Abgeordnetenhaus von Berlin **Drucksache 13 / 303**

13. Wahlperiode

Bericht

des Berliner Datenschutzbeauftragten

zum 31. Dezember 1995

Der Berliner Datenschutzbeauftragte hat dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§ 29 Berliner Datenschutzgesetz – BlnDSG –). Der vorliegende Bericht schließt an den am 28. März 1995 vorgelegten Jahresbericht 1994 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 1995 ab.

Wir kommen damit zugleich den Pflichten nach § 6 Abs. 3 Gesetz zu dem Staatsvertrag über den Rundfunk im vereinten Deutschland vom 31. August 1991 und zu Art. 36 des Einigungsvertrages nach.

Erstmals ist dieser Jahresbericht über das Internet (http://www.datenschutz-berlin.de) abrufbar, dabei stehen auch zitierte Dokumente zur Verfügung, die nicht im Anhang abgedruckt sind.

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.

Inhaltsverzeichnis

1. Rechtliche Rahmenbedingungen

1.1 Datenschutz in Berlin

Mit dem vergangenen Jahr ist die 12. Wahlperiode des Berliner Abgeordnetenhauses zu Ende gegangen. Das Parlament hat in dieser Zeit auf dem Gebiet des Datenschutzes bemerkenswerte Arbeit geleistet, die Berlin zu dem Bundesland gemacht hat, das die Vorgaben des Bundesverfassungsgerichtes zu einer *normenklaren Regelung der Datenverarbeitung und des Datenschutzes* am weitesten umgesetzt hat. Hierzu gehören die Neufassungen des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) sowie des Verfassungsschutzgesetzes, die Verabschiedung eines Ausführungsgesetzes zum Gerichtsverfassungsgesetz, des Landesarchiv- und Statistikgesetzes ebenso wie die Vielzahl neuer Bestimmungen, mit denen im „Artikelgesetz“ vom 26. Januar 1993[1] 23 Gesetze um Datenverarbeitungsregelungen ergänzt wurden. Rechtsverordnungen präzisieren die in den Gesetzen enthaltenen allgemeinen Bestimmungen und ermöglichen für künftige Verfahrensänderungen die erforderliche Flexibilität. Mit den Verordnungen über die Benutzung des Liegenschaftskatasters mit Hilfe automatisierter Abrufverfahren sowie die Abgabe digitaler Angaben aus dem Liegenschaftskataster[2] wurden im vergangenen Jahr die letzten Pflichten zur Schaffung von Datenschutzverordnungen eingelöst.

Als großes Gesetzesvorhaben wurde nunmehr endlich auch das *Landesbeamtengesetz*[3] mit den Regelungen über die Verarbeitung von Personaldaten an das Beamtenrechtsrahmengesetz angepaßt. Nicht realisiert wurde lediglich das *Sicherheitsüberprüfungsgesetz*[4], das zwar noch in den Gesetzgebungsprozeß eingeführt, aber nicht mehr zu Ende beraten wurde. Wie wichtig klare Rechtsgrundlagen für staatliche Informationsansprüche sind, zeigte die Debatte, die aufflammte, als die Jugendverwaltung daranging, den vom Bundesgesetzgeber vorgegebenen Anspruch auf einen *Kindergartenplatz* umzusetzen und Daten zur Ermittlung von Härtefällen zu erheben. Mangels präziser Vorgaben mußte sich die Jugendverwaltung vielerlei Vorwürfe darüber gefallen lassen, daß sie zu viele Daten über die persönlichen Verhältnisse von Eltern und Kindern sammele.[5]

Von grundlegender Bedeutung für die Arbeit des Datenschutzbeauftragten war die Änderung des Berliner Datenschutzgesetzes vom 3. Juli 1995[6], die die Aufgaben der *Aufsichtsbehörde für den nichtöffentlichen Bereich* von der Senatsverwaltung für Inneres auf den Berliner Datenschutzbeauftragten verlagerte (§ 33 Abs. 1)[7]. Damit wurde einer jahrealten Empfehlung Rechnung getragen, im Land Berlin die Datenschutzkontrolle über die öffentliche Verwaltung und über Privatunternehmen in einer Hand zusammenzuführen, um dem Bürger eine einheitliche, möglichst effektive Datenschutzkontrollinstanz zur Verfügung zu stellen.

Mit der gleichen Gesetzesänderung wurde die strenge Regelung des Berliner Datenschutzgesetzes abgemildert, nach der die Verarbeitung personenbezogener Daten von Behörden ausschließlich auf einer expliziten Rechtsgrundlage oder mit Einwilligung der Betroffenen möglich ist. Nunmehr genügt in den Fällen, in denen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden, die Erforderlichkeit für die Aufgabenerfüllung der Behörde (§ 6 Abs. 1 Satz 2 i. V. m. § 9 BlnDSG). Diese Bestimmung macht zwar grundsätzlich die spezialrechtliche Regelung von Datenverarbeitung und Datenschutz nicht entbehrlich, schafft aber Erleichterung in den Fällen der *„Trivialdatenverarbeitung“*, bei denen sich die Verwaltung z. B. allgemein zugänglicher Informationsquellen wie des Telefonbuchs bedient oder Adressenlisten für den Informationsversand im Interesse der Bürger verarbeitet.

Eine ähnliche Zielrichtung hatte bereits das Gesetz über die Informationsverarbeitung bei der allgemeinen Verwaltungstätigkeit vom 9. Oktober 1992 verfolgt, das eine Rechtsgrundlage für die in allen Verwaltungen wahrzunehmenden Grundfunktionen darstellt und Erleichterungen auch hinsichtlich der Meldepflichten schafft. Seit Jahren fordern wir, daß dieses Gesetz um allgemeine Bestimmungen für besondere Formen der Datenverarbeitung in der öffentlichen Verwaltung ergänzt wird, die nicht bereichsspezifisch, sondern für alle Verwaltungszweige relevant sind; hierunter fallen Probleme des PC-Einsatzes bei der Heimarbeit, des Outsourcing, der Ausgestaltung des Behördentelefonnetzes ebenso wie Aufgabe und Stellung des *Landesamtes für Informationstechnik* samt seiner neuen Funktionen beim Verwaltungsnetz[8]. Die Erarbeitung eines entsprechenden Gesetzes wird vordringliche Aufgabe in den nächsten Jahren sein.

Unbewältigt ist schließlich noch die Aufgabe, das Prinzip der *Informationsfreiheit* gesetzlich zu verankern. Zwar ist dieses Prinzip im Gegensatz zur brandenburgischen Verfassung (Art. 21 Abs. 4) in der Berliner Verfassung nicht ausdrücklich verbürgt. Es entspricht aber einem modernen Demokratieverständnis, den Bürgern Einsicht in Akten und sonstige amtliche Unterlagen auch dann zu gestatten, wenn sie nicht selbst unmittelbar betroffen sind; überwiegende öffentliche oder private Interessen sind dabei natürlich zu wahren. Die Koalitionsvereinbarung hatte in der letzten Legislaturperiode einen entsprechenden Auftrag enthalten; zur Realisierung kam es jedoch nicht.

Herausragendes Ereignis in der Gesetzgebung war die Verabschiedung der *neuen Verfassung von Berlin* am 22. Juni 1995 sowie die Zustimmung einer breiten Mehrheit der Bevölkerung am 22. Oktober 1995[9]. Die neue Verfassung enthält nicht nur an neuer Stelle in Art. 33 das Grundrecht auf Datenschutz, nämlich das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Die neue Verfassung hebt darüber hinaus die Stellung des Datenschutzbeauftragten hervor, der in Art. 47 nunmehr im Rahmen des Abschnitts über die Volksvertretung Verfassungsrang erhält. Auch damit wird Berlin dem Bundesverfassungsgericht in besonderer Weise gerecht, daß unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung ist.[10]

Von entscheidender Bedeutung für die weiteren legislativen Aktivitäten ist natürlich der Ausgang der Volksabstimmungen in den Ländern Berlin und Brandenburg über den *Neugliederungsvertrag* am 5. Mai 1996. Sollte es zur Bildung eines gemeinsamen Bundeslandes kommen, wird im Rahmen der Vereinheitlichung der Gesetzgebung das Datenschutzrecht zu den ersten Materien gehören, die aneinander angepaßt werden müssen.[1] Dies kann sich nicht auf die Datenschutzgesetze selbst beschränken, sondern wird auch die spezialrechtlichen Regelungen umfassen müssen.

Auch beim Weiterbestand beider Länder wird es einen großen Anpassungsbedarf geben. Es werden zunehmend mehr gemeinsame Verfahren entwickelt werden oder zumindest der Bedarf bestehen, auf Datenbestände des jeweils anderen Landes zuzugreifen. Eine sinnvolle Datenschutzpolitik ist nur dann möglich, wenn das beiderseitige Recht ein Höchstmaß an Übereinstimmung vorweist und auch die jeweiligen Landesbeauftragten ihre Aktivitäten aufeinander abstimmen. Dies wird in jedem Fall geschehen.

