorgeschriebenen Eingabekontrolle, liefe ins Leere. Daraus ergibt sich, daß aus Gründen der technisch-organisatorischen Absicherung des Systems eine Herausgabe des Paßwortes nicht in Betracht kommt.

Allerdings kann der Systemverwalter mit seinem *Super-User-Paßwort* die Dateien einsehen, wobei dies grundsätzlich nur zulässig ist, wenn die Systemverwaltung dies erfordert. Für Notfallsituationen, in denen der Systemverwalter nicht anwesend ist, empfiehlt sich allerdings, das Paßwort bei einer zentralen Stelle (z. B. der Geschäftsführung) verschlossen zu hinterlegen. In diesem und nur in diesem Fall ist die Geschäftsleitung zur Nutzung des Super-User-Paßworts berechtigt. Dies schließt allerdings nicht aus, daß im Bedarfsfall (etwa wenn tatsächliche Anhaltspunkte für einen Mißbrauch vorliegen) Kontrollen stattfinden. Der Systemverwalter hat in jedem Fall (z. B. auf Grund der Nutzung seines Super-User-Paßworts) die Möglichkeit, in die Dateien Einsicht zu nehmen. Eine solche Nutzung ist auch im Einzelfall zulässig, etwa für eine Notfallsituation zu Zeiten, in denen der Systemverwalter nicht anwesend ist. Dieser sollte sein Paßwort selbstverständlich für den Fall, daß er selbst nicht zur Verfügung steht, bei einer zentralen Stelle (u. U. die Geschäftsführung) verschlossen hinterlegen.

Daneben ist anerkannt, daß beim Vorliegen eines tatsächlichen Anhaltspunktes für eine Straftat, aber auch wegen eines schweren arbeitsrechtlichen Verstoßes ohne Beteiligung des Arbeitnehmers Kontrollmaßnahmen durchgeführt werden können. Soweit hierzu die Nutzung des Super-User-Paßworts erforderlich ist, kann es hierzu auch eingesetzt werden.

Es darf aber keinesfalls zu einer heimlichen Ausforschung des Arbeitnehmers ohne konkreten Anhaltspunkt genutzt werden. Grundsätzlich ist vielmehr davon auszugehen, daß der Arbeitgeber nicht ohne Beteiligung des Arbeitnehmers in dessen Arbeitsbereich eingreifen darf. Die gewünschten Kontrollen sind daher im Beisein des Arbeitnehmers, der dann sein Paßwort verdeckt eingeben kann, durchzuführen.

**Die Frage nach der Umweltkarte**

> *Benutzen Mitarbeiter der Berliner Verwaltung für Dienstgänge in Berlin öffentliche Verkehrsmittel, so werden ihnen die Fahrkosten durch Ausgabe von Einzelfahrscheinen erstattet. Die Senatsverwaltung für Inneres empfahl den Dienststellen, die betroffenen Beschäftigten durch Unterschriftsleistung versichern zu lassen, daß sie keinen privaten Fahrausweis (z. B. eine Umweltkarte) besitzen. Dieses Verfahren gab Anlaß zu Beschwerden.*

Die Empfehlung der Senatsverwaltung für Inneres im Rundschreiben II Nr. 46/1996 durch Unterschriftsleistung bestätigen zu lassen, daß die Dienstkraft nicht in Besitz eines privat beschafften Zeitfahrausweises ist, begründet sich durch die Erstattungspflicht aus dem Bundesreisekostengesetz, die sich nur auf tatsächlich entstandene Mehraufwendungen bezieht (§ 3 Abs. 1 BRKG).

Zurecht geht die Senatsverwaltung für Inneres davon aus, daß die Bediensteten nur einen Anspruch auf Erstattung der dienstlich veranlaßten Mehraufwendungen haben. Allerdings führt die Empfehlung der Innenverwaltung zu einer Erhebung von Personaldaten, die über das erforderliche Maß hinausgeht. Wir haben deshalb vorgeschlagen, daß den Bediensteten, die eine entsprechende Versicherung nicht abgeben wollen, die Möglichkeit eröffnet wird, entweder den Einzelfahrschein vor Antritt des Dienstganges bei der Dienststelle abzuholen und ihn anschließend abgestempelt als Nachweis für den durchgeführten Dienstgang abzugeben oder nach beendetem Dienstgang einen privat erworbenen und abgestempelten Fahrausweis gegen einen neuen *Dienstfahrschein* einzutauschen. Die Senatsverwaltung für Inneres hat uns mitgeteilt, daß sie diese alternative Verfahrensweise ebenfalls für korrekt hält. Da sie allerdings auf eine Modifizierung des entsprechenden Rundschreibens verzichtet hat, weisen wir die öffentlichen Stellen des Landes Berlin an dieser Stelle auf die datenschutzfreundlichere Alternative der Fahrkostenerstattung hin.

Derartige Mehraufwendungen entstehen nicht, wenn Mitarbeiter der Berliner Verwaltung für Dienstwege in Berlin öffentliche Verkehrsmittel benutzen und in Besitz eines privaten Zeitfahrausweises sind, den sie dem Notwendigkeitsgrundsatz (vgl. § 3 Abs. 2 BRKG) entsprechend einzusetzen haben. Aus Sicht des Senats sollte es daher grundsätzlich entsprechend dem dafür maßgebenden Rundschreiben dabei bleiben, daß die Mitarbeiter vor Ausgabe eines dienstlichen Fahrausweises nach dem Besitz eines privaten Zeitfahrausweises gefragt bzw. um die Abgabe der Versicherung gebeten werden, daß ihnen für den geplanten Dienstgang kein privater Zeitfahrausweis zur Verfügung steht, der benutzt werden könnte und müßte.

Der Senat hat gegen die vom Berliner Datenschutzbeauftragten dazu vorgeschlagene datenschutzfreundliche Alternative des Nachweises der entstandenen Fahrkosten durch Vorlage der benutzten dienstlich beschafften Fahrausweise nach dem Dienstgang bzw. den Eintausch benutzter Einzelfahrscheine gegen dienstliche Fahrausweise zwar grundsätzlich keine Bedenken, jedoch ist dieses Verfahren zeitaufwendiger. Vor allem aber wird dadurch nicht ausgeschlossen, daß Mitarbeiter trotz Besitzes von privaten Zeitfahrausweisen dennoch dienstlich beschaffte Fahrausweise erlangen und auch benutzen, obwohl dies wegen des privaten Zeitfahrausweises nicht notwendig wäre und somit der Erstattungsanspruch entfällt. Wegen der insoweit bestehenden Bedenken verzichtet die Senatsverwaltung für Inneres auf eine der erwähnten Alternative entsprechende Modifizierung des geltenden Rundschreibens und hält den Hinweis des Berliner Datenschutzbeauftragten in dem Jahresbericht 1997, der allen Behörden zur Verfügung steht, für ausreichend.

**Mitbestimmung und Datenschutz**

Datenschutzrechtliche Fragen zum Verhältnis zwischen Behördenleitung und Personalrat bzw. Unternehmensleitung und Betriebsrat begleiteten die deutsche Datenschutzdiskussion von Anfang an. Insbesondere ist bislang unklar geblieben, welche Stellung die Mitbestimmungsgremien gegenüber den betrieblichen und behördlichen Datenschutzbeauftragten haben.

Im Jahresbericht 1995[142] hatten wir über den Konflikt zwischen dem Betriebsrat eines Berliner Unternehmens und dem betrieblichen *Datenschutzbeauftragten* berichtet. Der Betriebsrat hatte das Recht des betrieblichen Datenschutzbeauftragten bestritten, die Einhaltung datenschutzrechtlicher Bestimmungen auch bei der Datenverarbeitung im Betriebsrat sicherzustellen. Wir hatten die Auffassung vertreten, daß der betriebliche Datenschutzbeauftragte nach dem Bundesdatenschutzgesetz den Schutz personenbezogener Daten im Unternehmen umfassend sicherzustellen hat und deshalb auch der Betriebsrat seiner Kontrollbefugnis unterliegt. Inzwischen hat das Bundesarbeitsgericht[143] diese Rechtsfrage im entgegengesetzten Sinn entschieden. Nach Auffassung des Bundesarbeitsgerichts nimmt der betriebliche Datenschutzbeauftragte keine neutrale Position zwischen Arbeitgeber und Betriebsrat ein, sondern ist trotz seiner Freiheit von fachlichen Weisungen der Arbeitgeberseite zuzuordnen. Die Datenverarbeitung beim Betriebsrat sei deshalb ausschließlich von der Aufsichtsbehörde nach dem Bundesdatenschutzgesetz zu kontrollieren.

Damit entsteht in privatwirtschaftlichen Unternehmen ein datenschutzrechtliches *Kontrolldefizit*, denn die Aufsichtsbehörde kann nach dem noch geltenden Bundesdatenschutzgesetz nur bei hinreichenden Anhaltspunkten für die Verletzung datenschutzrechtlicher Vorschriften tätig werden. In allen anderen Bereichen des Unternehmens hat daneben der betriebliche Datenschutzbeauftragte unabhängig von konkreten Anhaltspunkten für Datenschutzverstöße für die Sicherstellung des Datenschutzes zu sorgen. Diese Möglichkeit besteht hinsichtlich der Datenverarbeitung beim Betriebsrat jetzt nicht mehr. Um dieses Kontrolldefizit auszugleichen, sollte der Bundesgesetzgeber im Zuge der anstehenden Novellierung des Bundesdatenschutzgesetzes klarstellen, daß auch der Betriebsrat hinsichtlich seines

142 JB 1995, 6.3
143 Beschluß vom 11. November 1997 – 1 ABR 21/97, Computerrecht intern 1998, 7

Umgangs mit personenbezogenen Daten der Kontrolle durch den betrieblichen Datenschutzbeauftragten unterliegt. Gleichzeitig sollte die Unabhängigkeit des betrieblichen Datenschutzbeauftragten von der Unternehmensleitung gestärkt und zugleich dem Betriebsrat ein *Mitbestimmungsrecht bei der Bestellung des Datenschutzbeauftragten* auch dann eingeräumt werden, wenn diese Funktion einem vorhandenen Mitarbeiter des Unternehmens übertragen werden soll.

*In einem Unternehmen wurde die Einführung eines Informationssystems als Informationsbasis des Mitarbeiter-Know-how geplant. Das System sollte das Know-how aller Mitarbeiter erfassen und insbesondere der strategischen Personalplanung, -förderung und -entwicklung dienen sowie die gezielte Besetzung von Projekten fördern. In diesem Zusammenhang bat der Betriebsrat um umfangreiche Ergebnisberichte, wie sie für die Personalverantwortlichen vorgesehen waren, allerdings unter Auslassung*

- *des Namens,*
- *der Personalnummer und*
- *der PIN-Nummer (dies ist eine Nummer, die das System selbst jedem Datensatz fest zuordnet).*

Der Betriebsrat als Organ des Betriebes besitzt keine eigene Rechtspersönlichkeit und ist daher als Teil der speichernden Stelle des Betriebes anzusehen. Daraus folgt jedoch nicht, daß Informationen frei fließen können, vielmehr richten sich die Informationsansprüche des Betriebsrates nach dem Betriebsverfassungsgesetz, das den zulässigen Rahmen für die Nutzung der Arbeitnehmerdaten bestimmt (§ 28 Abs. 1 BDSG).

Danach steht dem Betriebsrat § 92 Betriebsverfassungsgesetz ein umfassendes und rechtzeitiges Informationsrecht bei der *Personalplanung* zu. Entsprechend hat der Arbeitgeber den Betriebsrat über die Personalplanung, insbesondere den Personalbedarf sowie über die sich daraus ergebenden personellen Maßnahmen und Bildungsmaßnahmen, anhand von Unterlagen zu unterrichten. Insoweit kann es erforderlich werden, daß der Arbeitgeber dem Betriebsrat bestimmte über das Personaldatensystem erhobene oder zu erhebende Daten zugänglich macht, sofern das Personaldatensystem für die Personalplanung erhebliche Daten enthält. Im Planungsstadium sind dabei regelmäßig nur anonymisierte Daten zu übermitteln, die als Entscheidungsgrundlage für die Personalplanung dienliche Informationen enthalten.

Der für den Betriebsrat vorgesehene Ergebnisbericht sollte daher nur Angaben enthalten, die einerseits dem Informationsbedürfnis des Betriebsrates Rechnung tragen, andererseits die Möglichkeit einer Personenbeziehbarkeit weitgehend einschränken.

### 4.4.2 Gesundheit

**Organtransplantationen**

Das *Transplantationsgesetz* vom 5. November 1997[144] ist nach langwierigen und zum Teil heftigen Debatten in Kraft getreten. Der Gesetzestext berücksichtigt im wesentlichen die von den Datenschutzbeauftragten im Gesetzgebungsverfahren geltend gemachten Gesichtspunkte. Insbesondere ist zu begrüßen, daß es nicht zu einer Widerspruchslösung und damit zu einem indirekten Erklärungszwang für Patienten gekommen ist. Die in §§ 3 und 4 verankerte *Zustimmungslösung,* die auf die Zustimmung des Organspenders zu Lebzeiten oder nach seinem Tode auf die Zustimmung der Angehörigen abstellt, hat sich in der Praxis allerdings erst noch zu bewähren. Es muß deutlich darauf hingewiesen werden, daß der mutmaßliche Wille eines möglichen Organspenders zwar ein geeignetes Entscheidungskriterium sein kann, daß dafür aber immer nur auf die Einzelsituation des jeweiligen verstorbenen Patienten abgestellt und nicht generell von einer pauschalierten Spendebereitschaft der Bevölkerung ausgegangen werden kann. Zu begrüßen ist vor allem, daß Angehörige den mutmaßlichen Willen zu prüfen haben und nicht Personen, die ein therapeutisches Interesse an der Organentnahme haben.

Der Senat stimmt mit der Meinung des Berliner Datenschutzbeauftragten überein.

144 BGBl. I, 2631

**Berlin – Stadt der Gesundheitsregister**

Berlin mit seinen mächtigen Forschungseinrichtungen beherbergt eine Reihe großer Datensammlungen mit medizinischen Daten.

Aus der DDR-Zeit stammt das Krebsregister der neuen Bundesländer, dessen Weiterführung zunächst durch das Krebsregistersicherungsgesetz gewährleistet wurde. Im vergangenen Jahr wurde der Staatsvertrag über das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen unterzeichnet. Er wird in der ersten Hälfte 1998 in Kraft treten und eine endgültige Rechtsgrundlage für diesen wichtigen Datenbestand darstellen.

In den letzten beiden Jahresberichten[145] informierten wir über die verschiedensten Maßnahmen, eine datenschutzgerechte Lösung für das *Qualitätssicherungsregister von Dialysepatienten* zu finden. Nachdem die Anonymisierung bzw. auch Deanonymisierung durch das Dazwischenschalten eines Treuhänders rechtlich wie auch technisch datenschutzgerecht ausgestaltet wurde, konnten mit ausdrücklicher Einwilligung der Betroffenen die Primärdaten erhoben werden. Zwischenzeitlich melden ca. 900 Dialyseeinrichtungen quartalsweise die Daten an den Datentreuhänder. Dieser gibt dann nach der Anonymisierung die Einzeldaten zur Speicherung an das Register weiter. Da es sich hierbei um Daten von fast 60 000 Patienten handelt, galt es, effiziente technische und dennoch datenschutzgerechte Lösungen zu suchen.

Als ein erster Schritt wurde im April begonnen, an die Patienten einen Patientenausweis in Form einer *Chipkarte* auszugeben. Aus unserer Sicht ist neben den Vorteilen, die diese Karte für die Patienten beispielsweise beim Wechseln der Behandlungseinrichtung, aber auch für die Ärzte und das Register selbst bietet, von entscheidender Bedeutung, daß weder die Behandlung noch die Meldung an das Register selbst „zwangsweise“ die Nutzung dieser Chipkarte voraussetzt. Somit wird der Dialysepatient nicht gezwungen, sich über die Karte „auszuweisen“. Sie kann ihm aber mit seiner Einwilligung in Zukunft erhebliche Vorteile bringen, wenn in besonders gesicherten Bereichen charakteristische Behandlungsdaten zusätzlich gespeichert werden. Gegenwärtig ist dies jedoch noch nicht vorgesehen.

Die Bearbeitung der vierteljährlich beim Treuhänder eingehenden großen Mengen an Patientendaten in Form von Meldebögen oder auch übersandten Disketten stellt einen erheblichen Arbeitsaufwand und auch ein Datenschutzrisiko dar. So wurde ein sehr komplexes und ausgeklügeltes Konzept erarbeitet, das auch die Online-Übertragung von Patientendaten durch die Behandlungseinrichtung an den *Datentreuhänder* und dann der anonymisierten Daten an das Register umfaßte. Dieses Konzept wurde vom Bundesamt für Sicherheit in der Informationstechnik begutachtet. Die Verschlüsselungen auf Grundlage von Kryptoprozessor-Chipkarten erlauben nach Ansicht des BSI einen hinreichenden Schutz, um medizinische Informationen sowohl über ISDN als auch über Internet zu übertragen. Die Gefährdung der Projektgeschäftsstelle gegen „Hacker“ soll durch geeignete Maßnahmen wie „Firewalls“ oder ISDN-D Kanal Filter verringert werden.

**Bundes-Gesundheitssurvey 1997/98**

Unbeschadet der Zuständigkeit des Bundesbeauftragten für den Datenschutz bat uns das in Berlin ansässige Robert-Koch-Institut – Bundesinstitut für Infektionskrankheiten und nicht übertragbare Krankheiten – um datenschutzrechtliche Beratung zum Bundes-Gesundheitssurvey 1997/98. Im Rahmen dieser Untersuchung sollen über 7 000 Personen im Alter von 18 bis 79 Jahren bundesweit zu gesundheitsrelevanten Themen befragt und einer medizinischen Untersuchung unterzogen werden. Die Datenerhebung selbst wird im Auftrage des Robert-Koch-Instituts durch ein privates medizinisches Forschungsinstitut durchgeführt. Bei diesem Projekt ist insbesondere das gewählte *Anonymisierungsverfahren* datenschutzrechtlich interessant, da es entsprechend dem Ablauf der Untersuchung in mehreren Stufen erfolgt. Zunächst wird für die ausgewählten Erhebungsorte eine

Der Staatsvertrag über das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen ist am 20. November 1997 unterzeichnet worden und wird nach Ratifizierung durch die beteiligten Länder noch im 1.Halbjahr 1998 in Kraft treten. Der Staatsvertrag enthält auch detaillierte Regelungen zum Datenschutz. Mit ihm wird das Gemeinsame Krebsregister auf eine für die beteiligten Länder gegenüber dem bisherigen Verwaltungsabkommen verbindlichere Grundlage gestellt.

Der Senat begrüßt, daß es in enger Zusammenarbeit mit dem Berliner Datenschutzbeauftragten gelungen ist, eine effiziente technische Lösung für das Qualitätssicherungsregister von Dialysepatienten zu finden, die gleichzeitig die Anforderungen des Datenschutzes erfüllt.

145 JB 1995, 5.14 und JB 1996, 4.5.1

Stichprobe aus den Melderegistern gezogen. Den Namen dieser Personen wird eine sogenannte „Bruttonummer“ zugeordnet. Wenn nun die um ihre Einwilligung gebetenen Personen zustimmen, werden alle nachfolgenden Befragungen und Untersuchungen nur noch mit einer „Nettonummer“ versehen. Damit ist sichergestellt, daß bei der Auswertung der Daten nicht mehr in einem einstufigen Verfahren auf die Adresse zugegriffen werden kann. Die beiden *Schlüsselbrücken* „Namen-Bruttonummer“ und „Bruttonummer-Nettonummer“ werden jeweils getrennt von den anderen Unterlagen aufbewahrt. Sie dienen dem Robert-Koch-Institut dazu, in einem Zeitraum von ca. 5 Jahren möglicherweise notwendige Nacherhebungen oder Ergänzungsuntersuchungen durchzuführen und die Betroffenen um ihre Mitwirkung zu bitten. Nach Ablauf dieser Frist werden auch diese Schlüsselbrücken gelöscht.

**Der Computer und der Tod**

*„In den Kliniken wächst die Angst“ – „Der Todescomputer“ – „Tödliche Medizin“ – „Ärzte kritisieren“ – „Wirbel um neues Softwareprogramm in Kliniken“ – „Darf ein Computer über das Leben entscheiden?“ – „Entsetzen über Todescomputer – Test auf Intensivstationen“ – „Überlebensprognose mit dem Computer“ – „Der virtuelle Todesstoß“ –.*

Diese Schlagzeilen der Berliner Tageszeitungen kennzeichnen die zum Teil mystifizierende Betrachtungsweise, in der sich die Öffentlichkeit mit der Informationstechnik auseinandersetzt. Es ging dabei um ein Computerprogramm namens „RIYADH“, welches in einem Berliner Krankenhaus als Hilfsmittel für die Qualitätssicherung eingesetzt wird. Durch die Auswertung der hier verarbeiteten Daten sollte untersucht werden, wie gut die Versorgung der Patienten in den Intensivstationen des Krankenhauses ist. Uns wurde versichert, weitere Nutzungen, etwa die Möglichkeit, während der Behandlung von Patienten in der Intensivstation deren Überlebenschancen zu verfolgen, würden nicht stattfinden. Insbesondere sollten keinerlei Auswertungsergebnisse unmittelbar in die Behandlung einfließen.

Praktisch handelt es sich um eine isolierte PC-Anwendung in einem abgeschlossenen Raum in der *Intensivstation.* Die Daten werden von Krankenschwestern, die am Bett keinen Dienst verrichten dürfen, in zeitlichem Abstand nach der Entlassung des Patienten aus der Intensivstation eingegeben. In der Intensivmedizin ist es weltweit seit Jahren üblich, ein *„Patientenscoring“* durchzuführen, d. h. die Überlebenschancen der Patienten abzuschätzen und auf Grund der gewonnenen Daten die Behandlung der Patienten zu verbessern. Dies ist bei Krankenhäusern mit besonders schwer erkrankten Patienten von großer Bedeutung. Man versucht seit Jahren, dieses Scoring, das bisher manuell durchgeführt wird, durch automatische Systeme zu ersetzen. In den USA wird seit Jahren das Programm *„APACHE“* verwendet, das hier jedoch nicht einsetzbar ist. Das Programm „RIYADH“ ist eine Neuentwicklung, die von den Autoren während eines Forschungsaufenthaltes in der Hauptstadt von Saudi-Arabien entwickelt worden ist. Da eine unmittelbare Rückkoppelung mit der Behandlung der Patienten nicht beabsichtigt ist, sagte das Krankenhaus die unverzügliche *Anonymisierung der Patientendaten* zu. Die Anonymisierung der Daten ist absprachegemäß unverzüglich vollzogen worden. In keinem Fall war oder ist daran gedacht worden, die Behandlung eines Patienten vorzeitig zu beenden, weil der Computer seine Überlebenschancen als gering bewertet hat. Eine derartige Vorgehensweise würde gegen das Strafrecht und das ärztliche Standesrecht verstoßen. Sie wäre auch ein Beispiel für eine automatisierte Entscheidung, die nach der EU-Datenschutz-Richtlinie verboten wäre (Art. 15). Die reißerische Berichterstattung, die nicht nur von der Boulevardpresse, sondern auch von anderen Zeitungen praktiziert wurde, erwies sich damit als gegenstandslos. Wir berichten über den Fall, um zu zeigen, daß Mystifizierung und unbegründete Angst vor der EDV ganz nah beieinander liegen und die Tätigkeit des Datenschutzbeauftragten zu einer realistischen Betrachtungsweise beitragen kann.

Der Senat stimmt mit der Meinung des Berliner Datenschutzbeauftragten überein.

Die Senatsverwaltung für Gesundheit und Soziales wird, soweit die entsprechende aufsichtsrechtliche Zuständigkeit gegeben ist, auch bei zukünftigem Auftauchen derartiger Vorkommnisse im Rahmen der zur Verfügung stehenden aufsichtsrechtlichen Mittel tätig werden.

**Krankengeschichten in fremden Händen**

*Ein Berliner Krankenhaus will die Archivierung der Krankengeschichten auf ein privates Unternehmen übertragen. Dazu schloß es einen Übernahmevertrag, durch den die Archivverwal-*

Der Senat stimmt mit der Meinung des Berliner Datenschutzbeauftragten überein.

*tung „im Auftrag für das Krankenhaus" durch einen privaten Unternehmer durchgeführt werden sollte. Dieser hätte uneingeschränkten Zugriff auf alle Patientendaten in den Krankengeschichten.*

Die Rechtsprechung hat in letzter Zeit intensiv die Bedeutung der ärztlichen Schweigepflicht hervorgehoben. So machte das Oberlandesgericht Düsseldorf[146], deutlich, daß es nicht gestattet ist, die *Daten von Patienten durch externe Firmen archivieren* zu lassen, wenn diese selbst unmittelbaren Zugriff auf die Dateninhalte haben. Im übrigen handelt es sich hierbei um eine Aufgabenübertragung und nicht um eine Datenverarbeitung im Auftrag[147]. Denn ein größeres Unternehmen soll mit einem hohen Grad an Selbständigkeit und Eigenverantwortlichkeit die Patientendokumentation und somit das Vertraulichste übernehmen, das gerade durch die ärztliche Schweigepflicht geschützt werden soll. Wenn dieses informationelle Herzstück der ärztlichen Tätigkeit aus dem Verfügungsbereich des Arztes herausgenommen und in fremde Hände gelegt wird, bleibt für die ärztliche Schweigepflicht kaum noch ein sinnvoller Wirkungsbereich.

Geplant war, das Krankengeschichtenarchiv auf dem Krankenhausgelände zu lassen, jedoch sollte der Auftragnehmer insbesondere die Verwaltung und Auswahl der Mitarbeiter selbst verantworten und auch die Archivstruktur organisieren. Der Auftragnehmer sollte verpflichtet werden, die Leistungen durch geeignetes Personal auszuführen und die Schulung, Einweisung, Überwachung und die Verpflichtung nach § 5 BDSG zu gewährleisten.

Dieser Vertrag gibt dem Auftragnehmer gegenüber dem Auftraggeber ein hohes Maß an Selbständigkeit. Trotz der verbleibenden Befugnisse des Krankenhauses, jederzeit Zugang zu allen Räumlichkeiten des Archivs zu erhalten und die sonstigen Vorgaben für den betrieblichen Ablauf des Krankenhauses zu unterstützen, fehlt jedoch die *unmittelbare Kontrolle der Krankenhausleitung* auf die Archivverwaltung, denn die entscheidenden Weisungen über den Datenzugriff, die Datenverwahrung und den Datentransport bleiben beim Auftragnehmer. Wir haben daher von dieser rechtlichen Konstruktion abgeraten. Das Herausverlagern von Archivverwaltungsfunktionen kann nur dann zulässig sein, wenn ein direkter Zugriff auf Patientendaten durch Mitarbeiter des beauftragten Unternehmens ausgeschlossen ist (z. B. durch den Einsatz von Containern, in denen das Archivmaterial vor der Weitergabe verschlossen wird) und wenn darüber hinaus durch eine ärztliche Verantwortung ein hinreichender Schutz vor Beschlagnahme gegeben ist. Denn nur Ärzte genießen zugunsten des Patienten diesen Schutz und das Zeugnisverweigerungsrecht nach der Strafprozeßordnung.

Die Senatsverwaltung für Gesundheit und Soziales wird, soweit die entsprechende aufsichtsrechtliche Zuständigkeit gegeben ist, auch bei zukünftigem Auftauchen derartiger Vorkommnisse im Rahmen der zur Verfügung stehenden aufsichtsrechtlichen Mittel tätig werden.

**Gedankenlosigkeiten**

Immer wieder finden sich gerade in der Medizin Mängel hinsichtlich der Datensicherheit. So wurden auch in diesem Jahr wieder *Befundberichte* von einem Krankenhaus, die für den weiterbehandelnden Arzt und die Patientin bestimmt waren, *falsch kuvertiert* und *vertauscht*. Auch eine gesetzliche Krankenversicherung leistete sich derartige Fehler: Dem Medizinischen Dienst der Krankenkassen wurde zur Begründung eines bestimmten rechtlichen Standpunktes ein *Gerichtsurteil* übersandt, in dem alle Versichertendaten aus dem Rechtsstreit und die Identität dieser Person ersichtlich waren. Dieses Urteil wurde vom Medizinischen Dienst, ebenfalls ohne Anonymisierung, an die beschwerdeführende Versicherungsnehmerin weitergeleitet, die uns daraufhin einschaltete. Da es sich im Urteil um den Fall einer manifesten Transsexualität (die einer besonderen Geheimhaltung unterliegt) handelte, war der Vorgang besonders prekär für die Krankenkasse.

Der Senat stimmt mit der Meinung des Berliner Datenschutzbeauftragten überein.

Die Senatsverwaltung für Gesundheit und Soziales wird, soweit die entsprechende aufsichtsrechtliche Zuständigkeit gegeben ist, auch bei zukünftigem Auftauchen derartiger Vorkommnisse im Rahmen der zur Verfügung stehenden aufsichtsrechtlichen Mittel tätig werden.

**Landesversorgungsamt und ärztliche Schweigepflicht**

*Aus dem ärztlichen Bereich des Landesversorgungsamtes wurde bekannt, daß im Rahmen eines Leistungsverfahrens sämtliche Akten eines Amtsangehörigen, der Leistungen beantragt hatte,*

Der Senat teilt die Auffassung des Berliner Datenschutzbeauftragten, der in der hier geschilderten Verfahrensweise einen schweren datenschutzrechtlichen Mangel sieht, und hält § 35 Abs. 1 SGB I sinngemäß auch im Bereich des Versorgungsamtes für anwendbar.

146 20 U 139/95
147 vgl. unten 4.8.1

*vor der Verwaltungsentscheidung dem ärztlichen Leiter bzw. seinem Vertreter vorgelegt werden muß. Im vorliegenden Fall waren diese zugleich Fach- und Disziplinarvorgesetzte des betreffenden Mitarbeiters, so daß ihnen im Ergebnis sämtliche medizinische Unterlagen zum Einblick vorlagen und ihnen die Sachentscheidungskompetenz zukam.*

Hierin lag ein schwerer datenschutzrechtlicher Mangel. Die Situation ist der Regelung in § 35 Abs. 1 Satz 3 SGB I vergleichbar, wonach Sozialdaten der Beschäftigten in der Krankenversicherung und ihrer Angehörigen, Personen, die Personalentscheidungen treffen oder an ihnen mitwirken können, weder zugänglich sein dürfen noch von Zugriffsberechtigten weitergegeben werden dürfen. Diese Regelung für die Krankenkasse soll verhindern, daß Dienst- und Fachvorgesetzte Kenntnis von Daten erhalten, die unter dem Schutz der ärztlichen Schweigepflicht stehen, damit diese nicht gegenüber anderen Mitarbeitern schlechtergestellt werden. Die Krankenkassen haben dafür eigene Abteilungen geschaffen, die aus dem üblichen Dienstbetrieb ausgegliedert sind, damit keine innerbetrieblichen Konfliktfälle entstehen können. Das Landesversorgungsamt hat sich noch nicht in der Lage gesehen, entsprechend zu verfahren.

Das Landesamt für Gesundheit und Soziales (LAGeSo) wurde aufgefordert, die Geschäftsanweisung baldmöglichst dahingehend zu ändern, daß Dienst- bzw. Fachvorgesetzte mit Personalentscheidungskompetenz bei Anträgen von Mitarbeitern des LAGeSo am Feststellungsverfahren im Rahmen des Schwerbehindertengesetzes, des sozialen Entschädigungsrechts und des Gesetzes über Pflegeleistungen in keinem Fall beteiligt sein dürfen.

**Umstrukturierung der bezirklichen Gesundheitsämter**

Von dieser schon im vergangenen Berichtsjahr aktuellen Thematik[148] ist auch dieses Jahr zu berichten. Die Senatsverwaltung für Gesundheit und Soziales hat nunmehr mit wünschenswerter Klarheit von den bezirklichen Gesundheitsämtern gefordert, daß ärztliche Aufgaben immer unter der Fachaufsicht des Amtsarztes stehen müssen, der als Leiter des Gesundheitsamtes letztlich die ärztliche Verantwortung für alle Tätigkeiten des Gesundheitsamtes im ärztlichen Bereich trägt. Gleichwohl verursacht die Umsetzung dieser Grundsatzposition in den Bezirksämtern noch immer Schwierigkeiten, da nicht mit hinreichender Deutlichkeit zwischen der ärztlichen fachlichen Verantwortung des Amtsarztes und der Kooperation zwischen Gesundheitsamt und Sozialamt oder Jugendamt unterschieden wird.

Der Hintergrund für die Erwähnung im Bericht ist die Integration von Kinder- und Jugendpsychiatrischen Diensten in die Abteilung Jugend (Zusammenlegung mit den Erziehungs- und Familienberatungsstellen) in mehreren Bezirken. Ein Schriftwechsel der Senatsverwaltung für Schule, Jugend und Sport mit dem Berliner Datenschutzbeauftragten in dieser Angelegenheit ist noch nicht abgeschlossen.

Konkrete Verstöße gegen geltendes Datenschutzrecht sind dem Senat bisher nicht bekannt.

### 4.4.3 Sozialverwaltung

Gemeinnützige Arbeit von Sozialhilfeempfängern in der Wohngeldstelle

*Im Wohnungsamt eines Bezirksamtes sind durch die Vermittlungsstelle des Sozialamtes immer wieder Sozialhilfeempfänger mit der Entsorgung von Wohngeldanträgen und Steuerunterlagen beschäftigt worden. Ein Hilfeempfänger überreichte persönlich bei uns seinen Einsatzzettel und erklärte: „Ich habe beim Aktenlesen gestaunt, was die Leute so verdienen!".*

Der Einsatz von Sozialhilfeempfängern für gemeinnützige Arbeiten ist nicht in Bereichen zulässig, in denen personenbezogene Daten anfallen. Dies bedeutet, daß Sozialhilfeempfänger mit der Entsorgung oder dem Transport von Akten weder in Wohngeldämtern, Sozialämtern oder Personalabteilungen noch in Gesundheitsämtern eingesetzt werden dürfen. Der freundliche Herr, der uns die entsprechenden Arbeitsbelege und Stundennachweise vorlegte, erklärte, daß er persönlich Zeuge von Vorfällen war, in denen Hilfeempfänger eingehend in den zu entsorgenden Akten gelesen hatten. Eine Aufsicht war nicht vorgesehen. Ohnehin wäre eine Beaufsichtigung praktisch nicht durchführbar.

Der zuständige Stadtrat sicherte uns unverzüglich zu, den weiteren Einsatz von Sozialhilfeempfängern endgültig zu unterbinden.

Die Verwaltung muß auch in anderen Bezirken in Zukunft sicherstellen, daß diese Art von Tätigkeiten nicht in Bereichen ermöglicht wird, bei denen personenbezogene Daten anfallen. Der Grund dafür ist nicht eine besondere Neugier oder Unzuverlässigkeit der Sozialhilfeempfänger, sondern der Umstand, daß ein *Arbeitsvertrag* mit den nach § 19 Abs. 3 Bundessozialhilfegesetz verpflichteten Menschen nicht zustande kommt.

Die Zuweisung von Sozialhilfeempfängern zu Arbeitseinsätzen im Rahmen der gemeinnützigen und zusätzlichen Arbeit (gzA) nach § 19 Abs. 2, 2. Alternative BSHG gehört zur Zuständigkeit der Bezirksämter von Berlin, Abt. Sozialwesen, Arbeitsgruppen „Hilfe zur Arbeit". Die Durchführung von Aufgaben nach dem BSHG ist eine Bezirksaufgabe (ohne Fachaufsicht ) nach § 3 Abs. 2 Satz 1 AZG.

Die Bezirksämter von Berlin entscheiden kraft Gesetz in eigener Zuständigkeit und Verantwortung.

Die Akquise geeigneter gzA-Einsatzstellen sowie die Auswahl geeigneter Hilfeempfänger liegt bei den bezirklichen Arbeitsgruppen „Hilfe zur Arbeit". Hilfeempfänger, die in öffentlichen Verwaltungen eingesetzt werden, unterzeichnen am ersten Tag des Arbeitseinsatzes vor Arbeitsaufnahme eine Erklärung zur Verschwiegenheitspflicht. Die Durchschrift dieser Verschwiegenheitserklärung wird dem Hilfeempfänger ausgehändigt, das Original wird an das zuweisende Bezirksamt von Berlin übersandt und dort zur Akte genommen.

Derzeit gelten noch die Ausführungsvorschriften über „Hilfe zur Arbeit" nach den §§ 19 und 20 BSHG, die am 1. Februar 1991 in Kraft getreten sind.

Nach Nr. 11 – Gemeinnützige und zusätzliche Arbeiten mit Mehraufwandsentschädigung – Abs. 3 Buchstabe f dieser AV kommen als Bereiche, in denen Arbeitsgelegenheiten zu schaffen sind, unter anderem Allgemeine Verwaltungstätigkeiten (Einsatz zu leichten Büroarbeiten; Registratur- und Botendienste; Mithilfe bei Verkehrszählungen; Aktenaussonderungen und andere kurzfristig anfallende Arbeiten) in Betracht.