1.2 Deutschland und Europa

Da der Bundestag erst Ende 1994 seine Arbeit wieder aufgenommen hat, hat sich im vergangenen Jahr in der *Bundesgesetzgebung* wenig geändert. Lange angemahnte Gesetzgebungsvorhaben etwa im Bereich der Justiz und der Steuerverwaltung sind zwar diskutiert, aber kaum einen Schritt vorangebracht worden. Erneut sind große Debatten um die Einführung des *„Großen Lauschangriffs“* geführt worden; trotz der anhaltenden Forderungen auf die Zulassung dieser Maßnahme durch die Sicherheitsbehörden sowie des Ausgangs der FDP-Mitgliederbefragung halten

1 Jahresbericht 1993, 1.2
2 vgl. 5.2
3 vgl. 5.5.5
4 vgl. 5.1
5 vgl. 5.6
6 GVBl. 1995, 404
7 vgl. 3.1, 6.1
8 vgl. 2.2
9 GVBl. S. 421, 719
10 BVerfGE 65, 46
11 Art. 52 Abs. 1 Ziffer 3 Neugliederungsvertrag

wir mit fast allen anderen Datenschutzbeauftragten des Bundes und der Länder an der Auffassung fest, daß die Intensität des Eingriffs in das Grundrecht auf freie Kommunikation in keinem akzeptablen Verhältnis zu den erwartbaren Erträgen für die Strafverfolgung steht.

Von zentraler Bedeutung für die Fortentwicklung des Datenschutzes ist das Inkrafttreten der *Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* (EU-Richtlinie)[12]. Die Richtlinie enthält eine Vielzahl von Bestimmungen, die interessante und weiterführende Aspekte aus den Datenschutzgesetzen der anderen Mitgliedsländer aufgreifen oder – wie zum Geltungsbereich der nationalen Gesetze in der Union oder zum Datenexport – zusätzliche europarechtliche Regelungen schaffen.

Die *deutschen Gesetzgeber* im Bund und in den Ländern sind aufgerufen, die Ansätze zur Verbesserung des Rechts auf informationelle Selbstbestimmung aufzugreifen und eine Rechtslage zu schaffen, die in der Tradition des wegbereitenden deutschen Datenschutzrechtes steht. Hierbei sollten auch bisher nicht gelöste und neu entstandene Probleme des Datenschutzes insbesondere im Hinblick auf die neuen technischen Entwicklungen aufgegriffen werden. Versuchen, in minimalistischer Weise nur die Bestimmungen der Richtlinie umzusetzen, die für die Harmonisierung unerläßlich sind, sollte entgegengewirkt werden.

Unter den änderungsbedürftigen Aspekten hervorzuheben ist die verstärkte Bedeutung des *Schutzes sensibler Daten*, die bereits von der Europaratskonvention[13] vorgegeben war; der deutsche Gesetzgeber hatte nur in sehr zurückhaltender Weise Sonderregelungen für „personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben“ (Art. 8 Abs. 1) geschaffen. Die Richtlinie fordert demgegenüber die *Untersagung* der Verarbeitung dieser Daten, wenn nicht relativ eng begrenzte Voraussetzungen vorliegen. Diese Voraussetzungen werden schwerlich im Bundesdatenschutzgesetz selbst Platz finden können; vielmehr wird die Umsetzung der Richtlinie auch neue gesetzliche Regelungen in bisher vernachlässigten Bereichen erzwingen, etwa in der Strafprozeßordnung, einem zu schaffenden Arbeitnehmerdatengesetz oder bundesrechtlichen Vorgaben zur Verarbeitung medizinischer Daten. Trotz des Widerstandes der Kirchen gegen ihre Einbeziehung in die Richtlinie, der von den deutschen Kirchen erheblich heftiger vorgebracht wurde als selbst von Kirchen mit Staatsreligionen wie Spanien oder Dänemark, wird man um grundsätzliche Erörterungen über die Verarbeitung von Daten über die Mitglieder von Religionsgemeinschaften in staatlichen und privaten Datensammlungen nicht herum können.

Ein im deutschen Recht jedenfalls als allgemeiner Grundsatz ungewohnter Gedanke ist das *Widerspruchsrecht gegen rechtmäßige Datenverarbeitung* (Art. 14), wenn er auch in einigen Rechtsmaterien schon verankert ist (vgl. § 28 Abs. 3 Bundesdatenschutzgesetz, § 76 Abs. 2 Sozialgesetzbuch X, § 10 Abs. 4 Post- und Telekommunikations-Regulierungsgesetz). Gleichwohl verkörpert er ein wesentliches Gegengewicht gegen die generalklauselartigen Befugnisnormen des Datenschutzrechtes. Das Widerspruchsrecht würde Betroffenen die Möglichkeit geben, aus sich aus ihrer besonderen Situation ergebenden Gründen Widerspruch gegen die Verarbeitung seiner Daten einzulegen. Dies hätte etwa Bedeutung im Rahmen von Arbeitsverhältnissen, wenn der Arbeitnehmer vom Arbeitgeber zwar zulässigerweise gespeicherte, gleichwohl aber für das Arbeitsverhältnis nicht unerläßliche Daten gelöscht haben will. Das Widerspruchsrecht sollte daher als eine neuartige, den individuellen Aspekt des informationellen Selbstbestimmungsrechts in besonderem Maße betonende Regelung eingeführt werden.

Das Verbot, *Entscheidungen (gegen Personen) nur auf Grund automatisierter Vorgänge* zu treffen (Art. 15), ist in der informatikkritischen Literatur ein alter Topos, der bisher nur in das französische Recht Eingang gefunden hat. Im deutschen Recht konterkariert z. B. § 37 Abs. 4 Verwaltungsverfahrensgesetz diesen Gedanken zwar, gleichwohl findet sich eine der Richtlinie entsprechende Regelung in § 56 f Abs. 4 Beamtenrechtsrahmengesetz sowie den Folgevorschriften des Bundes und der Länder. Auch in der Rechtsprechung gibt es Tendenzen, dieses Prinzip anzuerkennen.[13 a] Die Übernahme dieser Vorschrift erscheint daher nicht nur geboten, sondern sogar als eine wesentliche Bestimmung zur Gewährleistung der informationellen Selbstbestimmung bei zunehmender Automatisierung.

Artikel 27, der entsprechend niederländischen Rechtsgedanken die Ausarbeitung und Verbindlichmachung von *Codes of Conduct* für einzelne Gesellschaftsbereiche zuläßt, ist dem deutschen Satzungsrecht vergleichbar (vgl. z. B. die Regelungen zur ärztlichen Schweigepflicht in den Ärztlichen Berufsordnungen). Die Übernahme der Vorschrift wird es weiten Bereichen gestatten, die allgemeinen gesetzlichen Bestimmungen durch selbstgestaltete Regelungen zu untersetzen.

Der künftigen Ausgestaltung der *Kontrollinstanzen* und ihrer Befugnisse kommt naturgemäß eine erhebliche Bedeutung zu. Das ursprünglich favorisierte Idealbild einer *einheitlichen* „Kontrollstelle“ in jedem Mitgliedsstaat ist in föderal organisierten Staaten nicht zu realisieren. Gleichwohl ergibt sich aus dem Regelungskonzept des Artikels 28 der Richtlinie, die vor allem die Effektivität der Arbeit betont, daß eine Zersplitterung der Datenschutzkontrolle, wie sie derzeit in der Bundesrepublik besteht, nicht richtlinienkonform ist. Vielmehr muß Anliegen der Umsetzung sein, einen möglichst klar organisierten, schlanken Kontrollapparat zu schaffen. Insoweit ist die neue Berliner Regelung vorbildlich und wird von den zuständigen Stellen der Europäischen Kommission auch als nachahmenswert angepriesen.

Die Datenschutzkontrollbehörden müssen die ihnen zugewiesenen Aufgaben „in völliger Unabhängigkeit“ wahrnehmen. Trotz aller Verhandlungskunst der deutschen Innenministerien bei der Vorbereitung der Richtlinie, die darauf abzielte, den deutschen Status quo zu erhalten, besteht kein Zweifel, daß „*völlige Unabhängigkeit*“ die Einbindung der Datenschutzkontrollinstanzen in ministerielle Weisungsstränge ausschließt. Die Aufrechterhaltung eines Zustandes, in dem die Aufsichtsbehörden der fachlichen Weisung durch übergeordnete Stellen unterliegen, ist gemeinschaftswidrig. Darüber hinaus wirft auch die organisatorische, dienstrechtliche oder rechtsaufsichtliche Einbindung die Frage auf, ob das Kriterium der „völligen Unabhängigkeit“ erfüllt ist.

Den Kontrollinstanzen müssen auch *ohne Anlaß umfassende Untersuchungs- und wirksame* (im englischen und französischen Text deutlicher: *effektive*) *Einwirkungsbefugnisse* zur Verfügung stehen. Dies schließt die Begrenzung der Kontrolle im nichtöffentlichen Bereich auf die Anlaßkontrolle aus. Auf der anderen Seite sollten (auch im öffentlichen Bereich) die Befugnisse über die Empfehlungskompetenz hinaus auf konkrete Weisungsbefugnisse ausgedehnt werden.