148 JB 1996, 4.4.2

Es handelt sich vielmehr um eine hoheitliche Anweisung sozialrechtlicher Natur. Da ein Arbeitsvertrag nicht vorliegt, ist auch eine Datenschutzverpflichtung rechtlich nicht möglich, weil sie keinerlei verpflichtenden Charakter entfalten kann. Wir hatten in früherer Zeit schon auf die Unzulässigkeit des Einsatzes hingewiesen. Auch das Verwaltungsgericht Berlin[149] hat entschieden, daß Hilfeempfänger aus Gründen des Sozialhilferechts auch in der Registratur eines Amtsgerichts, wie z. B. mit dem Öffnen und Verteilen von eingehender Post, mit dem maschinellen Frankieren der ausgehenden Post, dem Sortieren eingehender Postzustellungsurkunden in der Mahnabteilung oder mit Eintragungen auf Aktendeckeln und Karteikarten oder Botengängen nicht befaßt werden dürfen. Selbst wenn ein Arbeitsvertrag geschlossen wird, ist der Einsatz der Sozialhilfeempfänger in geschützten Bereichen nicht zulässig, weil dadurch kein öffentlich-rechtliches Dienstverhältnis mit der gesteigerten Geheimhaltungspflicht begründet wird.

Das im Bericht des Berliner Datenschutzbeauftragten zitierte Urteil des Verwaltungsgerichts Berlin vom 3. Januar 1988 – Az. 8 A 142.86 – bezieht sich lediglich auf die „Zusätzlichkeit" von Arbeiten nach § 19 BSHG, jedoch nicht auf datenschutzrechtliche Verfehlungen.

**Heimaufsicht und Pflegeakten**

*Ein Altersheim bestritt die Befugnis der Heimaufsicht der Senatsverwaltung für Soziales, in die Pflegedokumentation der Heimbewohner Einsicht zu nehmen.*

Es gehört zu den Voraussetzungen eines Heimbetriebes, daß die Wahrung der Interessen und Bedürfnisse der Bewohner „insbesondere die ärztliche oder gesundheitliche Betreuung, gesichert ist" (§ 6 Ziff. 2 Heimgesetz – HeimG –). Der Betrieb des Heimes erfordert, daß die Betreuung der Bewohner auch soweit sie „pflegebedürftig" sind, in dem Heim selbst oder in angemessener anderer Weise gewährleistet ist (§ 6 Abs. 3 HeimG). Der Betrieb des Heimes ist zu untersagen, wenn die Anforderungen des § 6 HeimG nicht erfüllt sind (§ 16 Abs. 1 HeimG). Die Heimaufsicht kann nach § 9 Abs. 2 HeimG Prüfungen und Besichtigungen vornehmen, in die geschäftlichen Unterlagen des Auskunftspflichtigen Einsicht nehmen, sich mit den Bewohnern in Verbindung setzen und die Beschäftigten befragen. Diese Befugnisse dienen letztlich dazu, den Zielsetzungen des Heimgesetzes Rechnung zu tragen, nämlich Bedürfnisse der Heimbewohner vor Beeinträchtigungen zu schützen. Diese umfassende Aufgabenbeschreibung durch den Gesetzgeber rechtfertigt die Befugnis der Heimaufsicht, auch in die Pflegedokumentation Einblick zu nehmen. Denn gerade die Pflegedokumentation enthält jene Informationen, die eine Überprüfung zum Wohle der Heimbewohner individuell möglich macht. Zwar heißt es in § 9 Abs. 4, daß die für die Heimaufsicht zuständigen Behörden verpflichtet sind, Daten der Pflegebedürftigen nur in anonymisierter Form an die in § 9 Abs. 4 Satz 1 zweiter Halbsatz genannten Stellen zu übermitteln (Bundesministerien für Arbeit und Sozialordnung sowie für Gesundheit und Familie). Diese Regelung kann jedoch nicht dahingehend ausgelegt werden, daß die Heimaufsicht selbst keine personenbezogenen Daten der Heimbewohner zur Kenntnis nehmen darf. Vielmehr ergibt sich aus der Befugnis, die Mitarbeiter einschließlich des Pflegepersonals über die Pflege im einzelnen zu befragen und auch die Möglichkeit, direkten Kontakt zu den Heimbewohnern aufnehmen zu dürfen, daß der Gesetzgeber keinen Zweifel daran läßt, daß die Heimaufsicht direkt und unmittelbar die Pflege eingehend zu prüfen hat und dabei selbstverständlich auch die Möglichkeit haben muß, personenbezogene Daten der Heimbewohner zur Kenntnis zu nehmen. Die Anonymitätsvorschrift in § 9 Abs. 4 Satz 2 ist somit eng begrenzt und nur auf die Übermittlungsbefugnis nach Abs. 4 Satz 1 zu beschränken.

Der Senat stimmt mit der Meinung des Berliner Datenschutzbeauftragten überein.

Die Senatsverwaltung für Gesundheit und Soziales wird, soweit die entsprechende aufsichtsrechtliche Zuständigkeit gegeben ist, auch bei zukünftigem Auftauchen derartiger Vorkommnisse im Rahmen der zur Verfügung stehenden aufsichtsrechtlichen Mittel tätig werden.

**Psychogruppen und Sekten**

*Eine Psychogruppe beschwerte sich darüber, daß das Sachgebiet „Neue religiöse und weltanschauliche Bewegungen und sogenannte Psychogruppen" bei der Senatsverwaltung für Schule, Jugend und Sport in einem Schreiben an die Gruppe selbst Mitarbeiter namentlich benannt hatte.*

Einen datenschutzrechtlichen Verstoß konnten wir hierbei selbstverständlich nicht feststellen, da die persönliche Anrede von Vereinsmitgliedern in einem an den Verein gerichteten

Die durch die Beschwerde einer Psychogruppe ausgelöste Prüfung der Arbeitsweise der Dienststelle „sogenannter Psychogruppen und Sekten" in der Senatsverwaltung für Schule, Jugend und Sport durch einen Mitarbeiter des Berliner Datenschutzbeauftragten bestätigte den verantwortlichen Umgang mit datenschutzrechtlich relevanten Vorgängen und die datenschutzrechtliche Unbedenklichkeit der Verfahrensweise der Dienststelle über den konkreten Beschwerdefall hinaus.

149 Urteil v. 1. März 1986 – 8 A 142.86

Schreiben keine unbefugte Offenbarung darstellt, wenn diese Personen vereinsrechtliche Funktionen innehaben. Dazu zählen auch Arbeits- oder Dienstverhältnisse mit dem Verein.

Diesen Vorfall sowie ein Beratungsersuchen nahmen wir zum Anlaß, Rechtsgrundlagen und Verfahrensweise dieser Dienststelle zu überprüfen. Die Ergebnisse haben grundsätzliche Bedeutung für derartige Einrichtungen.

Die Tätigkeit dieser Senatsdienststelle ist eine allgemeine Verwaltungstätigkeit, die eine beratende Funktion gegenüber hilfesuchenden Bürgern zum Gegenstand hat. Sie ist neben den bezirklichen Jugendämtern die zuständige Behörde für die Erfüllung der Aufgaben nach dem Kinder- und Jugendhilfegesetz (KJHG/SGB VIII). Jeder junge Mensch hat das Recht auf Förderung seiner Entwicklung und Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit (§ 1, 2 SGB VIII). Die Pflege und Erziehung der Kinder ist das natürliche Recht der Eltern. Über ihre Betätigung wacht die staatliche Gemeinschaft. Im Rahmen der Jugendhilfe hat die Senatsverwaltung für Jugend die Aufgabe, die *Geeignetheit einer Einrichtung und ihrer Mitarbeiter* zu überprüfen. Dabei soll die zuständige Behörde auch den Erfordernissen des Einzelfalles entsprechend vor Ort Überprüfungen durchführen, ob die Voraussetzungen für die Erteilung einer Erlaubnis weiter bestehen. In diesem Umfang dürfen auch Sozialdaten gespeichert werden. Daten, die zur Erfüllung unterschiedlicher Aufgaben der öffentlichen Jugendhilfe erhoben worden sind, dürfen auch zusammengeführt werden, wenn und solange dies wegen eines unmittelbaren Sachzusammenhangs erforderlich ist (§ 63 Abs. 2 SGB VIII).

Bei der *Genehmigung einer Kindertagesstätte* nach § 47 SGB VIII ist die Geeignetheit zu überprüfen. Es ist mit den Zielsetzungen des Kinder- und Jugendhilfegesetzes vereinbar, daß die Genehmigungsstelle nach § 47 KJHG bei dem Sachgebiet „Neue religiöse und weltanschauliche Bewegungen und sogenannte Psychogruppen“ anfragt, ob Erkenntnisse über die zu genehmigende Einrichtung vorliegen. Die dort bekannten Informationen dürfen für das Genehmigungsverfahren auch genutzt werden, wenn der antragstellenden Einrichtung die Gründe für die dann ergehende sachliche Entscheidung mitgeteilt werden.

Auch die Speicherung von *Daten Betroffener,* die auf Grund eigener Erfahrungen mit den Einrichtungen Rat und Hilfe bei der Senatsdienststelle suchen, ist unbedenklich, weil und soweit die Einwilligung der Betroffenen vorliegt. Eine Übermittlung dieser Daten an private Dritte oder andere Verwaltungsstellen oder gar an die Mitglieder betroffener Psychogruppen darf in keinem Falle ohne Zustimmung der Betroffenen erfolgen. Dies ist den Betroffenen beim Beratungsgespräch zuzusichern, um eine tragfähige Vertrauensgrundlage für die Arbeit mit ihnen herzustellen. Den Betroffenen/Hilfesuchenden ist Einsicht in die sie selbst betreffenden Gesprächsprotokolle mit der Dienststelle zu geben.

Hinzuweisen ist auf eine mißverständliche Formulierung im Datenschutzbericht (S. 131, 2. Absatz): Bei den im Vergleich zu den anderen Aufgaben der Dienststelle eher geringen beratenden Anteilen der Arbeit handelt es sich um solche informierenden und aufklärenden Charakters und nicht um eine psychosoziale Beratung. Diese Scheidung hervorzuheben ist uns ein Anliegen, um möglicherweise falschen Erwartungen der Öffentlichkeit zu wehren.

### 4.4.4 Wohnen

**Datenschutz für Mieter und Vermieter**

*Im vergangenen Jahr*[150] *haben wir ausführlich zur Zulässigkeit der Erhebungen von Mieterdaten bei Wohnungsbewerbern Stellung genommen. Oft wurden wir gefragt, wie die „Einwilligung“ des Bewerbers in die Datenerhebung auf den Fragebögen zu werten ist.*

Die Verarbeitung von Daten eines *Mietinteressenten* durch den Vermieter oder einem von ihm beauftragten Makler ist zwar zulässig, wenn der Betroffene darin eingewilligt hat (§ 4 Abs. 1 BDSG). Eine Einwilligung ist jedoch dann unwirksam, wenn der Betroffene die Entscheidung nicht „freiwillig“ getroffen hat, insbesondere, wenn ihm die Einwilligung unter Ausnutzung einer wirtschaftlichen Machtposition „abverlangt“ wurde. Derartige Einwilligungen geben nicht den wahren Willen des Betroffenen wieder. Insbesondere im Verhältnis Arbeitgeber/Arbeitnehmer und Vermieter/Mieter (bzw. Mietinteressent) ist in der Regel zweifelhaft, ob die Einwilligung freiwillig erfolgt.

Sowohl durch die vom Berliner Datenschutzbeauftragten festgestellten Entwicklungen auf dem Berliner Wohnungsmarkt als auch durch den Abbau der administrativen Maßnahmen in Bezug auf die Wohnraumversorgung der unterschiedlichsten Personengruppen hat die wohnungspolitische Verantwortung der Wohnungsbaugesellschaften zugenommen. Die Wohnungsbaugesellschaften müssen völlig eigenverantwortlich den Personenkreis, der in den Kooperationsverträgen festgelegt ist, mit angemessenem Wohnraum versorgen. Darüber hinaus ist es ihre Aufgabe, die bisherigen ausgewogenen Mietstrukturen in den Wohngebäuden und den Wohnanlagen durch eine entsprechende zielgerichtete Neuvermietung möglichst so zu gestalten, daß die Wohnzufriedenheit vor allem der dort wohnenden Mieter auch künftig gewährleistet ist. Wohnunzufriedenheit führt zu steigender Fluktuation, Wohnungsleerstand und damit zu sinkenden Mieteinnahmen. Wie der Berliner Datenschutzbeauftragte richtig festgestellt hat, haben die Wohnungsbaugesellschaften in ihren Fragebögen für die Wohnungsbewerber auch Daten abgefragt, die für die wohnungspolitischen Anforderungen nicht erforderlich sind.

150 JB 1996, 3.3

| Bericht des Berliner Datenschutzbeauftragten | Stellungnahme des Senats |
|---|---|

Obwohl sich die Situation auf dem Berliner Wohnungsmarkt inzwischen deutlich – zumindestens in einigen Marktsegmenten – zugunsten der Wohnungssuchenden entspannt hat, ist bei Einwilligungen von *Wohnungsbewerbern* in die Datenerhebung durch den Vermieter grundsätzlich noch von nicht freiwilligen Einwilligungen auszugehen. Es bleibt also dabei, daß die Verarbeitung von Mieterdaten nur zulässig ist, soweit dies im Rahmen des Mietvertrages erforderlich ist (§ 28 Abs. 1 Ziff. 1 BDSG).

Eine zu weitgehende Datenverarbeitung kann nicht auf die Einwilligung des Betroffenen gestützt werden.

Positiv anzumerken ist, daß die Senatsverwaltung für Bauen, Wohnen und Verkehr unsere Empfehlungen für ein datenschutzgerechtes Verfahren bei Wohnungsbewerbungen – nach Aufforderung durch den Unterausschuß „Datenschutz“ des Abgeordnetenhauses von Berlin – in ein Rundschreiben an die öffentlichen Wohnungsbaugesellschaften aufnehmen wird.

Unabhängig von den Datenschutzanforderungen verursacht jede nicht benötigte Information erhebliche Kosten – und Verwaltungsaufwand. Die Wohnungsbaugesellschaften wurden daher mit Rundschreiben vom 27. April 1998 von der zuständigen Senatsverwaltung aufgefordert, anhand der aufgezeigten Empfehlungen des Berliner Datenschutzbeauftragten für ein datenschutzgerechtes Verfahren bei Wohnungsbewerbungen zu sorgen und die Fragebögen für die Wohnungsbewerber zu aktualisieren und gesetzeskonform zu gestalten.

Darüber hinaus wurden die Wohnungsbaugesellschaften in dem Rundschreiben gebeten, zusätzliche Fragestellungen, die sich auf Grund ihres Handelns ergeben, an die Senatsverwaltung für Bauen, Wohnen und Verkehr zu übermitteln, damit diese erforderlichenfalls mit dem Berliner Datenschutzbeauftragten weitergehend erörtert werden können. Der Senat schließt sich der Auffassung des Berliner Datenschutzbeauftragten an, daß durch die Angaben der Wohnungsbewerber in den Fragebögen eine generelle Einwilligung zu der Verarbeitung der Daten nicht automatisch gegeben ist. Es liegt ausschließlich in der Verantwortung der Wohnungsbaugesellschaften, gesetzeskonforme und informationsrelevante Fragestellungen vorzugeben und anschließend mit den erhaltenen Daten sach- und informationsgerecht umzugehen.

*Bei Aufwendungszuschüssen für familiengerechte Miet- und Genossenschaftswohnungen im neueren Sozialwohnungsbestand hat der Verfügungsberechtigte – Bauherr oder dessen Rechtsnachfolger (Vermieter) – vor der Auszahlung bestimmte Nachweise zu erbringen. Vorzulegen sind unter anderem Wohnungsberechtigungsscheine der Mieter, melderechtliche Aufenthaltsbescheinigungen aller in der Wohnung wohnhaften Personen sowie Kindergeldnachweise der Mieter.*

Die Investitionsbank Berlin (IBB) vertrat dazu die Auffassung, daß diese Nachweise – die umfangreiche personenbezogene Daten z. B. der Mieter enthalten – ausschließlich über den Bauherrn oder Vermieter einzureichen sind. Damit besteht die Möglichkeit, daß dieser von den Angaben über seine Mieter Kenntnis erlangt. Personenbezogene Daten sind gemäß § 10 Abs. 1 BlnDSG grundsätzlich unmittelbar beim Betroffenen (Mieter) selbst zu erheben. Eine Rechtsgrundlage, in der bestimmt ist, daß diese personenbezogenen Daten ausschließlich über den Vermieter an die IBB zu übermitteln sind, gibt es nicht. Wir haben empfohlen, daß den Mietern die Möglichkeit eingeräumt wird, ihre Daten unmittelbar – und nicht über den Vermieter – an die IBB zu übermitteln. Nur dadurch kann – sofern der Mieter dies wünscht – eine Kenntnisnahme der personenbezogenen Daten durch den Vermieter ausgeschlossen werden. Sowohl Vermieter als auch Mieter sind über diese Möglichkeit der Datenübermittlung ausreichend zu informieren.

Das Verfahren wurde auf Grund unserer Empfehlung grundsätzlich geändert. Danach räumt die IBB den Mietern nunmehr die Möglichkeit ein, ihre Daten auch unmittelbar der IBB zu übermitteln. Der Antrag auf Gewährung von Aufwendungszuschüssen wird weiterhin vom Vermieter gestellt, sieht jedoch alternativ auch die Unterlagenübersendung durch den Mieter vor. Der Vermieter hat mit seiner Unterschrift zu bestätigen, daß die Mieter über die veränderten Sachverhalte informiert wurden.

Die Ausführungen des Berliner Datenschutzbeauftragten sind zutreffend.

*Die Information der Mieter darüber, daß der Vermieter eine Abgeschlossenheitsbescheinigung (ggf. mit dem Ziel der Umwandlung der Miet- in eine Eigentumswohnung) beantragt hat, hat uns auch im vergangenen Jahr beschäftigt. Ein Vermieter hatte sich darüber beschwert, daß seine Daten aus dem Antragsverfahren vom Bau- und Wohnungsaufsichtsamt eines Bezirkes an eine Mieterberatungsgesellschaft übermittelt wurden. Diese hatte daraufhin die betroffenen Mieter über den Umstand der Beantragung und seine Folgen informiert.*

Die Unterrichtung der Mieter durch das Bezirksamt – hier über die Mieterberatungsgesellschaft – war unzulässig. Wie mehrfach in der Vergangenheit mußten wir auch in diesem Fall gegenüber dem zuständigen Bau- und Wohnungsaufsichtsamt – in Ermangelung einer bereichsspezifischen Rechtsgrundlage für die Datenübermittlung – einen datenschutzrechtlichen Mangel feststellen. Einigkeit bestand mit dem Bezirksamt darüber, daß dieser Vorgang einmal mehr die Notwendigkeit aufgezeigt hat, diesen

Der Senat ist weiterhin der Auffassung, daß entsprechende Information der betroffenen Mieter politisch erwünscht ist – allerdings bei Beachtung der Schranken aus gegebenen rechtlichen Rahmenbedingungen. Der Senat ist – wie bereits in der Stellungnahme zum Jahresbericht 1996 des Berliner Datenschutzbeauftragten festgestellt – auch weiterhin der Auffassung, daß eine ergänzende (bereichsspezifische) Regelung durch das Land Berlin wegen der im Rahmen der konkurrierenden Gesetz-

Bereich datenschutzgerecht zu regeln. Um so bedauerlicher ist der Umstand, daß der Senat und die Fraktionen von CDU und SPD eine mieterfreundliche Gesetzesinitiative von der Fraktion Bündnis 90/Die Grünen zur Schaffung einer normenklaren Rechtsgrundlage auf Landesebene[151] wegen der aus ihrer Sicht fehlenden Gesetzgebungskompetenz abgelehnt haben.

Wir sind nach wie vor der Auffassung, daß hier – angesichts der berechtigten Mieterinteressen – ein dringender Regelungsbedarf besteht. Der Gesetzgeber ist gefordert, entsprechende bereichsspezifische Regelungen (wenn nicht auf Landes-, dann) auf Bundesebene zu schaffen.

gebung durch den Bund wahrgenommenen Rechtsetzung mit Sperrwirkung für das Land unzulässig wäre. Das Problem der unzulässigen landesrechtlichen Regelung wird hier aufmerksam verfolgt und bei Gelegenheit jeweils mit dem Ziel einer angemessenen Regelung problematisiert.

Da auf Bundesebene keine Bereitschaft zur hier angemahnten Gesetzesänderung ersichtlich ist und weil der Berliner Datenschutzbeauftragte das Informationsbedürfnis der Mieter als deren berechtigtes Interesse sieht, sollte dort erwogen werden, das Thema gegebenenfalls über den Bundesdatenschutzbeauftragten zu problematisieren.

**Sitzt der Vermieter bald mit auf dem Sofa?**

*Mehrere öffentliche Wohnungsbaugesellschaften planen derzeit die Einführung von Fernmeß- und Fernwirkdiensten zur automatischen Ablesung beispielsweise des Strom-, Wasser- und Heizenergieverbrauchs. Dies soll auf der Basis der flächendekkend vorhandenen Kabelfernseh-Infrastruktur realisiert werden. Gleichzeitig ist unter der Überschrift „Multimedia-Wohnen" die Erprobung von dem Umfang und Inhalt nach bisher nicht genauer spezifizierten, interaktiven Informations- und Kommunikationsdiensten geplant.*

Dieser von der Gemeinnützigen Siedlungs- und Wohnungsbaugesellschaft Berlin ursprünglich für den Juli 1997 mit zahlreichen Kooperationspartnern aus der Privatwirtschaft geplante Modellversuch mußte allerdings auf Grund von Problemen mit der technischen Infrastruktur auf unbestimmte Zeit verschoben werden.

Nach § 31 a BlnDSG dürfen ferngesteuerte *Messungen oder Beobachtungen in Wohnungen* oder Geschäftsräumen nur dann vorgenommen werden, wenn der Betroffene zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes der Dienste unterrichtet worden ist und nach der Unterrichtung schriftlich eingewilligt hat. Die Einwilligung kann jederzeit widerrufen werden. Zusätzlich werden Anforderungen an die technische Realisierung solcher Dienste gestellt: So muß der Betroffene jederzeit erkennen können, wann ein solcher Dienst in Anspruch genommen wird *(„rote Lampe")* und welcher Art dieser Dienst ist; darüber hinaus muß die Möglichkeit bestehen, den Dienst jederzeit abzuschalten, soweit dies mit dem Vertragszweck vereinbar ist *(„roter Knopf")*.

Bei der Einführung von Informations- und Kommunikationsdiensten sowie von Mediendiensten sind darüber hinaus die datenschutzrechtlichen Bestimmungen des Teledienstedatenschutzgesetzes bzw. des Mediendienste-Staatsvertrages zu beachten. Danach sind entsprechende Dienste so auszugestalten, daß nur möglichst wenige oder überhaupt keine personenbezogenen Daten für die Erbringung des Dienstes erhoben und verarbeitet werden; gleichzeitig soll den Nutzern ein anonymer Zugang zu den entsprechenden Diensten eröffnet werden, soweit dies technisch möglich und wirtschaftlich vertretbar ist.

Die Wohnungsbaugesellschaften müssen sich, um wettbewerbsfähig auf dem Wohnungsmarkt zu bestehen, als Dienstleistungsunternehmen profilieren. Mit der Verwaltungskostenpauschale der II. Berechnungsverordnung (II BV) müssen die Wohnungsbaugesellschaften ihre Verwaltungsaufgaben bewältigen, da die Mehrkosten im Verwaltungsbereich immer zu Lasten der Instandhaltung der Wohngebäude gehen. Die Mieter haben im übrigen den Anspruch, möglichst in kurzer Frist die Mietkosten pauschal abgerechnet zu erhalten, und es ist das Bestreben, die Betriebskosten zu senken. Diese Anforderungen sind nur durch neue technische, wirtschaftliche und finanzielle Lösungen möglich. Infolge des technischen Fortschritts ist es zum Beispiel heute möglich, den Verbrauch von Wärme, warmen und kalten Wasser, Elektroenergie etc. kontinuierlich zu erfassen und zeitbeliebig abzurechnen, ohne daß manuelle Ablesemöglichkeiten und zeitliche Verzögerungen infolge der erforderlichen Datenaufbereitung eintreten. Damit kann dem allgemeinen Anspruch der Mieter, in ihren Verbrauch selbst direkt regelnd einzugreifen und wohnungskonkret abzurechnen, entsprochen werden. Die aufgezeigte negative Auswirkung auf den Mieter und seinen Lebensbereich in der Wohnung ist nicht ersichtlich und kann somit auch nicht nachvollzogen werden. Eine Überwachung der Mieter setzt voraus, daß die Meßpunkte als Mikrofilm oder als Kamera gestaltet sind. Bei keiner der anzuwendenden technischen Lösungen ist das angedacht.

**Datenerhebung bei Schornsteinfegern**

*Anläßlich einer Neueinteilung der Kehrbezirke bat die Senatsverwaltung für Bauen, Wohnen und Verkehr die Schornsteinfeger, umfangreiche Materialien mit personenbezogenen Daten – z. B. das Kehrbuch für das Kalenderjahr 1995, Aufrechnungen für das Jahr 1997 – der von der Senatsverwaltung eingesetzten Einteilungskommission zur Überprüfung vorzulegen. Gegen das Verfahren wurden datenschutzrechtliche Bedenken vorgetragen. Da sich die Einteilungskommission aus Bezirksschornsteinfegermeistern und Meistergesellen (Mitglieder der Schornsteinfegerinnung) zusammensetzte, wurde befürchtet, daß diese unzulässig Einsicht in die Betriebsunterlagen ihrer Kollegen erhalten.*

Die datenschutzrechtlichen Bedenken waren unberechtigt. Die Senatsverwaltung für Bauen, Wohnen und Verkehr ist nach § 23 Abs. 1 Schornsteinfegergesetz (SchfG) berechtigt, periodisch

Der Senat nimmt die Ausführungen des Berliner Datenschutzbeauftragten in diesem Punkt zur Kenntnis.

Die zuständige Senatsverwaltung für Bauen, Wohnen und Verkehr wird auch weiterhin die Einhaltung der datenschutzrechtlichen Vorschriften bei Einteilung durch die Aufklärung der Mitglieder der Nachprüfungskommission (früher: Einteilungskommission) sicherstellen. Zu diesem Zweck wird den Mitgliedern der Überprüfungskommission eine entsprechende Erklärung zur Einhaltung der datenschutzrechtlichen Geheimhaltung abverlangt.

151 JB 1996, 4.4.4

oder aus besonderen Gründen nachzuprüfen, ob eine *Neueinteilung der Kehrbezirke* vorzunehmen ist. Neben der Gewährleistung der Feuersicherheit ist insbesondere auch die Gleichwertigkeit der Kehrbezirke hinsichtlich der Gebühreneinnahmen ein Prüfungsmerkmal für die Neueinteilung der Kehrbezirke. Zu diesem Zweck hat der Kehrbezirksinhaber alle erforderlichen Auskünfte zu erteilen und auf Anforderung die von ihm geführten Aufzeichnungen vorzulegen (§ 23 Abs. 2 SchfG). Dies sind insbesondere die nach § 19 Abs. 1 SchfG zu führenden Unterlagen mit Aufzeichnungen zu den Feuerungsanlagen (z. B. Name, Anschrift des Eigentümers; Art der Anlage; durchgeführte Arbeiten usw.) und das in § 19 Abs. 2 SchfG geregelte Kehrbuch mit den entsprechenden Gebühreneintragungen (Aufrechnungen).

Bei der Vorlage der Unterlagen an die Einteilungskommission handelte es sich um eine weisungsgebundene *Datenerhebung im Auftrag* der Senatsverwaltung[152]. Die Aufgabe der Einteilungskommission bestand lediglich darin, das gegenwärtig in Berlin erzielte und erzielbare Einnahmevolumen aus den regelmäßig wiederkehrenden Gebührenentgelten der Kehrbezirksinhaber festzustellen bzw. zu überprüfen. Die Kommission hatte keine eigenständigen Befugnisse. Sie überprüfte – zum Teil in Anwesenheit und unter Kontrolle eines Vertreters der Senatsverwaltung nach deren Vorgaben – die von den Kehrbezirksinhabern vorgelegten Unterlagen lediglich auf deren Vollständigkeit und Richtigkeit. Bei festgestellten Mängeln (z. B. nicht korrekten Gebührenberechnungen) wurden diese im Beisein und nach Rücksprache mit dem Betroffenen vor Ort korrigiert. Die auf Grund der festgestellten Daten zu treffenden Entscheidungen – z. B. Maßnahmen gegenüber den Betroffenen, Neueinteilungen der Bezirke usw. – wurden ausschließlich von der Senatsverwaltung getroffen und umgesetzt. Die Daten der Kehrbezirksinhaber werden bei der Kommission nicht aufbewahrt. Alle Unterlagen gingen komplett an den Betroffenen zurück bzw. wurden – soweit erforderlich – an die Senatsverwaltung für Bauen, Wohnen und Verkehr weitergeleitet. Die Mitglieder der Einteilungskommission hatten sich zu Beginn ihrer Tätigkeit verpflichtet, über die von ihnen im Zusammenhang mit dieser Aufgabe bekanntwerdenden Unterlagen und Informationen Stillschweigen zu bewahren.

Anläßlich der datenschutzrechtlichen Prüfung haben wir gegenüber der Senatsverwaltung die Anforderungen an eine Datenverarbeitung im Auftrag nochmals ausdrücklich klargestellt und darauf hingewiesen, daß die datenschutzrechtliche Verantwortung stets beim Auftraggeber (Senatsverwaltung für Bauen, Wohnen und Verkehr) liegt. Er hat den Auftragnehmer (Einteilungskommission) unter besonderer Berücksichtigung der getroffenen Datensicherungsmaßnahmen sorgfältig auszusuchen und vertraglich sicherzustellen, daß dieser die Vorschriften des BlnDSG befolgt und sich der Kontrolle des Berliner Datenschutzbeauftragten unterwirft.

## 4.5 Wissen und Bildung

### 4.5.1 Wissenschaft und Forschung

**Schnellerer Zugang zu Bits, Bytes und Büchern**

*Immer mehr Studenten, aber auch Mitarbeiter der Universitäten und Hochschulen möchten die Angebote der zentralen Hochschuleinrichtungen zum Zugang zu Informationen nutzen. Wollte in der Vergangenheit ein Student die Zentraleinrichtung Datenverarbeitung der Freien Universität (ZEDAT) nutzen, so hatte er sich unter Vorlage seines Studentenausweises nach Ausfüllen eines Formulars anzumelden. Der Zugang zu diesen technischen Einrichtungen, insbesondere auch zum Internet blieb ihm eine Zeitlang verwehrt, bis geprüft war, ob der Student auch tatsächlich an der Universität eingeschrieben war. Durch die starke Zunahme der Anmeldungen war es auch erforderlich, zu Beginn jedes Semesters zu überprüfen, ob sich unter den eingetragenen Nutzern Personen befanden, die nicht mehr als Mitglieder der Hochschule eingeschrieben waren. Die ZEDAT bat uns zu prüfen, ob es möglich wäre, daß die Zentrale Universitätsverwaltung jeweils einen aktuellen Datenbestand aller immatrikulierten Studenten zur Verfügung stellen könnte.*

Der Senat stellt fest, daß der Datenschutz auch bei der Verwendung moderner Kommunikations- und Informationstechnik für die Wahrnehmung der Aufgaben der Hochschulen und die Benutzung ihrer Einrichtungen zum Tragen kommt. Die für Berlin vorgeschlagene einheitliche Lösung hinsichtlich der Verwendung der studentischen Chipkarte für die Erfüllung der hoheitlichen Aufgaben der Hochschulverwaltungen wird ausdrücklich begrüßt. Der Senat teilt die Auffassung des Berliner Datenschutzbeauftragten, daß der verbindliche Einsatz von Chipkarten im hoheitlichen Bereich nach § 6 Abs. 1 BlnDSG auf einer expliziten Rechtsgrundlage beruhen muß und eine entsprechende Änderung des § 6 BerlHG zur Folge haben müßte.

Zu den angeführten Beispielen aus der Forschung stellt der Senat fest, daß die in § 30 BlnDSG geregelten Anforderungen für die Verarbeitung personenbezogener Daten für Forschungszwecke beachtet worden sind und die Forscherinnen und Forscher und der Berliner Datenschutzbeauftragte im gemeinsamen Interesse konstruktiv zusammenarbeiten.

152 vgl. 4.8.1

Die datenschutzrechtlichen Regelungen des Berliner Hochschulgesetzes erlauben es zwar, den Namen und die Anschrift eines Studenten oder Mitarbeiters an Zentraleinrichtungen zu übermitteln, die Nutzung der *Matrikelnummer* für diesen Zweck ist aber zunächst nur auf Grundlage der Einwilligung der Studenten zulässig. Ein ähnliches Problem stellte sich auch für die Universitätsbibliothek. Eine Problemlösung zeichnet das Berliner Hochschulgesetz vor. Danach werden die Hochschulen ermächtigt, durch *Satzung* die Befugnis zur Verarbeitung weiterer personenbezogener Daten von Hochschulangehörigen zu schaffen. Diese Befugnis gilt explizit auch für die Besonderheiten bei der Benutzung der Hochschuleinrichtungen. Der Akademische Senat der Freien Universität beschloß Anfang 1997 eine entsprechende Satzung, nach der eine Übermittlung der Daten aller Universitätsangehörigen an die ZEDAT und die Universitätsbibliothek erlaubt wurde. Diese Regelung bringt durch die festgeschriebenen Nutzungsmöglichkeiten keine datenschutzrechtlichen Nachteile für die Betroffenen mit sich, grenzt den Mißbrauch durch Nichtberechtigte ein und erlaubt den Hochschulangehörigen unmittelbar nach Anmeldung die Nutzung der zentralen Einrichtungen.

**Abfrage von Prüfungsergebnissen telefonisch und übers Internet?**

*Manches Prüfungsamt an den Hochschulen ist stark gefordert, wenn eine große Zahl von Studenten gleichzeitig die Ergebnisse ihrer Prüfungen erfahren möchte. Dazu werden in den Prüfungsämtern Listen mit den Prüfungsergebnissen ausgelegt. Diese Listen enthalten aber nicht den Namen, sondern lediglich die Matrikelnummer und die entsprechenden Noten. Um den Studenten einen vereinfachten Zugang zu diesen Informationen zu ermöglichen, entstand die Idee, eine automatisierte telefonische Auskunft zu installieren. Der interessierte Student wählt eine bestimmte Telefonnummer und wird aufgefordert, auf der Tastatur des Telefonapparats die Matrikelnummer und eine Codenummer für das Fach einzugeben. Selbstverständlich erfolgt die akustische Auskunft wieder ohne Nennung des Namens.*

In dieser Form, so stellten wir fest, überschreitet das Auskunftssystem nicht die bislang auf den Listen verfügbaren Informationen an die Studierenden. Etwas anders gestaltete sich die Problematik, als von einem Fachbereich ein Konzept entwickelt wurde, ähnlich des telefonischen Voicesystems die Möglichkeiten des *Internets* für die *Notenauskunft* zu nutzen. Durch eine Internetabrufmöglichkeit sahen wir die Gefahr, daß der bisherige Stand der Öffentlichkeit der Angaben unverhältnismäßig ausgeweitet wird. Wenn wie bisher die Listen ausgehängt werden, so können diese wiederum nur in der Universität selbst eingesehen werden. Die telefonische Auskunft ist zwar von jedem Ort aus abrufbar, doch setzt sie die Kenntnis der Telefonnummer und der Codenummer des Fachs sowie die entsprechend richtige Matrikelnummer voraus. Um einen unberechtigten Zugriff auf ein derartiges Auskunftssystem über das Internet einzuschränken, empfahlen wir verschiedene Möglichkeiten, die gegenwärtig noch geprüft werden. Eine Möglichkeit ist eine Beschränkung der IP-Adressen. Dies würde die Abfragemöglichkeiten der Studenten von zu Hause aus einschränken, entspräche aber dem bisher in den Räumen der Universität erfolgenden Aushang. Ein solches System würde relativ unflexibel bei den häufigen Veränderungen der zugriffsbefugten Geräte reagieren. Des weiteren wäre zu prüfen, ob eine Speicherung der Daten beim Abrufenden verhindert bzw. ein Ausdruck dieser Daten erschwert werden kann. Würde man beispielsweise die Anzahl der Zugriffe beschränken, so wäre eine zusätzliche Sicherheit gegen *„Hacker“* gegeben. Außerdem empfahlen wir zu prüfen, ob die im Antwortfeld angegebene Matrikelnummer nicht in der eingegebenen Form, sondern um einige Stellen gekürzt wiedergegeben werden sollte.

**Der „gläserne Student“**

*An verschiedenen deutschen Hochschulen werden derzeit Versuche durchgeführt, Studentenausweise als multifunktionale Chipkarten auszugeben. In Berlin beschäftigen sich viele Hochschulen mit der Frage, ob mit dem Chip im Studentenausweis Kosten eingespart und Verwaltungsaufwand reduziert werden können. Auch für die Studenten soll die Karte viele Erleichterungen im Kontakt mit der Hochschulverwaltung oder bei der Inanspruchnahme von Dienstleistungen erbringen.*

Unter Federführung der Technischen Fachhochschule, die bereits 1998 die Erprobung der *Chipkarte in Studentenhand* beginnen will, und unter Mitwirkung eines Berliner Systemhauses mühen sich die drei Universitäten sowie einige weitere Hoch- und Fachhochschulen mit unterschiedlicher Intensität, in anderen Bundesländern erprobte Konzepte zu übertragen.