2. Technische Rahmenbedingungen

2.1 Entwicklung der Informationstechnik

Die Entwicklung der Informationstechnik hat sich auch im Berichtsjahr an den schon in den Vorjahren beobachteten Trends orientiert:

- Das *Preis-Leistungs-Verhältnis* hat sich für Hardware und für Standardsoftware weiter verbessert;
- der Trend zur *Miniaturisierung* hält weiter an;
- die „Datenautobahnen“ werden weiter ausgebaut: Neue *Online-Dienste* werden eingerichtet, das *Internet* wirkt für immer mehr Teilnehmer anziehend;[14]
- Bild- und Sprachverarbeitung werden weiter digitalisiert und somit für „*Multimedia*“ erschlossen;[15]

12 Amtsblatt der Europäischen Gemeinschaften Nr. L 281/31
13 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) vom 28. Januar 1981
13 a vgl. OLG, Beschluß v. 17. 5. 1995 [2 Ss (OWi) 46 B/95]
14 vgl. 2.2, 4.1
15 vgl. 2.2, 4.2

- *Proprietäre (herstellerabhängige) Systeme* werden im Rahmen von „Right"- oder „Downsizing" weiter von offenen Systemen zurückgedrängt. Allerdings ist die Tendenz erkennbar, sie zu den offenen Systemen hin zu öffnen, um so die Leistungsvorteile der meisten proprietären Systeme auch dort zugänglich zu machen, wo man sich ansonsten herstellerunabhängig ausstatten möchte;
- Rechnerleistung wird durch *Client-Server-Systeme* über lokale Netze an den Arbeitsplatz gebracht;[16]
- durch *Outsourcing* wird komplexe Datenverarbeitung in spezialisierte Unternehmen ausgelagert;[17]
- neue *Chipkartenanwendungen* werden konzipiert, vornehmlich mit Prozessorchipkarten, die multifunktional eingesetzt werden können.[18]

Erkennbar sind bereits erste Tendenzen, die gegenüber den Entwicklungen der Vorjahre gegenläufig wirken:

Die „Demokratisierung" des Einsatzes von Informationstechnik, hervorgerufen durch die Ausbreitung preiswerter Personalcomputer, die für jeden erschwinglich und für jeden einfach benutzbar sind und so zur Informatisierung der Privathaushalte und kleinen Unternehmen führten, wird partiell durch *komplexe Vernetzungen* rückgängig gemacht. Obwohl sie große Verbreitung für professionelle Anwendungen finden, ist die Beherrschung von Client-Server-Netzen ohne detaillierten Sachverstand kaum noch möglich. Der Trend, auch in der Welt der kommerziellen oder administrativen Datenverarbeitung auf den Einsatz von DV-Profis verzichten zu können, wird dadurch gebrochen. Ohne die Vorhaltung eigener Fachleute oder Einschaltung von Beratungsfirmen sind moderne Bürosysteme kaum noch zu beherrschen, ein Zustand, der an die Zeiten vor dem PC erinnert.

Kein Trend, aber ein Ereignis, das weltweit große Medienbeachtung fand, ist die Markteinführung des neuen *Microsoft-Betriebssystems WINDOWS 95* für Personalcomputer als Nachfolger des *Betriebssystems MS-DOS*. Für kaum ein anderes Produkt wurde ein vergleichbarer Werbeaufwand getrieben wie für diese Software.

WINDOWS 95 mag in vieler Beziehung wesentliche Vorteile gegenüber MS-DOS bieten, die in der besseren Auslastung der modernen Prozessoren, in einem wirkungsvolleren Multitasking (gleichzeitige Erfüllung mehrerer Aufgaben), in neuen und verbesserten Möglichkeiten des Mensch-Maschine-Dialogs, in der Befreiung von engen Namenskonventionen usw. liegen. Verbesserungen für Datenschutz und Datensicherheit sind dagegen nach ersten Erfahrungen nicht zu erkennen. Verfahren zur Benutzeridentifizierung und -authentifizierung sind ebensowenig Bestandteil von WINDOWS 95 wie die Sperrbarkeit des Bootens von der Diskette. Der Einsatz von speziellen Werkzeugen für die Speicher-, Benutzer- und Zugriffskontrolle bleibt daher auch beim PC-Einsatz unter WINDOWS 95 erforderlich, wenn personenbezogene Daten verarbeitet werden sollen.

Die Software für die Verbindung mit *weltweiten Datennetzen* ist in WINDOWS 95 bereits integriert, nämlich für die Nutzung des neuen *Microsoft Networks MSN*. Es bietet (zumindest bald) den vollen Zugriff auf das Internet und auf das World Wide Web sowie eine E-Mail-Adresse.

Aus datenschutzrechtlicher Sicht ist die Nutzung des MSN durch Systeme, die vertrauliche Daten verarbeiten, kritisch zu beobachten.

WINDOWS 95 verfügt über ein *Agenten-Programm* (Registration Wizard), mit dem die PC-Festplatte durchsucht wird und Daten zur Person des PC-Besitzers (Name, Adresse), die Seriennummer der Systemsoftware, Angaben zum Hardwareprofil und zu Softwarepaketen an Microsoft übertragen werden. Begründet wird dies mit der Rationalisierung der Kundenerfassung und dem gegenseitigen Interesse der PC-Benutzer und Microsoft an einer optimierten Hard- und Softwareaustattung, also der Beratung des Benutzers und dem Kundendienst einerseits, dem Microsoft-Marketing andererseits. Die Übermittlung der Daten erfolgt natürlich nur, wenn der Benutzer sich für die Nutzung des MSN bei Microsoft erstmalig angemeldet hat (dabei sind weitere Daten für das Gebühreninkasso – z. B. Kreditkartennummer – anzugeben). Alle weiteren Datenübermittlungen erfolgen durch den „Registration Wizard" immer dann, wenn man sich für eine Sitzung am MSN anmeldet. Die Übermittlung durch den „Registration Wizard" kann abgeschaltet werden, ist jedoch standardmäßig aktiviert.

Die *Ausforschung der Festplatten* der Kundensysteme hat dazu geführt, daß Regierungen, die an der Erhaltung ihrer Staatsgeheimnisse interessiert sind, Bedenken gegen den Einsatz von WINDOWS 95 geäußert haben. In der Tat beruhen die Angaben über die Wirkungsweise auf den Informationen des Herstellers. Ob noch weitere Daten – zum Beispiel Anwendungsdaten aus dem PC oder Daten aus Systemen, die mit dem PC vernetzt sind, übertragen werden können, ist unseres Wissens noch nicht hinreichend untersucht worden.

2.2 Informations- und kommunikationstechnische Infrastruktur der Berliner Verwaltung

Der Aufbau umfassender Infrastrukturen für die Daten- und Sprachkommunikation stellt einen wesentlichen Aspekt der Modernisierung der Berliner Verwaltung dar. Aus diesem Grund sind in den letzten Jahren große Anstrengungen unternommen worden, ein neues Verwaltungsdatennetz in Form eines *Metropolitan Area Network (MAN)* aufzubauen und ein ISDN-Vernetzungskonzept für das Behördentelefonnetz zu entwickeln.

Das MAN ist die Voraussetzung für den Aufbau der großen Anwendungsverfahren im Personalwesen (IPV – Integrierte Personalverwaltung), Sozialwesen (BASIS – Berliner Automatisiertes Sozialhilfe Interaktionssystem), Haushaltswesen (AHW – Automatisiertes Haushaltswesen) und der Stadtplanung (FIS – Fachübergreifendes Informationssystem). Es ermöglicht den dezentralen Zugriff auf zentrale Ressourcen über das Sicherheitsrechenzentrum des Landesamtes für Informationstechnik (SRZ) sowie die Unterstützung bei der Systemverwaltung lokaler Netze durch das zentrale und die lokalen Service- und Administrationszentren (SAZ/LAZ). Vorgesehen ist der Zugriff auf das Internet und internationale Online-Dienste sowie die Bereitstellung von Informationsangeboten im Internet. Wir haben uns auch in diesem Jahr intensiv an den Beratungen zu den Infrastrukturprojekten beteiligt, insbesondere bei der Begleitung der Risikoanalysen und der Erstellung der Sicherheitskonzepte.

Mit diesen ehrgeizigen Projekten werden die Weichen für die Zukunft des Einsatzes der Informationstechnik in der Berliner Verwaltung gestellt. Technische Perfektion einerseits und leere Kassen andererseits dürfen gleichwohl den Datenschutz und die Sicherheit der Informationstechnik nicht zu kurz kommen lassen.