Dabei wird an folgende Funktionsbereiche gedacht:

- hoheitliche Aufgaben der Hochschulverwaltung wie Immatrikulation bei Hochschulwechsel, Rückmeldung, Exmatrikulation, Ausgabe von Studienbescheinigungen, Prüfungsorganisation;
- nicht-hoheitliche Aufgaben der Hochschulverwaltung: Zugang zu Funktionsräumen (z. B. PC-Kabinette, Labors), Parkplätze, Kopiergeräte usw.;
- Bibliotheksausweis;
- kontoungebundene *GeldKarte* (elektronische Geldbörse) zur Nutzung in universitären (Einschreibgebühr, Inanspruchnahme kostenpflichtiger Dienstleistungen – z. B. Kopierer, Mensa, bewirtschaftete Parkräume) und außeruniversitären (Copyshops, Buchhändler, BVG [„Semester-Ticket"]) Akzeptanzstellen.

Die Funktionsbereiche können – abhängig von der Flexibilität der gewählten Chipkartentechnologie und den rechtlichen Rahmenbedingungen – beliebig erweitert werden.

Für Berlin wird eine einheitliche Lösung angestrebt, die nach der Erprobung für die hoheitlichen Aufgaben der *Hochschulverwaltung* für die Studenten verbindlich eingeführt werden soll. Wir haben in den ersten Beratungsgesprächen deutlich gemacht, daß der verbindliche Einsatz von Chipkarten im hoheitlichen Bereich nach § 6 Abs. 1 BlnDSG auf einer expliziten Rechtsgrundlage beruhen muß. Dies gilt auch dann, wenn prinzipiell nicht mehr Daten verarbeitet werden sollen. Jedoch findet im Vergleich zu vorher eine völlig andersartige Verarbeitung mit einer Technologie statt, die überdies neuartige datenschutzrechtliche Risiken aufwirft. Diese Verarbeitungsform ist durch die Rechtsgrundlagen für die bisherige Verarbeitung personenbezogener Daten der Studenten nicht mehr gedeckt.

Selbstverständlich muß eine solche multifunktionale Chipkartenanwendung auch höchsten Sicherheitsanspüchen genügen. Wir werden daher das noch zu entwickelnde Sicherheitskonzept genau daraufhin überprüfen, ob es den Mindestanforderungen zur informationstechnischen Sicherheit bei Chipkarten entspricht, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits im Dezember 1996 aufgestellt hat[153].

**Abbau der Feindbilder?**

Unter der Überschrift „Datenschutz als Sündenbock beliebt, aber ungeeignet" nahmen wir im Jahresbericht 1996 grundsätzlich zu den Auffassungen über angebliche Behinderungen oder Blockaden der Forschung durch den Datenschutz Stellung[154]. Im vergangenen Jahr wurde die Diskussion mit der *Deutschen Forschungsgemeinschaft* und der *Arbeitsgemeinschaft der wissenschaftlichen medizinischen Fachgesellschaften* fortgesetzt. Ein zentrales Problem der Diskussion zwischen Vertretern der Forschung und der Datenschutzbehörden von Bund und Ländern im Juli 1997 war das Verhältnis von Einwilligungserklärungen der Betroffenen auf der einen Seite und Zweckbindungsgebot sowie Löschungsregeln auf Seiten der Forschung. Es war zu klären, inwieweit personenbezogene Daten, die auf Grund einer Einwilligungserklärung der Betroffenen erhoben werden, zu einem späteren Zeitpunkt und nach ihrer Anonymisierung für ein nicht durch die Einwilligung gedecktes Projekt beispielsweise für eine Anschlußstudie verwendet werden dürfen. Auch wurde diskutiert, ob Daten nach einer hinreichenden Anonymisierung für eine weitere Speicherung und wissenschaftliche Auswertung genutzt werden dürfen und eine Löschung dadurch ersetzt werden kann. Entscheidend ist hierbei, ob bei kleinen Fallzahlen und umfangreichen über den Betroffenen erhobenen Daten die verfassungsrechtlichen

153 Anforderungen zur informationstechnischen Sicherheit bei Chipkarten, in: Datenschutz und Datensicherung 5/97, S. 254 ff. (leicht gekürzt), vollständig in unserem Internetangebot

154 JB 1996, 4.5.1

Ansprüche an eine hinreichende Anonymisierung umgesetzt werden können. Diese Diskussion ist noch nicht abgeschlossen und wird 1998 fortgesetzt.

In Berlin haben wir nicht festgestellt, daß die hier tätigen Forscher hinsichtlich des Datenschutzes ein Feindbild kultiviert hätten.

**Beispiele aus der Forschung**

Im vergangenen Jahr suchte wiederum eine Vielzahl von Wissenschaftlern unsere Behörde auf und bat um datenschutzrechtliche Beratung zu ihren häufig sehr komplex angelegten Forschungsprojekten. An den nachfolgenden Beispielen soll verdeutlicht werden, daß es sehr wohl möglich ist, auch bei komplizierten Forschungsvorhaben die legitimen Interessen der Betroffenen, insbesondere ihr Recht auf informationelle Selbstbestimmung und die Wünsche der Wissenschaftler nach Datenzugang und freier Forschung durch im Einzelfall häufig sehr unterschiedliche Verfahren zum Ausgleich zu bringen.

*Im Jahre 1976 befragte eine Forschergruppe der Freien Universität Berlin fast 400 Strafgefangene in Berliner Justizvollzugsanstalten. Die damalige Untersuchung lieferte wertvolle Erkenntnisse über subjektive Ursachenkonstellationen einer kriminellen Entwicklung und zu persönlichen Einstellungen und Zukunftsabsichten*[155]*. Es wurde der Wunsch an uns herangetragen zu prüfen, unter welchen Bedingungen es möglich ist, die weiteren Lebensverläufe der seinerzeit Befragten, insbesondere eine mögliche „kriminelle Karriere" der letzten 20 Jahre nachzuzeichnen. Zu diesem Zweck erteilte die Senatsverwaltung für Justiz die Genehmigung, nach Bestimmung dieser Personen die Haftunterlagen, insbesondere die Gefangenenpersonalakten der Betroffenen, so sie im weiteren Verlauf ihres Lebens in Berlin inhaftiert waren, nach bestimmten Kriterien durchzusehen.*

Wir empfahlen dazu, einen standardisierten Erhebungsbogen zu entwickeln, der schon einen hohen Anonymisierungsgrad aufwies. Gesondert davon wurden die unmittelbar auf die Person zeigenden Daten erhoben. In einem zweiten Schritt baten die Wissenschaftler die Dienststelle des Bundeszentralregisters um eine unbeschränkte Auskunft zu wissenschaftlichen Zwecken nach dem Bundeszentralregistergesetz. Auch für diesen Arbeitsschritt unterbreiteten wir Vorschläge, um eine zügige und sichere, jegliche unberechtigte Einsichtnahme ausschließende Verfahrensweise zu finden. Im weiteren gingen die Wissenschaftler der Frage nach, warum für eine recht große Anzahl der Betroffenen kein Bundeszentralregisterauszug mehr vorliegt. Sie beantragten für diese Personen eine Auskunft aus dem Melderegister und erfuhren so, daß ca. 15 % der Probanden zwischenzeitlich in einem Alter, das nur etwa 50 % der durchschnittlichen statistischen Lebenserwartung entspricht, verstorben waren. Resultierend aus der *Brisanz dieser Datenerhebung* haben wir bereits mehrfach sowohl die datenschutzrechtlichen als auch technisch-organisatorischen Aspekte dieses Projekts geprüft. Dies betraf sowohl die Datenerhebung in der entsprechenden Justizvollzugsanstalt als auch den Sicherheitsstandard bei den auswertenden Forschern im Institut selbst.

*Im Unterschied zu dem zuvor beschriebenen Forschungsprojekt, das vom Forschungsansatz her eine Einwilligung der Betroffenen ausschloß, beabsichtigte das Max-Planck-Institut für Bildungsforschung eine komplexe Untersuchung mit Einwilligung der Betroffenen. Dabei sollten bestimmte Grundüberzeugungen von Schülern, ihre Auswirkungen auf die Schulleistung und ihre Freundschaften zu anderen Kindern untersucht werden. Im Rahmen dieses Projektes sollten sowohl die Kinder selbst als auch ihre Eltern befragt werden. Um die Auswirkungen auf die Schulleistungen zu analysieren, wurden auch die Lehrer gebeten, sich zu den Leistungen und Einstellungen sowie zum Verhalten der einzelnen Schüler zu äußern.*

Wir gaben den Wissenschaftlern eine Reihe von Hinweisen, die es erlaubten, auf den einzelnen Schüler bezogen, die Daten codiert, d. h. bei frühestmöglicher Löschung des Personen-

155 JB 1981, 2.7; JB 1982, 4.1

bezuges zusammenzuführen. Dieses Verfahren wurde den Eltern, von deren Einwilligung die Teilnahme der Schüler an diesem Projekt abhing, ausführlich dargelegt. Auf unsere Anregung hin gestalteten die Wissenschaftler die Erhebungsbögen so, daß sie unmittelbar nach der Datenerhebung eine Codierung vornehmen und die Namen sowie den Hinweis auf die einzelne Schule löschen können.

*Insgesamt mit sechs Forschungsprojekten wandten sich Sexualwissenschaftler und Sexualmediziner der Charité zur Beratung an uns. Dabei sollten Frauen zu nachfolgenden Komplexen befragt werden:*

- *In-vitro-Fertilisation und Erfolgsaussichten bei anderen Formen von künstlicher Befruchtung,*
- *das Wohlbefinden von Frauen nach einer Gebärmutterentfernung,*
- *zu sexuellen und psychosomatischen Ursachen bei auftretenden Schmerzen,*
- *Befragungen zur familiären Vorbelastung bei Brustkrebs,*
- *eine Untersuchung zum erhöhten Risiko für Herz-, Kreislauf- und Stoffwechselerkrankungen bei Frauen in den Wechseljahren.*

Das Gemeinsame dieser Projekte bestand darin, daß die Frauen auf Grundlage früherer Behandlungsunterlagen durch den behandelnden Arzt angeschrieben und um ihre Einwilligung zur Teilnahme am jeweiligen Forschungsprojekt gebeten wurden. Die Einwilligung umfaßte auch die Befugnis, an verschiedenen Stellen vorliegende Einzelangaben oder Laborergebnisse zum Zwecke der Untersuchung *anonymisiert* zusammenführen zu dürfen. Den Forschern war also vor Erteilung der Einwilligung weder der Name noch irgendein anderes Datum der betroffenen Frauen bekannt. Erst nach Eingang der Einwilligungserklärung wurden die Daten in einer anonymisierten Form zusammengefügt und ausgewertet. Jeglicher Personenbezug wurde dann gelöscht.

*Eine datenschutzrechtlich interessante Lösung wurde bei einer Befragung Jugendlicher zur Drogenaffinität in der Techno-Party-Szene gefunden.*

Die Sozialwissenschaftler befragten vor Ort in den einzelnen Diskotheken die Jugendlichen. In diesem Zusammenhang baten sie die Jugendlichen um ihre Einwilligung für ein mögliches Interview. Es wurde eine Antwortkarte ausgegeben. Die Jugendlichen setzten ihre Personalien darauf und der Sozialwissenschaftler signierte den Antwortbogen mit einem Code, der auf der Antwortkarte wiederholt wurde. Die Personenbeziehbarkeit war hier nur solange gegeben, bis die Jugendlichen mit der von ihnen selbst ausgefüllten Karte um einen Interviewtermin gebeten wurden. Für diesen Termin stand es ihnen frei, zuzusagen oder ihre Einwilligung zu einem Interview zurückzuziehen, indem sie nicht erschienen. Ein Bezug zum Erhebungsort (d. h. zur einzelnen Diskothek) war damit weder notwendig noch möglich.

Aus der Sicht des Senats wird die Auffassung des Berliner Datenschutzbeauftragten geteilt.

*Aus Unachtsamkeit kann die zugesicherte Anonymität gefährdet werden.*

Die Hochschule eines anderen Bundeslandes führte im vergangenen Jahr eine *Umfrage zur Nutzung von Telekommunikationsmedien* in Berlin durch. Die Forscher erklärten, daß es sich dabei um eine anonyme Untersuchung handle. Zugleich schlugen sie aber vor, die anonymen Antwortbögen an die angegebene Faxnummer zu senden. Dabei wurde offenbar von den Forschern übersehen, daß regelmäßig die absendende Faxnummer, die bei privaten Anschlüssen häufig mit dem Namen versehen ist, im Fax-Ausdruck dem Empfänger mit übermittelt werden. Die eingangs den Wissenschaftlern versicherte Anonymität wird bei diesem Rücklaufverfahren ad absurdum geführt.

Ein ähnliches Problem zeigte sich auch bei einem *Projekt der Frauenforschung.* Leider wurde im Begleitschreiben nicht darauf verwiesen, daß weder die zurückzusendenden Umschläge noch die Erhebungsbögen einen Hinweis auf die absendende Einrichtung enthalten sollten.

**DDR weiterhin Forschungsprojekt**

Im Jahresbericht 1996[156] legten wir die datenschutzrechtlichen *Probleme eines Forschungsprojekts zur justitiellen Bewältigung der DDR-Vergangenheit* dar. Zwischenzeitlich wurde für die Enquete-Kommission des Deutschen Bundestages zur „Überwindung der Folgen der SED-Diktatur im Prozeß der Deutschen Einheit“ ein umfangreiches Gutachten erstellt. Das bislang angewandte Verfahren der Anonymisierung hat sich bewährt. Es wurde, um künftige Forschungen zu erleichtern, um einen wichtigen Aspekt ergänzt. Die zum Zwecke der Anonymisierung erstellten Zwischenkopien werden nun nicht mehr wie ursprünglich vorgesehen nach erfolgtem zweiten Kopieren vernichtet, sondern für die Nutzung bei künftigen Projekten der staatsanwaltschaftlichen Akte beigefügt.

Auch der *Landesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR im Land Berlin* bemüht sich im Rahmen seiner Aufgabe zur Errichtung und Unterhaltung eines Dokumentations- und Ausstellungs*zentrums darum,* durch *Zeitzeugenbefragungen* authentische Daten für die gegenwärtigen und künftigen Nutzungen zu speichern. Dies geschieht mit Einwilligung der Betroffenen. Um den Betroffenen jedoch die Tragweite ihrer Einwilligung klarzumachen, war es erforderlich, eine tiefgegliederte Einwilligungserklärung zu erarbeiten. Dabei ging es einmal um das Einverständnis in die Archivierung von Tonbändern bzw. abgeschriebenen Texten, aber auch um eine nichtanonymisierte Nutzung dieser Daten hinsichtlich des eigenen Namens, aber auch anderer vom Betroffenen genannten Namen. Der befragte Zeitzeuge kann sich entscheiden, ob er damit einverstanden ist, daß seine Angaben personenbezogen oder anonym zur Information der Öffentlichkeit und zur wissenschaftlichen Forschung genutzt werden können. Eine kommerzielle Nutzung dieser Unterlagen wird explizit ausgeschlossen.

Ein anderer Aspekt der Beforschung der DDR-Vergangenheit zeigte sich bei einem Projekt der Hochschule eines anderen Bundeslandes zum *Einfluß der Staatssicherheit auf ehemalige Bezirkszeitungen in der DDR.* Von dieser Untersuchung war auch eine Zeitung aus Berlin betroffen. Das Projekt selbst wirft eine Reihe von Fragen zur wissenschaftlichen Nutzung und Veröffentlichung von Unterlagen der ehemaligen Staatssicherheit bei der „Gauck-Behörde“ auf. Einer der Forscher, vormaliger Personalchef der ebenfalls untersuchten Zeitung aus Berlin, erhielt als Wissenschaftler Einsicht in die personenbezogenen Unterlagen gegenwärtiger und ehemaliger Mitarbeiter dieser Zeitungen. Dieser Zugang war ihm zuvor als Personalchef nicht zugänglich. Da dieses Forschungsprojekt mittlerweile auch zu personalrechtlichen Konsequenzen geführt hat, liegt die Vermutung nahe, daß unter dem Mantel wissenschaftlicher Forschung oder publizistischer Aufbereitung die vom Gesetzgeber im Stasi-Unterlagengesetz vorgesehene Beschränkung der Auskünfte für Mitarbeiter nicht-öffentlicher Stellen umgangen werden sollen.

### 4.5.2 Schule

**Immer wieder Unklarheiten beim Schülerbogen**

*Auf den Deckeln von Schülerbogen fanden wir u. a. folgende Eintragungen:*

- *Gespräch mit Mutter über . . . Verhaltensauffälligkeiten und Herumtreiben am Nachmittag. Empfehlung: Hortplatz beantragen . . . Phosphatfreie Diät wurde abgebrochen.*
- *der Mutter mitgeteilt, daß . . . häufig im Unterricht träumt. Es ist nicht klar, ob es nur auf Hörprobleme zurückzuführen ist.*
- *. . . leidet unter Neurodermitis. Gespräch mit Frau . . .: Sie leidet unter Haarausfall. Soziales Verhalten und Arbeitsverhalten lassen keine Rückschlüsse auf psychisches Verhalten durch die Schule zu.*
- *. . . ist unruhig, kippelt mit seinem Stuhle. Er ist oft desorientiert, kennt sein Material nicht und kann Arbeitsanweisungen nur unvollständig umsetzen. Seine Feinmotorik ist unausgeprägt und er schreibt nur unvollständig von der Tafel ab.*

Die Auffassung des Berliner Datenschutzbeauftragten, auf dem Pappdeckel des Schülerbogens sollten keine Vermerke über das Verhalten des Schülers und über die Inhalte von Gesprächen mit den Erziehungsberechtigten aufgenommen werden, wird geteilt. Das LSA Berlin ist bereits gebeten worden, die Schulen anzuweisen, derartige Eintragungen zu unterlassen.

Nicht geteilt wird die Aussage, daß der Schulleiter periodisch und bei jedem Schulwechsel verpflichtet sei, den Schülerbogen zu bereinigen. Nach § 11 Abs. 2 Satz 1 der Verordnung über die Verarbeitung personenbezogener Daten nach § 5a des Schulgesetzes für Berlin (SchuldatenVO) vom 13. Oktober 1994 (GVBl. S. 435) erfolgen solche Überprüfungen nur auf Antrag der Erziehungsberechtigten oder des volljährigen Schülers.

156 JB, 3.2

*oder in der Oberstufe:*

- *. . . ein Gespräch mit der Mutter wegen der Drogenabhängigkeit. Am . . . den Schüler nach Hause geschickt, wegen Übelkeit; ohne Genehmigung der Eltern.*

Auf den Aktendeckeln haben diese Eintragungen nichts verloren. Der Schülerbogen („die Schülerakte") ist eine Akte, in die neben Name, Anschrift sowie Angaben über die Erziehungsberechtigten die Schullaufbahn, Zeugnisabschriften, Empfehlungen zum Schulanfang, Oberschulempfehlungen oder Unterlagen über das Verhalten des Schülers einschließlich etwaiger Ordnungsmaßnahmen aufzunehmen sind. Ein Teil dieser Angaben wird unmittelbar auf dem *Aktendeckel* oder seinen Innenseiten aufgenommen. Darunter sind auch Vermerke über die „Zusammenarbeit mit den Erziehungsberechtigten, Jugendämtern, Jugendgesundheitsfürsorgestellen u. a. Behörden". Diese Vermerke können nicht wie ein etwaiger Briefwechsel oder auch Erziehungs- und Ordnungsmaßnahmen der Akte entnommen werden, da dieser Aktendeckel die Schüler über ihre gesamte Schulzeit – also ggf. bis zum Abitur – begleitet. Wenn hier also, wie aus den obigen Beispielen ersichtlich, in der Grundschule Vermerke vorgenommen werden, so sind sie nur schwer zu löschen. An den meisten Berliner Schulen wird daher hier nur vermerkt, daß ein Gespräch oder ein Kontakt stattgefunden hat, ohne den Inhalt darzulegen. Wenn dies erforderlich ist, wird dazu ein gesondertes Schriftstück angefertigt, das im Schülerbogen abgeheftet wird und dann bei Schulwechsel oder fehlender Erforderlichkeit entnommen und vernichtet werden kann.

Doch wie ist mit den Daten zu verfahren, die, wenn nur von kurzer zeitlicher Bedeutung sind und unzulässigerweise auf dem Pappdeckel des Schülerbogens gespeichert wurden? Da der Schülerbogen selbst auch der Dokumentation des Schulwegverlaufs dient, kann er nicht einfach ausgetauscht und neu angelegt werden. Wir empfehlen daher, auf dem Aktendeckel die unzulässig gespeicherten oder nicht mehr erforderlichen Daten zu schwärzen und den alten Schülerbogen zu kopieren. Die Kopie wäre zu beglaubigen und dann in den neu anzulegenden Schülerbogen aufzunehmen. Der alte Aktendeckel kann dann vernichtet werden. Auch wenn dieses Verfahren sehr aufwendig ist, sehen wir keine andere Möglichkeit, diese unzulässigerweise sonst auf Dauer gespeicherten Daten zu löschen.

In einem anderen Fall erhielten wir Kenntnis davon, daß im Schülerbogen selbst Schriftstücke aufgenommen und bei Schulwechsel der nachfolgenden Schule übermittelt wurden, die eine stigmatisierende Wirkung hatten. Diese Schriftstücke waren zum Teil den Eltern nicht bekannt. So wurde ohne Kenntnis der Eltern ein Gesprächsprotokoll verfaßt und der nachfolgenden Schule mit dem Schülerbogen zur Kenntnis gegeben. Damit wurde der Versuch gemacht, die Probleme, die gerade durch einen Schulwechsel und damit für das Kind durch einen Neuanfang gelöst werden sollten, an die neue Schule zu transportieren. Die betreffenden Unterlagen wurden auf unsere Hinweise hin an der neuen Schule aus dem Schülerbogen entfernt.

Jeder Schulleiter ist periodisch und bei jedem Schulwechsel verpflichtet, vor der Weitergabe des Schülerbogens an die nachfolgende Schule diesen bezüglich der Erforderlichkeit der dort gespeicherten Daten zu überprüfen und nicht mehr erforderliche Unterlagen zu entnehmen und zu vernichten.

**Vergeßliche Lehrer?**

*„Liebe Eltern,*

*die Gesamtkonferenz unserer Schule hat beschlossen, daß jede Schülerin und jeder Schüler unserer Schule ein Paßbild abgeben muß. Bei ca. 500 Schülern ist es für die Lehrer und die Schulleitung nicht möglich, jedem Gesicht einen Namen zuzuordnen. Um also die Identifikation unserer Schüler schneller vornehmen zu können, möchten wir jede Schülerkarteikarte mit einem Paßfoto versehen.*

*Mit freundlichen Grüßen*

*Die Schulleitung"*

Die Auffassung des Berliner Datenschutzbeauftragten wird geteilt.

Mit dem Paßfoto werden personenbezogene Daten erhoben. Der Umfang der an Berliner Schulen zu erhebenden Daten ist im Schulgesetz und in der Schuldatenverordnung abschließend geregelt. Die Aufnahme eines *Paßbildes* in diese Datensammlungen ist nicht vorgesehen. Lediglich für *Schülerausweise* werden Lichtbilder benötigt, aber hier ist der Zweck gerade nicht die Beschulung des Kindes, sondern der Nachweis der Schülereigenschaft gegenüber Dritten. Des weiteren wird durch den Beschluß einer Gesamtkonferenz eine Erhebung personenbezogener Daten mit Auskunftspflicht keinesfalls legitimiert. Die Schulen haben keine Satzungsbefugnis wie beispielsweise die Hochschulen.

Einige Monate zuvor erreichte uns eine Anfrage zu einem ähnlichen Projekt. Hier bestanden einige wesentliche Unterschiede. Die betreffende Schule hatte doppelt so viele, nämlich über 1 000 Schüler. Es war nicht vorgesehen, das Paßbild auf der Schülerkarteikarte oder anderen der Schulverwaltung dienenden Unterlagen zu speichern. Die Paßfotos sollten auf den Schülerleitbogen geklebt werden und damit nur den betreffenden Lehrern in der Jahrgangsleitung für die Arbeit im Kurssystem zur Verfügung stehen. Der wichtigste Unterschied ist, daß an dieser Schule die Paßfotos nur mit entsprechender schriftlicher Einwilligung erhoben und gespeichert werden sollten.

**Was Schulsekretärinnen dürfen und was nicht**

*Durch Anfrage erfuhren wir von einem Schreiben des Landesschulamtes, in dem festgestellt wird, daß zur Führung der Schülerbögen allein die zuständigen Klassenlehrer oder Tutoren und nicht die Schulsekretärinnen zu beauftragen sind. Dieses Schreiben führte in der praktischen Schulverwaltungsarbeit zu Irritationen. Es ist an vielen Schulen gängige Praxis, daß die Schulsekretärinnen die Schülerbögen eigenverantwortlich komplettieren, auf Richtigkeit durchsehen und dann entsprechend dem Schulleiter vorlegen.*

Die Schulsekretärin ist nach Schulverfassungsgesetz schulische Mitarbeiterin und der Schulleiter ist im Rahmen seiner Verwaltungsaufgaben ihr gegenüber, im Unterschied zu den Lehrern, weisungsberechtigt. Die Sicherstellung des Datenschutzes ist eine der Aufgaben des Schulleiters. Die Schulsekretärin ist bei ihrer Aufgabenerfüllung ausschließlich mit Verwaltungsaufgaben zu beauftragen, die sie entsprechend den Weisungen des Schulleiters erfüllt. Das Weisungsrecht des Schulleiters kann nicht delegiert werden, daraus ergibt sich, daß die *Schulsekretärin „als verlängerter Arm des Schulleiters“* tätig ist. Diese Konstellation schließt beispielsweise eine Bestellung der Schulsekretärin zur Schuldatenschutzbeauftragten aus. Gleichwohl dürfte aber ein Schulleiter, im Interesse einer rationellen Organisation der Verwaltungsaufgaben, die technisch-organisatorischen Arbeiten der Führung des Schülerbogens der Schulsekretärin übertragen können. Nach der Schuldatenverordnung kontrolliert der Schulleiter die Führung der Bögen. Der Lehrer bzw. ausnahmsweise auch der Schulleiter nimmt Eintragungen vor, die über einen längeren Zeitraum für die Unterrichts- und Erziehungsarbeit schriftlich festzuhalten sind. Solche Eintragungen sind individuell und haben eine pädagogische Qualität. Diese Eintragungen kann natürlich keine Schulsekretärin vornehmen. Die Anlage des Bogens und das Abheften bestimmter Unterlagen, wie der Zeugnisdurchschriften, können aber auf Weisung des Schulleiters von der Schulsekretärin vorgenommen werden. Es bestehen auch keine Bedenken, wenn der Schulleiter anweist, daß die Schulsekretärin die Schülerbögen nach bestimmten Kriterien durchsieht und Unterlagen markiert, die beispielsweise bei einem Schulwechsel für die Löschung entnommen werden sollten. Die Entscheidung über die Löschung selbst trifft der zuständige Lehrer bzw. der Schulleiter. Wir baten das Landesschulamt um Stellungnahme, die auch in diesem Fall seit gut einem halben Jahr auf sich warten läßt.

Die Auffassung des Berliner Datenschutzbeauftragten wird geteilt.

**„Tugendnoten“ für Schüler?**

*Im Rahmen des Modellversuchs „Schule in erweiterter Verantwortung“ haben zwei Schulen begonnen, ihren Schülerinnen und Schülern Bescheinigungen über die Teilnahme an einem besonderen Unterrichtsangebot auszustellen. Diese* Bescheinigung

Hierbei handelt es sich um ein zeitlich begrenztes Vorhaben zweier Berliner Realschulen, die sich im Rahmen des „Modellprojekts Schule in erweiterter Verantwortung“ ein selbst definiertes Ausbildungsprofil gegeben haben und ihren Schülerinnen

enthält Noten für die Zuverlässigkeit, die Leistungsbereitschaft, die Sorgfalt, die Selbständigkeit, die Verantwortungsbereitschaft, die Teamfähigkeit und für die Umgangsformen. Auf dem Zeugnis ist vermerkt, daß es sich hierbei um eine inoffizielle Beurteilung handelt und die Noten subjektive Einschätzungen der Lehrer sind.

Zunächst steht es zwar jedem Schüler frei, dieses Zweitzeugnis bei *Bewerbungen* zu nutzen. Dies trifft aber nur solange zu, wie das Projekt auf einzelne Schulen beschränkt und deshalb weniger bekannt ist. Solange dürften sich aus dem Fehlen des Zweitzeugnisses in den Bewerbungsunterlagen für die Bewerber keine nachteiligen Konsequenzen ergeben. Aus Presseberichten war zu entnehmen, daß bei der Bewerberauswahl dem Zweitzeugnis durchaus Bedeutung zugemessen wird. Für den einstellenden Betrieb ist die Note auf dem *Zeugnis* und damit auch auf einem *Zweitzeugnis* mangels anderer Einschätzungen ein objektives Merkmal, an dem er seine Bewerberauswahl ausrichten wird. Für die Schüler kann also der *faktische Zwang* entstehen, die Zweitzeugnisse den Bewerbungsunterlagen beizufügen, um keine Nachteile gegenüber Mitbewerbern auf dem Arbeitsmarkt zu haben. Die Zweitbenotung kann somit trotz der erklärten „Unverbindlichkeit" für den einzelnen Schüler enorme Bedeutung gewinnen. Wir gaben zu bedenken, daß durch die Zweitzeugnisse eine schul- und datenschutzrechtliche Gemengelage zwischen dem staatlichen Bildungs- und Erziehungsauftrag, dem Persönlichkeitsrecht der Schüler und dem Elternrecht entsteht. Eine rechtliche Nachprüfbarkeit der Benotung ist für den betroffenen Schüler kaum möglich. Die Senatsschulverwaltung teilte uns auf eine entsprechende Anfrage mit, daß dieses Modellprojekt gegenwärtig noch kontrovers diskutiert wird und durch eine enge schulaufsichtliche Begleitung sichergestellt werden soll, daß die Erfahrungen dieses Projekts solide ausgewertet werden.

und Schülern über die Teilnahme an einem besonderen Unterrichtsangebot „Ausbildungsorientierung" eine Bescheinigung ausstellen. Dabei werden allgemein verständliche Einschätzungen über die Beherrschung einiger benannter Schlüsselqualifikationen abgegeben. Die für Absolventen des besonderen Unterrichtsangebotes ausgegebenen Bescheinigungen stellen kein Zweitzeugnis dar. Vom Charakter her sind sie den Bescheinigungen für die Teilnahme an Arbeitsgemeinschaften oder Interessengruppen oder für sportliche Leistungen ähnlich, die ebenfalls nicht Bestandteil von Zeugnissen sind, aber mit den Zeugnissen gemeinsam ausgeteilt werden. Insoweit treffen die Ausführungsvorschriften über Noten und Zeugnisse auf die von beiden Realschulen ausgegebenen Bescheinigungen nicht zu. Die Senatsverwaltung für Schule, Jugend und Sport wird den Berliner Datenschutzbeauftragten weiterhin über die Durchführung des Vorhabens unterrichten.

**Daten von Abc-Schützen**

*„Fragebogen-Skandal; Senat horcht die Eltern von Abc-Schützen aus". So und ähnlich war es im Frühjahr anläßlich der Einschulungsuntersuchungen in der Presse zu lesen. Erbost reagierten einige Eltern auf Fragebögen der Jugendgesundheitsdienste der Bezirke, in denen nach der Erwerbstätigkeit der Eltern, den Sorgerechtskonstellationen bis hin zur Zahl der Wohnräume in der Wohnung, der Heizungsart oder Angaben zu Feuchtigkeit und Schimmel in der Wohnung abgefragt wurden. Auch wurden viele Fragen zu früheren Erkrankungen der Kinder gestellt, was in der Natur der Sache bei Einschulungsuntersuchungen liegt.*

Wir stellten nach einer Befragung der 23 Bezirke fest, daß die Bezirksämter den Eltern anläßlich der Einschulungsuntersuchungen fünf verschiedene Fragebögen vorlegen. Gerade die auch inhaltlich stark differierenden Erhebungsbögen lassen den Schluß zu, daß die Datenerhebung erheblich verbessert werden muß. Zwar ist auf den meisten Bögen ein Hinweis auf die *Freiwilligkeit* gegeben, dieser sollte jedoch verdeutlicht werden. Auch war der Zweck, zu dem diese Daten erhoben werden sollen, und die Rechtsgrundlage nicht auf allen Bögen hinreichend benannt. Für die Schulreifeuntersuchung liegt die Zuständigkeit bei den bezirklichen Jugendgesundheitsdiensten. Die Fachaufsicht wird von der Senatsverwaltung für Gesundheit und Soziales ausgeübt. Um eine Klärung der Angelegenheit zu beschleunigen, erarbeiteten wir eine Synopse zum Inhalt der verschiedenen Erhebungsbögen und empfahlen unter Federführung der Fachaufsicht, eine Verständigung zwischen den Jugendgesundheitsdiensten noch rechtzeitig vor Beginn der Einschulungsuntersuchungen für das Schuljahr 1998/99 zu erreichen und sicherten unsere beratende Mitwirkung zu. Leider deutet sich an, daß auch die Schulreifeuntersuchungen im Frühjahr 1998 durch die Berliner Bezirke noch nicht mit einem abgestimmten, möglichst einheitlichen Datenerhebungsbogen durchgeführt werden können.

Der geschilderte Sachverhalt ist grundsätzlich zutreffend. Der „Presse" gegenüber wurde verdeutlicht, daß die zuständige Senatsverwaltung bislang nur alle 3 bis 4 Jahre die Ergebnisse der Einschulungsuntersuchungen landesweit auswertet. Im Jahr 1997 waren jeweils die Bezirke eigenverantwortlich zuständig.

In einer Gesprächsrunde mit Vertretern des Berliner Datenschutzbeauftragten am 4. September 1997 wurde sowohl auf die Zuständigkeiten als auch auf die unterschiedlichen Erhebungs- bzw. Elternfragebögen hingewiesen. Der Berliner Datenschutzbeauftragte empfahl einen einheitlichen Dokumentationsbogen und zeigte seine Bereitschaft, an einer Lösung mitzuwirken, die es erlaubt, die für den gesetzlich vorgegebenen Zweck erforderlichen Daten möglichst einheitlich zu erheben.

Für das Schuljahr 1998/1999 konnte dieses jedoch noch nicht erreicht werden. Das Landesamt für Gesundheit und Soziales befindet sich jedoch in einem Abstimmungsprozeß mit den bezirklichen Kinder- und Jugendgesundheitsdiensten, um ab 1999 eine einheitliche, standardisierte Erfassung und Auswertung zu erreichen.

**Werbung in der Schule**

*Kaum war aus der Senatsschulverwaltung zu vernehmen, daß die Ausführungsvorschriften zur Werbung an Schulen deutlich gelockert werden sollten, schon wurden mit Beginn des Schul-*

Es ist beabsichtigt, den Schulen in einem die AllA-Werbung ergänzenden Rundschreiben Hinweise u. a. auch zur Beachtung des Datenschutzes zu geben.

*jahres 1997/98 verschiedenste Unterlagen an Schulen verteilt. So verteilte ein Verlagsunternehmen ein „Verkehrsquiz für clevere Kinder". Die Rätsel waren einfach zu lösen, die Eltern brauchten „nur" ihre personenbezogenen Daten einzusetzen und ihre Zustimmung zum Erhalt eines kleinen Gewinns geben. Der Gewinn wird aber nur im Zusammenhang mit Werbegesprächen von Außendienstmitarbeitern übergeben.*

Eine Nutzungsbeschränkung der Adreßangaben einschließlich der Angaben zum Kind wird nicht erklärt, so daß hier eine *Weitergabe der Angaben im Adreßhandel* rechtlich zulässig wäre. Von den Außendienstmitarbeitern wurde die Schule gebeten, den Rücklauf der Karten von den Eltern selbst zu organisieren und die Karten in der Schule zu sammeln. Die Antwortkarten mit den personenbezogenen Daten würden dann abgeholt werden. Der Schule wurde eine Vergütung dieser Leistung etwa in Höhe der eingesparten Portogebühren versprochen. Rechtlich betrachtet, stellt ein solches Verfahren eine Auftragsdatenverarbeitung durch die Schule als Auftragnehmer und den betreffenden Verlag als Auftraggeber dar. Bei dieser Rechtskonstruktion würde die Schule als öffentliche Stelle im Auftrag Privater tätig werden und die *Schulpflicht zur Erhebung und Veräußerung personenbezogener Daten nutzen.* Wir teilten der Senatsverwaltung für Schule, Jugend und Sport mit, daß ein solches Vorgehen zu beanstanden wäre. Der betroffene Schulleiter hat sich im übrigen durch die versprochene Belohnung nicht in Versuchung bringen lassen und diese Datenerhebung im Auftrag des Verlages abgelehnt.

### 4.5.3 Statistik

**Zensus oder Volkszählung 2001?**

Bei Erscheinen dieses Jahresberichtes hat die Amtliche Statistik noch eine Frist von drei Jahren zur Vorbereitung der für das Jahr 2001 geplanten Volkszählung. Im Jahresbericht 1996[157] skizzierten wir das Grundproblem: Einerseits scheint eine *Volkszählung* nach herkömmlichem Muster sowohl aus Kostengründen als auch aus Gründen der mangelnden Akzeptanz der Betroffenen auszuscheiden, andererseits wurden mögliche Verfahren zur Nutzung vorhandener Register für statistische Auszählungen noch nicht hinreichend erprobt. Nach wie vor ist die Diskussion über das „wie" eines Zensus auf der Grundlage von *Registerauszählungen* nicht abgeschlossen. Eine Entscheidung der Europäischen Union, insbesondere durch den Erlaß einer Richtlinie oder Empfehlung, in der die zulässigen Methoden für den Zensus 2001 festgeschrieben werden, steht ebenfalls noch aus.