Zentrale Systembetreuung für die Verwaltung – das Projekt SAZ/LAZ

Eine wesentliche Komponente des künftigen Berliner Verwaltungsnetzes sind das (im LIT angesiedelte) *Service- und Administrationszentrum (SAZ)* sowie die *lokalen Administrationen (LAZ)*. Diese Struktur soll eine zentrale Systembetreuung für alle Berliner Verwaltungsstellen ermöglichen. Die dezentral installierten Rechnersysteme und -netze der einzelnen Standorte sollen durch zentrale Administrations-, Support- und Managementfunktionen unterstützt werden. Bereits im letzten Jahresbericht wiesen wir auf die zentrale Bedeutung dieses Projektes und die damit zusammenhängenden Risiken hin. Unsere Empfehlung, eine *Risikoanalyse* auf Basis des IT-Sicherheitshandbuchs des BSI und darauf aufbauend ein Datenschutz- und Datensicherheitskonzept zu erarbeiten, wurde realisiert.

Die erste Version betrachtete jedoch nur einen engen, das SAZ/LAZ-Projekt direkt betreffenden Rahmen, das heißt, es wurde nur auf die Sicherheit der unmittelbar zugehörigen Infrastruktur (Hardware und Software) eingegangen. Nicht betrachtet wurden bisher die Gefahren und Risiken, die durch SAZ und LAZ für die administrierten Systeme, z. B. die lokalen Netze der Auftraggeber, entstehen. SAZ und LAZ können jedoch nicht

16 Jahresbericht 1994, 2.1, 3.3
17 Jahresbericht 1994
18 vgl. 3.2

separat betrachtet werden. Die zentrale Aufgabe des System- und Netzwerkmanagements steht in direktem Zusammenhang mit den administrierten Verfahren und den zugrundeliegenden Netzen einerseits, den Schnittstellen des SAZ nach „außen“ (z. B. nicht durch das SAZ administrierte Rechner, Netzwerke oder Verfahren) andererseits.

Diese Aspekte wurden in die zweite Version der Risikoanalyse bereits teilweise eingearbeitet. Dazu zählt die Behebung von Fehlern in entfernten Systemen. Ein vollständiges *zentrales Fehlermanagement* ist nur unter Verwendung eines entfernten Einloggens, teilweise sogar unter einer Systemverwalterkennung („root“) möglich. Dies birgt jedoch erhebliche Gefahren für alle Rechner in den lokalen Netzen der Auftraggeber. Hier müssen technisch-organisatorische Maßnahmen definiert werden, die geeignet sind, Mißbräuche durch interne oder bei einer Öffnung zum Internet[19] auch externe Angreifer zu verhindern. Auch die unterschiedlichen Arbeitsabläufe der verschiedenen Managementbereiche müssen auf Gefahren, die von ihnen ausgehen könnten, hin untersucht werden.

Der Risikoanalyse liegen die Sicherheitsmechanismen des Distributed Computing Environment (DCE) der Open Software Foundation zugrunde. Dabei handelt es sich um eine herstellerunabhängige Sammlung von Systemkomponenten, die eine Kommunikation offener Systeme in einer sicheren Umgebung ermöglicht. DCE wurde ausgewählt, um den hohen Sicherheitsanforderungen, die an ein Management-Projekt wie SAZ/LAZ zu stellen sind, gerecht zu werden. Die für die Sicherheit wesentlichen Dienste „Security Service“ und „Distributed File System“ (DFS) ermöglichen Zugriffsschutz, Authentisierung und Verschlüsselung der wesentlichen Komponenten.

Das Sicherheitsrechenzentrum des Landesamtes für Informationstechnik

Bereits im letzten Jahresbericht[20] haben wir den für 1995 geplanten Bau eines *Sicherheitsrechenzentrums (SRZ)* des *Landesamtes für Informationstechnik* erwähnt und unsere Erwartungen zu den damit verbundenen umfangreichen technischen und organisatorischen Maßnahmen zur Gewährleistung eines – insbesondere auch unter Berücksichtigung datenschutzrechtlicher Aspekte – sicheren Betriebs dieses Rechenzentrums dargelegt. Immerhin handelt es sich dabei um einen Rechenzentrumskomplex, der „dunkel“, das heißt im Normalfall ohne unmittelbare Überwachung und Steuerung vor Ort, betrieben werden soll. Dementsprechend sind hohe Anforderungen an die zu installierenden Sicherheits- und Überwachungseinrichtungen zu stellen. Dabei handelt es sich um eine herstellerunabhängige Sammlung von Systemkomponenten, die eine Kommunikation offener Systeme in einer sicheren Umgebung ermöglicht. Inzwischen wurde das SRZ seiner Bestimmung übergeben.

Ausgehend von einer umfassenden Risikoanalyse denkbarer Bedrohungsszenarien wurde ein *Sicherheitskonzept* entwickelt und umgesetzt, das die Risiken für den ordnungsgemäßen Rechenzentrumsbetrieb bis auf vertretbare minimale Restrisiken reduziert.

Umfangreiche bauliche Maßnahmen zur Abwehr von *äußeren Bedrohungen,* wie etwa Brandstiftung, Terroranschläge oder Wassereinbrüche, waren getroffen worden. Ferner wurde Vorsorge getroffen, um möglichen Gefahren im Innern des Gebäudes begegnen zu können. So wurden die wichtigsten technischen Anlagen und Aggregate redundant ausgelegt, um im Falle einer *Havarie* Ausweichmöglichkeiten sofort nutzen zu können. Zumindest kann ein Notbetrieb des Rechenzentrums bis zum Einleiten und Wirksamwerden gezielter Sicherungs- bzw. Bekämpfungsmaßnahmen gewährleistet werden. Die zu diesem Zweck installierten Überwachungs- und Schutzeinrichtungen sind in wesentlichen Teilen so gestaltet worden, daß erste notwendige Maßnahmen automatisiert anlaufen, wenn durch voneinander unabhängige Systeme ein Havariefall diagnostiziert wird.

Alle Meldungen der verschiedenen Sicherheitssysteme werden nach einer softwaregestützten Filterung und Aufbereitung zum *Sicherheitsleitstand* im LIT-Dienstgebäude weitergeleitet, dort dem Wachpersonal auf entsprechend ausgestatteten Monitoren angezeigt und gegebenenfalls in akustische bzw. visuelle Alarmsignale umgesetzt. Außerdem werden die betroffenen Bereiche mittels einer umfangreichen *Videoübertragungstechnik* auf den Bildschirmen der Leitwarte dargestellt, so daß sich die Mitarbeiter über den augenblicklichen Zustand visuell informieren können und bei den einzuleitenden Maßnahmen unterstützt werden. In vielen Fällen erfolgt diese Unterstützung bereits durch vorprogrammierte Hinweise auf den dafür vorgesehenen Terminals. In einer Dienstanweisung wird die notwendige Vorgehensweise beschrieben. Sowohl die softwaregestützten als auch die manuellen Anweisungen unterliegen einer ständigen Aktualisierung und Anpassung an bisher noch nicht bzw. unvollständig erfaßte Gegebenheiten.

Einen wesentlichen Anteil bei der Überwachung des „unbemannten“ Rechenzentrums nimmt die *Zugangskontrolle* ein. Sie basiert auf diversen paarweise angeordneten Ein- und Ausgangslesern für Magnetkarten und dient der Verhinderung des Zutritts unberechtigter Personen sowie der Feststellung des Aufenthaltsortes Zugangsberechtigter. Die Kartenleser sind sowohl in den eigentlichen Eingangsbereichen, die als zeitgesteuerte Schleusen angelegt sind, als auch an anderen neuralgischen Punkten, wie z. B. den Übergängen zwischen den verschiedenen inneren Sicherheitszonen, installiert. Die Differenzierung des Zugangs zu bestimmten Zonen innerhalb des Rechenzentrums erfolgt softwaregestützt durch die auf den Magnetkarten gespeicherten Daten. Über Videokameras und die damit verbundene Bildübertragung zur Leitwarte wird auch eine visuelle Kontrolle durch das dortige Wachpersonal ermöglicht, um die notwendige manuelle Freischaltung der Eingangstüren abzusichern. Dies soll zusätzlich dadurch unterstützt werden, daß zeitgleich mit der Benutzung eines Eingangslesers ein elektronisch gespeichertes Vergleichsbild des Karteninhabers auf einem Monitor in der Sicherheitsleitwarte erscheint, da man nicht davon ausgehen kann, daß alle zugangsberechtigten Personen dem Leitwartenpersonal persönlich bekannt sind. Zudem soll damit natürlich auch der Zugang solcher Personen verhindert werden, die auf eine wie auch immer geartete Weise in den Besitz einer gültigen Magnetkarte gelangt sind.

Gegen die damit für die LIT-Mitarbeiter verbundene Bildspeicherung gab es Widerstände beim örtlich zuständigen Personalrat. Wegen des hohen Schutzbedarfs der im SRZ zu verarbeitenden Daten und der außerordentlichen Bedeutung der Funktionsfähigkeit des SRZ für die Berliner Verwaltung gehen wir jedoch von der Angemessenheit dieser Verfahren bei der Authentifizierung aus.

Festzuhalten ist, daß mit dem Sicherheitsrechenzentrum ein wesentlicher Teil der von uns empfohlenen technischen und organisatorischen Maßnahmen zur Gewährleistung eines hohen Datenschutz- und Datensicherheitsniveaus Realität geworden ist.