Das Statistische Bundesamt hat ein sogenanntes *Bundesmodell* für den gemeinschaftsweiten Zensus 2001 entwickelt. Mit diesem Modell wird versucht, den Datenanforderungen der Europäischen Union durch Auswertung verschiedener Datenbasen gerecht zu werden. Grunddaten zur Bevölkerung (Alter, Geschlecht, Familienstand, Staatsangehörigkeit, Geburtsort und -land sowie Haupt- und Nebenwohnung) sollen für die gesamte Bevölkerung in tiefer regionaler Gliederung durch Auswertung aus dem *Melderegister* bereitgestellt werden. Die Daten zur Erwerbstätigkeit zusammenzutragen, gestaltet sich schwieriger. Als Datenquelle wurden die Datenbestände der Bundesanstalt für Arbeit ausgemacht, in denen etwa 85 % aller Erwerbstätigen in tiefer sachlicher und regionaler Gliederung gespeichert sind. Diese Daten sollen für die Beamten durch die Auswertung der Personalstandsstatistik ergänzt werden. Für die Anzahl und Struktur der selbständigen und mithelfenden Familienangehörigen verbleibt nur die Methode der Schätzung, so daß hier Zahlen lediglich bis auf Kreisebene gewonnen werden könnten. Daten zum Pendlerverhalten, aber ohne Angabe der genutzten Verkehrsmittel, könnten wiederum aus den Datenbeständen der Beschäftigtenstatistik erzeugt werden. Die weiteren Merkmale zur Erwerbstätigkeit, zum Wohnen, zur Bildung und zur Struktur der Haushalte müßte dann durch Hochrechnung auf Grundlage der Einprozent-Stichprobe des Mikrozensus ergänzt werden.

Damit ist auch für jeden Außenstehenden nachvollziehbar, daß die Statistiker in der zur Verfügung stehenden Zeit bei der Bereinigung von Registerfehlern und dem Konzipieren der Auswer-

157 JB 1996, 4.5.3

tungen noch große Probleme zu lösen haben. Im Unterschied zur konventionellen Volkszählung, in der für jeden Betroffenen auf einem recht kurzen Erhebungsbogen demographische Daten, Daten zur Erwerbstätigkeit, zum Pendlerverhalten, zu Bildung, aber auch zur Struktur der Haushalte sowie zu den Einkommens- und Wohnverhältnissen erhoben werden, stehen hier in der Auswertung verschiedenste Daten nebeneinander, die ohne ein „einheitliches Personenkennzeichen" kaum kleinregional bzw. in einer entsprechenden Strukturtiefe auszuwerten sein dürften. Bei einer konventionellen Volkszählung ist ein Verknüpfungsmerkmal nicht erforderlich und die Anonymisierung der Einzeldaten kann zügig erfolgen. Sollen aber beispielsweise auch die Beschäftigtendaten nach demographischen Strukturangaben ausgewertet werden, wäre eine Verknüpfung des Datenbestandes der Bundesanstalt für Arbeit und der Personalstandsstatistik für die Beamten mit den Melderegisterdaten aus statistischer Sicht wünschenswert. Daher verstärken sich in der letzten Zeit Forderungen, wenn auch nicht für den Zensus 2001, dann doch für spätere statistische Zählungen, die Möglichkeiten einer *Registerverknüpfung* zu prüfen. Im Volkszählungsurteil von 1983[158] hat das Bundesverfassungsgericht in diesem Zusammenhang formuliert: „Auch die Übernahme sämtlicher Daten aus bereits vorhandenen Dateien der Verwaltung ist keine zulässige Alternative zur vorgesehenen Totalzählung. Denn die Nutzung von Daten aus verschiedenen Registern und Dateien würde voraussetzen, daß technische, organisatorische und rechtliche Maßnahmen getroffen werden, die es erlauben, diese Daten, bezogen auf eine bestimmte Person oder Institution, zusammenzuführen. Eine solche Maßnahme wäre z. B. die Einführung eines einheitlichen, für alle Register und Dateien geltenden Personenkennzeichens ... Dies wäre aber gerade ein entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und katalogisieren. Die Verknüpfung vorhandener Dateien wäre danach auch nicht das mildere Mittel."

Um die zu befürchtenden Datenlücken grob schließen zu können, haben Statistiker einzelner Bundesländer ein *Ländermodell* entwickelt. In diesem Modell ist vorgesehen, über eine Straßenschlüsseldatei sowohl Einwohnermelderegister als auch Datenerhebungen bei den Gebäudeeigentümern miteinander zu verbinden. Ein ergänzender Vorschlag sieht vor, auf Grund der Melderegisterdaten eine postalische Vollerhebung bei den Betroffenen durchzuführen, um so auf die einzelne Person bezogen Datensätze zu erhalten, die den Datenbedarf abdecken könnten. Eine solche postalische Erhebung würde zwar zusätzliche Kosten verursachen, jedoch nicht zu einer Vermengung von Daten des Verwaltungsvollzuges (Melderegister) und statistisch erhobenen Daten führen, wenn der Empfänger dieser Angaben allein das Statistische Landesamt wäre und eine Rückübermittlung an die Meldebehörden, wie dies bereits durch das Volkszählungsurteil ausgeschlossen wurde, unzulässig bleibt.

Unabhängig von der nicht abgeschlossenen Diskussion zur *Methodik des Zensus 2001* hat das Statistische Landesamt Schritte unternommen, die statistischen Auswertungen des Melderegisters weiter zu entwickeln. Durch eine Rechtsverordnung[159], die im Gefolge des Landesstatistikgesetzes[160] erlassen wurde (ÜbermittlungsVO), ist rechtlich abgesichert, daß dem Statistischen Landesamt monatlich anonymisierte Einzeldatensätze aus dem Melderegister übermittelt werden. Diese Einzeldatensätze beinhalten den Geburtstag, das Geschlecht, das Alter, den Familienstand, die Staatsangehörigkeit, die Religionszugehörigkeit, den Wahlausschluß, das Kennzeichen zur Erwerbstätigkeit sowie Zu- und Abgangsdaten einschließlich der Angaben über die Haupt- und Nebenwohnung. Als Hilfsmerkmale werden die Adreßdaten bereitgestellt. Aus diesen Daten lassen sich keine Informationen gewinnen, die Aufschluß über die Zugehörigkeit des Einzelnen zu bestimmten Haushalten oder Haushaltstypen erlauben. Daher beabsichtigt das Statistische Landesamt im Rahmen rechtlich zulässiger Testarbeiten zur Vorbereitung von Statistiken nach § 2 Abs. 4 Landesstatistikgesetz i. V. m. § 3 Abs. 1 Bundesstatistikgesetz auf Grundlage eines in Baden-Württemberg entwickelten Verfahrens über Namensgleichheiten und andere im Melde-

158 BVerfGE 65, 56
159 GVBl. 1993, 661
160 GVBl. 1992, 365

register verzeichnete Daten Haushaltszusammenhänge statistisch abzubilden. Wir prüften die rechtliche Zulässigkeit und kamen zu dem Schluß, daß eine solche Aufbereitung zu dem Zweck „Erprobung neuer statistischer Methoden“ unter bestimmten Bedingungen zulässig ist. Eine dieser Bedingungen ist, daß für diesen Test keine flächendeckenden Daten für Berlin, sondern nur die ausgewählter Gebiete aufbereitet werden dürften. Sollte sich diese Methode für statistische Zwecke bewähren, wäre die Übermittlungsverordnung entsprechend zu ergänzen.

**Einzelstatistik – Kampagnen**

Die alljährlich im Mai durchgeführte „kleine Volkszählung“, der *Mikrozenus*, führt auch bei uns immer wieder zur einer Vielzahl von Anfragen bezüglich der Rechtmäßigkeit und des Verfahrens der Datenerhebung. Diese Anfragen bieten uns wiederum Gelegenheit zu prüfen, ob das Statistische Landesamt und seine Interviewer die rechtlichen Vorschriften einhalten.

So, wie die gesamte Berliner Verwaltung, ist auch das Statistische Landesamt gefordert, Möglichkeiten zur Einsparung ausfindig zu machen. Jährlich werden bei der Mikrozensuserhebung den Betroffenen mit der Ankündigung der Interviewer eine Reihe von *Unterlagen zur Information* in den Briefkasten gesteckt. So wurde angeregt, bei den Wiederholungsbefragungen im zweiten, dritten und vierten Jahr auf einige dieser Unterlagen, die bereits bei der Erstbefragung übergeben wurden, zu verzichten. Nach der Regelung des § 17 Bundesstatistikgesetz sind die Befragten schriftlich über den Zweck, die Art und den Umfang der statistischen Erhebung und weitere Aspekte des Verfahrens einschließlich ihrer Rechte und Pflichten zu informieren. Zwar war vorgesehen, weiterhin den Betroffenen den Gesetzestext beizulegen, jedoch sollten die erläuternden Schreiben eingespart werden. Wir empfahlen im Interesse einer hohen Akzeptanz, insbesondere bei Erhebungen mit Auskunftspflicht eindeutige und wenig juristisch und akademisch formulierte Erläuterungen den Betroffenen zuzusenden. Insbesondere nach Ablauf von zwei bis drei Jahren kann nicht mehr bei den Betroffenen vorausgesetzt werden, daß sie die Information der Vorjahre noch kennen oder aufbewahrt haben. Wir teilten dem Statistischen Landesamt mit, daß wir eine derartige Einsparungsmaßnahme auch rechtlich nicht für zulässig halten.

Nach Anfrage beim Berliner Datenschutzbeauftragten wurden vom Statistischen Landesamt weiterhin bei den Wiederholungsbefragungen im 2., 3. und 4. Jahr die vollständigen Unterlagen zur Information an die Befragten ausgehändigt, die sie bereits bei der Befragung im 1. Jahr erhalten hatten. Eine Vereinfachung/Einsparung war und ist nicht möglich.

Die Empfehlung des Berliner Datenschutzbeauftragten, im Interesse einer hohen Akzeptanz, insbesondere bei den Erhebungen mit Auskunftspflicht, eindeutige und wenig juristisch und akademisch formulierte Erläuterungen den Betroffenen zuzusenden, stimmt überein mit dem gleichgerichteten Bemühen des Statistischen Landesamtes. Unverzichtbar ist jedoch die Überlassung der einschlägigen Gesetzestexte, auch wenn diese für die Befragten möglicherweise schwerer zu lesen sind als die anderen enthaltenen Unterlagen wie Anschreiben, Fragebogen und Hinweise (Erläuterungen).

Nicht erst im Zusammenhang mit dem für 2001 angestrebten Zensus wird das „Gebäude“ der Amtlichen Statistik einer Revision unterzogen. Die Bundesstatistik als Ganzes wird durch vielfältige Initiativen einem Einspardruck ausgesetzt. Daß Sparvorschläge nicht nur Streichungen und Qualitätsverschlechterungen mit sich bringen müssen, zeigen die Veränderungen bei der für 1998 vorgesehenen *Einkommens- und Verbrauchsstichprobe (EVS)*. Die EVS wird auf freiwilliger Grundlage in einem Abstand von 5 Jahren durchgeführt. Auch aus datenschutzrechtlicher Sicht sind Verbesserungen erkennbar. Es werden nicht mehr wie bisher über das gesamte Jahr über 70 000 Haushalte befragt, sondern jeweils nur 1/4 in jedem Quartal. Dies führt einerseits zur Entlastung der beteiligten Haushalte, aber auch zu einer wesentlich schnelleren Aufbereitung der Daten in den Statistischen Ämtern. Während bei der EVS 1993 nach den Vermögensverhältnissen der betreffenden Haushalte erst beim letzten Interview gefragt wurde, ist die Erhebung dieser Angaben für 1998 im ersten Interview vorgesehen. Das bisherige Verfahren löste einen zum Teil nicht unerheblichen Unmut der Betroffenen aus, da sie diesen Teil der Befragung bei der von ihnen gegebenen Einwilligung zur Teilnahme an der EVS nicht vorhersahen und andererseits ihre – wenn auch kleine – Vergütung für die Teilnahme an dieser Statistik nur erhalten konnten, wenn sie auch im letzten Interview diese mitunter heiklen Angaben machten.

Mit der Neukonzeption der im Jahre 1998 durchzuführenden EVS hat sich das im Jahresbericht 1997 angesprochene Problem bezüglich der EVS des Jahres 1993 erledigt.

**Erster Mietspiegel für die östlichen Bezirke Berlins**

*Im August des Berichtsjahres wurde der erste Mietspiegel für die Ostbezirke veröffentlicht. Als Datenbasis waren zunächst die Vermieter über die Vermieterverbände gebeten worden, möglichst maschinell Einzeldatensätze aus ihren Datenbeständen bereitzustellen. Um die Plausibilität dieser Angaben zur prüfen, befragten die Mieterverbände parallel und ebenfalls auf freiwilliger Grundlage Mieter. Dieses Verfahren führte zu einer breiten Datenbasis, so daß mehrere Hunderttausend Wohnungsdaten ausgewertet werden konnten.*

Zur datenschutzrechtlichen Darstellung der Datenerhebung zum Mietspiegel für die östlichen Bezirke (und West-Staaken) ist eine Stellungnahme entbehrlich.

Zur aus datenschutzrechtlicher Sicht angeregten rechtlichen Regelung der Erstellungsmethodik und des Verfahrens für künftige Mietspiegel besteht nur Handlungsbefugnis auf Bundesebene, weil der Bund seine im Rahmen der konkurrierenden Gesetzgebung gegebene Gesetzgebungsbefugnis mit § 2 Abs. 5

Die Erhebung bietet die Möglichkeit zu einer Angleichung und Zusammenführung des Mietspiegels Ost und des Mietspiegels West. Unsere Hinweise zur Gestaltung der Erhebungsbögen bei den Mietern als auch zur Anonymisierung der Einzelangaben wurden berücksichtigt, so daß der Datenbestand in seiner anonymisierten Form als eine Grundlage für künftige Mietspiegel mit genutzt werden kann. Damit stehen für künftige Stichprobenverfahren sowohl die Ergebnisse der Gebäude- und Wohnungszählung der Amtlichen Statistik aus dem Jahre 1995 als auch die Mietspiegelerhebung, mit der gut zwei Drittel des Ostberliner Wohnungsbestandes erfaßt wurden, zur Verfügung. Eine personen-, wohnungs- oder adreßbezogene Nutzung sowohl der Daten des Statistischen Landesamt als auch des Mietspiegels ist durch die Anonymisierungsmaßnahmen einerseits und durch die beschränkte Einwilligung der Betroffenen andererseits ausgeschlossen worden.

Die Erhebung zu dem 1998 zu veröffentlichenden Mietspiegel für die Westbezirke Berlins konnte ohne Datenschutzprobleme abgeschlossen werden, und der nächste Mietspiegel für die Ostberliner Bezirke befindet sich in der Vorbereitungsphase. Ein Festschreiben der Methodik für einen Mietspiegel in einer bundes- oder landesrechtlichen Vorschrift wäre aus unserer Sicht zu begrüßen. Dies würde auch die Möglichkeit bieten, durch Rechtsvorschrift die Ergebnisse des Mietspiegels gerichtsfest gegen Deanonymisierungsversuche zu schützen. Im Jahre 1997 wurde versucht, auf dem Klageweg Einzeldaten, die zur Erstellung eines Mietspiegels genutzt wurden, zu deanonymisieren und deren Herausgabe zu erzwingen. In unserer diesbezüglicher Stellungnahme konnten wir aber feststellen, daß durch die Einwilligungserklärung der Betroffenen ein solches Verfahren ausgeschlossen ist.

## 4.6 Wirtschaft

### 4.6.1 Banken und Versicherungen

**Scoring-Verfahren**

*Bei der Beantragung von Kreditkarten, Kundenkarten oder auch kleinerer Konsumentenkredite waren verschiedene Kunden von Finanzdienstleistungsunternehmen überrascht darüber, in welchem Umfang personenbezogene Daten über sie erhoben und gespeichert wurden. Unter anderem wurden folgende Daten erfragt:*

- *Nationalität,*
- *Familienstand,*
- *Anzahl der unterhaltspflichtigen Kinder,*
- *schon vorhandener Besitz von EC-Karten oder Kreditkarten (mit Nummernangabe)*
- *Wohnstatus (wohnhaft zur Miete/bei den Eltern, in Haus-/Wohneigentum),*
- *Name des Arbeitgebers, Branche, seit wann dort beschäftigt,*
- *Beruf,*
- *ausgeübter Beruf,*
- *monatliche Abzahlungen.*

Die Abfrage dieser Daten dient der *Bonitätsüberprüfung.* Das *Finanzdienstleistungsunternehmen* benötigt Angaben, um feststellen zu können, ob es mit dem Antragsteller einen Vertrag eingehen möchte. Da es bei der Ausgabe von Kunden- und Kreditkarten bzw. bei der Gewährung von Konsumentenkrediten grundsätzlich auch schon während der Vertragsanbahnung innerhalb des berechtigten Interesses des Finanzdienstleistungsunternehmens liegt, daß es das Ausfallrisiko und die Bonität (Zahlungsfähigkeit) des Antragstellers beurteilen kann, unterliegen Bonitätsangaben der Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses. Die Abfrage der Bonitätsdaten muß sich jedoch am Verhältnismäßigkeitsgrundsatz (Erforderlichkeit) orientieren. Dies war so lange unstreitig, wie die Finanzdienstleistungsunternehmen eine am Einzelfall orientierte Überprüfung der Kreditwürdigkeit des Kunden durchführten.

Inzwischen ist es aber üblich, bei der Bonitätsüberprüfung ein *Scoring-Verfahren* durchzuführen, bei dem die Antworten zu den soziodemographischen und auch anderen Fragen in einem

MHG wahrgenommen hat. Gemäß § 2 Abs. 5 Satz 4 MHG ist die Bundesregierung ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates Vorschriften über den näheren Inhalt und das Verfahren zur Aufstellung und Anpassung von Mietspiegeln zu erlassen. Eine solche Rechtsverordnung hat die Bundesregierung – nach Prüfung – vor längerer Zeit für nicht erforderlich erklärt.

Im Rahmen der Diskussion über eine grundlegende Mietrechtsnovellierung wird auch vorgeschlagen, die Bundesregierung zu verpflichten, durch Rechtsverordnung mit Zustimmung des Bundesrates Vorschriften über den näheren Inhalt und das Verfahren zur Aufstellung und Anpassung von Mietspiegeln zu erlassen (s. Bericht der Bund-Länder-Arbeitsgruppe „Mietrechtsvereinfachung“ zur Neugliederung und Vereinfachung des Mietrechts mit Textvorschlägen [hier § 560 c Abs. 5 BGB – Vereinfachungsentwurf]). Im Rahmen solcher Rechtsverordnung könnte auch die datenschutzrechtliche Problematik gelöst werden.

mathematisch-statistischen Verfahren verarbeitet werden. Einzelne erhobene Daten werden dabei häufig nur in Kombination und Abhängigkeit mit anderen Daten gewichtet. Das Ergebnis dieses Prozesses wird in sog. Score-Punkten ausgedrückt und gibt an, mit welcher Risikowahrscheinlichkeit statistisch gesehen bei dem jeweils beantragten Produkt – in der Regel einem Darlehen – damit gerechnet werden muß, daß dieses nicht zurückgezahlt werden kann.

Die Einfügung des Scoring-Verfahrens sollte nicht dazu führen, daß die bisher aus § 28 BDSG abgeleitete Verpflichtung der Finanzdienstleister, nur Daten im Rahmen der Erforderlichkeit abzufragen, nun mit dem Hinweis aufgehoben wird, die Daten würden wegen einer (nicht nachprüfbaren, einige Finanzdienstleister berufen sich bei der Gewichtung der erhobenen Daten auf das Betriebsgeheimnis) statistischen Relevanz zur Bonitätsprüfung benötigt. Selbst wenn man bei jedem erhobenen Datum in den uns bekannten Fällen eine mathematisch-statistische Bedeutung für eine abstrakte Bonitätsanalyse unterstellt, scheint der Umfang der zur Zeit von verschiedenen Finanzdienstleistern erhobenen Daten (auch bei kleineren Warenkrediten) eher auf eine um sich greifende *„Scoring-Wut“* als auf eine Datenerhebung, die sich am Erforderlichkeitsgrundsatz orientiert, hinzudeuten.

Für die *Durchführung rechtmäßiger Scoring-Verfahren* sollten die Finanzdienstleistungsunternehmen folgende Aspekte berücksichtigen:

Der Datenumfang sollte sich orientieren an der *Art des Vertrages*, den der Finanzdienstleister mit dem jeweiligen Kunden abzuschließen beabsichtigt. Hieran halten sich nicht diejenigen Finanzdienstleister, die etwa bei kleinen von ihnen finanzierten Ratenkäufen die gleichen Daten abfragen wie bei Kunden- und Kreditkarten, obwohl das Risiko des Kreditgebers bei einem Ratenkauf durch die ständige Reduzierung der Forderung durch die zu bezahlenden Raten deutlich geringer ist.

Finanzdienstleister sind gerne bereit, Kunden Kreditkarten, Kundenkarten und Warenkredite zu gewähren. Die geringen Voraussetzungen hierfür stehen in einem deutlichen Kontrast zu dem Umfang der abgefragten Daten. Zu fordern ist, daß die Datenabfrage darauf beschränkt wird, festzustellen, ob der jeweilige Kunde den von der Bank jeweils festgesetzten Mindeststandard für das jeweilige Produkt erfüllt (Abfrage der Knock-out-Kriterien).

Die Erhebung einzelner Daten erscheint, auch wenn hierdurch das mathematisch-statistische Verfahren der Banken behindert wird, durch die Erhebung anderer Daten an Bedeutung verlieren. So könnten etwa die Daten „Höhe des Monatseinkommens“, „Höhe der Monatsraten anderer Kredite“, „Anzahl der unterhaltspflichtigen Kinder“ und ähnliche Daten ersetzt werden durch ein zusammenfassendes Datum wie „Verfügbares monatliches Einkommen“.

Einige Daten werden nur erhoben, um das bisherige Verfahren zu verfeinern *(Testlauf)*. Für die Berechnung des Score-Werts des Antragstellers werden diese Daten nicht benötigt. Datenerhebungen zur Verfeinerung des Scoring-Verfahrens ohne konkrete Verwendung sind rechtswidrig. Die Datenverarbeitung ist nicht im Rahmen der Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen erforderlich, eine Anwendung des § 28 Abs. 1 Nr. 2 BDSG scheitert an den überwiegenden schutzwürdigen Interessen des Betroffenen, dessen Daten ohne sein Wissen zur Verfeinerung des von dem Finanzdienstleister durchgeführten Scoring-Verfahrens verwendet werden.

Für bestimmte besonders sensible Daten sollte ein *„Scoring-Verbot“* gelten. Dies gilt etwa für Religionszugehörigkeit, Gesundheitsdaten, aber auch die Staatsbürgerschaft. Es erscheint nicht hinnehmbar, daß Ausländer wegen ihrer jeweiligen Nationalität schlechter beurteilt werden als etwa Deutsche, nur weil nach statistischen Erhebungen die Nationalität des Betroffenen auf eine schlechtere Bonität hindeutet. Bezüglich des Arbeitsverhältnisses sollte es dem Finanzdienstleister ausreichen, daß der Kunde in einem unbefristeten Arbeitsverhältnis steht. Es erscheint aber unverhältnismäßig, wenn im Scoring-Verfahren durch eine Frage nach der Branche die Chance auf dauerhafte Beschäftigung

gescort wird. Hierdurch werden „allein auf Grund statistischer Überlegungen“ Kunden, die in Risikobranchen wie Bergbau oder Stahlindustrie arbeiten, gegenüber anderen benachteiligt.

In der Regel werden die Kunden nicht darüber informiert, wozu ihre personenbezogenen Daten abgefragt werden.

Obwohl es im Rahmen der Novellierung des Bundesdatenschutzgesetzes voraussichtlich erst im kommenden Jahr eine Spezialnorm für automatisierte Einzelentscheidungen wie Scoring-Verfahren geben wird, ist es schon jetzt ein Element des informationellen Selbstbestimmungsrechts, daß der Betroffene über die Tatsache einer automatisierten Einzelentscheidung und über die bei der Einzelentscheidung zu berücksichtigenden Kriterien hingewiesen wird.

**Lotto-Förderung durch Bankenfusion?**

*Ein Lotterie-Unternehmen aus Nordrhein-Westfalen schickte Werbematerial an Bürger aus den neuen Ländern. An das Werbeschreiben war eine Einzugsermächtigung angeheftet, auf der die Bankleitzahl und die Kontonummer des Beworbenen aufgedruckt war. Besonders überrascht waren die betroffenen Bürger darüber, daß die Lottogesellschaft ihre aktuelle Bankverbindung kannte, obwohl diese im Rahmen einer Sparkassenfusion erst vor wenigen Tagen geändert worden war.*

Ein Berliner Rechenzentrum führt für die *Sparkassenorganisation* in den neuen Bundesländern Datenverarbeitungsaufgaben durch. Eine der Aufgaben des Rechenzentrums ist es, die in den neuen Ländern häufig durchgeführten Sparkassenfusionen EDV-mäßig zu betreuen. Zwei Monate vor einer Fusion werden von dem Rechenzentrum sogenannte *Großeinreicher* (z. B. Rentenrechnungsstelle, Bundesanstalt für Arbeit, Versicherungen, aber auch Lottogesellschaften) darüber informiert, welche Banken von der Fusion betroffen sind. Die Großeinreicher haben nunmehr die Möglichkeit, alte Bankleitzahlen und Kontonummern (ohne Namensbezug) an das Rechenzentrum zu übersenden. Das Rechenzentrum übermittelt daraufhin die neue Kontonummer und die neue Bankleitzahl für das jeweilige Konto. Sofern es sich bei den geänderten Kontonummern und Bankleitzahlen bei den jeweiligen Großeinreichern um Kundenkonten handelt und das Vertragsverhältnis zu dem Kunden fortbesteht, bestehen gegen die oben dargestellte Verfahrensweise keine Bedenken. Es liegt sowohl im berechtigten Interesse der speichernden Stelle (der Sparkasse) als auch eines Dritten (des Großeinreichers), daß der Zahlungsverkehr zwischen den fusionierten Banken und dem Großeinreicher durch die Fusion nicht behindert wird. Insoweit ist das Verfahren auch im Interesse des Betroffenen, da auch er ein Interesse an einem funktionierenden Zahlungsverkehr hat.

Die Großeinreicher haben allerdings die Möglichkeit, sämtliche ihnen bekannten alten Kontonummern und Bankleitzahlen von dem Rechenzentrum in neue Kontonummern und Bankleitzahlen transferieren zu lassen, also auch die Kontonummern und Bankleitzahlen von Kunden, die vor vielen Jahren ihre Geschäftsbeziehungen zu dem jeweiligen Großeinreicher abgebrochen haben, oder z. B. von Personen, die einen Briefwechsel mit dem Großeinreicher führten und deren Bankverbindung etwa auf dem Briefbogen ersichtlich war.

Von der Werbemaßnahme der Lottogesellschaft waren insbesondere Bürger betroffen, die vor vielen Jahren einmal Kunden der Gesellschaft gewesen waren. Teilweise ließ sich allerdings nicht ermitteln, wie die Lottogesellschaft in den Besitz der alten Bankverbindung gelangt ist.

Die Übermittlung der neuen Bankverbindung von Kunden, die nicht oder nicht mehr Kunden der Lottogesellschaft waren, erfolgte rechtswidrig. Die Datenübermittlung liegt weder im berechtigten Interesse der Sparkassen noch der Lottogesellschaft. Demgegenüber haben die betroffenen Bürger ein überwiegendes schutzwürdiges Interesse daran, daß nur Unternehmen, mit denen sie im Geschäftskontakt stehen, ihre neue Bankverbindung erhalten. Wir haben das Rechenzentrum und die verantwortlichen Sparkassen aufgefordert, das Verfahren zu ändern.

Die Großeinreicher sollten vertraglich verpflichtet werden, nur Bankverbindungen von aktuellen Kunden an das Rechenzentrum zur Erlangung der neuen Bankverbindung zu übersenden. Die vertragliche Verpflichtung sollte durch eine Vertragsstrafenklausel und durch Stichprobenkontrollen bestärkt werden.

**Ein unverbindliches Kreditzertifikat als Datensammelinstrument**

*Ein Kreditinstitut führte eine bundesweite Werbeaktion durch, bei der Kunden und Nichtkunden der Bank angeboten wurde, sich sofort Klarheit über ihren Kreditspielraum zu verschaffen. Nach der Beantwortung von fünf Fragen (Alter, Dauer des Beschäftigungsverhältnisses, Anzahl der Personen im Haushalt, Haushaltsnettoeinkommen, Höhe der regelmäßigen monatlichen Zahlungsverpflichtungen) würde die Bank jedem Interessenten ein Kreditzertifikat erstellen. Die Fragen konnten schriftlich auf einem „Gutschein für Ihr persönliches Kreditzertifikat" oder direkt am Schalter beantwortet werden.*

Die Werbung erweckte den Eindruck, daß der Betroffene nach Erhalt des Kreditzertifikats über ein konkretes Kreditangebot der Bank verfügt, welches er bei Bedarf verwenden kann. Eine derartige Interpretation entspricht auch dem Sinn des Wortes „Zertifikat". Erst dem Kleingedruckten eines dem Gutschein beigefügten Faltblatts konnte entnommen werden, daß das Kreditzertifikat für die Bank keine Bindungswirkung hat. Da nicht zu erwarten ist, daß alle Interessenten, die den Gutschein ausgefüllt haben, vorher das *Kleingedruckte* des Faltblatts gelesen haben, muß davon ausgegangen werden, daß viele Betroffene in der Erwartung die ausgefüllten Gutscheine an die Bank übersandt haben, hierfür ein für die Bank bindendes Zertifikat zu erhalten. Auch Interessenten, die die auf dem Gutschein vorgegebenen Fragen gegenüber Bankmitarbeitern beantworteten, wurden nicht auf den *unverbindlichen Charakter des Kreditzertifikats* hingewiesen. Diese Information wurde erst bei der Übergabe des Kreditzertifikats gegeben.

Da das Kreditinstitut wegen der ungenügenden Information der Interessenten davon ausgehen mußte, daß diese ihre personenbezogenen Daten in der falschen Erwartung preisgaben, eine bindende Kreditzusage zu erhalten, widersprach die so durchgeführte Datenerhebung dem Grundsatz von Treu und Glauben und war somit rechtswidrig (§ 28 Abs. 1 Satz 2 BDSG).

**Ein überraschendes Angebot**

*Der PKW eines Petenten wurde gestohlen und später von den Dieben mit schweren Beschädigungen abgestellt. Der Petent ließ den von der Polizei gefundenen PKW in eine Werkstatt bringen und bat seine Versicherung um Regulierung des Schadens. Einige Tage später erhielt er zu seiner Überraschung von einem Verwertungsunternehmen ein Angebot zum Kauf des beschädigten PKWs. Er bat um Prüfung, wie das Verwertungsunternehmen in den Besitz seines Namens gelangt ist und Angaben zum Halter des PKWs erhalten hat.*

Um die Höhe des Schadens beim PKW festzustellen, beauftragte die Versicherung einen Sachverständigen, ein Gutachten über die Schadenshöhe zu erstellen. Wenn der Sachverständige feststellt, daß der Wert des PKWs nach erfolgter Reparatur nicht höher ist als die Kosten der Reparatur, müßte der Restwert des PKWs eigentlich auf Null gesetzt werden. Da aber auch beschädigte Wagen häufig einen nicht unbeträchtlichen Restwert haben, bittet der Sachverständige Verwertungsunternehmen, Restwertangebote zu machen. Das höchste Restwertangebot wird dann als Restwert des beschädigten Wagens angesetzt.

Bei hohem Restwert ist es üblich, daß das Verwertungsunternehmen den beschädigten PKW in Augenschein nimmt. Um dem Verwertungsunternehmen die Fahrzeugidentifizierung zu erleichtern, wurde diesem unter anderem der Name des Fahrzeughalters mitgeteilt. Wir haben den Sachverständigen darauf hingewiesen, daß es zur Fahrzeugidentifizierung in der Regel ausreicht, wenn dem Verwertungsunternehmen das amtliche Kennzeichen des PKWs sowie der Standort mitgeteilt wird. Nur in dem Ausnahmefall, daß ein Fahrzeug ohne Kennzeichen abgestellt ist und weitere Informationen zur Fahrzeugidentifizierung (Farbe, genauer Standort) etwa wegen der Größe der Werkstatt nicht zu einer sicheren Fahrzeugidentifizierung führen (eventuell unter Hilfe eines Mitarbeiters der Werkstatt), ist der Sachverständige berechtigt, den Namen des Fahrzeughalters bekanntzugeben.

**Schweigepflichtentbindungserklärung**

Bei der *Regulierung von Personenschäden* benötigen Versicherungen in der Regel Informationen des behandelnden Arztes.

Dieser darf nur dann Aussagen über den bei seinem Patienten eingetretenen Personenschaden machen, wenn und soweit sein Patient ihn von der *ärztlichen Schweigepflicht* (§ 203 Abs. 1 Nr. 1 StGB) befreit hat. Die Versicherungen dürfen nur Fragen an den Arzt richten, die von der Schweigepflichtentbindungserklärung gedeckt sind. Da diese häufig vom juristisch nicht geschulten Betroffenen persönlich formuliert wurden, sind sie oft mißverständlich. Wir empfehlen deshalb Versicherungen, in Zweifelsfällen den betroffenen Bürger noch einmal zu bitten, die von der Versicherung verwendete Standarderklärung zu unterzeichnen.

Die Versicherung darf auch bei weitgehender Schweigepflichtentbindungserklärung nur Fragen an den Arzt richten, die zur Regulierung des Personenschadens erforderlich sind. Eine Versicherung verwendete in ihrem Standardfragebogen folgende Frage: „Haben Sie die verletzte Person bereits vor diesem Unfall behandelt, wenn ja, wann und weshalb?“

Die Versicherung gab an, daß sich diese Frage ausschließlich auf Krankheiten oder Verletzungen beziehen sollte, die in einem ursächlichen Zusammenhang mit dem geltend gemachten Personenschaden stehen. Dieser kausale Zusammenhang läßt sich jedoch dem Wortlaut der Frage nicht entnehmen. Die Frage erweckt vielmehr den Anschein, als solle der behandelnde Arzt über alle Behandlungen berichten, die in der Zeit vor dem Unfall durchgeführt wurden. Die Versicherung hat unsere Anregung aufgegriffen und die von uns kritisierte Frage wie folgt umformuliert: „An welchen Krankheiten hat Ihr(e) Patient(in) vor dem Unfall gelitten, die den aktuellen Befund beeinflussen oder überlagern?“

**Handwerk in der Informationsgesellschaft**

*Die Handwerkskammer Berlin bat uns um Auskunft, ob datenschutzrechtliche Bedenken dagegen bestehen, daß ein Teil der in der Handwerksrolle erfaßten Daten – Namen, Anschrift, Telefonnummer, Gewerk, Spezialisierung – in einer separaten Datenbank für Nutzer aus dem Internet zur Verfügung gestellt werden. Über eine Suchmaske, bei der ein potentieller Kunde mindestens zwei Kriterien, z. B. Stadtteil und Gewerk/Gewerbe eingeben muß, sollte der Internetnutzer eine zufällige und auf fünf Adressen beschränkte Auswahl an eingetragenen Gewerbebetrieben erhalten. Diese Dienstleistung soll potentiellen Auftraggebern die Möglichkeit geben, sich eine Übersicht über die lokalen Handwerksbetriebe zu verschaffen.*

Die Eingabe von Datenbanken ins Internet, die jedermann frei zugänglich sind, ist datenschutzrechtlich unbedenklich. Allerdings dürfen die Daten der Handwerksrolle nur unter den einschränkenden Voraussetzungen des § 6 Handwerksordnung (HandwO) übermittelt werden. So darf gemäß § 6 Abs. 3 HandwO eine Einzelauskunft aus der Handwerksrolle nur jemandem erteilt werden, der ein *berechtigtes Interesse* glaubhaft darlegt. Bei einer listenmäßigen Übermittlung muß der Auskunftsbegehrende gemäß § 3 Abs.1 Satz 2 HandwO ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegen, und es darf außerdem kein Grund zu der Annahme bestehen, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. Gemäß § 6 Abs. 5 HandwO darf der Empfänger die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Da auch öffentliche Stellen Zugang zum Internet haben, ist auch die Einschränkung des § 6 Abs. 4 HandwO zu beachten. Öffentlichen Stellen sind nur auf Ersuchen Daten aus der Handwerksrolle zu übermitteln, soweit die Kenntnis tatsächlicher oder rechtlicher Verhältnisse selbständiger Handwerker zur Erfüllung ihrer Aufgabe erforderlich ist. Die Prüfung dieser rechtlichen Voraussetzungen für die Auskunftserteilung aus der Handwerksrolle ist bei Abfragen über das Internet bisher nicht möglich. Sie würde voraussetzen, daß der Anfragende sich identifiziert und mit Hilfe einer digitalen Signatur authentifiziert. Die rechtlichen Voraussetzungen dafür hat der Bundesgesetzgeber zwar mit dem seit August 1997 geltenden Signaturgesetz und der Signaturverordnung[161] geschaffen, die entsprechenden Instanzen und Produkte sind aber noch nicht verfügbar. Auch müßte durch Ver-

In der Angelegenheit wurde im Rahmen der Zuständigkeit die Handwerkskammer zu dem dargestellten Sachverhalt um eine Äußerung gebeten. Die Handwerkskammer hat zunächst darauf hingewiesen, daß sie in allen datenschutzrechtlichen Fragen stets und regelmäßig vorab die Kooperation mit dem Datenschutzbeauftragten suche. Zu dem konkreten Sachverhalt hat sie mit Schreiben vom 16. April 1998 mitgeteilt, daß sie an dem Vorhaben, eine entsprechende Datenbank im Internet einzurichten, festhalte, jedoch – die Anregungen des Datenschutzbeauftragten aufgreifend – alle Betriebe im Rahmen ihrer Jahresumfrage auf die einzurichtende Datenbank hingewiesen hat und Eintragungen nur auf ausdrücklichen Antrag der einzelnen Handwerker vornehmen wird. Bisher seien etwa 7 500 entsprechende Anträge gestellt worden. Der Zugriff auf die Datenbank wird voraussichtlich ab Mai 1998 möglich sein.

161 vgl. oben 3.3

schlüsselung sichergestellt werden, daß die Auskunft nicht mit der Bekanntgabe im Internet weltweit veröffentlicht und damit auch Personen ohne berechtigtes Interesse zugänglich würde.

Es bestehen dennoch keine datenschutzrechtlichen Bedenken gegen eine Interneteinspeisung, wenn die betroffenen Handwerker hierzu vorher eine formgültige Einwilligungserklärung abgegeben haben. Da für das von der Handwerkskammer vorgesehene Verfahren keine gesetzliche Grundlage zur Verfügung steht, ist allerdings das Vorliegen einer Einwilligungserklärung des Betroffenen auch erforderlich. Der von der Handwerkskammer vorgeschlagene Hinweis auf eine Widerspruchsmöglichkeit in einem Mitteilungsblatt reicht demgegenüber nicht aus.

### 4.6.2 Verkehrsunternehmen

**BahnCard**

Das BahnCard-Verfahren[162] hat sich in der Praxis bewährt. Bei der Umsetzung des Verfahrens kam es allerdings vereinzelt zu Datenschutzverstößen.

> *Ein Petent war beispielsweise darüber erbost, daß sein bei der Deutschen Bahn AG eingereichter Antrag von dieser an die CCO geschickt wurde, dort aber angeblich nicht eingegangen war. Auch sein zweiter Antrag blieb erfolglos, da er angeblich vergessen hatte, alle Unterlagen (Paßbild) mitzuliefern. Bei einer ihm kurz vorher zugegangenen Eingangsbestätigung hatte man ihn nicht darauf aufmerksam gemacht, daß der Antrag unvollständig gewesen sei.*

Bei derartigen Eingaben handelt es sich um Einzelfälle, die sich in keinem Massenverfahren ausschließen lassen. Wir haben der Deutschen Bahn AG allerdings empfohlen, folgende Verbesserungen des BahnCard-Verfahrens herbeizuführen:

Auf dem BahnCard-Antrag wird für die BahnCard pur auch dann das genaue *Geburtsdatum* abgefragt, wenn es nicht für bestimmte Vergünstigungen (z. B. Seniorenkarte) benötigt wird. Dies wird von der Deutschen Bahn AG damit begründet, daß die CCO die Datenerfassung durch getrennte Einscannung einerseits der Antragsdaten und andererseits des Bildes des Kunden vornimmt und – um das Bild anschließend wieder den restlichen Daten zuordnen zu können – auf der Rückseite des Bildes ein Code, aber auch das Geburtsdatum als zusätzliche Identifikation notiert werden. Wir haben die Deutsche Bahn AG aufgefordert, das Geburtsdatum nicht mehr für technische Zwecke zu erheben, zumal es möglich sein muß, andere Verfahren mit gleicher Zuordnungssicherheit zu schaffen.

Nach Erstellung der BahnCard werden die personenbezogenen Daten der BahnCard-Inhaber auch dann nicht sofort von der Citibank gelöscht, wenn der Karteninhaber keine automatische Verlängerung nach einem Jahr beantragt hat. Die Löschung erfolgt erst zwölf Monate nach Ablauf der Kartengültigkeit. Die lange Nachspeicherdauer wurde von der Deutschen Bahn AG, in deren Auftrag die CCO die Daten speichert, mit technischen Problemen erklärt. Nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Danach dürfen die Daten so lange gespeichert werden, wie sie im Rahmen des Nachvertragsverhältnisses benötigt werden. Bei der BahnCard erscheint eine Nachspeicherdauer von einem halben Jahr angemessen zu sein, da in dieser Zeitspanne erfahrungsgemäß Neuanträge gestellt werden und evtl. Nachfragen der Betroffenen oder rechtliche Auseinandersetzungen bezüglich der abgelaufenen BahnCard möglich sind. Die Deutsche Bahn AG hat inzwischen eine *Verkürzung der Nachspeicherdauer* entsprechend unseren Vorgaben veranlaßt.

Wir haben die Deutsche Bahn AG darauf aufmerksam gemacht, daß Punkt 9 der „Wesentlichen Bestimmungen der Deutschen Bahn AG zum Gebrauch der BahnCard“ offenbar von vielen Bürgern mißverstanden wird. Dort heißt es: „Ich willige ein, daß diese Gesellschaft zur Aufnahme und Abwicklung des BahnCard-Vertrages meine Antragsdaten erhält, verarbeitet und

162 JB 1995, 3.1

speichert.“ Teilweise gehen Kunden davon aus, daß die Abwicklung mit der Erstellung der BahnCard endet. Teilweise wurde zumindest mit der sofortigen Löschung der Daten nach Ablauf der Geltungsdauer der BahnCard gerechnet. Wir haben der Deutschen Bahn AG empfohlen, diese Mißverständnisse durch eine genauere Formulierung bei einer Neuauflage des BahnCard-Antragsformulars auszuräumen.

### 4.6.3 Werbung contra Markt- und Meinungsforschung

**Konsumentenbefragungen mit allen Tricks**

*Von Adreßhändlern und Direktwerbeunternehmen wurden mehrere bundesweite Konsumentenbefragungen durchgeführt. Per Wurfsendung oder per Post wurden Bürger mit der Bitte angeschrieben, zahlreiche Fragen über ihr Konsumverhalten und über ihre persönliche Lebenssituation unter Angabe ihres Namens und ihrer Anschrift zu machen. Bei den uns vorliegenden Fragebögen wurden unter anderem Angaben darüber abgefragt, welche Tageszeitung der Adressat liest, welche Whiskymarke er bevorzugt, wie hoch das jährliche Monatseinkommen ist und ob man bei einer Krankenversicherung auch Wert darauf legt, daß Kosten einer Psychotherapie übernommen werden. Außerdem wurde erfragt, an welchen Glücksspielen man teilnehme, welche Hobbys und Sportarten man betreibe, welche Kreditkarte man besitze und ob man zu Spenden bereit sei. Insgesamt enthielten die Bögen fast hundert Fragen.*

Derartige Umfragen dienen dazu, Konsumdaten an interessierte Unternehmen insbesondere für *Werbemaßnahmen* zu verkaufen. Personenbezogene Datensätze sind umso teurer, je detailliertere Informationen sie über die betreffende Person enthalten.

Wer an einer derartigen Befragung teilnimmt, die in der Regel mit einem Gewinnspiel verbunden wird, muß damit rechnen, daß seine personenbezogenen Daten von einer Vielzahl von Unternehmen für Werbezwecke verwendet werden. Zusätzliche Risiken entstehen, wenn die Daten international gehandelt werden. In den USA etwa bietet die Marketing-Industrie z. B. personenbezogene Daten über deutsche Verbraucher zum Kauf an, die für Werbezwecke weltweit genutzt werden können. Schon das deutsche Datenschutzgesetz privilegiert den Adressenhandel in bedenklicher Weise. In den USA dagegen ist Datenschutz gerade im Marketing-Bereich nahezu ein Fremdwort.

Um die Bürger zur Ausfüllung des Fragebogens zu bewegen, wird nicht nur ein Gewinnspiel angeboten. Häufig versuchen die Adreßhändler schon bei der Benennung ihres Unternehmens, das Vertrauen der Bürger zu erlangen. So nannte sich ein Adreßhändler wie ein renommiertes Sozialforschungsinstitut, ein anderer benutzte einen Namen, der von einer kleinen Veränderung abgesehen dem einer bekannten Wohlfahrtsorganisation entsprach.

Irreführend war auch der vom einem Adreßhändler benutzte Begriff „*Große Haushaltsumfrage in Deutschland*“. Der Begriff „Haushaltsumfrage“ wird von der Amtlichen Statistik bei der Durchführung des Mikrozensus verwendet. Beim Mikrozensus werden ebenso wie bei den ansonsten üblichen Umfragen Daten zum Zwecke der Übermittlung in anonymisierter Form gespeichert. Da der Begriff „Haushaltsumfrage“ auf Markt- und Meinungsforschung mit anonymisierten Daten hindeutet, nicht jedoch auf eine Datenerhebung von Adreßhändlern, ist die o. g. Überschrift mißverständlich.

Auch der teilweise verwendete Hinweis, daß die Angaben ausgewertet und für Marketing- und Marktanalysen verwendet werden, verschafft dem Befragten noch keine Klarheit über die von den Adreßhändlern beabsichtigte Verwendung der personenbezogenen Daten. Die Begriffe „Auswerten“ und „Marktanalyse“ deuten darauf hin, daß der Fragebogenersteller ein mit anonymisierten Daten arbeitendes Marktforschungsinstitut ist. Der Begriff „*Marketing*“ wird im Duden[163] wie folgt definiert: „Ausrichtung eines Unternehmens auf die Förderung des Absatzes durch Werbung, Beobachtung und Lenkung des Marktes sowie durch entsprechende Steuerung der eigenen Produkte“. Auch dieser Begriff, über dessen genaue Bedeutung viele betroffene

163 Deutsches Universalwörterbuch A – Z Mannheim 1989

Bürger keine genaue Vorstellung haben dürften, macht nicht deutlich, daß die Daten in nicht-anonymisierter Form verwendet werden sollen. Denkbar wäre auch, daß interessierten Unternehmen Marktanalysen zur Verfügung gestellt werden sollen, um ihre Werbestrategie mit Hilfe der anonymisierten Angaben der Bürger zu überarbeiten.

Die bisher durchgeführten Konsumentenbefragungen erfüllten nicht die Anforderungen, die an solche Umfragen zu stellen sind. So muß für die Befragten klar erkennbar sein, daß die Angaben nicht nur anonym, sondern auch personenbezogen ausgewertet und für welche Zwecke sie verwendet werden. Zur Erklärung der Zwecke sollten Begriffe wie *„Persönlich adressierte Werbung“*, *„Adreßhandel“* etc. benutzt werden. Umfangreiche Datenerhebungen im Rahmen einer Haushaltsumfrage erfordern die schriftliche Einwilligung des Betroffenen. Sofern der Fragebogen auch Familienangehörige betrifft, müssen auch diese – soweit Volljährigkeit bzw. Einsichtsfähigkeit vorliegt – zustimmen. Sofern die Einwilligungserklärung im Fragebogentext enthalten ist, ist die Erklärung im äußeren Erscheinungsbild hervorzuheben (vgl. § 4 Abs. 2 Satz 3 BDSG).

**Die wirkliche Markt- und Meinungsforschung**

Angesichts des Ideenreichtums, mit dem Adreßhändler an Daten aus dem Lebensumfeld der Bürger heranzukommen versuchen, beklagen Markt- und Meinungsforschungsinstitute, aber auch die Sozialforschung, daß die Bereitschaft der Betroffenen zur Beteiligung an seriösen Erhebungen sinkt. Noch gibt es keinen „blauen Engel“, an dem man solide arbeitende Unternehmen der Markt- und Meinungsforschung erkennen kann. Doch diese Idee halten wir in keiner Weise für abwegig und werden sie mit den Interessensverbänden der Markt- und Meinungsforschungsinstitute diskutieren.

Ein Merkmal der klassischen Markt- und Meinungsforschung ist, daß die Teilnahme des Betroffenen im Regelfall nicht honoriert wird. Steht der Adreßhandel oder die Vermarktung bestimmter Produkte im Mittelpunkt der Datenerhebung, so ist dies häufig mit Gewinnversprechungen verbunden. Im Unterschied dazu versuchen die Markt- und Meinungsforschungsinstitute durch Information über den Zweck der Befragung, jedoch kaum durch den Verweis auf einen Gewinn, die Betroffenen zur Mitarbeit zu bewegen. Die Markt- und Meinungsforschungsinstitute geben des weiteren bereitwillig darüber Auskunft, wie bei ihnen die *Anonymisierung* erfolgt. Adreßhändler sind dagegen gerade am Erhalt des Personenbezugs interessiert. Für einen bestimmten Zeitraum besteht zwar auch bei der Markt- und Meinungsforschung die Notwendigkeit, die unmittelbar identifizierenden Angaben, wie Namen und Anschrift oder die Telefonnummer zu speichern, aber die Institute können häufig sehr präzise mitteilen, wann diese Daten von den Erhebungsmerkmalen getrennt und wann sie gelöscht werden.

Dies gilt auch für den Fall, daß die Betroffenen gebeten werden, in eine Wiederholungsbefragung beispielsweise in einem halben Jahr einzuwilligen. Wir prüften dies in einem großen Institut, das in Berlin über 90 Arbeitsplätze für *Telefoninterviewer* verfügt. Die Interviewer sind vertraglich auf den Datenschutz verpflichtet und werden durch das Unternehmen entsprechend geschult. Wir prüften auch die entsprechenden Abfrageprogramme, mit denen dem Interviewer während des Interviews der dem Betroffenen mitzuteilende Text am Monitor eingeblendet wird. Der Interviewer gibt dann unmittelbar die Daten ein und hat die Möglichkeit, auf das Antwortverhalten des Befragten zu reagieren. So konnten wir nachvollziehen, wie im Falle der Einwilligung in ein Wiederholungsinterview die Telefonnummer gesondert gespeichert wird.

Mit ähnlichen Vorkehrungen werden auch *Haustürbefragungen* durch Interviewer durchgeführt. Die Interviewer kündigen sich häufig durch ein Informationsschreiben an und können sich sowohl durch einen Ausweis des Unternehmens als auch durch ihren Personalausweis ausweisen. Hier hat der Bürger zunächst eine einfache Kontrollmöglichkeit, indem er das entsprechende Markt- und Meinungsforschungsinstitut anruft und sich vergewissert, daß dieser Interviewer auch in dem betreffenden Gebiet Daten erhebt. Selbst dann ist niemand verpflichtet, einen Inter-

viewer in seine Wohnung zu lassen. Meist übergibt der Interviewer den entsprechenden Erhebungsbogen und holt ihn dann nach einigen Tagen wieder ab. Dazu muß natürlich gesondert die Anschrift und der Name notiert werden, wenn nicht das ganze Haus befragt werden soll. Häufig sind die Interviewer nach einem Begehungsplan tätig. Sie wählen beispielsweise an einem bestimmten Punkt beginnend jede 15. Wohnung aus und notieren den Namen und die Anschrift. Mit diesen Daten kann das Markt- und Meinungsforschungsinstitut nach der Erhebung stichprobenhaft überprüfen, ob der Interviewer die Befragung überhaupt durchgeführt oder was auch vorkommen soll, die Daten erfunden hat. Wir empfehlen bei einem solchen Vorgehen, den Betroffenen schon in den Informationsschreiben diese Verfahren transparent und verständlich zu erläutern.

Leider vertrat ein Markt- und Meinungsforschungsinstitut bei einer Befragung in Sanierungsgebieten die Auffassung, daß es genügt, den Betroffenen allgemein eine „absolute Anonymität“ zuzusichern. Da es aber offensichtlich war, daß die Interviewer sowohl den Namen als auch die Anschrift wenigstens zeitweise für die Durchführung des Verfahrens speichern mußten, sank die Akzeptanz zur Teilnahme an dieser Befragung erheblich, und Bürger wandten sich mit Eingaben an uns.

Einige Markt- und Meinungsforschungsinstitute beschäftigen sich mit der Frage, ob die Vorteile des *Internets* nicht auch für die Entwicklung neuer Umfragetechniken genutzt werden können. Neben einer Reihe von datenschutzrechtlich nicht relevanten Problemen, wie der fehlenden Repräsentativität, ist zu klären, wie bei solchen Umfragen die Anonymität durch ein entsprechendes Anonymisierungsverfahren gesichert werden kann. Hinzukommt, daß die Teilnahme an einer solchen Befragung ohne gesonderte Programmierung zu Lasten des Betroffenen geht, weil dieser die Internetnutzungsgebühren zu bezahlen hat. Daher werden solche Befragungen häufig mit begleitenden Werbemaßnahmen verbunden. Doch wie soll sich der Betroffene hier noch sicher sein, daß es sich um eine Befragung und nicht um eine Marketingmaßnahme handelt? Somit stellt sich das eingangs beschriebene Problem Markt- und Meinungsforschung oder Adreßhandel und Marketing auch bei Internetumfragen. Zu beachten ist auch, daß die seit August 1997 geltende *Multimedia-Gesetzgebung* des Bundes und der Länder[164] den Online-Diensteanbietern eine Verwendung von Bestands- oder Nutzungsdaten zur Befragung ihrer eigenen Kunden ohne deren ausdrückliche Einwilligung untersagt.

### 4.6.4 Datenverarbeitung für fremde Zwecke

**Das „Betreuungsverhältnis“ als wirtschaftliches Stigma**

*Kann ein Volljähriger auf Grund einer psychischen Krankheit oder einer körperlichen, geistigen oder seelischen Behinderung seine Angelegenheiten ganz oder teilweise nicht besorgen, so bestellt das Vormundschaftsgericht auf seinen Antrag oder von Amts wegen für ihn einen Betreuer. Wenn ein Betreuer unter Vorlage der Bestallungsurkunde eine SCHUFA-Selbstauskunft für den Betreuten beantragte, wurde das Merkmal „Betreuungsverhältnis“ in den Datenbestand der SCHUFA aufgenommen.*

Die SCHUFA hat eingeräumt, daß die ohne den Willen und das Wissen des Betreuers durchgeführte Speicherung des Merkmals „Betreuungsverhältnis“ rechtswidrig erfolgte, da das Interesse des Betroffenen an der Nichtspeicherung und -übermittlung des Datums (es handelt sich letztendlich um ein Datum über gesundheitliche Verhältnisse) höher einzuschätzen ist als ein etwaiges Interesse eines potentiellen Geschäftspartners des Betreuten an der Kenntnis des Betreuungsverhältnisses.

Die SCHUFA hält allerdings an ihrer Praxis fest, bei einem entsprechenden Wunsch des Betreuers das Merkmal „Betreuungsverhältnis“ zu speichern. Dies diene dem Schutz des Betreuten.

Mit der Schaffung des neuen Betreuungsrechts wollte der Gesetzgeber erreichen, daß verbliebene Fähigkeiten des Betreuten berücksichtigt werden und in seine Rechte nur eingegriffen wird, soweit dies zu seinem Schutz erforderlich ist. Die Teil-

164 siehe oben 3.3

nahme des Betreuten am Rechtsverkehr wird anders als im Minderjährigenrecht, das eine *partielle Geschäftsfähigkeit* nicht kennt, nur in dem nach dem Grad seiner Behinderung erforderlichen Umfang eingeschränkt. Der Betreute benötigt für Rechtsgeschäfte nur insoweit die Einwilligung des Betreuers, als es zur Abwendung einer erheblichen Gefahr für den Betreuten erforderlich ist. Nur insoweit stellt das Vormundschaftsgericht den Betreuten unter „Einwilligungsvorbehalt". Der Betreute bleibt außerhalb des Einwilligungsvorbehalts voll geschäftsfähig.

Nach dem Sinn der §§ 1896 ff. BGB muß verhindert werden, daß sich ein Einwilligungsvorbehalt de facto wie die bisherige Entmündigung auswirkt. Weiß der Geschäftspartner nämlich von einem Einwilligungsvorbehalt, so wird er sich unabhängig von dessen Umfang aus Furcht vor den Folgen des § 105 Abs. 1 BGB (Verträge sind bis zur Einwilligung des Betreuers schwebend unwirksam) unmittelbar an den Betreuer halten. Die von dem Gesetz gewünschte Selbständigkeit des Betreuten wird so bei vielen Rechtsgeschäften unmöglich gemacht.

Um diese Konsequenz zu vermeiden, dürfte das Datum „Betreuungsmerkmal" nur dann an den Vertragspartner der SCHUFA übermittelt werden, wenn für das konkrete Rechtsgeschäft ein Einwilligungsvorbehalt bestehen würde. Da aber der Umfang des Einwilligungsvorbehalts sehr unterschiedlich ist, die Vertragspartner der SCHUFA aus den verschiedensten Bereichen (Banken, Versandhandel, Mobilfunkunternehmen) stammen, dürfte es praktisch kaum möglich sein, die Information über den Einwilligungsvorbehalt auf Rechtsgeschäfte zu beschränken, die unter den Vorbehalt fallen.

**Partnerschafts- und Heiratsvermittlung mit unlauteren Mitteln**

*Mehrere Eingaben betrafen Partnerschafts- und Heiratsinstitute. Einige Heiratsinstitute setzen Kontaktanzeigen in die Zeitung, die den Anschein erwecken, als würde sich eine Privatperson per Annonce um einen Partner bemühen. In Wahrheit gehen jedoch die personenbezogenen Daten der Interessenten, die auf diese Anzeige antworten, an ein Heiratsinstitut, obwohl der Interessent mit hoher Wahrscheinlichkeit nicht geantwortet hätte, wenn er den kommerziellen Zusammenhang erkannt hätte.*

Ein Heiratsinstitut, welches eine Privatanzeige vortäuscht, erhebt die personenbezogenen Daten der Interessenten rechtswidrig (§ 28 Abs. 1 Satz 2 BDSG). Nach dieser Norm müssen Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Speichert das Heiratsinstitut die personenbezogenen Daten des Interessenten, so erfolgt die Speicherung rechtswidrig.

Partnerschafts- und Heiratsinstitute versuchen in der Regel, Neukunden dadurch zu werben, indem sie in Anzeigen auf Personen hinweisen, für die sie einen Partner oder eine Partnerin suchen, von denen auf Grund der angegebenen Eigenschaften (solvent, großzügig, reicher Unternehmer, bildhübsch, 18 Jahre alt) davon ausgegangen werden kann, daß ein großes Interesse an den jeweiligen in der Anzeige erwähnten Partnersuchenden besteht. Interessiert sich etwa eine Frau für den in der Anzeige erwähnten solventen und großzügigen 62jährigen Unternehmer mit einem Haus auf Mallorca, der Interesse an Reisen und Kultur hat und eine zärtliche Frau sucht, und wird diese Frau auf Grund dieses Lockangebots Kunde des Heiratsinstituts, so erfolgt die im Zusammenhang mit dem Vermittlungsvertrag erfolgende Datenerhebung und -speicherung rechtswidrig, wenn der 62jährige Unternehmer *gar nicht im Kundenbestand* des Vermittlungsinstituts vorhanden wäre. Auch in diesem Fall wäre wiederum von einer treuwidrigen Datenerhebung auszugehen.

Partnerschafts- und Heiratsinstitute dürfen von ihren Kunden nur die Daten speichern, die sie im Rahmen der Zweckbestimmung des Vertragsverhältnisses mit dem Betroffenen benötigen. So müßte etwa ein Mann Angaben darüber machen, welche Eigenschaften seine „Traumpartnerin" haben müßte. Außerdem kann das Institut die personenbezogenen Daten des Kunden speichern, die es benötigt, um den Kunden angemessen vorstellen zu können. So dürfen etwa Daten wie Alter, Größe, Gewicht, vom

Kunden angegebene Charaktereigenschaften, finanzielle Verhältnisse erhoben und gespeichert werden. Die Datenerhebung sollte sich allerdings an dem Grundsatz der Verhältnismäßigkeit orientieren. Hiergegen verstieß ein Heiratsinstitut, welches einen Kunden einer etwa *zehnstündigen Befragung* aussetzte. Auch wurden von Heirats- und Partnerschaftsvermittlungen teilweise Daten gespeichert, die nicht für den Vertragsgebrauch benötigt werden, wie etwa die Personalausweisnummer.

Besondere Vorsicht bei der *„mobilen Partnerschaftsvermittlung“*. Wer Interesse an einem der in der Zeitung veröffentlichten Lockangebote hat, erfährt bei einer telefonischen Kontaktaufnahme nicht einmal dessen Anschrift. Diese findet sich auch nicht im Telefonbuch bzw. Branchentelefonbuch. In einer Art „Überrumplungsmanöver“ bieten sie dem Interessenten an, ihm umgehend einen Hausbesuch abzustatten. Dabei wird von dem Interessenten nicht nur ein Porträtbild und die Preisgabe zahlreicher personenbezogener Daten verlangt, sondern außerdem die sofortige Zahlung von 500,− DM.

Wir gehen in diesem Fall davon aus, daß von dem „mobilen Partnerschaftsinstitut“ die personenbezogenen Daten nur erhoben wurden, um das Interesse vorzugaukeln, man wolle dem Kunden einen Partner vermitteln. Auch eine derartige Datenerhebung ist selbstverständlich rechtswidrig.

## 4.7 Telekommunikation und Medien

### 4.7.1 Entwicklung des Telekommunikationsrechts

**Europäischer Telekommunikationsdatenschutz verbessert**

Nach mehr als siebenjähriger Vorarbeit und einem längeren Vermittlungsverfahren hat der Rat der Europäischen Union am 1. Dezember 1997 die *Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (früher: ISDN-Richtlinie)* angenommen[165]. Damit wird die allgemeine Datenschutzrichtlinie um eine wichtige sektorspezifische Harmonisierungsrichtlinie ergänzt. Das Bündel von Maßnahmen, das die Europäische Kommission 1990 – knapp ein Jahr nach einer entsprechenden Aufforderung der Internationalen Datenschutzkonferenz in Berlin – zur *Sicherstellung eines europaweiten Mindeststandards beim Datenschutz* vorgeschlagen hatte, hat jetzt erfreulicherweise – wenn auch mit erheblicher Verzögerung – die Hürden des europäischen Gesetzgebungsprozesses überwunden. Es kommt jetzt darauf an, die Telekommunikationsrichtlinie in Deutschland und den anderen Mitgliedstaaten in relativ kurzer Zeit umzusetzen, da die Anpassungsfrist zeitgleich mit der Frist für die Allgemeine Datenschutzrichtlinie am 24. Oktober 1998 endet.

Seit der Vorlage des ersten Entwurfs für eine ISDN-Richtlinie im Sommer 1990 haben die Europäischen Datenschutzbeauftragten auf unsere Initiative hin mehrfach detaillierte Vorschläge zum Richtlinienentwurf in den verschiedenen Stadien des Gesetzgebungsverfahrens gemacht[166]. Zuletzt hat die Konferenz der Europäischen Datenschutzbeauftragten im September 1997 in Brüssel eine schnelle Verabschiedung des Richtlinienentwurfs befürwortet[167], obwohl der Entwurf die Empfehlungen der Datenschutzbeauftragten nur zum Teil berücksichtigt[168].

Im Laufe des Vermittlungsverfahrens ist der wichtige *Grundsatz der Vertraulichkeit der Kommunikation* dadurch relativiert worden, daß eine Ausnahme für das rechtlich zulässige Aufzeichnen von Kommunikationen im Rahmen einer rechtmäßigen Geschäftspraxis zum Nachweis kommerzieller Transaktionen oder einer sonstigen geschäftlichen Kommunikation aufgenommen wurde. Die Erforderlichkeit dieser Ausnahmeregelung war im Vermittlungsverfahren bis zuletzt umstritten. Nach deutschem Recht bedarf das Mitschneiden von Gesprächen z. B. im Rahmen des *Telefon-Banking* schon jetzt der ausdrücklichen Einwilligung aller Beteiligten. Das Aufzeichnen von Gesprächsinhalten ohne diese Einwilligung verstößt auch im Geschäftsverkehr gegen das Fernmeldegeheimnis und ist möglicherweise strafbar.

165 vgl. JB 1996, 4.7.1
166 JB 1994, Anlage 3.4; JB 1995, Anlage 3.7
167 Anlage 3.2
168 vgl. JB 1996, 4.7.1

Außerdem wurde in die jetzt angenommene Telekommunikationsrichtlinie auf Vorschlag Frankreichs gegen den ursprünglichen Widerstand des Europäischen Parlaments eine Regelung aufgenommen, wonach die Mitgliedstaaten den Betreibern gestatten können, bei der Veröffentlichung von gedruckten oder elektronischen Teilnehmerverzeichnissen von Teilnehmern, die ihre Daten *nicht* in derartigen Verzeichnissen veröffentlichen lassen wollen, *die Zahlung einer kostenorientierten Gebühr* zu verlangen. Diese Regelung verpflichtet den deutschen Gesetzgeber nicht dazu, das bisher geltende Telekommunikationsrecht zu Lasten der Teilnehmer zu verschlechtern. Die deutsche Regelung, wonach jeder Telefonkunde kostenlos und ohne Begründung seine Veröffentlichung in gedruckten oder elektronischen Teilnehmerverzeichnissen unterbinden kann, hat sich bewährt und sollte beibehalten werden.

Bereits bis Ende 1997 war die *Richtlinie vom 30. Juni 1997 über die Zusammenschaltung in der Telekommunikation im Hinblick auf die Sicherstellung eines Universaldienstes und der Interoperabilität durch Anwendung der Grundsätze für einen offenen Netzzugang (Zusammenschaltungs-Richtlinie)*[169] umzusetzen. Diese Richtlinie hat besondere Bedeutung für den liberalisierten Sprachtelefondienstmarkt. Sie sieht vor, daß die Mitgliedstaaten die Wahrung der Vertraulichkeit von übertragenen oder gespeicherten Informationen in allen Organisationen sicherstellen, die ihre Einrichtungen mit öffentlichen Telekommunikationsnetzen zusammenschalten. Die Mitgliedstaaten können darüber hinaus in *Zusammenschaltungsvereinbarungen* zwischen Netzbetreibern Bedingungen für den Datenschutz als grundlegende Anforderung auferlegen, um die Einhaltung der Vorschriften über den Datenschutz, die Vertraulichkeit übertragener oder gespeicherter Informationen und den Schutz der Privatsphäre sicherzustellen.

In einer dritten Richtlinie haben das Europäische Parlament und der Rat am 20. Mai 1997 Regelungen über den *Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz (Fernabsatz-Richtlinie)*[170] getroffen. Darin ist in Übereinstimmung mit der Telekommunikationsrichtlinie vorgesehen, daß Telefaxgeräte und Voice-Mail-Systeme nur bei vorheriger Einwilligung des Adressaten für Zwecke des *Direktmarketings* eingesetzt werden dürfen. Andere Formen der Telekommunikation, insbesondere der Sprachtelefondienst, dürfen nur dann nicht für Werbezwecke verwendet werden, wenn der Verbraucher dies offenkundig abgelehnt hat *(opt-out-Lösung).* Darüber hinaus eröffnet die Telekommunikationsrichtlinie den Mitgliedstaaten die Möglichkeit, das Telefonmarketing von der ausdrücklichen Einwilligung der angerufenen Teilnehmer abhängig zu machen *(opt-in-Lösung).* Außerdem verlangt die zuletzt genannte Richtlinie den gebührenfreien Schutz vor unerbetenen Anrufen.

Mit zunehmender Nutzung der *elektronischen Post* wird auch dieses Medium zur Versendung von unaufgeforderter Werbung eingesetzt. In den USA hat die sogenannte *junk mail (spamming)* zu einer erheblichen Beeinträchtigung des Netzverkehrs geführt. In Deutschland hat sich erstmals ein Gericht dafür ausgesprochen, die bisherigen Grundsätze zur unerwünschten Telefon-, Telefax- und Btx-Werbung auch auf E-mail-Werbung zu übertragen[171]. Dies erscheint konsequent, zumal die Überprüfung und Leerung des „elektronischen Briefkastens“ beim Nutzer Zeit- und Kostenaufwand verursachen. Häufig wird E-mail-Werbung auch nicht von vornherein als solche gekennzeichnet, so daß sie erst geladen und gelesen werden muß, um überhaupt den Werbecharakter zu erkennen. Darin liegt nicht nur eine Belästigung des Nutzers, sondern auch ein Eindringen in seine Privatsphäre, gegen das er sich effektiv schützen können muß. Die EG-Fernabsatzrichtlinie schreibt zwar nur eine opt-out-Lösung in diesem Bereich vor, hindert den deutschen Gesetzgeber aber nicht, mit einer opt-in-Lösung einen darüber hinausgehenden Datenschutz vorzusehen.

Im Dezember 1997 hat die Europäische Kommission ein *Grünbuch zur Konvergenz der Branchen Telekommunikation, Medien und Informationstechnologie und ihren ordnungspolitischen Auswirkungen – ein Schritt in Richtung Informationsgesellschaft*[172] veröffent-

169 ABl. EG Nr. L 199, 32
170 ABl. EG Nr. L 144, 19
171 Landgericht Traunstein, Beschluß vom 14. Oktober 1997 – 2 HKO 3755/97
172 KOM (97) 623 endg.; Ratsdok. 13289/97; BR-Drs 1064/97

licht. Damit wird ein europaweiter Konsultationsprozeß zu einem zukünftigen Regelungsrahmen für die zusammenwachsenden Bereiche der Telekommunikation, der Medien und der Informationstechnologie eröffnet. Während bisher auf europäischer Ebene vorwiegend Regelungen zum Datenschutz im Telekommunikationsbereich auf der *Transportebene* getroffen wurden, fehlen entsprechende Regelungen für den Rundfunkbereich (z. B. für die Ausgestaltung von Decodern für das digitale Fernsehen) weitgehend. Dagegen ist der Datenschutz in Deutschland bereits jetzt zum großen Teil *konvergenzfest* in der Weise geregelt, daß zumindest im Kern die gleichen Datenschutzgrundsätze für alle genutzten Dienstearten (Telekommunikation-, Tele-, Mediendienste und Rundfunk) gelten. Insbesondere unterliegen Informationen über die Nutzung dieser Dienste entweder dem Fernmeldegeheimnis, oder sie dürfen nicht ohne Einwilligung des Betroffenen zu einem Nutzungsprofil zusammengeführt werden. Differenzen gibt es allerdings hinsichtlich der anonymen oder pseudonymen Nutzungsmöglichkeit, die in digitalen Telekommunikationsnetzen (bisher) nicht möglich ist, dagegen bei Tele- und Mediendiensten zumindest als eine Option vorgeschrieben und beim Rundfunk die Regel ist. In dem Maße, wie zukünftig unterschiedliche Dienste in verschiedenen Netzen (also z. B. Rundfunk nicht nur in Kabelnetzen, sondern auch über das Telekommunikationsnetz) verbreitet werden, wird die Aufrechterhaltung eines hohen konvergenzfesten Datenschutzstandards auch auf europäischer Ebene entscheidend. Ein hoher einheitlicher Datenschutzstandard ist keine Barriere für das Zusammenwachsen der verschiedenen Dienstearten, sondern vielmehr eine seiner Voraussetzungen. Auch das digitale Fernsehen wird von den Zuschauern nur akzeptiert werden, wenn sie – wie beim herkömmlichen Fernsehen – sicher sein können, daß ihr Sehverhalten nicht unbemerkt registriert wird.

Die Europäische Kommission hat sich im Oktober 1997 in einer *Mitteilung über Sicherheit und Vertrauen in elektronische Kommunikation – ein europäischer Rahmen für digitale Signaturen und Verschlüsselungen –*[173] für die Entwicklung harmonisierter Regelungen zum Einsatz digitaler Signaturen und zur inhaltlichen Verschlüsselung ausgesprochen. Dabei hat die Kommission die Bedeutung des Datenschutzes und der Vertraulichkeit hervorgehoben und betont, daß in der Informationsgesellschaft Bürger und Unternehmen, die für immer mehr Aspekte ihres Lebens und ihrer Geschäftstätigkeit Online-Dienste benutzen, es vorziehen werden, in der *anonymen Offline-Welt* zu bleiben, wenn sie befürchten müssen, daß ihre Kommunikation und Transaktionen im Netz mit Hilfe von Schlüsselhinterlegungssystemen, die das Überwachungspotential der Behörden stärken, übermäßig kontrolliert werden[174]. Die Kommission strebt die Vorlage einer europäischen Richtlinie zur digitalen Signatur 1998 und die Inkraftsetzung eines gemeinsamen Rahmens im Bereich der Kryptographie bis zum Jahr 2000 an[175].

Bereits im März 1997 hat der Ministerrat der *Organisation für wirtschaftliche Entwicklungs- und Zusammenarbeit* (OECD) eine Empfehlung zu weltweit gültigen *Richtlinien für eine Kryptographie-Politik* beschlossen, in der die Mitgliedstaaten zur Förderung von Verschlüsselungsverfahren aufgefordert und acht Grundprinzipien zum Einsatz der Kryptographie formuliert werden. Dazu zählen das Recht des Nutzers, ein Verschlüsselungsverfahren seiner Wahl einsetzen zu können, und die Bedeutung derartiger Verfahren für die Gewährleistung eines effektiven Datenschutzes. Der OECD-Ministerrat weist allerdings auch auf die möglichen neuen Risiken für den Persönlichkeitsschutz hin, die durch Datensammlungen entstehen können, die im Zuge einer notwendigen Sicherheitsinfrastruktur für digitale Signaturen angelegt werden müssen. In der Frage des Zugriffs der Sicherheitsbehörden auf Schlüsselduplikate enthalten die OECD-Richtlinien keine eindeutige Festlegung, allerdings fordern sie die Regierungen zu einer sorgfältigen Abwägung zwischen dem Schutz der Privatsphäre der Nutzer und den Interessen der Strafverfolgungsbehörden auf. Eine generelle Pflicht zur voraussetzungslosen Hinterlegung von Zweitschlüsseln ist damit jedenfalls nicht vereinbar.