ISDN-Vernetzungskonzept für die Berliner Verwaltung

Jedenfalls derzeit ist das Telefon für die tägliche Verwaltungsarbeit erheblich wichtiger als der Anschluß an Datenverarbeitungseinrichtungen. Der Neugestaltung des Behördentelefonnetzes im Rahmen des ISDN-Vernetzungskonzepts kommt daher erhebliche Bedeutung zu. Den Datenschutz- und Datensicherheitsproblemen wurde im vergangenen Jahr wesentlich mehr Bedeutung zugemessen als vorher. Die im letzten Jahresbericht geäußerte Kritik[21] ist also konstruktiv aufgenommen worden.

Eine externe Firma wurde beauftragt, eine von uns mehrfach geforderte umfassende Risikoanalyse zu erstellen. Alle wesentlichen Risiken wurden erkannt und bestimmt. Die Maßnahmen zur Verringerung und Minimierung der Risiken sind sinnvoll und der Tragweite des Konzeptes angemessen. Die Sicherheit des ISDN-Netzes der Berliner Verwaltung hängt jetzt von der vollständigen Umsetzung dieses Sicherheitskonzeptes ab. Eine Teilumsetzung wäre nicht ausreichend, da viele Maßnahmen gegenseitige Abhängigkeiten aufweisen und somit aus Sicherheitssicht ein nicht tragfähiges Grundgerüst entstehen würde.

19 vgl. 4.1
20 Jahresbericht 1994, 2.2
21 Jahresbericht 1994, 2.2

Die nach der Definition von Sicherheitsmaßnahmen durchgeführte *Restrisikoanalyse* zeigt auf, daß auch bei Umsetzung aller empfohlenen Maßnahmen nicht alle Risiken beseitigt sind. Sie beruhen auf der Gefahr menschlichen Versagens bzw. mißbräuchlichen Handelns Berechtigter und können nur durch organisatorische Maßnahmen verringert werden. Dies birgt immer ein erhebliches Risiko; der Auswahl der mit der Wartung, Konfiguration und Administration beauftragten Personen kommt daher höchste Bedeutung zu.

Weiterhin ungelöst bleibt die Problematik der *Unterdrückung der Zielnummernanzeige* bei Telefonaten im Behördennetz. So existieren Aussagen der Telekom, daß diese derzeit nicht in der Lage sei, eine zielnummernbezogene Unterdrückung der Rufnummernanzeige zu realisieren, wenn hinter der Vermittlungsstelle der Telekom eine Nebenstellenanlage installiert ist. Demgegenüber enthält § 9 Abs. 1 Satz 3 der Telekom-Datenschutzverordnung (TDSV) eine Verpflichtung der Telekom, die Übermittlung der Rufnummer des anrufenden Anschlusses an den angerufenen Anschluß einer telefonischen Beratungsstelle in der Vermittlungsstelle dieses Anschlusses auszuschließen. Die im Datenschutzkonzept vorgeschlagene Maßnahme, die Übermittlung der Rufnummer des Anrufenden in der Software der Transitzentrale zu unterdrücken, kann somit nur als vorübergehende Hilfskonstruktion betrachtet werden. Diese Hilfskonstruktion kann für einen Übergangszeitraum akzeptiert werden, bis die flächendekkende Einführung des Euro-ISDN es dem Betroffenen ermöglicht, über die Übermittlung seiner Rufnummer selbst zu entscheiden. Sichergestellt werden muß gleichwohl, daß die Anschlüsse, bei denen die Rufnummernanzeige nicht erfolgt, in öffentlichen Teilnehmerverzeichnissen als solche gekennzeichnet sind.

Infrastrukturprojekt BROSiA

Im letzten Jahresbericht wurde über das auf dem Projekt GIBES (Grundlagen der Ausstattung mit IT-Infrastruktur für die Bezirke und Senatsverwaltungen) aufbauende Projekt BROSiA (Berliner Rahmenkonzept für Organisation, Sicherheit und Anwendungsentwicklung beim IT-Einsatz) berichtet. Mit BROSiA sollte ein Gesamtwerk geschaffen werden, in dem grundlegende IT-Vorschriften zur Organisation der Datenverarbeitung in der Berliner Verwaltung, zur Berücksichtigung ihrer Sicherheit und zur Durchführung von IuK-Projekten definiert werden. Das Projekt sollte nach dem Vorbild anderer konzeptioneller Projekte durch Hinzuziehung von externem Sachverstand realisiert werden. Ergebnisse liegen nicht vor, da man sich vom Auftragnehmer trennte und das Projekt ruhen ließ.

Diese Denkpause fällt mit der Realiserungsphase mehrerer Großprojekte zusammen. Dies legt einen Vergleich zum Hausbau nahe: Während die Geschosse der Vollendung entgegengehen, wurden die Planungen am „gemeinsamen Dach“ vorerst eingestellt.

Ein aus Datenschutzsicht wichtiges Ziel von BROSiA war die Definition eines IT-Sicherheitsrahmenkonzeptes für die Berliner Verwaltung. Wegen des Wegfalls dieses Konzeptes existiert zur Zeit kein koordinierender Rahmen für die Sicherheit bei den unterschiedlichen Projekten. Sie realisieren vielmehr unterschiedliche Sicherheitsmechanismen.

Die Einführung einer modernen Kommunikationsinfrastruktur macht die Definition einer berlinweiten Sicherheitspolitik notwendig. Eine Koordination der verschiedenen Projekte und Bereiche der Berliner Verwaltung könnte z. B. durch eine generelle Nutzung des DCE realisiert werden.

3. Schwerpunkte im Berichtsjahr

3.1 BahnCard

Mit der Übernahme der Aufgaben der Aufsichtsbehörde am 1. August war die bislang ungeklärte Frage zu beantworten, welche *Aufsichtsbehörde für die Deutsche Bahn AG* zuständig sein sollte. Die Senatsverwaltung für Inneres hatte zuvor unter Hinweis auf die öffentlichen Aufgaben der Bahn den Bundesbeauftragten für die richtige Kontrollstelle gehalten, dieser seine Kompetenz für die privatisierten Teile der früheren Bundesbahn jedoch nicht für gegeben betrachtet. Um diesen leidigen Kompetenzkonflikt zu Lasten des Bürgers zu beenden, haben wir im Hinblick auf den Unternehmenssitz der Bahn AG in Berlin in Abstimmung mit den anderen Aufsichtsbehörden die Zuständigkeit übernommen.

Damit übernahmen wir ein Problem, das bereits Wochen zuvor die Öffentlichkeit intensiv beschäftigt hatte: die datenschutzrechtliche Bewertung der *neuen BahnCard*. Die neue Karte, die ebenfalls zum Kauf von Fahrkarten zum halben Preis berechtigt, unterscheidet sich von der alten dadurch, daß sie auf Wunsch des Kunden zusätzlich zum BahnCard-Teil eine *Kreditkartenfunktion* hat. Hinzu kam das Angebot einer Electron-Guthabenkarte, mit der man nur über ein vorher eingezahltes Guthaben verfügen kann. Hierfür hatte die Bahn AG einen *Kooperationsvertrag mit der Citibank* abgeschlossen, die ihrerseits Lizenznehmerin von VISA International ist. Die Abwicklung wurde einer Tochter der Citibank, der Citicorp Card Operations GmbH (CCO) übertragen; die Herstellung der Karten einschließlich der hierfür erforderlichen Datenverarbeitung erfolgt im wesentlichen in Rechenzentren der Citibank in den USA. Dieses Projekt sorgte aus verschiedenen Gründen für heftige öffentliche Diskussionen.

Auch wenn die Bahnkunden lediglich eine einfache BahnCard ohne Kreditkartenteil beantragen wollten, wurden sie anfangs aufgefordert, Formulare auszufüllen, bei denen eine Reihe privater Informationen des Kunden angegeben werden sollte. Gegen dieses Verfahren hatten sich andere Aufsichtsbehörden von Anfang an gewandt. In einer Presseerklärung zeigten sie die Probleme auf und führten erste Verhandlungen mit der Deutschen Bahn AG. Dies führte zum Entwurf neuer Formulare, in denen vor allem für die drei BahnCard-Typen BahnCard pur, BahnCard mit VISA-Kreditkartenteil und Electron-Guthabenkarte drei optisch getrennte Bereiche vorgesehen waren.

Nachdem der Berliner Datenschutzbeauftragte für die private Datenverarbeitung in Berlin und damit auch für die Deutsche Bahn AG zuständig geworden war, wurde sofort das Gespräch mit der Deutschen Bahn AG, der Citibank NA, New York, der Citibank-Privatkunden AG und der CCO aufgenommen. Neben einigen weiteren Problemen des *Formulars* selbst wurden vor allem die auf der Rückseite des Formulars abgedruckten Geschäftsbedingungen und die Voraussetzungen geprüft, unter denen Citibank die Daten der BahnCard-Kunden in die USA übermitteln darf. Diese Verhandlungen führten zu weiteren Erfolgen. Nach einer zweiten Gesprächsrunde wurden auch für die ausstehenden Probleme Zusicherungen gemacht, so daß keine datenschutzrechtlichen Bedenken mehr gegen das Verfahren bestehen.