173 KOM (97) 503 endg.
174 vgl. auch die Meinungsumfrage Eurobarometer 46.1 über die Privatsphäre in der Informationsgesellschaft, 1/97
175 vgl. oben 3.3

Auch die *Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat in einer Gemeinsamen Erklärung zur Kryptographie* Stellung genommen[176] und die OECD-Leitlinien begrüßt. In ihrer Gemeinsamen Erklärung bekräftigt die Internationale Arbeitsgruppe die Forderung, daß zur Sicherstellung der Vertraulichkeit jedem Teilnehmer elektronischer Telekommunikationsdienste ermöglicht werden muß, seine Nachrichten auf einem von ihm frei zu wählenden Niveau zu verschlüsseln. Die Durchsetzung auch in Deutschland erörterter gesetzlicher Verpflichtungen, nur bestimmte, zugelassene (weil von den Sicherheitsdiensten überwindbare) Schlüssel zu benutzen, würde zu einer Umkehrung des bisherigen Verhältnisses von grundsätzlicher Vertraulichkeit und ausnahmsweise erlaubtem Zugriff auf den Inhalt der Kommunikation führen. Zudem sind alle entsprechenden Regelungen und Lizenzierungserfordernisse mit geringem technischem Aufwand zu umgehen.

**Liberalisierung des deutschen Sprachtelefondienstes**

Zum Zeitpunkt der Veröffentlichung dieses Jahresberichts wird das Monopol der Deutschen Telekom AG für den Sprachtelefondienst im Festnetz der Vergangenheit angehören. Verschiedene Wettbewerber – darunter auch regionale Anbieter – versuchen gegenwärtig, sich auf diesem Markt zu etablieren. Die Abschaffung des Sprachtelefondienst-Monopols hat zunächst zu einer erheblichen Verunsicherung der Kunden angesichts einer verwirrenden Vielfalt unterschiedlicher Tarifmodelle geführt. Hinsichtlich der Geltung der datenschutzrechtlichen Bestimmungen hat sich allerdings nichts geändert: Die Datenschutzvorschriften des Telekommunikationsgesetzes (TKG) sowie der Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV)[177] gelten auch für die neu hinzukommenden Anbieter von Telekommunikationsdienstleistungen unverändert fort. Hinzu kommt seit Anfang 1998 die Telekommunikations-Kundenschutzverordnung[178], die ebenfalls datenschutzrechtliche Regelungen enthält.

Die derzeit geltende TDSV basiert noch auf einer Ermächtigungsgrundlage aus dem Post- und Telekommunikationsregulierungsgesetz (PTRegG), das im Rahmen der Postreform II erlassen worden war[179]. Diese Vorschrift des PTRegG ist mit dem Inkrafttreten des Telekommunikationsgesetzes[180] durch den § 89 TKG ersetzt worden. Damit ist die TDSV in ihrer jetzigen Form novellierungsbedürftig geworden. Die Bundesregierung hat jedoch bisher noch keinen Entwurf für eine neue Datenschutzverordnung in diesem Bereich vorgelegt. Hier soll die Verabschiedung der ISDN-Richtlinie der Europäischen Union abgewartet werden, um die Rechtsvorschriften der Datenschutzverordnung in einem Zug sowohl an das TKG als auch an die Bestimmungen der ISDN-Richtlinie anpassen zu können. Diese Richtlinie ist mittlerweile verabschiedet worden[181]. Es steht zu hoffen, daß der Gesetzgeber bei dieser Gelegenheit eine Anpassung an die datenschutzfreundlichen Regelungen des Informations- und Kommunikationsdienste-Gesetzes sowie des Mediendienste-Staatsvertrages vornehmen wird. So sollte auch für Telekommunikationsdiensteanbieter eine Verpflichtung zur datenarmen Gestaltung ihrer Dienste eingeführt werden. Darüber hinaus halten wir nach wie vor im Hinblick auf den Schutz des Angerufenen bei Einzelverbindungsnachweisen die Einführung des „holländischen Modells“ für wünschenswert, bei dem jeder Teilnehmer selbst entscheiden kann, ob seine Rufnummer bei Einzelverbindungsnachweisen des Diensteanbieters ausgewiesen werden soll.

**Begleitgesetz zum Telekommunikationsgesetz**

Zum Telekommunikationsgesetz wurde 1997 ein Begleitgesetz geschaffen[182]. Das Gesetz enthält in seinem Artikel 2 zahlreiche Änderungen von Rechtsvorschriften für die – so die Amtliche Begründung des Entwurfs – „. . . erforderliche Schließung von Strafbarkeitslücken bei der Verletzung des Post- und Fernmeldegeheimnisses sowie die *Sicherstellung der Überwachung von Telekommunikation* durch die dazu berechtigten Behörden . . .“

Der Senat bittet um Verständnis dafür, daß zu Detailfragen innerhalb eines Gesetzgebungsverfahrens keine Stellungnahme abgegeben wird. Die angesprochenen Problemstellungen sind und werden im weiteren Verfahren von den Berliner Vertretern in den zuständigen Gremien berücksichtigt.

176 Anlage 5
177 vgl. dazu JB 1996, 4.7.1
178 Telekommunikations-Kundenschutz-Verordnung v. 11. Dezember 1997, BGBl. I, 2910
179 BGBl. 1994 I, 2325; dazu JB 1994, 5.1
180 BGBl. 1996, I, 1120; dazu JB 1996, 4.7.1
181 vgl. oben 3.3
182 BGBl. 1997 I, S. 3108

Dahinter verbirgt sich die Änderung bzw. Ergänzung einer Vielzahl von Rechtsvorschriften um Regelungen zur Überwachung des Post- und Telekommunikationsverkehrs, die zum Teil in der redaktionellen Anpassung, zum Teil aber auch in der Schaffung neuer Eingriffsbefugnisse bestehen.

Gleichzeitig werden Strafvorschriften hinsichtlich der Verletzung des Post- oder Fernmeldegeheimnisses auf bei privaten Dienstleistungsunternehmen beschäftigte Mitarbeiter ausgedehnt.

Aus Datenschutzsicht von besonderer Bedeutung war die vorgeschlagene Änderung der Strafprozeßordnung (StPO) durch einen neuen § 99 a, der die *Übermittlung von Bestands- und Verbindungsdaten an die Strafverfolgungsbehörden* im Rahmen von Strafermittlungsverfahren regelt und diese unter einen Richtervorbehalt stellt. Wir hatten bereits in den vergangenen Berichtsjahren immer wieder auf die Notwendigkeit der Ersetzung des § 12 Fernmeldeanlagengesetz (FAG) hingewiesen[183].

Der Innenausschuß des Bundesrates hat in seinen Empfehlungen für die Beschlußfassung im Bundesrat[184] die vorgeschlagenen Eingriffsbefugnisse nochmals verschärft: So wurde vorgeschlagen, das Gesetz zur Einschränkung des Artikels 10 Grundgesetz (G 10) derart zu erweitern, daß die Identifikation der von einer Person benutzten Anschlußnummer durch technische Maßnahmen auch dann ermöglicht werden sollte, wenn dabei das Fernmeldegeheimnis unbeteiligter Dritter technisch bedingt unvermeidbar beeinträchtigt wird. Hierzu verweist der Innenausschuß auf die sog. *„IMSI-Catcher“*, die technisch in der Lage sind, derartige Funktionen auszuführen. Beim IMSI-Catcher handelt es sich um ein Gerät, das in GSM-basierten Mobilfunknetzen eine Basisstation simuliert und die von den Funktelefonen abgestrahlten Funkwellen auffangen kann, um so die netzinterne Rufnummer zu ermitteln. Zusätzlich gibt es auch Versionen des Geräts, die es zugleich ermöglichen, den Inhalt des Gesprächs mitzuhören, ohne daß die Betroffenen davon erfahren. Die Technik dieser Geräte bedingt es aber, daß möglicherweise auch Dritte, die sich in der Nähe des Verdächtigen mit einem anderen Fernmeldegerät aufhalten, in die Fernmeldeüberwachung einbezogen werden.

Darüber hinaus schlug der Innenausschuß des Bundesrates vor, die Regelung des bisherigen § 12 FAG unverändert als neuen § 99 a StPO ohne die von der Bundesregierung vorgesehenen Beschränkungen zu übernehmen. Wir haben gegenüber den Berliner Vertretern im Bundesrat eine umfangreiche Stellungnahme zum Begleitgesetz zum Telekommunikationsgesetz abgegeben. Dabei haben wir unter anderem die Legalisierung des Einsatzes von IMSI-Catchern zur Strafverfolgung abgelehnt. Es ist im Hinblick auf den Verhältnismäßigkeitsgrundsatz der Verfassung nicht hinnehmbar, wenn durch den Einsatz derartiger Geräte regelmäßig in Kauf genommen wird, daß in das Fernmeldegeheimnis unbeteiligter Dritter eingegriffen wird. Darüber hinaus haben wir empfohlen, den ursprünglichen Vorschlag der Bundesregierung hinsichtlich des § 99 a StPO mit einigen Änderungen zu übernehmen, anstatt einfach den bereits jetzt verfassungsrechtlich bedenklichen § 12 FAG dem Inhalt nach in die Strafprozeßordnung zu integrieren. Der Bundesrat hat in seiner Stellungnahme die Vorschläge des Innenausschusses des Bundesrates dennoch größtenteils übernommen.

Zwar ist im Laufe der weiteren Beratung des Begleitgesetzes die Regelung zum Einsatz von IMSI-Catchern wieder gestrichen worden, jedoch ist es wiederum nicht gelungen, den § 12 FAG durch eine verfassungskonforme Regelung in der Strafprozeßordnung zu ersetzen: Dieser soll nunmehr weiter in Kraft bleiben und nicht, wie ursprünglich vorgesehen, zum 31. Dezember 1997 außer Kraft treten. Allerdings hat der Innenausschuß des Bundestages die Bundesregierung aufgefordert, bis spätestens April 1998 eine verfassungskonforme Lösung hinsichtlich des geplanten § 99 a StPO zu finden. Eine Verlängerung des § 12 FAG über das Jahr 2000 hinaus wird vom Innenausschuß explizit abgelehnt.

183 vgl. zuletzt JB 1996, 4.7.1
184 BR-Drs 369/1/97 vom 23. August 1997

### 4.7.2 Einzelne Dienstleistungen

**Kundendaten in Verzeichnissen**

Die TDSV räumt den Kunden in § 10 Abs. 3 ein differenziertes Wahlrecht dahingehend ein, der Eintragung ihrer Daten in *elektronischen oder allgemein in gedruckten öffentlichen Kundenverzeichnissen* des Diensteanbieters ganz oder teilweise zu widersprechen. Einträge von Kunden, die von diesem Recht Gebrauch gemacht haben, sollten in den Teilnehmerverzeichnissen gesondert gekennzeichnet werden. Zweck der Vorschrift war es insbesondere, die Kunden gegen die Aufnahme ihrer Daten in elektronische Verzeichnisse (z. B. CD-ROM) zu schützen.

Diese Kennzeichnung ist allerdings bei der Herausgabe der Telefonbücher für das Jahr 1997/98 unterblieben. Statt der gesetzlich vorgesehen *Kennzeichnung der Einzeldatensätze* hat die Telekom vielmehr in die Teilnehmerverzeichnisse einen allgemeinen Hinweis eingefügt, daß in den Verzeichnissen Datensätze von Kunden enthalten sein könnten, die der Veröffentlichung ihrer Daten in elektronischen Verzeichnissen widersprochen haben. Die Telekom hat dies damit begründet, daß durch die Kennzeichnung von Einzeldatensätzen ein neuer, sensibler Datenbestand entstehen könne. Darüber hinaus stünde die Regelung der TDSV im Widerspruch zu den Bestimmungen des § 89 Abs. 8 TKG, die einen Eintrag in öffentliche gedruckte oder elektronische Verzeichnisse nur nach Maßgabe des Antrags des Kunden zulassen.

Dieses scheinbar datenschutzfreundliche Vorgehen der Telekom kann nur unzureichend verdecken, daß es hier wohl weniger um den Schutz der Kunden vor Diskriminierung als mehr um die Sicherung eines Wettbewerbsvorteils gegenüber mißliebigen Konkurrenten bei der Veröffentlichung elektronischer Teilnehmerverzeichnisse geht. Daß die Telekom hierzu eine für sie geltende Datenschutzbestimmung unterläuft, ist nicht akzeptabel. Der Bundesbeauftragte für den Datenschutz hat die Telekom unterdessen auf die Verpflichtung zur Einhaltung der Bestimmungen des § 10 Abs. 3 TDSV hingewiesen. Es bleibt abzuwarten, ob die Telekom bei der Veröffentlichung der nächsten Auflage der Telefonbücher ihre datenschutzrechtlichen Verpflichtungen dann vollständig umsetzen wird.

Der oben geschilderte Vorgang steht im direkten Zusammenhang zu den zahlreich am Markt angebotenen *Telefonbüchern auf CD-ROM*, deren Leistungsumfang ständig vergrößert wird. Wir hatten bereits im vergangenen Berichtszeitraum auf die Datenschutzproblematik dieser Verzeichnisse hingewiesen[185]. Die dort geschilderten Probleme sind mittlerweile durch neue Leistungsmerkmale beispielsweise der Version 4 des Produkts *D-Info* (D-Info 97) der Firma Topware erheblich verschärft worden: So ist es mittlerweile auch möglich, die in den Teilnehmerverzeichnissen eingetragenen personenbezogenen Daten von Kunden (wie Name, Adresse usw.) auf Grund von nur unvollständig bekannten Telefonnummern aufzufinden. Durch diese Suchmöglichkeit kann insbesondere die aus Datenschutzgründen bisher praktizierte Verkürzung von Einzelverbindungsnachweisen der Deutschen Telekom AG unterlaufen werden.

Nachdem der Deutschen Topware Service GmbH der Vertrieb der CD-ROM „D-Info 3.0“ vom Oberlandesgericht Karlsruhe aus urheberrechtlichen Gründen[186] untersagt worden war und das entsprechende Verfahren unterdessen in der Revision beim Bundesgerichtshof anhängig ist, wird die „D-Info 97“ jetzt von der Topware CD-Service Ges.mb.H. mit Sitz im österreichischen Riezlern im Kleinen Walsertal angeboten. Dadurch sollen offensichtlich die rechtlichen Schwierigkeiten des Angebots in Deutschland umgangen werden. Das Landgericht Mannheim hat jedoch unterdessen am 8. Juli 1997 wieder eine einstweilige Verfügung, diesmal gegen die österreichische Gesellschaft, erlassen.

**Komfortauskunft – wenig komfortabel für die Betroffenen**

Im Sommer 1997 lieferte die Telekom ein Lehrstück an mißlungener datenschutzrechtlicher Öffentlichkeitsarbeit: Als Beilage zur Telefonrechnung für den August 1997 wurde ein Faltblatt verschickt, in dem unter dem Titel „Bei der Auskunft tut sich was“

185 vgl. zuletzt JB 1995, 4.3

186 Oberlandesgericht Karlsruhe, Beschluß v. 25. September 1996 – 6 U 46/96 in Datenschutzberater 12/96, S. 14

auf neue und künftige Informationsdienste der Deutschen Telekom hingewiesen wurde. Unter dem Stichwort „Komfortauskunft“ informierte die Telekom in diesem Faltblatt über ihre Absicht, künftig gegen Entgelt neben Rufnummern auch *Adressen und Berufsbezeichnungen über die telefonische Auskunft* zu übermitteln.

§ 11 Abs. 3 TDSV sieht vor, daß über die Rufnummern hinausgehende Auskünfte der in Teilnehmerverzeichnissen veröffentlichten Daten dann erteilt werden können, wenn der Kunde mit einer weitergehenden Auskunftserteilung einverstanden ist. Darüber hinaus wird dem Diensteanbieter eine *Pflicht zur Information der Kunden* mittels einer der nächsten Fernmelderechnung beizulegenden Antwortkarte auferlegt. Das Einverständnis des Kunden gilt als erteilt, wenn er nicht innerhalb von vier Wochen eine entgegenstehende Erklärung abgibt.

Das oben geschilderte Vorgehen der Telekom ließ bei den Datenschützern in der gesamten Bundesrepublik die Telefone heißlaufen: Zum einen hatte die Telekom versäumt, in ihrem Faltblatt darauf hinzuweisen, daß sich die Komfortauskunft nur auf bereits in Telefonverzeichnissen veröffentlichte Daten bezieht, so daß Kunden, die ohne Anschrift und sonstige Angaben dort eingetragen sind, für die Komfortauskunft nach den gesetzlichen Bestimmungen von vornherein ausscheiden. Darüber hinaus wurde das Faltblatt während der Haupturlaubszeit verschickt, so daß viele Kunden erst nach Ablauf der vierwöchigen Frist diese Mitteilung überhaupt zur Kenntnis nehmen konnten.

Gleichzeitig ähnelte die Beilage von der äußeren Aufmachung her den sonst üblichen Werbebeilagen, so daß sie von vielen Bürgern achtlos weggeworfen wurde. Die Telekom hatte darüber hinaus versäumt, darauf hinzuweisen, daß ein Widerspruch gegen die Aufnahme von Daten in die Komfortauskunft *jederzeit* – also auch nach Ablauf der vierwöchigen Widerspruchsfrist – möglich ist (dies ist mittlerweile in einer späteren Beilage zur Fernmelderechnung erfolgt).

Dieses unüberlegte Vorgehen hat dazu geführt, daß eine große Anzahl von Kunden der Verwendung ihrer Daten für die Komfortauskunft bei der Telekom widersprochen hat: Bis zum Ende des Jahres 1997 waren dort mehr als eine Million Widersprüche eingegangen.

Darüber hinaus haben sich zahlreiche Kunden darüber beschwert, daß sie einer nachträglichen Zweckänderung ihrer Daten für die Auskunft ausdrücklich widersprechen müssen. Demgegenüber hätte man erwartet, daß eine solche Zweckänderung nur nach ausdrücklicher Einwilligung erfolgt wäre[187].

Es steht zu hoffen, daß die Telekom und andere Diensteanbieter im Telekommunikationsbereich für die Zukunft aus dieser mißglückten Aktion eine Lehre ziehen werden.

**Einzelverbindungsnachweisen mit vollständigen Zielnummern**

Verschiedentlich war in der Presse darüber berichtet worden, daß die Telekom die Einführung von Einzelverbindungsnachweisen mit vollständigen Zielnummern der angerufenen Anschlüsse plant. Für diese Form des Einzelverbindungsnachweises existiert bereits seit längerem eine gesetzliche Grundlage[188]; allerdings hatte die Telekom bisher aus Datenschutzerwägungen auf die Erstellung solcher Nachweise verzichtet, da insbesondere der *Schutz von Anrufen bei telefonischen Beratungsstellen* (wie etwa der Telefonseelsorge oder der Aids-Beratung) dadurch gefährdet wäre. Gleiches gilt, wenn ein Anschluß von mehreren Personen benutzt wird. Die Einführung von Einzelverbindungsnachweisen mit vollständigen Zielnummern soll jetzt Anfang 1998 erfolgen.

Hinsichtlich des Schutzes von Anrufen bei Beratungsstellen konnte in der Zwischenzeit bei der *Telefonseelsorge* eine Verbesserung erreicht werden: Die Beratungsstellen haben mittlerweile sog. „800“-Rufnummern erhalten, die von den Anrufern kosten-

187 entsprechend hatte sich der Berliner Datenschutzbeauftragte im Rahmen der Beratungen zur TDSV im Jahre 1995 geäußert, vgl. JB 1995, 4.3

188 vgl. § 6 Abs. 4, 7 TDSV

frei angewählt werden. Entsprechend werden die Anrufe bei diesen Einrichtungen auch nicht auf Einzelverbindungsnachweisen ausgewiesen.

Für den Inhaber eines normalen Telefonanschlusses bleibt es unbefriedigend, daß er – im Gegensatz etwa zu unseren holländischen Nachbarn – keinen Einfluß darauf haben soll, ob ein Anruf bei ihm auf dem Einzelgebührennachweis des Anrufers erscheint.

**Pornos aus dem Uninetz**

Rechtliche Probleme wirft die an allen Berliner Hochschulen übliche Eröffnung von *Zugängen zum Internet für Studenten und Hochschulmitarbeiter* auf. Der Internetzugang wird – bisher noch – kostenlos ermöglicht; dabei steht die Nutzung zu wissenschaftlichen Zwecken im Vordergrund, ohne daß in der Praxis eine private Nutzung ausgeschlossen wäre. Noch vor Inkrafttreten des Teledienstedatenschutzgesetzes wurde ein Arzt an einem Universitätsklinikum verhaftet, der im Verdacht steht, über seinen privaten Computer unter Nutzung des von der Hochschule zur Verfügung gestellten Internetzugangs Bilder und Videos mit *Kinderpornografie im Internet* verbreitet zu haben. Der Datenschutzbeauftragte der Humboldt-Universität hatte zuvor einen entsprechenden Hinweis von einem Außenstehenden, einem sogenannten *Net-Hunter,* erhalten, der News-Groups im Internet beobachtet, um strafbares Verhalten festzustellen. Daraufhin veranlaßte der Datenschutzbeauftragte der Hochschule eine umfassende Protokollierung sämtlicher Bewegungen des Verdächtigen im Netz. Nachdem sich der Verdacht erhärtet hatte, wurde Strafanzeige bei der Staatsanwaltschaft erstattet, die nach einer Hausdurchsuchung einen Haftbefehl gegen den Verdächtigen erwirkte.

Jeder Benutzer von universitären Zugängen zu Datennetzen wird in dieser Hochschule auf die Einhaltung einer *Computerbetriebsordnung* verpflichtet, wonach die Datennetze nur für Zwecke des Universitätsbetriebs in Forschung, Lehre und Verwaltung der Universität zu nutzen sind. Jeglicher Mißbrauch von Datennetzen, insbesondere strafbares Verhalten oder Verstöße gegen das Jugendschutz- oder Datenschutzrecht, sind zu unterlassen, zu verhindern bzw. dem Rechenzentrum der Hochschule zur Kenntnis zu geben. Auf die strafrechtliche Verantwortlichkeit wird ausdrücklich hingewiesen. Die Betreiber der Hochschulnetze sind außerdem berechtigt, bei konkreten Anhaltspunkten für schwere Verstöße gegen Nutzungsregeln personenbezogene Daten der Benutzer zu verarbeiten und zu nutzen. Die elektronische Post unterliegt dem Fernmeldegeheimnis. Eine Verarbeitung oder Nutzung der Nachrichteninhalte ist nur mit Einwilligung des Betroffenen zulässig. Der betroffene Arzt hatte außerdem bei der Beauftragung des Hochschulrechenzentrums ausdrücklich eingewilligt, daß seine Daten (wie auch die aller anderen Benutzer) in einer Protokolldatei gespeichert werden, die bei Rechtsverstößen im Beisein und unter Kontrolle des behördlichen Datenschutzbeauftragten zur Wahrung der Interessen der Hochschule verwendet werden darf.

Daß das Verhalten der Hochschule vor diesem Hintergrund datenschutzrechtlich nicht zu beanstanden war, wird auch durch die arbeitsrechtliche Rechtsprechung zur verdeckten Beobachtung von Arbeitnehmern gestützt. So ist die *verdeckte Videoüberwachung* von Arbeitnehmern dann für zulässig gehalten worden, wenn der Arbeitgeber konkrete Anhaltspunkte dafür hat, daß der Arbeitnehmer Straftaten begangen hat oder begeht, und dieser Verdacht nicht auf andere Weise aufgeklärt werden kann. Der Arbeitgeber muß es auch nicht hinnehmen, daß der Arbeitnehmer einen ihm zur Verfügung gestellten Zugang zum Internet für strafbare Handlungen nutzt.

Seit dem Inkrafttreten des Teledienstedatenschutzgesetzes am 1. August 1997 stellt sich allerdings die Frage, ob *Hochschulen*, die ihren Mitarbeitern und Studenten einen (kostenlosen) Zugang zum Internet ermöglichen, damit als *Anbieter von Telediensten* angesehen werden müssen. Dann nämlich wäre die beschriebene Verfahrensweise in dem Fall von Kinderpornographie jetzt nicht mehr zulässig. Zwar hat der Bundesgesetzgeber den Begriff des Teledienstes so umfassend definiert, daß jedes entsprechende Angebot unabhängig davon, ob es geschäftsmäßig oder gewerblich, kostenfrei oder gegen Entgelt gemacht wird, nach den

Der Senat teilt im wesentlichen die Ausführungen des Berliner Datenschutzbeauftragten zu dem Thema „Pornos aus dem Uni-Netz“. Hervorzuheben ist, daß zwar der betreffende Arzt Beschäftigter des Universitätsklinikums war, es sich jedoch bei dem betreffenden Internet-Zugang nicht um einen für alle Hochschulmitglieder des Universitätsklinikums nutzbaren gehandelt hat, sondern dieser Internet-Zugang für den Arzt in seiner Funktion als Beschäftigter der Humboldt-Universität zu Berlin eingerichtet und zur Nutzung zur Verfügung gestellt worden war. In dem Bericht wird ausdrücklich festgestellt, daß das Verhalten der Hochschule, insbesondere die Einholung der Einwilligung der Benutzer und Benutzerinnen in die Speicherung ihrer Daten in einer Protokolldatei datenschutzrechtlich nicht zu beanstanden war.

(siehe auch Stellungnahme zu 3.3)

Regeln des Teledienstedatenschutzgesetzes zu beurteilen ist. Das würde bedeuten, daß alle Verbindungsdaten unmittelbar nach Ende der Verbindung zu löschen wären, da eine Abrechnung nicht stattfindet. Die Einwilligung in die Speicherung von Nutzungsdaten dürfte den Nutzern nicht abverlangt werden, weil ihnen ein anderer kostenfreier Zugang – jedenfalls bisher – nicht möglich ist.

Dieses Beispiel macht deutlich, daß die neuen Datenschutzvorschriften für Teledienste (entsprechendes gilt für Mediendienste) nicht uneingeschränkt auf *Angebote eines Arbeitgebers oder Dienstherrn* an seine Beschäftigten bzw. einer Hochschule an ihre Studenten angewandt werden können. Wenn man überhaupt den Arbeitgeber bzw. die Hochschule in dieser Situation als Diensteanbieter im Sinne des Gesetzes verstehen will (was der Gesetzgeber offenbar nicht beabsichtigt hat), so ist doch zu berücksichtigen, daß sowohl der Beschäftigte als auch der Student gegenüber der Hochschule, an der sie tätig sind, in einem Rechtsverhältnis stehen, das weitergehende Verpflichtungen vorsieht. Diese Verpflichtungen, den eröffneten Zugang zum Internet nicht zweckzuentfremden und insbesondere nicht für strafbare Handlungen zu nutzen, gelten neben dem und zusätzlich zum Teledienstedatenschutzgesetz in der gleichen Weise, wie z. B. das Bundesdatenschutzgesetz für das Kontokorrentverhältnis beim Homebanking gilt. Allerdings müssen die Bediensteten, soweit sie über das Hochschulrechenzentrum Zugang zum Internet erhalten, auf die Möglichkeit hingewiesen werden, daß ihre Aktivitäten in diesem Bereich unter besonderen Ausnahmebedingungen auch ohne ihr Wissen überwacht werden können. Auch eine rechtzeitige Beteiligung der Personalvertretung ist in diesen Fällen notwendig. Entsprechend müssen auch die Studenten, die das Internet über Hochschulrechner nutzen, informiert werden. Eine lückenlose Protokollierung der Bewegungen von Mitarbeitern oder Studenten im Netz, ohne daß die Hochschule oder der Arbeitgeber Kenntnis von strafbaren Inhalten hat, ist dagegen unzulässig.

### 4.7.3 Telekommunikation in der Berliner Verwaltung

#### Abrechnung privater Telefongespräche

Im Berichtszeitraum ist die Abrechnung privater Telefongespräche und die damit verbundene Speicherung und sonstige Verarbeitung personenbezogener Daten in der Berliner Verwaltung auf eine gesetzliche Grundlage gestellt worden. Im Rahmen des Haushaltsstrukturgesetzes 1997[189] ist ein neuer § 5 in das *Informationsverarbeitungsgesetz* eingefügt worden, der die Abrechnung privater sowie die Kontrolle dienstlicher Nutzung kommunikationstechnischer Verbindungen regelt.

Danach ist im Regelfall für die Abrechnung *privater Telefongespräche* die Erstellung eines summarischen Nachweises vorgesehen. Beschäftigte, die dies wünschen, können allerdings auch einen Einzelverbindungsnachweis mit um die letzten vier Ziffern gekürzten Zielnummern erhalten.

Zur Kostenkontrolle von gebührenpflichtigen *Dienstgesprächen* darf eine Dienststelle Verbindungsdaten über die geführten Gespräche in Gruppen von in der Regel mehr als zehn Beschäftigten verarbeiten. Damit ist einerseits eine bessere Kostenverfolgung als in der Vergangenheit möglich; andererseits wird durch die gruppenweise Zuordnung der Gespräche eine Verhaltens- oder Leistungskontrolle ausgeschlossen, da keine Daten über das Telefonverhalten einzelner Mitarbeiter gespeichert werden.

Dies erfolgt nur in den Fällen, in denen ein Verdacht eines Dienstvergehens wegen mißbräuchlicher Nutzung dienstlicher Telekommunikationseinrichtungen für private Zwecke oder Verletzung entsprechender arbeitsvertraglicher Pflichten vorliegt. In diesen Fällen dürfen in einem abgestuften Verfahren über einen Zeitraum von längstens drei Monaten auch Daten über kleinere Gruppen von Beschäftigten bzw. über einzelne Beschäftigte gespeichert werden.

189 Gesetz zur Beseitigung des strukturellen Ungleichgewichts des Haushalts (Haushaltsstrukturgesetz) 1997, GVBl. S. 69

Der Berliner Datenschutzbeauftragte hat im Gesetzgebungsverfahren mehrmals zu den beabsichtigten Regelungen Stellung genommen; wir begrüßen, daß hier eine datenschutzfreundliche Regelung erreicht werden konnte.

Einzelheiten des Verfahrens sind in der *Verordnung über die Speicherung, die Löschung und sonstige Verarbeitung von Verbindungsdaten zur Abrechnung privater und Kontrolle dienstlicher Nutzung kommunikationstechnischer Verbindungen* vom 1. Juli 1997[190] geregelt. Gleichzeitig ist die *Rahmendienstvereinbarung* über den Einsatz und den Betrieb von digitalen Telefonnebenstellenanlagen zwischen der Senatsverwaltung für Inneres und dem Hauptpersonalrat novelliert worden[191]. Bedauerlicherweise haben die beteiligten Stellen es hier versäumt, den Berliner Datenschutzbeauftragten zu beteiligen.

Zur privaten Nutzung dienstlicher Telekommunikationsanlagen wurde zum Jahresende auch eine *Allgemeine Anweisung der Innenverwaltung*[192] erlassen. Sie greift leider eine Empfehlung nicht auf, die wir bereits zur vorherigen Verwaltungsvorschrift gegeben hatten: Bei der Abrechnung der privaten Entgelte kann nach wie vor ein Formular verwendet werden, bei dem die nachfolgenden Einzahler erkennen können, wie viele Privatgespräche die Mitarbeiter geführt haben, die ihr Entgelt bereits gezahlt haben. Dies verstößt gegen § 5 Abs. 2 BlnDSG.

*Eine Kontrolle der technischen und organisatorischen Maßnahmen bei den ISDN-Nebenstellenanlagen sowie der Ausgestaltung des Telefoneinsatzes bei den Patienten im Virchow-Klinikum führte zu recht unterschiedlichen Ergebnissen. Während die Maßnahmen zum Datenschutz bei den ISDN-Anlagen unzureichend waren, fiel die Bewertung des Telefoneinsatzes bei den Patienten um so besser aus.*

Für die Administration der Telekommunikationsanlagen steht ein Programm zur Durchführung der *Systemverwaltung* zur Verfügung, das den Zugriff über mehrere Berechtigungsstufen ermöglicht. Alle Systemverwalter verfügen jedoch nur über eine einzige Kennung mit identischem Paßwort einer mittleren Berechtigungsstufe. Eine Änderung dieses Paßwortes ist den Systemverwaltern – auch bei einem Mitarbeiterwechsel – nicht möglich. Ebenso ist den Systemverwaltern, und damit letztlich auch den Verantwortlichen, der Zugriff auf die Protokolle zur Kontrolle der Systemadministration und Wartung entzogen, denn dieses ist nur unter der höchsten Berechtigungsstufe möglich.

Diese höchste Berechtigungsstufe wird jedoch nur dem *Hersteller und Lieferanten* der Nebenstellenanlagen, der ebenfalls den Auftrag zur Wartung der Systeme hat, eingeräumt. Dessen Aktivitäten können aus den oben genannten Gründen von der datenschutzrechtlich verantwortlichen Stelle in keiner Weise nachvollzogen werden. Der Auftragnehmer verwehrt demzufolge dem Auftraggeber jegliche Kontrollmöglichkeit.

Dies ist ein *außerordentlicher Mangel der Organisationskontrolle* (§ 5 Abs. 3 Nr. 10 BlnDSG). Die Durchführung sämtlicher Systemverwaltungsaufgaben an der Telekommunikationsanlage unter Benutzung einer einzigen Benutzerkennung, also auch die Pflege der personenbezogenen Stammdaten einschließlich der Nutzungsberechtigungen, ist darüber hinaus ein erheblicher Mangel der Eingabekontrolle (§ 5 Abs. 3 Nr. 7 BlnDSG), da nicht nachvollzogen werden kann, wer hier bestimmte Datenänderungen vorgenommen hat.

Eine ähnliche Problematik wurde bei der *Gebührenabrechnung* festgestellt . Die Gebührendatensätze befinden sich auf einem mit der Telekommunikationsanlage verbundenen separaten Rechner. Für die Gebührenabrechnung steht den Mitarbeitern ausschließlich eine spezielle Benutzeroberfläche zur Verfügung. Die Anmeldung erfolgt auch hier über eine einzige Kennung und ein Paßwort für alle Administratoren. Die Gebührenabrechnungssoftware ermöglicht vielfältige Auswertungsmöglichkeiten, die bis auf einzelne Verbindungen hin differenziert werden können und so Aufschluß über das individuelle Kommunikationsverhalten einzelner Mitarbeiter geben können. Die Nutzung dieses

Rahmendienstvereinbarungen nach dem PersVG werden zwischen dem zuständigen Personalrat und der zuständigen Behörde ausgehandelt. Die Änderungen der hier betroffenen Rahmendienstvereinbarung Telekommunikation waren allerdings ausschließlich in Folge neuer Gesetzes- und Verordnungsvorschriften erforderlich geworden. An der Novellierung der betroffenen Vorschriften des IVG und der Rechtsverordnung war der Berliner Datenschutzbeauftragte beteiligt.

Die zu verwendende Nachweisliste hält den datenschutzrechtlichen Anforderungen stand, da hier lediglich der Name des Beschäftigten und der Betrag des zu zahlenden Entgeltes zu ersehen ist. Wegen der unterschiedlichen Tarifierung kann daraus nicht auf die Anzahl und Dauer der geführten privaten Gespräche geschlossen werden. Hinzuweisen ist darauf, daß eine individuelle Abrechnung über Einzelnachweise und -einzahlungen zu einem kaum vertretbar hohen Verwaltungsaufwand führen würde.

190 GVBl. S. 383
191 DBl. I Nr. 7 vom 19. September 1997, S. 138
192 Allgemeine Anweisung über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Berlin vom 16. Dezember 1997, Dienstblatt I S. 40 ff.

Abrechnungssystems wird nur durch organisatorische Anweisungen eingegrenzt. Eine Protokollierung der Zugriffe und Auswertungen findet nicht statt.

Die Gebührendatensätze stellen jedoch vor dem Hintergrund der vielfältigen Auswertungsmöglichkeiten – auch bei verkürzter Zielrufnummernspeicherung – einen sehr sensiblen Datenbestand dar, so daß eine Protokollierung sämtlicher (also auch der lesenden) Zugriffe bzw. Auswertungen angezeigt wäre. Eine Kontrollmöglichkeit der Zugriffe muß hier – auch zur Entlastung der Systemadministratoren – gegeben sein. Aber auch hier hat nur die Wartungsfirma Zugriff auf die Systemebene.

Nicht nur die Administration, sondern auch die Durchführung der *Wartungsarbeiten* an der Telekommunikationsanlage und dem Gebührenserver kann durch Mitarbeiter nicht nachvollzogen werden. Es kann daher nicht festgestellt werden, ob (ungewollte) Manipulationen an der Konfiguration der Telekommunikationsanlagen, an Gebührendatensätzen oder an gespeicherten Daten erfolgt sind. Selbst die von Mitarbeitern durchgeführten Systemverwaltungsarbeiten können nicht nachvollzogen werden. Wegen der fehlenden Kontrollmöglichkeiten kann daher in diesem Zusammenhang von einer ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden und die nach § 19 Abs. 1 Satz 2 BlnDSG geboten ist, nicht die Rede sein.

Die Telekommunikationsanlagen werden beim Auftreten bestimmter Fehler einer *Fernwartung (Fernüberwachung)* durch die Wartungsfirma unterzogen. Sollte ein Fehler ein Einwählen in die Telekommunikationsanlage notwendig machen, wird von der Wartungsfirma über einen Rückruf der Telekommunikationsanlage die Verbindung zu einer bestimmten Rufnummer der zentralen Wartungsstelle aufgebaut. Die Wartungsmitarbeiter identifizieren sich mit einem Paßwort gegenüber der Telekommunikationsanlage. Dieses Paßwort kann nicht vom Betreiber geändert werden. Der von der Wartungsfirma initiierte Verbindungsaufbau wird zwar an der Systemkonsole auf dem Bildschirm und auf dem Drucker signalisiert, so daß eine unbemerkte Fernwartung nicht möglich ist, es kann jedoch weder während der Wartung noch im nachhinein nachvollzogen werden, welche Aktionen von der Wartungsfirma durchgeführt wurden. Demzufolge kann auch nicht festgestellt werden, ob Daten oder Programmbestände in unzulässiger Weise verändert worden sind. Damit liegen auch bei der Fernwartung erhebliche Mängel der Organisationskontrolle (§5 Abs. 3 Nr. 10 BlnDSG) vor.

Dagegen ist die *Gebührenerfassung und -abrechnung bei Telefonaten der Patienten des Virchow-Klinikums positiv zu bewerten. Die Ablauforganisation läßt eine anonyme Telefonnutzung* durch die Patienten zu. Der Patient zieht sich an einem Automaten anonym eine Telefonchipkarte und erhält damit gleichzeitig eine kartenbezogene Rufnummer, die auf der Chipkarte gespeichert ist. Durch das Ziehen einer Karte am Automaten wird auf dem Gebührenrechner ein Konto generiert und der am Automaten eingezahlte Betrag automatisch auf das entsprechende Telefonkartenkonto gebucht. Der Patient kann nun diese Telefonchipkarte in jedes dafür vorgesehene Telefon, z. B. in seinem Krankenhauszimmer, stecken und aktivieren. Damit ist er unter der auf der Karte angegebenen Rufnummer an diesem Telefon erreichbar. Ein Wechsel des Telefons ist jederzeit durch Deaktivierung der Karte und anschließende Aktivierung an einem anderen Telefon möglich. Wenn telefoniert wird, werden die Gebühren vom jeweiligen Telefonkartenkonto abgebucht. Die dabei anfallenden Verbindungsdatensätze enthalten jeweils die um 3 Ziffern verkürzte Rufnummer des gerufenen Teilnehmers. Ist das Guthaben aufgebraucht, kann die Telefonkarte jederzeit am Automaten nachgeladen werden. Da zu keiner Zeit bekannt ist, welcher Patient welche Telefonkarte gezogen hat, ist eine anonyme Nutzung der Telefone durch die Patienten möglich.

**Mitarbeiterdaten im Internet**

Bereits seit mehreren Jahren sind öffentliche Stellen der Berliner Verwaltung – insbesondere Universitäten und sonstige Hochschulen – dazu übergegangen, Daten ihrer Mitarbeiter, wie z. B. Name, Postanschrift, Arbeitsgebiet, Telefon- und Faxnummer, neben den üblichen gedruckten Verzeichnissen auch in elek-

Der Senat ist mit dem Berliner Datenschutzbeauftragten der Meinung, daß der Aufnahme von Mitarbeiterdaten (sog. Basiskommunikationsdaten: Nachname, Postanschrift und Raumnummer in der Dienststelle, Arbeitsgebiete, Telefon-, Faxnummern, E-Mail- und X400-Adressen) in interne gedruckte und elektro-

tronischer Form zur Verfügung zu stellen. Neben Datenbanken, die nur Mitarbeitern dieser Einrichtungen zur Verfügung stehen, werden solche Verzeichnisse zunehmend auch im Internet veröffentlicht. Während gegen die Aufnahme derartiger Mitarbeiterdaten in interne elektronische Verzeichnisse keine grundsätzlichen datenschutzrechtlichen Bedenken bestehen, sind bei der Veröffentlichung dieser Verzeichnisse im Internet folgende *Grundsätze* zu beachten:

*Basiskommunikationsdaten von Arbeitnehmern* (z. B. Postadresse, E-mail-Adresse usw.) können ohne die Einwilligung des Arbeitnehmers in öffentliche elektronische Verzeichnisse aufgenommen werden, wenn hierfür eine arbeitsvertragliche Notwendigkeit besteht[193]. Andere (zusätzliche) Daten dürfen nur mit der Zustimmung des Arbeitnehmers in solchen Verzeichnissen veröffentlicht werden, vorausgesetzt, daß diese Daten in Beziehung zu der beruflichen Tätigkeit des Arbeitnehmers stehen (spezielle Interessengebiete; Veröffentlichungen usw.).

In jedem Fall muß der Arbeitgeber die Arbeitnehmer gründlich und umfassend über die Art der in das Verzeichnis aufgenommenen Daten informieren sowie darüber, ob sie ihr Einverständnis für bestimmte Einträge im Hinblick auf die oben getroffene Unterscheidung verweigern können und welche Konsequenzen eine Verweigerung haben kann. Die Arbeitnehmer müssen ein Recht auf Einsicht in die über sie gespeicherten Daten haben sowie das Recht, ihre Daten im Bedarfsfall korrigieren zu lassen und ihre Einwilligung zurückzuziehen.

Darüber ist es in der Regel nicht erforderlich, Daten über *alle* Mitarbeiter einer Einrichtung in elektronischen Verzeichnissen zu veröffentlichen: Während die bei Funktionsträgern in herausgehober Stellung bejaht werden kann und z. B. bei Wissenschaftlern ein Interesse daran als gegeben angenommen werden kann, daß Daten über sie im Internet verfügbar sind, gilt dies nicht für sonstige Mitarbeiter von Einrichtungen der öffentlichen Verwaltung (z. B. Pförtner, Reinigungspersonal usw.). Bei den letztgenannten Personengruppen ist daher die Veröffentlichung auch von Basisdaten unzulässig.

Darüber hinaus sollte auf Grund der besonderen Gefährdung des informationellen Selbstbestimmungsrechts der Mitarbeiter bei einer weltweiten Veröffentlichung ihrer Daten – nämlich auch in Ländern, in denen kein oder kein hinreichender Datenschutzstandard besteht – den Betroffenen grundsätzlich eine *Widerspruchsmöglichkeit* gegen die Aufnahme ihrer Daten in öffentliche elektronische Verzeichnisse eingeräumt werden.

### 4.7.4 Datenschutz und Medien

Über die zeitgleich zu den Beratungen zum Informations- und Kommunikationsdienste-Gesetz des Bundes[194] stattfindenden Arbeiten zu einem *Staatsvertrag der Länder über Mediendienste*[195] hatten wir bereits in unserem Jahresbericht 1996 umfassend berichtet[196]. Dieser Staatsvertrag ist zum 1. August 1997 in Kraft getreten.

Zu den betroffenen Diensten gehören insbesondere

- Verteildienste in Form von direkten Angeboten an die Öffentlichkeit für den Verkauf, den Kauf oder die Miete oder Pacht von Erzeugnissen oder die Erbringung von Dienstleistungen (Fernseheinkauf),
- Verteildienste, in denen Meßergebnisse und Datenermittlungen in Text oder Bild mit oder ohne Begleitton verbreitet werden,
- Verteildienste in Form von Fernsehtext, Radiotext und vergleichbaren Textdiensten sowie
- Abrufdienste, bei denen Text-, Ton- oder Bilddarbietungen auf Anforderungen aus elektronischen Speichern zur Nutzung übermittelt werden, mit Ausnahme von solchen

nische Verzeichnisse keine grundsätzlichen datenschutzrechtlichen Bedenken entgegenstehen. Nicht übersehen werden darf jedoch, daß das gedruckte Telefonverzeichnis der Berliner Verwaltung vernünftigerweise allen Bürgern und Besuchern der Stadt in den öffentlichen Bibliotheken seit Jahrzehnten zur Verfügung steht.

Die Modernisierung der Berliner Verwaltung, der länderübergreifende Informationsaustausch und insbesondere der Zwang zur Erhöhung der Bürgernähe (§ 2 GGO I) machen heutzutage darüber hinaus eine verbesserte Präsenz und Ansprechbarkeit aller derjenigen Mitarbeiter im staatlichen Bereich erforderlich, die Außenkontakte haben.

Im wesentlichen sollte man deshalb von dem – auch § 2 IVG zugrundeliegenden – Prinzip ausgehen, daß die Basiskommunikationsdaten (wohlgemerkt einschließlich der Arbeitsgebiete) dieser Mitarbeiter auch im Intra- und Internet immer dann ohne Extra-Einwilligung veröffentlicht werden dürfen, wenn diese Mitarbeiter in einem öffentlich zugänglichen Dienstgebäude tätig sind, an dessen Zimmertüren Namensschilder angebracht sind.

Nur bei internem Servicepersonal, Pförtnern, reinen Schreibkräften, Reinigungspersonal und bei Mitarbeitern mit besonderer Gefährdung des informationellen Selbstbestimmungsrechts wird man ihren eigenen Wunsch berücksichtigen müssen, der einerseits auf Nichtveröffentlichung, andererseits aber auch auf (selektive) Veröffentlichung gerichtet sein kann.

Die Informationspflichten des Arbeitsgebers und Einsichtsrechte der Arbeitnehmer sieht der Senat ansonsten wie der Berliner Datenschutzbeauftragte.

193 vgl. Bericht und Empfehlungen der Datenschutzbeauftragten der Europäischen Union zu Telekommunikation und Datenschutz im Arbeitsverhältnis, JB 1996, Anlage 4.3

194 vgl. dazu oben 3.3

195 Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag – MDStV) vom 23. Juni 1997 (GVBl. S. 361)

196 vgl. JB 1996, 4.7.1

Diensten, bei denen der individuelle Leistungsaustausch oder die reine Übermittlung von Daten im Vordergrund steht, ferner von Telespielen.

Die datenschutzrechtlichen Bestimmungen entsprechen im wesentlichen denen des Teledienstedatenschutzgesetzes. Mit der Harmonisierung der Datenschutzbestimmungen des Mediendienste-Staatsvertrages mit denen des IuKDG ist es gelungen, in diesem Bereich ein einheitliches, hohes Datenschutzniveau sicherzustellen.

Es wird jetzt darauf ankommen, die Bestimmungen des Staatsvertrages mit Leben zu erfüllen. Zu diesem Zweck hat sich der Berliner Datenschutzbeauftragte aus Anlaß der Internationalen Funkausstellung Berlin 1997 in einem Schreiben an die wichtigsten Diensteanbieter, Netzbetreiber und Endgerätehersteller gewandt, um auf die Neuregelungen hinzuweisen, die nicht allein den technischen Spezialisten überlassen bleiben können, sondern weitreichende Führungsentscheidungen erfordern. Die Anbieter von Mediendiensten, also Verteildiensten der Massenkommunikation wie z. B. Video-on-demand, Tele-Shopping, Fernseh- und Radiotext, müssen ihre Systeme technisch und organisatorisch so gestalten, daß Nutzer ihre Verbindung jederzeit abbrechen und die Dienste gegen Kenntnisnahme durch Dritte geschützt abrufen können. Vor allem müssen sie es den Nutzern ermöglichen, die Angebote anonym oder unter Pseudonym in Anspruch zu nehmen und zu bezahlen. Damit soll die Herstellung persönlicher *Nutzungsprofile über Seh- und Abrufgewohnheiten* verhindert werden. Bereits jetzt werden auf dem Markt verschiedene anwendungsreife und kostengünstige *anonyme Zugangstechnologien* wie z. B. vorausbezahlte Chipkarten angeboten. Diese Verfahren müssen allerdings bereits bei der Konzeption z. B. von *Set-Top-Boxen* berücksichtigt werden, um aufwendige und „teure“ Nachrüstungen zu vermeiden. Die einzige, gegenwärtig in Deutschland mit großem Aufwand vertriebene Set-Top-Box genügt diesen datenschutzrechtlichen Anforderungen gegenwärtig noch nicht.

Unterdessen haben die Beratungen zum *4. Rundfunkänderungsstaatsvertrag* begonnen, in dem Regelungen zum digitalen Fernsehen getroffen werden sollen. Hier wird es entscheidend darauf ankommen, eine Harmonisierung der Regelungen des Rundfunkstaatsvertrags mit denen des Mediendienstestaatsvertrages zu erreichen. Wir haben gegenüber der in Berlin zuständigen Senatskanzlei entsprechend Stellung genommen.

Entsprechend dem Wunsch des Berliner Datenschutzbeauftragten werden die datenschutzrechtlichen Regelungen im Vierten Rundfunkänderungsstaatsvertrag in Abstimmung mit den Datenschutzbeauftragten der Länder formuliert.

Bemerkenswerterweise ist in das *Fernsehsignalübertragungsgesetz*[197] des Bundes eine ausdrückliche Regelung aufgenommen worden, die Kontrolle der Zugangsberechtigung zu verschlüsselten Fernsehsignalen (Sendungen) nicht zur Erhebung oder Verarbeitung personenbezogener Daten der Kunden des Kabelfernsehbetreibers berechtigt (§ 6 Abs. 2). Damit bekräftigt der Bundesgesetzgeber den Grundsatz, daß Mediennutzungsprofile grundsätzlich nicht erstellt werden dürfen.

Darüber hinaus haben wir uns auch für eine Übernahme der Regelungen aus dem Mediendienste-Staatsvertrag in den *Mediendienstestaatsvertrag Berlin – Brandenburg* ausgesprochen. Die Beratungen zu diesem Staatsvertrag waren bis zum Ende des Berichtszeitraums noch nicht abgeschlossen.

Bei der Novellierung des Medienstaatsvertrages Berlin-Brandenburg werden die Vorschläge des Berliner Datenschutzbeauftragten berücksichtigt.

### 4.8 Organisation und Technik

#### 4.8.1 Datenverarbeitung im Auftrag oder Funktionsübertragung

Obgleich wir mehrfach Hinweise und Beispiele zur Abgrenzung der Datenverarbeitung im Auftrag von der Funktionsübertragung gegeben haben[198], stößt sie immer wieder auf Schwierigkeiten, die jedoch ausgeräumt werden müssen, weil von der richtigen rechtlichen Einordnung der Tätigkeiten ihre datenschutzrechtliche Zulässigkeit abhängt. Für öffentliche Stellen sollen folgende Abgrenzungshilfe gegeben werden:

Zu den Fragen des Datenschutzes im IT-Auftragsrecht vertritt der Senat die Auffassung, daß hier entsprechend den Bemühungen der unter Beteiligung der beiden Datenschutzbeauftragten tätigen interministeriellen Arbeitsgruppe Berlin-Brandenburg zum IT-Recht ein möglichst überregional einheitliches Recht gelten sollte.

Bei der *Datenverarbeitung im Auftrag* unterstützt der Auftragnehmer den Auftraggeber in einer oder mehreren Phasen der Datenverarbeitung und betreibt in vollständiger Abhängigkeit von ihm die Datenverarbeitung entsprechend seinen Weisungen bezüglich Art und Umfang. Für eine Auftragsdatenverarbeitung sprechen

197 Fernsehsignalübertragungsgesetz vom 14. November 1997, BGBl. I, 2710
198 JB 1993, 3.2; JB 1994, 3.3

- eine fehlende Entscheidungsbefugnis des Auftragnehmers über die Daten,
- der Umgang nur mit Daten, die der Auftraggeber zur Verfügung stellt,
- ein Auftragsschwerpunkt, der auf die praktisch-technische Durchführung einer Datenverarbeitung gerichtet ist, die nach außen der Auftraggeber vertritt,
- eine fehlende (vertragliche) Beziehung des Auftragnehmers zum Betroffenen.

Nimmt der Auftragnehmer dagegen mehr als diese „Hilfsfunktion" wahr, weil ihm neben der Datenverarbeitung für den Auftraggeber weitere Aufgaben oder Funktionen zur eigenständigen Erfüllung übertragen werden, ändert sich der datenschutzrechtliche Charakter der Rechtsbeziehung. Die dabei übermittelten Daten dienen dann nicht mehr dem Geschäftszweck, diese im Auftrag für den Auftraggeber gemäß seinen Weisungen zu verarbeiten, sondern dazu, daß der Auftragnehmer eine gewisse vertraglich geschuldete Leistung in eigener Verantwortlichkeit erarbeiten und erbringen möchte, zu deren Erfüllung er die übermittelten Daten benötigt. In diesem Fall wird dem Auftragnehmer eine ganze Aufgabe übertragen, die er eigenverantwortlich wahrnimmt, so daß hier ein Fall der *Funktionsübertragung* vorliegt. Daran ändert auch die Tatsache nichts, daß die Beteiligten weiterhin von „Auftragsverhältnis, Beauftragung" o. ä. sprechen. Der Begriff der Datenverarbeitung im Auftrag ist enger als der des Auftrags und nicht mit diesem zu verwechseln.

Eine *Funktionsübertragung* kann wiederum im Wege einer *Delegation* oder der Erteilung eines *Mandats* erfolgen:

Im Falle eines *Mandats* ändert sich die originäre Zuständigkeit nicht. Die beauftragte Stelle wird lediglich ermächtigt, im Namen des Auftraggebers für diesen nach außen zu handeln, etwa indem der Auftragnehmer unter dem Briefkopf des Auftraggebers tätig wird. Widerspruch und Klage sind unverändert gegen den Mandatsgeber zu richten. Zwar erfolgt hier de facto ein Wechsel in der (gesetzlich festgelegten) Zuständigkeit. Für die Erteilung eines Mandats ist jedoch eine gesetzliche Grundlage nicht erforderlich.

Im Fall der *Delegation* wird die Zuständigkeit für die gesamte Aufgabe auf eine andere Stelle übertragen, die nicht nur selbständig tätig wird, sondern auch *im eigenen Namen* entscheidet. Widerspruch und Klage richten sich gegen den „Delegationsempfänger", also diejenige Stelle, die im Rahmen der Delegation die neue Zuständigkeit erhalten hat. Da gesetzlich geregelte Zuständigkeiten nur durch Gesetz geändert werden können, bedarf die Delegation einer gesetzlichen Ermächtigung.

Wird zum Beispiel einer anderen Stelle nicht nur die Erstellung der Lohn- und Gehaltsabrechnung auf Grund der übergebenen Daten übertragen, sondern darüber hinaus die Aufgabe, in eigener Verantwortung die Errechnung der Löhne und Gehälter entsprechend den Tarifverträgen zu ermitteln, die erforderlichen Steuererklärungen zu erstellen oder die Löhne und Gehälter auszuzahlen, so handelt es sich um eine Funktionsübertragung. Entscheidet diese Stelle nach außen im eigenen Namen, so liegt der Unterfall der Delegation vor. Wird sie dagegen lediglich ermächtigt, im Namen der Lohn- und Gehaltsstelle für diese (unter deren Briefkopf) nach außen zu handeln, so hat eine Mandatsübertragung stattgefunden.

Für eine Funktionsübertragung in der einen oder anderen Form sprechen

- die Überlassung von Nutzungsrechten an herausgegebenen Daten,
- eine gewollte Dienstleistung, die über die praktisch-technische Datenverarbeitung hinausgeht (Personalverwaltung, Inkasso, Werbung, Kontenbearbeitung u. ä.),
- die fehlende Möglichkeit, auf einzelne Phasen der Verarbeitung oder Nutzung Einfluß zu nehmen (z. B. bei Umfragen, Bestelldienst, Kundenbetreuung, Vermittlung oder Datenbank-Recherchen),
- die auf den Auftragnehmer abgewälzte Verantwortlichkeit für die Zulässigkeit und Richtigkeit der Daten (siehe Haftungsregelungen im Vertrag),

- der Umgang mit Daten, die der Auftragnehmer von Dritten oder vom Betroffenen beschafft,
- die Kontaktaufnahme des Auftragnehmers mit dem Betroffenen.

Ergibt die Abgrenzung, daß die Tätigkeit der für die Erfüllung der Aufgabe eingeschalteten Stelle als Auftragsdatenverarbeitung anzusehen ist, so folgt daraus für den Auftraggeber, daß er „Herr der Daten“ bleibt und für die Datenverarbeitung verantwortlich ist. Er gilt als datenverarbeitende Stelle im Sinne des § 4 Abs. 3 Nr. 1, 2 BlnDSG. Seine Pflichten ergeben sich aus § 3 Abs. 1, 4 BlnDSG (vgl. auch § 11 Abs. 1, 2 BDSG).

Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten, d. h. die zur Datenverarbeitung überlassenen Daten nicht anderweitig verwenden und nicht länger aufbewahren, als der Auftraggeber bestimmt.

Auch wenn die Auftragsdatenverarbeitung für Auftraggeber und -nehmer eine Reihe von zusätzlichen Verpflichtungen (z. B. die vertragliche Ausgestaltung sowie die Unterrichtung nach § 3 Abs. 4 BlnDSG) mit sich bringt, so hat diese rechtliche Einordnung auch erhebliche Vorteile. Durch die Bindung des Auftragnehmers an die Weisungen des Auftraggebers wird er quasi als rechtliche Einheit mit der speichernden Stelle betrachtet. Dies hat die Konsequenz, daß die Übertragung der personenbezogenen Daten an den Auftragnehmer zur Durchführung der weisungsgemäßen Aufgabe und die Rückführung an den Auftraggeber nicht als Datenübermittlung zu bewerten sind. Auch die übrigen Datenverarbeitungsschritte (§ 4 Abs. 2 BlnDSG) werden datenschutzrechtlich aus der Sicht des Auftraggebers beurteilt, auch wenn sie tatsächlich durch den Auftragnehmer wahrgenommen werden.

Ergibt die Abgrenzung nach den genannten Kriterien, daß die öffentliche Stelle mehr als bloße Datenverarbeitungsschritte, nämlich eine gesamte Funktion übertragen hat, hängen die rechtlichen Konsequenzen davon ab, welcher der beiden Unterfälle einschlägig ist: Ist ein *Mandat* erteilt worden, so stellt die Weitergabe von Daten zwischen Mandatsgeber und Mandatsnehmer nur eine interne, dem Zweckbindungserfordernis unterliegende Nutzung und keine Datenübermittlung dar, obgleich es sich beim Mandat um einen Unterfall der Funktionsübertragung handelt.

Demgegenüber sind bei der *Delegation* Datentransfers zwischen Auftraggeber und Auftragnehmer als Datenübermittlungen anzusehen. Der Auftragnehmer ist nicht Teil der datenverarbeitenden Stelle, sondern Dritter. Er hat alle Anforderungen, die die datenschutzrechtlichen Bestimmungen an die Verarbeitung personenbezogener Daten stellen, selbst zu erfüllen.

Die bei der Funktionsübertragung in Betracht kommenden Fallkonstellationen können wiederum relativ leicht voneinander abgegrenzt werden je nach dem, ob es sich um öffentliche, hoheitliche Aufgaben oder um öffentliche, nicht-hoheitliche Aufgaben oder um nicht-öffentliche Aufgaben (z. B. fiskalischer Art) handelt, und je nach dem, ob es hierbei jeweils um die Übertragung auf öffentliche oder aber auf nicht-öffentliche Stellen geht:

- Wird eine *öffentliche, hoheitliche Aufgabe* auf eine *öffentliche Stelle* übertragen, so wird – im Fall des Mandats – der Auftragnehmer Teil der auftraggebenden Stelle, die Weitergabe der Daten ist interne Nutzung, deren Zulässigkeit sich allein an dem in § 11 Abs. 1 BlnDSG genannten Zweckbindungserfordernis orientiert. Ein Beispiel ist die Übertragung der Personalaktenführung einer öffentlichen Stelle auf eine andere öffentliche Stelle, wobei letztere als Auftragnehmerin ermächtigt ist, im Namen des Auftraggebers für diesen nach außen (etwa unter Nutzung des Briefkopfes des Auftraggebers) zu handeln. Liegt dagegen der Fall einer Delegation vor, entscheidet der Auftragnehmer selbständig. Die Weitergabe von Daten stellt eine Datenübermittlung dar, deren Zulässigkeit sich nach § 12 BlnDSG richtet. Ein Beispiel ist die Vollzugshilfe der Feuerwehr nach § 3 Abs. 2 ASOG.
- Wird eine öffentliche, hoheitliche Aufgabe auf eine *nicht-öffentliche Stelle* übertragen, so kann es sich hierbei nur um

den Unterfall der Delegation handeln, weil eine Mandatserteilung bei privaten Stellen nicht möglich ist. Voraussetzung für eine derartige Delegation ist die Beleihung, die nur durch oder auf Grund Gesetzes sowie nach Veröffentlichung des Beleihungsaktes erfolgen darf. Da Beliehene (z. B. Schornsteinfeger, Notare, amtlich beeidigte Sachverständige, Gerichtsvollzieher) immer als öffentliche Stellen gelten, richtet sich die Zulässigkeit des zwischen Auftragnehmer und Auftraggeber stattfindenden Datenaustauschs nach § 12 BlnDSG.

- Wird eine *öffentliche, nicht-hoheitliche Aufgabe* auf eine andere *öffentliche Stelle* übertragen, so gilt im Falle der Mandatserteilung dasselbe wie bei einer hoheitlichen Aufgabe. Als (frei erfundenes) Beispiel mag hier die Ausrichtung eines Empfangs durch das Protokoll einer öffentlichen Verwaltung unter dem Briefkopf der anderen (beauftragenden) Verwaltung dienen. Wird der Empfang dagegen unter dem eigenen Briefkopf des Auftragnehmers durchgeführt, so handelt es sich um den Unterfall der Delegation, die (im Gegensatz zur Beleihung) auch ohne gesetzliche Ermächtigung durch Vertrag möglich ist. Datentransfers zwischen den beiden beteiligten Stellen erfolgen innerhalb des öffentlichen Bereichs, so daß die Zulässigkeit der Datenübermittlung nach § 12 BlnDSG zu beurteilen ist.

- Wird eine öffentliche, nicht-hoheitliche Aufgabe auf eine *nicht-öffentliche Stelle* übertragen, so ist auch hier eine Mandatserteilung nicht möglich. Der Fall der Delegation, die mangels Beleihungserfordernisses keiner gesetzlichen Ermächtigung bedarf, trägt die Besonderheit, daß die beauftragte nicht-öffentliche Stelle wie eine öffentliche Stelle behandelt wird, weil sie Aufgaben der öffentlichen Verwaltung wahrnimmt (§ 2 Abs. 1 Satz 2 BlnDSG). Die hieraus zu ziehende wichtige Konsequenz ist, daß Datentransfers zwischen Auftragnehmer und Auftraggeber innerhalb des öffentlichen Bereichs stattfinden, so daß sich die Zulässigkeit der Datenübermittlung nach § 12 (und nicht nach § 13) BlnDSG richtet. Dieses Ergebnis ist sachgerecht, weil somit in den Fällen der Funktionsübertragung, die zumeist eine zweckgleiche Datenverarbeitung beinhaltet, die Rechtmäßigkeit der Datenübermittlung auf Grund von § 12 Abs. 1 Satz 2 BlnDSG (zweckgleiche Datenübermittlung im öffentlichen Bereich) an dem dort genannten (weniger strengen) Kriterium der Erforderlichkeit gemessen werden kann (ohne etwa für den Datenaustausch eine Rechtsgrundlage fordern zu müssen). Unter diese Fallkonstellation fallen z. B. die mit der Reform der öffentlichen Verwaltung beauftragten Management-Firmen.

- Wird eine *nicht-öffentliche Aufgabe* (z. B. fiskalischer Art) auf eine öffentliche Stelle übertragen, so kann dies im Wege des Mandats erfolgen, so z. B. wenn das Landesverwaltungsamt Diensträume einer anderen öffentlichen Verwaltung unter deren Briefkopf bewirtschaftet. Erfolgt die Bewirtschaftung hingegen unter dem Briefkopf des Landesverwaltungsamts, so handelt es sich um den Fall der Delegation, die keiner gesetzlichen Grundlage bedarf und bei der eine zwischen Auftraggeber und Auftragnehmer stattfindende Datenübermittlung nach § 12 BlnDSG zu beurteilen ist.

- Wird die nicht-öffentliche Aufgabe dagegen auf eine *nicht-öffentliche Stelle* übertragen, so kann dies wiederum (mangels Zulässigkeit der Mandatserteilung) nur im Wege der Delegation erfolgen. Als Besonderheit gegenüber den anderen Fallkonstellationen ist der Umstand hervorzuheben, daß wegen der Übertragung einer nicht-öffentlichen Aufgabe die private Stelle nicht als öffentliche Stelle im Sinne des § 2 Abs. 1 Satz 2 BlnDSG anzusehen ist. Es handelt sich also um eine Datenübermittlung an eine Stelle außerhalb des öffentlichen Bereichs, so daß die Zulässigkeit nach § 13 (und nicht nach § 12) BlnDSG zu beurteilen ist. Typisches Beispiel hierfür ist die von beauftragten Privatunternehmen durchzuführende Inkassotätigkeit. Die Zulässigkeit der von diesen Unternehmen durchzuführenden Datenverarbeitungsschritte beurteilt sich ihrerseits nach den Bestimmungen des (für den Privatbereich geltenden) BDSG.

### 4.8.2 Defekte Speichermedien

*Ein bezirkliches Krankenhaus teilte uns mit, daß eine voll bespielte optische Speicherplatte (WORM) seines elektronischen Krankengeschichtenarchivs wegen eines Defekts nicht mehr lesbar sei. Die Lieferfirma, die das System technisch auch betreute, hatte erklärt, daß die defekte WORM nur beim Hersteller in den USA wieder lesbar gemacht werden kann.*

Eine Auslieferung der optischen Platte an die US-amerikanische Herstellerfirma würde bedeuten, daß zumindest nach der Reparatur die in den Krankenakten archivierten personenbezogenen Patientendaten den Mitarbeitern des Unternehmens im Klartext offenbart werden würden. Dies würde eine Verletzung der ärztlichen Schweigepflicht bedeuten, die u. U. auch strafrechtlich relevant wäre, denn eine solche Offenbarung ist von § 26 Abs. 3 Berliner Krankenhausgesetz nicht abgedeckt.

Eine Lesbarmachung der defekten WORM beim Hersteller in den USA wäre daher nur zulässig, wenn die WORM durch einen der *ärztlichen Schweigepflicht* unterliegenden Mitarbeiter des Krankenhauses (das kann auch ein IT-Fachmann sein, der als ärztlicher Erfüllungsgehilfe gelten kann) in die USA transportiert wird, dort die Reparatur oder Datenrekonstruktion der WORM unter Kontrolle dieses Mitarbeiters erfolgt und dann von ihm wieder nach Berlin gebracht wird. Diese Lösung setzt voraus, daß die realen Kontrollmöglichkeiten vorab auf Wirksamkeit geprüft und mit dem Hersteller abgestimmt werden.

Eine solche Lösung ist natürlich wenig praktikabel und zu aufwendig. Wir haben daher empfohlen, die defekte WORM physisch zu zerstören und den Datenbestand auf einer neuen WORM erneut aufzubauen. Dieses war möglich, weil die gescannten Daten auf anderen Datenträgern gesichert worden waren. Anderenfalls wäre ein erneutes Einscannen der in Papierform noch vorliegenden Krankengeschichten erforderlich gewesen.

*Ein anderes Bezirksamt sah berechtigterweise die Gefahr, daß Computerhardware, die personenbezogene Daten enthält, an Firmen unter Umständen zwecks Fehlersuche oder Fehlerbehebung herausgegeben werden müsse, und erarbeitete eine Mustervereinbarung zur Einhaltung der datenschutzrechtlichen Vorschriften in solchen Fällen.*

Das Bezirksamt wollte sich zunächst von den Unternehmen bestätigen lassen, daß die Fehlersuche bzw. -behebung nicht vor Ort, sondern nur in der Firma möglich ist und daß die Mitnahme der Hardware zur Auftragserfüllung unabdingbar ist. Ein solcher Fall tritt nach unserer Kenntnis bei heutigen Standardsystemen (PCs und Server) nur in zwei seltenen Fällen auf:

- wenn die Festplatte während der Garantiezeit defekt wird oder
- wenn der Defekt in einem System auftritt, dessen Gehäuse nur durch den Hersteller oder dessen Beauftragte geöffnet werden kann und für das kein Vor-Ort-Service angeboten wird.

Der letzte Fall dürfte heutzutage kaum mehr in Betracht kommen. Der erste Fall jedoch tritt auf, wenn bei Schäden in der Garantiezeit der Hardware-Lieferant bzw. -Hersteller prüfen will, ob der aufgetretene Schaden und dessen Ursache die Garantiebedingungen erfüllen. Nur in diesem Falle ist eine vertragliche Regelung zum Schutz der personenbezogenen Daten auf der Festplatte erforderlich.

Ansonsten gehen wir von folgendem aus:

- Die Lokalisierung des defekten Bauteils in einem System ist einem Servicetechniker stets vor Ort möglich.
- Die Reparatur defekter Bauteile ist in der Regel unökonomisch im Vergleich zum Austausch. Der Austausch defekter Teile erfolgt vor Ort, auch um die Beschränkung der Systemverfügbarkeit zu minimieren.
- Die Festplatte ist die einzige fest eingebaute Hardwarekomponente, die nach Unterbrechung der Stromversorgung noch schutzbedürftige Daten enthalten kann. Aus diesem Grunde tritt das zu behandelnde datenschutzrechtliche Risiko nur für dieses Bauteil auf.

Der Senat stimmt mit der Meinung des Berliner Datenschutzbeauftragten überein.

Die Senatsverwaltung für Gesundheit und Soziales wird, soweit die entsprechende aufsichtsrechtliche Zuständigkeit gegeben ist, auch bei zukünftigem Auftauchen derartiger Vorkommnisse im Rahmen der zur Verfügung stehenden aufsichtsrechtlichen Mittel tätig werden.

- Auch eine defekte Festplatte wird nur ausgetauscht. Für den Fall, daß keine Garantieaspekte mehr berührt werden, kann die defekte Festplatte vernichtet werden. Die Rekonstruktion der auf ihr enthaltenden Daten erfolgt über die Datensicherung. Der Fall, daß diese grob fahrlässig unterlassen worden ist, soll außer Betracht gelassen werden.

Der Anwendungsfall für den vorgelegten Muster-Vereinbarungsentwurf ist daher auf die Fehlerursachenforschung bei Festplatten im Garantiefall beschränkt. Auf jeden Fall hat die Firma ausführlich die Gründe darzustellen, weshalb die Fehlersuche und -behebung nicht vor Ort erfolgen kann und weshalb eine Mitnahme der Hardware und der Datenbestände zur Auftragserfüllung unabdingbar ist. Damit nicht aus Bequemlichkeit oder aus der Fehleinschätzung des Begehrens der Firma eine unnötige Gefährdung der Vertraulichkeit der gespeicherten Daten möglich ist, haben wir dem Bezirksamt empfohlen, uns von jedem Einzelfall, in dem die Herausgabe von Hardware mit personenbezogenen Daten erfolgen soll, einschließlich dieser Begründung zu unterrichten. Diese Empfehlung erstreckt sich auch auf alle anderen privaten und öffentlichen datenverarbeitenden Stellen des Landes, wenn Unsicherheit darüber besteht, wie man sich in solchen Fällen verhalten sollte.

Die *externe Fehlersuche und -behebung* ist Auftragsdatenverarbeitung, für die im öffentlichen Bereich des Landes § 3 Abs. 1 und 4 BlnDSG anzuwenden sind. Dies bedeutet, daß für die Tätigkeiten das Berliner Datenschutzgesetz vertraglich auch auf den privaten Auftragnehmer zu erstrecken ist, die Kontrollkompetenz des Berliner Datenschutzbeauftragten mit seinen Befugnissen für die öffentlichen Stellen des Landes vertraglich abgesichert und bestimmte Meldepflichten erfüllt werden müssen. Soweit für die Daten sogar Offenbarungsverbote vorliegen und Datenverarbeitung im Auftrag nicht spezialrechtlich geregelt ist, ist die Herausgabe von Festplatten mit personenbezogenen Daten gänzlich unzulässig (z. B. im Geltungsbereich der ärztlichen Schweigepflicht).

Ein anderes Bezirksamt lieferte eine Woche später einen konkreten Anwendungsfall:

> *Der behördliche Datenschutzbeauftragte bat uns um Rat, weil die Festplatte eines Personal Computers, der den vollständigen Datenbestand eines Amtes in der Abteilung Sozialwesen enthielt, beschädigt war. Die Wartungsfirma hatte eine neue Festplatte eingebaut, der Sicherungsbestand war eingespielt worden, die defekte Festplatte mit den Sozialdaten sollte jedoch zum Nachweis des Garantiefalls an die Herstellerfirma geschickt werden.*

Der behördliche Datenschutzbeauftragte war diesen Plänen entgegengetreten und erhielt von uns mit folgenden Hinweisen Schützenhilfe, da es sich um Sozialdaten handelte, die einer besonderen Geheimhaltung unterliegen:

- Da zumindest der Hersteller in der Lage sein dürfte, den Datenbestand trotz des Defekts sichtbar zu machen, kommt eine Herausgabe der defekten Festplatte an diesen nur dann in Betracht, wenn die Daten verschlüsselt sind.
- Wenn die Rekonstruierbarkeit der Daten nicht ausgeschlossen werden kann, käme es mit der Übersendung der Festplatte an den Hersteller, u. U. sogar ins Ausland, zu einer Offenbarung von Sozialdaten, für die eine Rechtsgrundlage nicht erkennbar ist.
- Wollte man – was in Zweifel zu ziehen ist – die Bereitstellung der Festplatte zum Nachweis eines der Gewährleistung unterliegenden Defekts wie auch Wartung und Fernwartung als Datenverarbeitung im Auftrag ansehen, wären die beiden Voraussetzungen des § 80 Abs. 5 SGB X zu prüfen, wonach eine Störung des Betriebsablaufes zu befürchten sein muß oder die Arbeit erheblich kostengünstiger im Auftrag erledigt werden kann und der größte Teil des Datenbestandes in der öffentlichen Stelle verbleibt. Beide Voraussetzungen waren eindeutig nicht gegeben.