Gegen das BahnCard-Verfahren haben sich viele Bürgerinnen und Bürger schriftlich und telefonisch an mich gewandt. Viele Kunden haben sich darüber beschwert, daß die Bahn sich zur Herstellung der BahnCard der Citibank bedient und daß diese wiederum die Daten zur Herstellung der Karte in die USA übermittelt. Ich mußte sie darauf hinweisen, daß es nicht die Aufgabe der Aufsichtsbehörde ist, private Datenverarbeiter bei der Auswahl ihrer Kooperationspartner zu beschränken. Auch der *Datenfluß über die Grenzen Deutschlands und Europas hinaus* kann nicht von vornherein unterbunden werden, vielmehr kann die Aufsichtsbehörde lediglich die Datenübermittlung an Dritte und ins Ausland so mitzugestalten versuchen, daß kein deutsches Datenschutzrecht verletzt wird. Soweit die Daten in Länder wie die USA übermittelt werden, wo ein dem deutschen Datenschutzrecht entsprechendes Datenschutzniveau fehlt, ist diese Aufgabe besonders schwierig.

Auf dreierlei Weise wurde die datenschutzrechtliche Zulässigkeit des Verfahrens herbeigeführt:

- Die Betreiber des Verfahrens wurden veranlaßt, die Formulare mit ihren Fragen und Erklärungen datenschutzgerecht zu gestalten;
- die auf der Rückseite der Formulare abgedruckten allgemeinen Geschäftsbedingungen wurden verbessert;

- in Vereinbarungen zwischen der Deutschen Bahn AG und den beteiligten Citibank-Unternehmen in Deutschland und den USA wird ein umfassender Datenschutz der BahnCard-Kunden in den USA, aber auch in Deutschland gewährleistet.

Die wichtigste *Veränderung bei den Formularen* stellt die klare *Wahlmöglichkeit* zwischen der Visa-Kreditkarte, der Electron-Guthabenkarte und der BahnCard ohne jede Zahlungsfunktion dar. Soweit die Citibank durch die Erhebung nach dem alten Formular von Erwerbern der einfachen BahnCard unzulässig auch Daten zum Kreditkartenteil erhalten hatte, hat sich die Citibank verpflichtet, diese Daten so schnell wie möglich zu löschen. Überflüssige Fragen auf dem Formular sind gestrichen oder modifiziert und die Einteilung zwischen Angaben zur BahnCard und notwendigen Angaben zur Ausstellung der VISA-Kreditkartenfunktion deutlich durch rote Überschriften herausgestellt worden. Das gilt auch für den Teil des Formulars, wo auf die jeweiligen Datenschutzklauseln hingewiesen wird. Gegen die Gestaltung des Antragsformulars bestehen damit keine datenschutzrechtlichen Bedenken mehr. Allerdings wäre es kundenfreundlicher und übersichtlicher, wenn es für jede Version der Karte ein gesondertes Formular gäbe. Mißverständnisse könnten hierdurch vermieden werden.

Auf der *Rückseite des Formulars* sind unter anderem die *Wesentlichen Bestimmungen* der Bahn *zum Gebrauch der BahnCard* und die *Nutzungsbedingungen für die VISA-Kreditkartenfunktion* und *Electron-Guthabenkartenfunktion* der Citibank Privatkunden AG abgedruckt. Danach willigt der BahnCard-Kunde ein, daß die CCO die in dem Kartenantrag enthaltenen Daten zur Aufnahme und Abwicklung des BahnCard-Vertrages erhält, verarbeitet und speichert. Außerdem willigt er ein, daß seine Antragsdaten zur Aufstellung und Abwicklung der BahnCard an die *Rechenzentren der Citibank in den USA* übermittelt sowie dort verarbeitet und gespeichert werden. Bemerkenswert ist in beiden Klauseln, daß die Rechenzentren der Citibank in den USA sich verpflichten, die Daten auf einem dem Datenschutzgesetz vergleichbar hohen Schutzniveau zu verarbeiten. Die in diesen Klauseln vorgesehene Geltendmachung der Rechte der Bahnkunden ist nicht nur gegenüber der Citibank, sondern auch gegenüber der Deutschen Bahn AG möglich. Die Übermittlung der Kreditkartenabrechnungsdaten an die VISA-International-Association wurde transparent gemacht und ihre Zulässigkeit an die Einwilligung des BahnCard-Kunden geknüpft.

Die größte Bedeutung haben eine

- Datenschutzvereinbarung in Ergänzung zum Kooperationsvertrag zwischen Deutscher Bahn AG und der Citibank Privatkunden AG

sowie eine

- Vereinbarung zum gebietsübergreifenden Datenschutz zwischen den beteiligten deutschen und amerikanischen Citibank-Unternehmen.

Darin verpflichten sich die Vertragspartner,

- die Daten *aller* BahnCard-Kunden in den USA lediglich zur Herstellung der BahnCard – also nicht zu Marketingzwekken – zu nutzen;
- die Daten der Kunden von reinen BahnCards ohne VISA-Teil auch in Deutschland nicht zu Marketingzwecken zu verwenden; die Deutsche Bahn AG darf mit diesen Daten lediglich für die sogenannte „bessere“ BahnCard, also die BahnCard mit VISA-Kreditkartenteil werben;
- die Daten von Kunden von BahnCards mit Kreditkartenteil oder von Electron-Guthabenkarten nur für „financial services“ in Deutschland zu nutzen; das bedeutet, daß die Citibank diese Daten innerhalb ihres Konzerns lediglich für Bank- und Versicherungsgeschäfte verwenden darf; weitere Angebote können derartigen Sendungen nur beigepackt werden;
- eingehende, im Vertrag im einzelnen beschriebene Datensicherungsmaßnahmen – insbesondere auch in den USA – zu treffen.

Der BahnCard-Kunde kann seine Rechte auf Auskunft, Löschung, Sperrung oder Schadensersatz gegenüber der Deutschen Bahn AG oder der Citibank geltend machen, auch wenn der Schaden nicht in Deutschland, sondern in den USA entstanden ist. Schließlich kann der Berliner Datenschutzbeauftragte als für die Deutsche Bahn AG zuständige Datenschutzaufsichtsbehörde in den USA vor Ort selbst *Datenschutzprüfungen* vornehmen oder durch einen Beauftragten vornehmen lassen.

Im Hinblick auf die dargestellten Datenschutzmaßnahmen sind sowohl die Übermittlung der Daten von der Deutschen Bahn AG an die CCO als auch die Übermittlung der Daten an die Rechenzentren in den USA zulässig.

Diese grundsätzliche Bewertung des BahnCard-Verfahrens schließt natürlich nicht aus, daß es bei der konkreten Umsetzung des Verfahrens zu weiteren, z. B. technisch bedingten, Datenschutzproblemen kommt.

Die Bedeutung dieses Falles liegt vor allem darin, daß es gelungen ist, bei grenzüberschreitendem Datenverkehr mit den USA hinreichende Datenschutzregelungen zu treffen. Sie sind insoweit vorbildlich für die Umsetzung der EU-Datenschutzrichtlinie, die einen Datenexport nur dann erlaubt, wenn ein angemessener Datenschutz im Empfängerland sichergestellt ist. Dessen ungeachtet ist zu hoffen, daß auch der Gesetzgeber der USA sich des Datenschutzes im privaten Sektor annimmt.

3.2 Chipkarten – Computer in der Brieftasche

Chipkarten sind auf das Format einer Scheckkarte miniaturisierte IuK-Komponenten. Es gibt reine Speicherchipkarten zur Aufnahme von Daten, wie z. B. die Telefonkarten, die einen Kontostand enthalten, der bei Gebrauch der Chipkarte in einem Kartentelefon reduziert wird, bis das Konto erschöpft ist und die Chipkarte unbrauchbar wird.

Ebenfalls allgemein bekannt ist die *Krankenversichertenkarte,* deren Besitz für alle Versicherten in *gesetzlichen* Krankenversicherungen Pflicht ist und die den Krankenschein mittlerweile ersetzt hat.[22] Dabei handelt es sich ebenfalls um eine reine Speicherchipkarte, die einen gesetzlich vorgegebenen Inhalt hat, der neben den identifizierenden Merkmalen des Besitzers dessen Krankenversicherungsstatus beschreibt. Die Daten werden mit Karten-Terminals in Arztpraxen und Krankenhäusern gelesen, in den dort vorhandenen IT-Systemen weiterverarbeitet, mit Daten zur Abrechnung der kassenärztlichen Leistung ergänzt und (per Post oder über Telekommunikationsdienste) weitergegeben.

Eine größere Bedeutung haben Karten, in die Mikroprozessoren und Speicherbauteile integriert sind. Solche Prozessorchipkarten sind als *Kleinstcomputer* anzusehen, die – zumindest nach derzeitigem technischen Standard – nicht über eine Mensch-Maschine-Schnittstelle verfügen. Ihre Verwendung bedarf also zusätzlicher Karten-Terminals zum Lesen der gespeicherten Daten, zum Aktivieren der Funktionen der Mikroprozessoren, zum Beschreiben der Speicher. Ein Karten-Terminal kann einerseits als isoliertes Gerät zur Erschließung der Daten und Funktionen von Chipkarten angesehen werden. Andererseits erschließen sich die Anwendungsmöglichkeiten von Chipkarten vor allem dann, wenn das Karten-Terminal auch als Ein- und Ausgabeeinheit in eine „normale“ IT-Systemkonfiguration eingebettet ist, die die Weiterverarbeitung von Daten aus einer Chipkartenanwendung bzw. die Aufbereitung von auf Chipkarten abzulegenden Daten ermöglicht. Sie kann ihrerseits in Netze eingebunden sein.

Zum Verständnis von komplexeren Anwendungen von Chipkarten ist es wichtig, Chipkarten und die (zumindest noch) davon untrennbaren Karten-Terminals als Bestandteil übergeordneter Infrastrukturen zu sehen. Sicherheitsbetrachtungen zum Einsatz von Chipkarten verlieren ihren Sinn, wenn nicht die Sicherheit dieser Infrastrukturen mitbetrachtet wird.

Derzeit sind zwei wichtige Anwendungsbereiche von Chipkarten in der Diskussion, die gesellschaftliche Bedeutung gewinnen werden und unter dem Aspekt des Datenschutzes zur Wahrung der informationellen Selbstbestimmung und der informationstechnischen Sicherheit größter Aufmerksamkeit bedürfen:

22 Jahresbericht 1993, 2.3

- Chipkartenanwendungen im bargeldlosen Zahlungsverkehr
- Gesundheits- oder Patientenchipkarten zur Aufnahme medizinischer Daten[23].

Beide Anwendungsbereiche zeigen – mit unterschiedlicher Zielsetzung – vergleichbare Funktionen:

- Chipkarte als Speicher von Daten, die hinsichtlich ihrer Vertraulichkeit und Integrität hohen Schutzbedarf aufweisen (Kontodaten, medizinische Individualdaten);
- Chipkarte als Mittel zur Authentifizierung ihres Trägers für die Gewährung des Zugriffs auf sicherheitsrelevante Daten und Funktionen (Kontoverfügungen, Änderung medizinischer Individualdaten);
- Chipkarte als Mittel zur Zertifizierung (Signatur) von Dokumenten (Verträge, Willenserklärungen, Befunde etc.).

Weil Chipkarten als miniaturisierte Computer anzusehen sind, die nicht über eigene Mensch-Maschine-Schnittstellen verfügen, ergeben sich folgende *Konsequenzen:*

- Chipkarten sind besonders leicht transportable Rechner. Die besonderen Risiken der IT-Sicherheit, die bei anderen transportablen Rechnern wie Laptops oder Notebooks berücksichtigt werden müssen, gelten in verstärktem Maße für Chipkarten.
- Der Umgang mit Chipkarten bedarf zwischengeschalteter technischer Systeme (Karten-Terminal), die ebenfalls zu sichern sind. Eine Chipkarte bildet zusammen mit dem Karten-Terminal ein vollwertiges Rechnersystem mit Ein- und Ausgabekomponente.
- Zu geringe Speicher- und Prozessorkapazitäten bilden noch Schranken für Sicherheitsfunktionen. Die technische Entwicklung dürfte diese Engpässe bald beseitigen.

Allgemein sind an die *Sicherheitsfunktionen* folgende Anforderungen zu stellen:

- Zugriffs- und Nutzungsberechtigungen sollten soweit wie möglich von der Chipkarte selbst geprüft und gesteuert werden.
- In Anwendungen sollten sich alle beteiligten Rechner (incl. Chipkarten) gegenseitig authentifizieren. Die Authentifizierung des Benutzers hat gegenüber der Chipkarte zu erfolgen, wobei für die Zukunft angestrebt werden sollte, daß dies möglichst ohne zwischengeschaltete Systeme erfolgen kann.
- Ein Mindestschutz muß realisiert sein, damit bei unbefugter Nutzung einer Chipkarte die strafrechtliche Vorschrift zur Ausspähung von Daten (§ 202 StGB) greift.

Überlegungen zur *informationstechnischen* Sicherheit von Chipkarten betreffen

- die Sicherheit bei der Herstellung, der Initialisierung und dem Versand der Chipkarten;
- die Sicherheitsmaßnahmen gegen unbefugte Nutzung auf dem Kartenkörper;
- die Sicherung des Chips gegen mechanische Manipulation und Auslesung;
- die Basisalgorithmen für die Schutzfunktionen der Software (Verschlüsselung, elektronische Unterschrift, Generierung von Zufallszahlen);
- die Schutzfunktionen und -mechanismen des Chipkarten-Betriebssystems (Authentifizierung des Benutzers, Rechteverwaltung, verschlüsselte Datenübertragung usw.);
- die Sicherheit des Zusammenwirkens von Chipkarte, Karten-Terminal und Hintergrundsystemen;
- die Sicherheit der Karten-Terminals gegen die Manipulation ihrer Hard- und Software.

23 vgl. 3.2

Gesundheitschipkarten

Die erwähnte Krankenversichertenkarte enthält in § 291 Sozialgesetzbuch V (SGB V) präzise vorgegebene Daten zum Status des Versicherten. Sie enthält keinen Prozessor und daher konsequenterweise auch keine *Sicherheitsfunktionen* gegen die Verfälschung oder unbefugte Nutzung. Gegen die ausdrücklichen Einwände des Bundesbeauftragten für den Datenschutz wurde mit dem Kostenargument auf jede technische Sicherheit bei der Krankenversicherungskarte verzichtet. Es muß daher nicht verwundern, daß zum Beispiel im Internet darauf hingewiesen wird, daß durch die einfache Nutzung der Chipkarte durch andere Personen als den Inhaber der Karte die Krankenversorgung auch für illegal in Deutschland sich aufhaltende Personen möglich gemacht wird – ein humaner Aspekt des leichtfertigen Verzichtes auf die maschinelle Authentifikation mit der Chipkarte?

Diese Situation kann bei der neuen Generation von Chipkarten im Gesundheitswesen nicht aufrechterhalten werden, auf Sicherheitsfunktionen kann nicht verzichtet werden: Die verschiedenen Modelle von Gesundheitschipkarten, Gesundheitspässen oder Patientenchipkarten sollen sensible medizinische Daten der Patienten tragen und für medizinische Zwecke erschließbar machen.

Im März 1994 hatte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einem ersten Beschluß zu den Chipkarten im Gesundheitswesen geäußert.[24] Unter dem Eindruck verschiedener Modellversuche zu Patientenchipkarten wurde die Diskussion bei den Datenschutzbeauftragten fortgeführt. Am Ende stand ein neuer Beschluß vom November 1995[25], der sich wesentlich detaillierter zu den datenschutzrechtlichen Anforderungen äußert.

Der Beschluß betont die besondere Schutzwürdigkeit der medizinischen Daten aus der Sicht der Patienten, aber auch der Ärzte, deren Handeln in der Chipkarte transparent gemacht werden kann, und stellt konkrete Forderungen

- zur Sicherung der *freien Entscheidung des Patienten* zum Inhalt der Karte, zu den Anlässen ihres Einsatzes und zum Umfang der Offenbarung sowie der freien Entscheidung von Ärzten und Apothekern, die Chipkarte des Patienten in Anspruch zu nehmen oder nicht;
- zur Absicherung, daß sich die Situation der Betroffenen im *therapeutischen Verhältnis* zwischen Arzt und Patient nicht verschlechtert;
- zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf der Karte und der sie umgebenden Infrastruktur durch *geeignete technische und organisatorische Verfahren*;
- zur Verhinderung neuer zentraler *medizinischer Datensammlungen*;
- zum uneingeschränkten *Leserecht* des Karteninhabers und
- zur Suche nach datenschutzfreundlichen *Alternativen.*

Eine pauschale datenschutzrechtliche Bewertung der bisher bekannten Projekte verbietet sich angesichts ihrer Heterogenität von selbst. Gemeinsam ist Projekten und Gedankenspielen, daß Daten über den gesundheitlichen Zustand von Patienten und zu ihrer Behandlung auf den Karten gespeichert oder mit ihrer Hilfe erschlossen werden sollen. Die Daten sollen dabei unterschiedlichen Zwecken dienen: Unterstützung bei der Diagnose und Behandlung im Normal- und Notfall, Anreiz zu gesundheitsgerechtem Verhalten, Kontrolle der Medikation einschließlich der Selbstmedikation usw. Für die Verfolgung dieser Ziele werden aber verschiedene Ansätze erprobt:

Einige Modellversuche streben eine *universale Gesundheitskarte* an, in der möglichst alle für die medizinische Behandlung aller ärztlichen Sparten nützlichen Daten der Krankengeschichte eines Patienten gespeichert werden, gegebenenfalls unter Verwendung von optischen Speichertechniken auf der Karte, so daß

24 Jahresbericht 1994, Anlage 2.2
25 vgl. Anhang 2.10

auch Röntgenbilder oder ähnlich komplexe und umfangreiche Informationen aufgenommen werden können. Bei diesen Versuchen wird die Multifunktionalität der Chipkarten-Betriebssysteme dazu ausgenutzt, den verschiedenen ärztlichen Sparten eigene Speicherbereiche zuzuordnen, die unterschiedlichen Zugriffsberechtigungen unterliegen. Mit Hilfe von *Professional Cards* können dann die unterschiedlichen Fachärzte auf dem ihrer Fachkompetenz unterliegenden Speicherbereich der Chipkarte Datenänderungen durchführen und Leseberechtigungen wahrnehmen, die weniger engen Zugriffsbeschränkungen unterliegen. Bei diesen Versuchen trägt der Patient also einen Speicher mit sich, der unter Umständen die mehr oder weniger vollständige und detaillierte Krankengeschichte enthält.