Wir konnten also nur empfehlen, in Zukunft Wartungsverträge zu schließen bzw. Garantiebedingungen mit den Vertragspartnern abzusprechen, die einen datenschutzgerechteren Weg zur Inanspruchnahme der Gewährleistung zulassen.

In diesem Falle empfehlen wir, die defekte Festplatte unter Verzicht auf die Gewährleistung zu vernichten, was angesichts heutiger Hardwarepreise für Zubehör von Standard-PCs im Verhältnis zu den Risiken für die Vertraulichkeit der Sozialdaten auch angemessen ist.

*Eine Petentin suchte uns auf und übergab uns vier etikettierte und beschriebene Disketten, die sie bei einem Technikdiscounter als Leerdisketten erstanden hatte. Die Disketten enthielten sensible personenbezogene Daten und weitere als Betriebsgeheimnisse einer Baufirma anzusehende Informationen.*

Die Petentin hatte zwei Packungen mit je zehn Leerdisketten bei dem Discounter besonders günstig gekauft und zu Hause festgestellt, daß vier Disketten gebraucht und gefüllt waren. Die Packungen waren nicht in Folie eingeschweißt, sondern enthielten ihr Preisschild auf der Pappschachtel. Die vier Disketten wurden uns zur Prüfung übergeben. Sie enthielten u. a. den Namen des früheren Besitzers, des Inhabers einer Baufirma.

Es stellte sich heraus, daß dieser bei dem Discounter einige Zeit zuvor einen PC gekauft hatte, der bald darauf einen möglicherweise durch Virenbefall bewirkten Defekt aufwies, so daß die Festplatte nicht mehr gelesen werden konnte. Der Computerbesitzer reklamierte den Defekt beim Discounter, der dem besonders guten Kunden einen Gefallen tun wollte, indem er den Computer nicht wie üblich an die Service-Zentrale sandte, sondern versuchte, den Schaden sofort zu beheben. Der Kunde erhielt im Rahmen des Garantieaustausches einen neuen Rechner. Die Festplatte des defekten PCs konnte aktiviert und die sicherzustellenden Daten auf den neuen Rechner übertragen werden. Außerdem sollten die Daten auf Sicherungsdisketten überspielt werden und diese dem Kunden zusätzlich ausgehändigt werden, was versehentlich allerdings nicht geschah. Als dieses beanstandet wurde, waren die bespielten Disketten beim Discounter trotz intensiver Nachforschungen auch nicht mehr auffindbar. Wie dann die Disketten in die für den Verkauf bestimmten Schachteln gekommen sind, war nicht mehr nachvollziehbar.

Der Fall zeigt, daß beim Umgang mit bespielten Disketten besondere Sorgfalt geboten ist. Zu empfehlen ist, daß man grundsätzlich bespielte Disketten nicht mehr in den Originalverpackungen aufbewahren sollte. Dies gilt nicht nur in diesem Sonderfall. Auch sonst empfiehlt es sich, dafür zu sorgen, daß Neudisketten und bespielte Disketten nicht durcheinandergebracht werden.

## 5. Organisation des Datenschutzes

### 5.1 Sicherstellung des Datenschutzes

#### 5.1.1 Betriebliche und behördliche Datenschutzbeauftragte

Nachdem 1993 die *Koordinierungsrunde* der behördlichen Datenschutzbeauftragten der Bezirke mangels weiteren Interesses eingestellt wurde, wurde sie in diesem Jahr nach einer Initiative aus dem Bereich der bezirklichen Datenschutzbeauftragten wieder reaktiviert. Wir hatten in der Zwischenzeit auf eigene Initiativen verzichtet, weil die Notwendigkeit, sich in regelmäßigen Abständen wieder zu treffen, um Erfahrungen auszutauschen und sich bei besonderen Datenschutzproblemen abzustimmen, von den meisten Bezirken zunächst nicht erkannt wurde. In den meisten Fällen sind den bezirklichen Datenschutzbeauftragten für diese Aufgabe weder in personeller noch in materieller Hinsicht die erforderlichen Ressourcen zur Verfügung gestellt worden. Auch der Fortbildungsbedarf ist keineswegs hinreichend gedeckt. Somit stellt dieses Forum für die meisten bezirklichen Datenschutzbeauftragten eine geeignete Möglichkeit dar, aktuelle Fragen des Datenschutzes mit den Kolleginnen und Kollegen zu erörtern. Allerdings ist es nach wie vor nur eine Minderheit der Bezirke, deren behördliche Datenschutzbeauftragte ausreichend Interesse für diesen Gesprächskreis aufbringen.

Die Koordinierungsrunde befaßte sich bisher mit folgenden Themen:

Die *Aufgabenabgrenzung* zwischen dem Datenschutzbeauftragten nach SGB X und dem behördlichen Datenschutzbeauftragten ergibt sich aus den unterschiedlichen Rechtsgrundlagen für die

Bestellung der Datenschutzbeauftragten. Der behördliche Datenschutzbeauftragte wird auf Grund § 19 Abs. 5 BlnDSG bestellt, der Datenschutzbeauftragte für die Sozialdaten gemäß § 81 Abs. 4 SGB X. Die von den Datenschutzbeauftragten zu erfüllenden Voraussetzungen sowie ihre Aufgaben ergeben aus §§ 36, 37 BDSG, denn auf diese Vorschrift wird sowohl in § 19 Abs. 5 BlnDSG als auch in § 81 Abs. 4 SGB X verwiesen. Zwar ist es in den Bezirken aus Kapazitätsgründen sinnvoll, die beiden Funktionen zu trennen, es bestehen daüberhinaus aber keine Bedenken, wenn beide Funktionen in einer Person vereinigt werden. Wenn Sozialdaten und andere Daten gemeinsam verarbeitet werden, kann es zu Zuständigkeitsüberschneidungen kommen, wenn keine klare Trennung zwischen Sozialdaten und anderen Daten bei der automatisierten Verarbeitung technisch vorgegeben ist. Es ist daher notwendig, daß die Zugriffsberechtigungen für die unterschiedlichen Datenarten so definiert werden, daß der behördliche Datenschutzbeauftragte keinen Zugriff auf Sozialdaten haben muß, wenn er die Verarbeitung anderer personenbezogener Daten kontrolliert und umgekehrt.

Die *Mitwirkung bei der Personalauswahl* ist nach § 37 Abs. 1 Nr. 3 BDSG eine Aufgabe des behördlichen Datenschutzbeauftragten. Die Erfahrung mit den behördlichen Datenschutzbeauftragten der Bezirke zeigt allerdings, daß diese Aufgabe so gut wie nicht wahrgenommen wird, weil ihnen die dafür notwendige Zeit nicht eingeräumt wird .

Auf Grund fehlender technischer Kenntnisse müssen die bezirklichen Datenschutzbeauftragten bei der Kontrolle und Umsetzung technisch-organisatorischer Maßnahmen zum Datenschutz vor allem auf Mitarbeiter aus den IT- und den Organisationsstellen sowie System- und Verfahrensbetreuer zurückgreifen. Es wurde daher als notwendig angesehen, daß die *Schulung* zu diesen Themen stärker in die IT-Ausbildung integriert werden sollte.

Anlaß für die Behandlung der Fragen des *Brandschutzes in IT-Räumen* war der Brand im Rathaus Schöneberg im vergangenen Jahr. Die bezirklichen Datenschutzbeauftragten hörten dazu den Brandschutzbeauftragten der Senatsverwaltung für Inneres. Es wurde festgehalten, daß neben der besonderen Brandsicherung der IT-Räume (Rechenzentrum, Server-Raum, Wiring-Center) mit Sicherheitsverschluß, Stahltüren, Fenstersicherung auch die Anbringung von Feuerlöschern und dazugehörigen Hinweistafeln und diesbezügliche Schulung erforderlich sind.

Es wurden die datenschutzrechtlichen Konsequenzen des neuen § 5 Informationsverarbeitungsgesetz erörtert[199]. Datenschutzrelevant sind vor allem die Verbindungsdaten, deren Verarbeitung zusätzlich durch die Verordnung über die Speicherung, die Löschung und sonstige Verarbeitung von Verbindungsdaten zur Abrechnung privater und Kontrolle dienstlicher Nutzung kommunikationstechnischer Verbindungen sowie der Rahmendienstvereinbarung über den Einsatz und den Betrieb von digitalen Telefonnebenstellenanlagen geregelt sind. Sie müssen spätestens nach einem Monat wieder gelöscht werden.

Für die Erarbeitung einer *Checkliste*, mit der die behördlichen Datenschutzbeauftragten in ihren Ämtern effektiver technisch-organisatorische Prüfungen durchführen können, wurde eine Arbeitsgruppe gebildet. In der Checkliste sind für die zehn Kontrollmaßnahmen des § 5 BlnDSG die wichtigsten Fragestellungen und Anforderungen zusammengestellt worden.

Auch die Beratungstätigkeit für *private Stellen* zu den unterschiedlichsten Anliegen des Datenschutzes hat zugenommen. Hilfestellungen bei der Formulierung von Ausschreibungstexten für die Einstellung betrieblicher Datenschutzbeauftragten, bei der Festlegung von Art und Umfang dieses neuen Aufgabengebietes, bei Fragen zu Aus- und Weiterbildungsmöglichkeiten für das breitgefächerte Aufgabenspektrum sowie zu speziellen Datenschutzproblemen beim täglichen Umgang mit personenbezogenen Daten bilden das Spektrum der Beratungsersuchen privater Unternehmen und ihrer betrieblichen Datenschutzbeauftragten.

199 vgl. oben 4.7.3

### 5.1.2 Dienstanweisung für das bezirkliche Bürgerbüro

Die datenschutzrechtlichen Anforderungen, die bei der Bündelung verschiedener, eigentlich den Fachämtern obliegenden Aufgaben in den Bürgerbüros der Bezirksämter zu beachten sind, hatten wir bereits ausführlich dargestellt[200]. Damit jeder Mitarbeiter des Bürgerbüros weiß, wie er sich aus datenschutzrechtlicher Sicht verhalten muß, hatten wir auch gefordert, seine Befugnisse und Verpflichtungen in einer *Dienstanweisung* zu regeln. Diese sollte wenigstens folgende für eine datenschutzkonforme Verfahrensweise wesentliche Punkte berücksichtigen:

Mitarbeiter des Bürgerbüros müssen über *Grundkenntnisse des Datenschutzrechts* verfügen und auf das *Datengeheimnis* (§ 8 BlnDSG) verpflichtet werden, wobei unabhängig hiervon im Einzelfall die Zulässigkeit der Datenverarbeitung nach den Vorschriften des BlnDSG bzw. den bereichsspezifischen Regelungen zu beurteilen ist. Der Leiter des Bürgerbüros ist für die regelmäßige *Schulung* der Mitarbeiter in Datenschutzangelegenheiten verantwortlich. Die Mitarbeiter sollten dahingehend unterwiesen werden, daß die in der Beratung oder Bearbeitung eines Sachgebietes erworbenen Erkenntnisse nicht zur zweckfremden *Verwendung* in einem anderen Sachgebiet herangezogen werden sollten. Die besondere *Sensibilität* von Sozialdaten sowie der Daten, die der ärztlichen Schweigepflicht unterliegen, sollte ebenso hervorgehoben werden wie der Umstand, daß in den Vorschriften des Sozialdatenschutzes nach dem SGB I und X eine besondere Schulung stattfinden muß.

Ein Hinweis darauf, daß das Bürgerbüro als datenverarbeitende Stelle selbst die *Verantwortlichkeit* in Datenschutzfragen trägt und der behördliche Datenschutzbeauftragte neben seinen (weisungsfrei durchzuführenden) Beratungs- und Kontrolltätigkeiten auch mit der Umsetzung datenschutzrechtlicher Belange befaßt werden kann, ist für das bessere Verständnis der im Bürgerbüro tätigen Mitarbeiter ebenso hilfreich wie derjenige, daß eine unbefugte Datenverarbeitung nach § 32 BlnDSG, § 85 SGB X bzw. § 43 BDSG strafbar ist. Die Mitarbeiter des Bürgerbüros sind verpflichtet, die *Einwilligung* des betroffenen Bürgers, die auch in mündlicher Form erteilt werden darf, einzuholen, wobei der Bürger vorher in hinreichendem Maße über die Datenverarbeitung aufgeklärt werden muß (§ 6 Abs. 3, 4 BlnDSG). Ein Aufklärungsschreiben sollte gut sichtbar als Aushang angebracht werden und vor allem auch den Hinweis enthalten, daß der Bürger weiterhin die Wahlmöglichkeit hat zwischen der Inanspruchnahme des Bürgerbüros und der des Fachamtes.

Bereits in dem vom Projekt „Modellbezirksamt“ der Senatsverwaltung für Inneres herausgegebenen Erfahrungsbericht zum Teilprojekt „Bürgeramt“ vom März 1995 wurde hingewiesen, daß die Projektgruppe sich mit dem Berliner Datenschutzbeauftragten darauf verständigt hat, für die Modellbürgerämter in Weißensee und Köpenick eine Dienstanweisung zu erlassen, „in der alle für diesen Bereich spezifizierten Regelungen zu Datenschutz und Datensicherheit aufgenommen werden.“ Bis zum Abschluß des Projekts „Modellbezirksamt“ wurde gemeinsam mit den beiden Bezirken an einer entsprechenden Dienstanweisung gearbeitet, die anschließend in eigener Verantwortung von den Bezirken fertiggestellt werden mußte. Ein Muster für einen Hinweis zum Datenschutz hat die Senatsverwaltung für Inneres in dem ebenfalls im März 1995 erschienenen Leitfaden zur Einrichtung von Bürgerämtern veröffentlicht. Beide Hinweise gelten weiterhin als Handlungsempfehlungen für weitere bezirkliche Bürgerämter.

Begrüßenswert ist, daß der Berliner Datenschutzbeauftragte in seinem Jahresbericht zum 31. Dezember 1997 diese Empfehlungen weiter konkretisiert hat.

### 5.1.3 Geschäftsordnung

In den Jahren 1984 und 1986 hatten wir die in der *Zentralen Hauptverteilungsstelle des Landesverwaltungsamtes* durchlaufende Post stichprobenartig[201] daraufhin durchgesehen, ob und wie sie gegen unbefugte Einsichtnahme geschützt ist. Die Senatsverwaltung für Inneres hatte die Feststellungen seinerzeit zum Anlaß genommen, mit einem Rundschreiben über die Geheimhaltung beim Dienstpostaustausch in der Berliner Verwaltung[202] auf die Rechtslage hinzuweisen.

Wir haben in der Hauptverteilungsstelle des Landesverwaltungsamtes erneut eine stichprobenartige Prüfung durchgeführt.

Das Ergebnis war insgesamt erfreulich. Die langjährigen Bemühungen, die Beschäftigten in der Berliner Verwaltung für den Datenschutz bei dem Versand von Unterlagen mit personenbezogenem Inhalt zu sensibilisieren, haben dazu geführt, daß ein Großteil der Sendungen verschlossen (überwiegend in Briefumschlägen oder verschließbaren Umlaufmappen) war.

Dennoch haben wir wiederum eine Vielzahl von offen *versandten Akten und Schriftstücken* mit sensiblen personenbezogenen Daten vorgefunden, die zum Teil besonderen Geheimhaltungsvorschriften unterliegen (z. B. *Steuer- oder Sozialgeheimnis).* Darunter befanden sich Ermittlungs- und Prozeßakten, Steuerakten, Akten des Ausgleichsamtes, Gewerbeakten sowie Schriftstücke im Zusammenhang mit Zwangsvollstreckungen, Mitteilungen

200 JB 1994, 3.4
201 vgl. JB 1985, 2.4; JB 1986, 4.5
202 DBl. I Nr. 19 vom 18. Dezember 1985 und DBl. I Nr. 15 vom 11. September 1987

über Vaterschaftsanerkennung, Auskünfte aus dem Zentralen Schuldnerverzeichnis, Ersuchen um Erlaß eines Haftbefehls oder Unfallanzeigen. Vereinzelt befanden sich die Akten oder Schriftstücke

- in nicht verklebten Briefumschlägen,
- in verschließbaren Umlaufmappen, die nicht mit den dafür vorgesehenen Klebestreifen verschlossen waren, oder
- die Schriftstücke waren gefaltet und mit einem „Tacker“ geheftet.

Diese Formen der Versendung sind unzureichend, da keine Sicherung der personenbezogenen Daten vor dem Zugriff Unbefugter besteht. Es wird nicht gewährleistet, daß die so versandten Unterlagen bei dem Transport nicht gelesen werden können, wie es § 5 Abs. 2 BlnDSG vorschreibt. Somit haben wir die wenigen in der eben beschriebenen Weise versandten Unterlagen dem offenen Versand zugerechnet.

Im übrigen haben wir festgestellt, daß – entgegen der Überprüfungen in den Jahren 1984 und 1986 – das Spektrum der betroffenen Behörden nicht mehr quer durch die Berliner Verwaltung zieht. Bei dieser Stichprobe sind nur einige wenige Verwaltungen besonders aufgefallen, erneut wiederum die Justizverwaltung.

**5.1.4 Dateienregister**

Das Berliner Datenschutzgesetz sieht in § 19 vor, daß die behördlichen Datenschutzbeauftragten der öffentlichen Stellen des Landes für jede personenbezogene automatisierte Datei, die nicht nur vorübergehend aus verarbeitungstechnischen Gründen vorgehalten wird, und für jede nichtautomatisierte Datei, aus der Daten übermittelt werden, eine Dateibeschreibung zu führen haben, die genaue Aussagen zu Inhalt, Zweckbestimmung, Rechtsgrundlagen, Übermittlungen, Lösch- und Sperrfristen, technisch-organisatorische Schutzmaßnahmen und Angaben zur informationstechnischen Umgebung enthält. Sie haben ferner eine Geräteverzeichnis, welches für alle informationstechnischen Systeme, mit denen personenbezogene Daten verarbeitet werden, die aktuelle Ausstattung mit Hard- und Software beschreibt sowie den jeweiligen Standort der wichtigsten Komponenten benennt.

Diese internen Verzeichnisse sind dem Berliner Datenschutzbeauftragten für die Führung des Dateienregisters vorzulegen. Dabei sind Formvorschriften zu beachten, die in der *Dateienregisterverordnung* genauer festgelegt sind. Abgesehen von bestimmten Ausnahmen haben die Bürger das Recht, ohne Angabe von Gründen in das Dateienregister einzusehen. Ansonsten dient das Dateienregister der Prüftätigkeit des Berliner Datenschutzbeauftragten.

Voraussetzung dafür, daß das Dateienregister sinnvoll für die vorgesehenen Zwecke genutzt werden kann, ist seine *Vollständigkeit und Aktualität.* Dies bedeutet, daß die öffentlichen Stellen des Landes ihrer Meldepflicht pünktlich und umfassend nachkommen und an eine regelmäßige Aktualisierung denken. Viele öffentliche Stellen sehen sich dazu jedoch nicht in der Lage. Dies hat verschiedene Gründe:

Auch viele große öffentliche Stellen haben ihre behördlichen Datenschutzbeauftragten nur mit einem geringen Zeitbudget für ihre Aufgaben ausgestattet. Der Vollzeit-Datenschutzbeauftragte ist auch bei den Bezirksämtern, den Senatsverwaltungen und den großen nachgeordneten Behörden eine sehr seltene Ausnahme. Die behördlichen Datenschutzbeauftragten haben meistens mit mühsamer Sammel- und Forschungstätigkeit die Erstmeldungen erstattet. Aber insbesondere beim Geräteregister können sie dem häufigen Aktualisierungsbedarf, der durch die schnelle Entwicklung der Informationstechnik gegeben ist, nicht mehr nachkommen. Dies wird auch dadurch erschwert, daß innerhalb der Behörden die Meldungen zu den internen Registern und dem Dateienregister als nicht nachvollziehbares bürokratisches Hindernis für den Aufbau der Informationstechnik angesehen werden.

Die Unvollständigkeit des Registers hat zur Folge, daß Dateien, die nicht gemeldet worden sind bzw. nicht in die internen Verzeichnisse aufgenommen wurden, der Kontrolle durch den Ber-

Auch der Senat hält es für sachgerecht, wenn im Zuge der Anpassung des BlnDSG an die EU-Datenschutzrichtlinie eine Reform hinsichtlich der Meldepflichten zum Dateienregister erfolgt, die im übrigen auch § 2 Abs.2 IVG betrifft. Die jetzigen Meldepflichten stehen in Anbetracht ihres bürokratischen Aufwandes in keinem Verhältnis zum Nutzen des zentralen Dateienregisters.

liner Datenschutzbeauftragten bzw. durch den behördlichen Datenschutzbeauftragten praktisch entzogen sind. Die gesetzeswidrige Unterlassung der Meldung wird mit einer Verschonung mit Kontrollen „belohnt“.

Die mangelnde Aktualität des Registers macht es für die Vorbereitung von Kontrollmaßnahmen praktisch unbrauchbar. Vor Kontrollen bleibt es wichtig, Informationen zur Vorbereitung zeitnah gesondert einzuholen.

Die *Einsichtnahme durch Bürger* erfolgt sehr selten, wenn überhaupt, dann für empirische Erhebungen oder zur Vorbereitung politischer Initiativen. Der wichtigste Grund für die Öffentlichkeit des Dateienregisters, nämlich die Unterstützung des Bürgers bei der Durchsetzung seiner eigenen Datenschutzrechte, spielt überhaupt keine Rolle.

Angesichts dieser Erkenntnisse ist festzustellen, daß der erhebliche, aber meist vergebliche bürokratische Aufwand, den die meldepflichtigen Stellen für die Umsetzung der Meldepflicht treiben und der ebenfalls erhebliche technische und organisatorische Aufwand zur Führung des öffentlichen Dateienregisters beim Berliner Datenschutzbeauftragten, in keinem angemessenen Verhältnis zu dem Nutzen für den Datenschutz steht.

Die Meldepflicht bedarf also einer *Reform*, die den Meldeaufwand der meldepflichtigen Stellen reduziert, den Aktualisierungsbedarf erheblich verringert und von der technischen Entwicklung unabhängiger ist.

Allerdings sollten auch nach der Reform die für *Kontrollzwecke* notwendigen Mindestinformationen vor Ort und beim Berliner Datenschutzbeauftragten zur Verfügung stehen und dem Bürger ein zweckmäßiges Mittel zur Gewinnung von *Transparenz* bei der behördlichen Datenverarbeitung in die Hand gegeben werden.

Die EU-Datenschutzrichtlinie vom 24. Oktober 1995 sieht ebenfalls Meldepflichten an die unabhängigen Kontrollstellen vor, die im Vergleich zu den Meldepflichten des Berliner Datenschutzgesetzes eingeschränkt sind. Sie erlaubt ferner eine Vereinfachung der Meldung oder sogar eine Ausnahme von der Meldepflicht, wenn unabhängige Datenschutzbeauftragte die Umsetzung des Datenschutzrechts kontrollieren und die datenverarbeitenden Stellen ein eingeschränktes internes Register zur Einsichtnahme der Öffentlichkeit bereithalten. Das neue EU-Recht gibt also bereits Denkrichtungen an und die Anpassung des Berliner Datenschutzgesetzes an das EU-Recht sollte der Anlaß sein, die Meldepflicht zum Dateienregister grundlegend zu reformieren.

### 5.2 Der Berliner Datenschutzbeauftragte

#### 5.2.1 Die Dienststelle

Beim *Personalbestand* der Dienststelle gab es im vergangenen Jahr keine Veränderungen. Trotz der vergleichsweise guten Ausstattung steht die Anzahl der Mitarbeiterinnen und Mitarbeiter nach wie vor in einem krassen Mißverhältnis zu den zu bewältigenden Aufgaben. So steht etwa für die technisch-organisatorischen Prüfungen bei PCs ein einziger Experte zur Verfügung (für sämtliche Geräte in Verwaltung und Privatwirtschaft), entsprechend verhält es sich mit den anderen Techniken wie proprietäre Systeme, Netzwerke oder Client-Server-Anwendungen. Auch bei den Juristen haben die Mitarbeiterinnen und Mitarbeiter Arbeitsgebiete zu bewältigen, die sich jeweils über mehrere Geschäftsbereiche und Wirtschaftszweige erstrecken.

In dieser Situation können systematische Prüfungen nur in allergeringstem Umfang durchgeführt werden. Vielmehr muß sich die Arbeit auf exemplarische Sachverhalte beschränken, die uns üblicherweise durch Eingaben, Beratungsersuchen oder öffentliche Diskussionen bekannt werden. Große Bedeutung kommt der Verbreitung der Arbeitsergebnisse, auch in Form von Veröffentlichungen zu. Sollte es auf Grund der Haushaltssituation nicht möglich sein, mit der rasanten Ausbreitung der Informationstechnik auch die Kontrollbehörde zu verstärken, müssen künftig auf dem Gebiet der Öffentlichkeitsarbeit mehr Mittel bereitgestellt werden.

Zusätzliche Beschränkungen insbesondere der Prüftätigkeit müssen wir uns seit Mitte vergangenen Jahres auferlegen, seit der bisher zur Verfügung gestellte personengebunde Dienstwagen

des Datenschutzbeauftragten, der für die Aktitvitäten der gesamten Dienststelle genutzt werden konnte, gestrichen wurde. Die nunmehr mögliche – entgeltpflichtige – Nutzung der Fuhrbereitschaft des Fuhrparks kann die Flexibilität nicht bieten, die ein ständig zur Verfügung stehendes Fahrzeug hat.

Erneut beteiligten sich Mitarbeiterinnen und Mitarbeiter – in der Regel in ihrer Freizeit – an Aus- und Fortbildung auf dem Gebiet des Datenschutzes an den verschiedensten Berliner (und auch Brandenburger) Bildungseinrichtungen. In vielen Vorträgen wurden unsere Arbeitsergebnisse und auch weiterführende Gedanken dem Fachpublikum vorgetragen; hierunter befanden sich auch zum Teil auf Einladung der Organisatoren Vorträge im Ausland, z. B. Beiträge des Datenschutzbeauftragten zu datenschutzrechtlichen Aspekten der Verwendung von Namen und Pseudonymen bei der Datenverarbeitung vor dem 18. Weltkongreß für Rechtsphilosophie im August in Buenos Aires oder zur Aufarbeitung der DDR-Vergangenheit vor dem Internationalen Kongreß zum Datenschutz im September in Montreal sowie ein Vortrag des Vertreters des Datenschutzbeauftragten Dr. Dix zum Datenschutz in der Telekommunikation vor der Jahrestagung der Internetgesellschaft im Juni in Kuala Lumpur[203].

Nach wie vor wird die Dienststelle gerne von in- und ausländischen Gästen aufgesucht, um sich über den Datenschutz in Berlin, aber auch allgemein die Bedeutung des informationellen Selbstbestimmungsrechts in Deutschland aufklären zu lassen. So waren neben vielen Einzelpersonen u. a. auch Besuchergruppen aus China, Rußland und der Slowakei bei uns.

Ausweislich der Analyse des Haushaltsplans 1998 betragen die Kosten der gesamten Dienststelle etwa 1 DM pro Einwohner im Jahr (Senatsverwaltung für Inneres ohne nachgeordnete Behörden: 217 DM)

### 5.2.2 Zusammenarbeit mit dem Abgeordnetenhaus

Zur Einbringung des Jahresberichts 1996 sowie der Stellungnahme des Senats hierzu hat der Datenschutzbeauftragte erneut eine kurze Rede gehalten, in der leider auch auf die beschriebenen Mißstimmungen[204] eingegangen werden mußte[205].

Sehr konstruktiv verlief wiederum die Zusammenarbeit mit dem Unterausschuß Datenschutz des Ausschusses für Inneres, Sicherheit und Ordnung unter Leitung des Abgeordneten Rüdiger Jakesch. Intensiv beraten wurde neben einzelnen strittigen Themen des letzten Jahresberichts insbesondere der Entwurf für ein Sicherheitsüberprüfungsgesetz, bei dem deutliche datenschutzrechtliche Verbesserungen erzielt werden konnten[206].

Unser Rat wurde auch von anderen Ausschüssen, u. a. dem Petitionsausschuß, gesucht. Hinzu kam eine konstruktive Zusammenarbeit mit den Fraktionen und einzelnen Abgeordneten.

### 5.2.3 Kooperation mit anderen Datenschutzbehörden

Das Datenschutzgesetz verpflichtet zur Zusammenarbeit mit allen Stellen, die mit Kontrollaufgaben des Datenschutzes beauftragt sind (§ 24 Abs. 4 BlnDSG). Das wichtigste Gremium hierfür ist die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die unter dem Vorsitz des Bayerischen Landesbeauftragten für den Datenschutz Reinhard Vetter am 17./18. April in München sowie am 23./24. Oktober in Bamberg tagte; die Beschlüsse und anderen Dokumente sind im Anhang abgedruckt[207]. Tagesort der Konferenz im Jahr 1998 ist Wiesbaden. Intensiv wirkten wir auch bei den verschiedenen Arbeitskreisen der Konferenz mit, besonders beim Arbeitskreis Technik unter dem Vorsitz des Landesbeauftragten von Mecklenburg-Vorpommern, Dr. Werner Kessel. Die dort erstellten Arbeitspapiere[208] stellen wichtige Arbeitsmaterialen für die Prüf- und Beratungspraxis dar. Selbst führen wir den Vorsitz im Arbeitskreis Medien, der sich mit einer Vielzahl von datenschutzrechtlichen Problemen der Telekommunikation befaßte. Es kam auch zu einer Reihe von bilateralen Gesprächen, insbesondere mit dem brandenburgischen Landesbeauftragten Dr. Dietmar Bleyl.

203 vgl. unten 5.2.3
204 vgl. oben Einleitung sowie 3.2
205 Anlage 1
206 vgl. oben 4.1.2
207 Anlage 2
208 vgl. oben 2

An den Sitzungen des Düsseldorfer Kreises, in dem sich seit genau 20 Jahren die Obersten Aufsichtsbehörden für den privaten Bereichen zusammengeschlossen haben, nahmen wir teil, besonders intensiv an dem dort bestehenden Arbeitskreis für Kreditwirtschaft. Zur Koordination bei der Umsetzung des Teledienstgesetzes[209] war bereits 1996 von uns ein Koordinationskreis ins Leben gerufen worden, der sich um die Abstimmung der verschiedenen, mit der Kontrolle der On-line-Dienste befaßten Instanzen mühen soll. Neben dem für den Netzbereich zuständigen Bundesbeauftragten, den Landesbeauftragten und den Aufsichtsbehörden nimmt auch ein Vertreter der Datenschutzbeauftragten der Rundfunkanstalten teil. Nach anfänglichem Zögern der Aufsichtsbehörden[210] hat nunmehr eine fruchtbare Zusammenarbeit stattgefunden.

Die *Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation,* deren Sekretariat beim Berliner Datenschutzbeauftragten angesiedelt ist, hat sich in diesem Jahr zu zwei Arbeitssitzungen in Paris und Berlin getroffen. Die Sitzung in Paris wurde auf Einladung der französischen Datenschutzkommission gemeinsam mit der Europäischen Gruppe zu Internationalen Datennetzen (GERI) durchgeführt. Dabei standen erneut die zahlreichen noch ungelösten Datenschutzprobleme im Zusammenhang mit der stark wachsenden Nutzung des Internets im Vordergrund. Auf der erwähnten Jahrestagung der *Internet Society* in Kuala Lumpur wurde das von der Internationalen Arbeitgruppe zum Datenschutz in der Telekommunikation ausgearbeitete *Budapest-Berlin-Memorandum*[211] den Konferenzteilnehmern erläutert. Dieses Memorandum, das als eines der ersten international abgestimmten Dokumente die Datenschutzprobleme im Internet thematisiert, stieß bei der Internet Society auf großes Interesse. Diese regierungsunabhängige Berufsorganisation besteht aus über 100 Organisationen und 7 000 individuellen Mitgliedern aus mehr als 150 Ländern. Zu ihren Zielen zählt auch die Sicherstellung des Schutzes der Privatsphäre im Internet.

Schließlich konnten wir das *Budapest-Berlin-Memorandum zum Datenschutz im Internet* auch bei einer Sitzung der Europäischen Gruppe zum Schutz personenbezogener Daten nach Art. 29 der EG-Datenschutzrichtlinie erläutern. Diese Gruppe hat daraufhin die Europäische Kommission beauftragt, auf der Grundlage des Memorandums weitere Maßnahmen zur Verbesserung des Datenschutzes vorzuschlagen. Über Datenschutzprobleme im Internet haben wir auch auf der 19. Internationalen Datenschutzkonferenz in Brüssel berichtet.

Ein Gesprächskreis zum grenzüberschreitenden Datenverkehr, an dem neben europäischen und amerikanischen Experten auch Wirtschaftsvertreter von beiden Seiten des Atlantiks teilnahmen und der von uns zusammen mit dem American Institute for Comtemporary Evermam Studies in Washington organisiert wurde, setzte seine weiterführende Arbeit fort. Hauptthema ist dort die Frage, in welchem Verhältnis gesetzliche Regelungen und Selbstregelungsmechanismen stehen.

### 5.2.4 Öffentlichkeitsarbeit

Bereits seit dem 21. März 1996 ist der Berliner Datenschutzbeauftragte mit einem eigenen Programm unter „http://www.datenschutz-berlin.de“ im *Internet* präsent. Die durchschnittlich über 100 000 Dateiabrufe jeden Monat zeigen, daß unser Angebot mit Themen rund um den Datenschutz (Termine, Aktuelles, Datenschutzrecht, Technisch-organisatorische Maßnahmen) auf eine große – auch internationale – Resonanz stößt. Das große Interesse hat unsere Erwartungen übertroffen und war Anlaß und Ansporn dafür, dem Ausbau und der inhaltlichen Pflege des Programmes einen Schwerpunkt in unserer Öffentlichkeitsarbeit einzuräumen. Da datenschutzrelevante Themen zunehmend internationale Bezüge aufweisen, haben wir damit begonnen, unter „http://www.privacy.de“ ein Programmangebot mit englischen Texten aus den Bereichen „Data Protection and Privacy“ aufzubauen. Parallel hierzu hat sich der Berliner Datenschutzbeauftragte dazu bereit erklärt, für seine Kollegen – die Datenschutzbeauftragten des Bundes und der Länder – unter „http://www.datenschutz.de“ ein einheitliches Angebot mit Informationen

209 vgl. oben 3.3
210 vgl. JB 1996, 5.2.5
211 JB 1996, Anlage 5.1

zum Datenschutz in Deutschland zu verwalten. Auf europäischer und internationaler Ebene ist er maßgeblich an Projekten beteiligt, die sich mit der Koordinierung der vielfältigen und unterschiedlichen „Data Protection and Privacy"-Angebote im Internet befassen.

Traditionell veranstaltet der Berliner Datenschutzbeauftragte anläßlich der im zweijährigen Rythmus stattfindenden *„Internationalen Funkausstellung"* ein öffentliches Symposium zu einem datenschutzrelevanten Thema aus dem Bereich Telekommunikation und Medien. Im Rahmen der Veranstaltung am 1. September 1997 zu dem Thema: „Das Internet – Ende des Datenschutzes?" diskutierten Datenschutzbeauftragte, Wissenschaftler und Experten aus dem In- und Ausland mit interessierten Bürgern, Journalisten und Vertretern der Wirtschaft die Konsequenzen, die sich für den Datenschutz aus der Entwicklung des Internets ableiten lassen.

Sein besonderes Augenmerk richtet der Berliner Datenschutzbeauftragte auf eine konsequente und dabei informative *Pressearbeit.* Auch im vergangenen Jahr haben wir die Position des Datenschutzes in aktuellen Diskussionen mehrfach durch Erklärungen an die Presse öffentlich vertreten. Geäußert haben wir uns u. a. im Zusammenhang mit der Angabe von Patientennamen durch Ärzte in Fahrtenbüchern zum Nachweis für Werbungskosten gegenüber dem Finanzamt, zu Verbraucherbefragungen, zu datenschutzgerechten Decodern für digitales Fernsehen und Internet-TV und zum Datenschutz bei Multimedia.

Auf Grund der angespannten Haushaltslage, in der sich das Land Berlin befindet, waren und sind ausgeprägte *Sparmaßnahmen* erforderlich. Der Berliner Datenschutzbeauftragte hat diesem Umstand ebenfalls Rechnung tragen müssen. Davon betroffen waren insbesondere auch bereits geplante Projekte im Rahmen der Öffentlichkeitsarbeit, die unter den genannten Bedingungen nicht realisiert werden konnten. So konnte der Nachdruck des „Datenscheckheftes" – nachdem die Vorauflage aus dem Jahr 1996 auf Grund der immensen Nachfrage bei den Bürgern bereits frühzeitig vergriffen war – nicht erfolgen. Bereits konzipierte Vorhaben, unsere Reihe zum Berliner Informationsgesetzbuch zu erweitern, mußten zurückgestellt werden.

Ein Projekt, das bereits seit längerem in Vorbereitung war, konnte jedoch umgesetzt werden. Im Dezember 1997 ist in der Reihe „Materialien zum Datenschutz" mit dem Heft Nr. 25 eine Broschüre zum Thema *„Datenschutz und informationstechnische Sicherheit bei PCs"* erschienen und auf ein breites Interesse gestoßen.

Berlin, den 23. März 1997

Dr. Hansjürgen Garstka
Berliner Datenschutzbeauftragter

Berlin, den 25. Juni 1998

Der Senat von Berlin
Diepgen
Regierender Bürgermeister