Davon zu unterscheiden sind *Autorisierungskarten*, die selbst keine oder nur wenige grundlegende medizinische Daten des Patienten enthalten, die aber den Zugriff auf dezentral gespeicherte Datenbestände zum Patienten über Datenautobahnen ermöglichen, wenn der Patient dies autorisiert und der Arzt sich mit einer passenden Professional Card dazu legitimiert. So könnte zum Beispiel der Zugriff auf digital vorgehaltene Röntgenbilder, Tomographien, EKGs, EEGs und andere komplexe Datenbestände dort erfolgen, wo sie entstanden und gespeichert sind.

Andere Modellversuche verzichten auf einen umfassenden Anspruch und begnügen sich mit der Speicherung bzw. Erschließung von Daten von bestimmten *Risikopatienten*, z. B. von Patienten, die wegen ihrer mit Anfällen verbundenen Krankheiten schnelle und wirksame Hilfe benötigen (z. B. Diabetiker, Herzpatienten, Epileptiker etc.). Unter diese Katagorie fallen auch die allgemeinen Notfallkarten – auch für gesunde Patienten –, die z. B. im Falle eines Unfalles den Notärzten die für eine schnelle Hilfe erforderlichen Daten liefern.

Datenschutzrechtliche Betrachtungen zu den verschiedenen *Modellversuchen* haben sich an der Frage zu orientieren, ob es für das angestrebte gesundheitspolitische Ziel erforderlich ist, Daten im geplanten Umfang, in der geplanten Detaillierung, mit den vorgesehenen Zugriffsberechtigungen und in der vorgesehenen Form als Chipkarte zu nutzen. Welche Zwecke werden mit dem Konzept verfolgt? Können sie damit erreicht werden? Ist eine konkrete Zweckbindung überhaupt erreichbar? Die Frage zum Beispiel, ob die Krankengeschichte auf der Chipkarte die Kommunikation zwischen Arzt und Patient eher intensiviert oder unterbindet und somit dem gesundheitspolitischen Ziel größerer Patientennähe und -selbstverantwortung dient oder schadet, mag zwar primär gesellschaftspolitischer Art sein, hat aber auch entscheidende Bedeutung für die datenschutzrechtliche Bewertung. Je allgemeiner die gesundheitspolitische Zielsetzung formuliert ist und demzufolge die Menge der als nützlich angesehenen Daten und der möglicherweise interessierten Datennutzer ausgedehnt werden kann, desto mehr verschwimmen die konkreten Zwecke, für die ein Patient die Chipkarte herreichen soll, und um so schwieriger wird es, *Begehrlichkeiten* und *Mißbrauch* zu verhindern (z. B. im Arbeitsverhältnis).

Damit ist klar, daß grundsätzliche datenschutzrechtliche Hindernisse jenen Projekten am wenigsten entgegengehalten werden können, bei denen der gesundheitliche Nutzen für den Patienten am unmittelbarsten deutlich wird. Wenn plausibel wird, daß einem Patienten in einer konkreten gesundheitlichen Notsituation mit dem Einsatz seiner Chipkarte besser geholfen werden kann als ohne, dann macht es Sinn, diese Vorteile gegen anderweitige Risiken abzuwägen und technische und organisatorische Maßnahmen zu konzipieren, die die Risiken abbauen, aber dem Nutzen nicht entgegenstehen.

Diese Bedingungen sind bei den Projekten gegeben, bei denen Kranke spezielle Chipkarten für ihre besondere medizinische Betreuung erhalten. Sie sind ferner dort zu bejahen, wo die Chipkarte zur Erschließung von Daten eingesetzt wird, die nur mit aufwendigen und den Patienten belastenden Methoden gewonnen werden können, es also medizinisch richtig ist, ihn vor der Wiederholung solcher diagnostischer Maßnahmen zu bewahren. Voraussetzung dafür ist aber auch, daß ein Arzt sein Handeln auf die Daten stützen kann, die er auf der Chipkarte findet oder mit ihrer Hilfe erschließen kann, daß er sich auf ihre Richtigkeit, ihre zuverlässige und vertrauenswürdige Herkunft und auf ihre Aktualität verlassen kann und darf.

Der Berliner Gesundheitspaß

Seit Anfang 1995 werden in der Senatsverwaltung für Gesundheit Überlegungen zu einem Berliner Gesundheitspaß angestellt. Erörterungen fanden in diversen thematisch unterschiedenen Arbeitsgruppen statt, an denen sich die an der Umsetzung der Gesundheitsreform beteiligten Institutionen, die gesetzlichen Krankenkassen, die kassen- und kassenzahnärztlichen Vereinigungen, die Zahnärzte- und Ärztekammern, die Berliner Krankenhausgesellschaft und die Senatsverwaltung für Gesundheit beteiligten. Wegen der unbestritten wichtigen datenschutzrechtlichen Aspekte wurden auch wir frühzeitig an der Diskussion beteiligt.

Die gesundheitspolitischen Zielsetzungen wurden zu Beginn des Projektes von der Senatsverwaltung für Gesundheit vorgegeben:

- erhebliche Verbesserung der Information des Bürgers über seine Gesundheit, damit er in die Lage versetzt wird, sich aktiver um seine gesundheitlichen Belange zu kümmern und seine Interessen besser wahrzunehmen; dazu zählt auch der Schutz seiner persönlichen Daten, weil er sie selbst in Verwahrung hat;
- Optimierung der auf den Bürger orientierten Kommunikation zwischen den Gesundheitseinrichtungen, so daß Mehrfachuntersuchungen vermieden und Maßnahmen kostensparend besser abgestimmt werden können;
- Verbesserung der Transparenz der Leistungsangebote der Gesundheitseinrichtungen und damit Qualitätsverbesserung;
- Stärkung der Rolle des Hausarztes als lebenslanger „Gesundheitsbegleiter“ des Bürgers;
- Verbesserung der Gesundheitsberichterstattung und damit der Entscheidungsgrundlagen der Entscheidungsträger.

Der Gesundheitspaß soll als *Universal-Gesundheitspaß* konzipiert werden, in dem lebenslang alle Informationen gesammelt werden sollen, die es dem Einzelnen ermöglichen, sich selbst kompetent um seine Gesundheit zu sorgen.

Unter den oben beschriebenen Kategorien der Projekte zu Gesundheitschipkarten reiht sich der Berliner Gesundheitspaß in die allumfassenden multifunktionalen und deshalb datenschutzrechtlich kritischen Chipkarten ein, die einer allgemeinen politischen Zielsetzung folgen. Allerdings ist die Realisierungsform immer offengelassen worden. Sie soll erst in einer späteren Phase des Projektes konkretisiert werden. Dies gilt auch für die sicherheitstechnischen Aspekte.

Wir haben bei den Erörterungen betont, daß es mit Chipkarten möglich ist, höchste Sicherheitsansprüche zu befriedigen, daß dieses jedoch auch für die Infrastruktur gelten muß, mit der die Chipkarten gelesen, ausgewertet und weiterverarbeitet werden. Diese können keinen ökonomischen Abwägungen ausgesetzt werden. Immerhin können versehentliche oder manipulative Datenveränderungen auf dem Chip lebensbedrohende Wirkung haben. Damit stellt die Sicherheit einen Kostenfaktor dar, der nicht wie bei der Krankenversichertenkarte der Kostenminimierung geopfert werden darf.

Neben diesen hohen finanziellen Hürden bestehen Zweifel, ob die angestrebten gesundheitspolitischen Ziele erreichbar sind. Hinzu kommen die Bedenken der beteiligten Organisationen. So fürchten die Ärztevertretungen intensivere Kontrollen und zusätzlichen Aufwand; die Kostenträger bezweifeln den Beitrag des Gesundheitspasses zur Kostensenkung und Erhöhung der Transparenz.

Angesichts dieser in den Arbeitsgruppen artikulierten Zweifel wurde von der Senatsverwaltung für Gesundheit von der schnellen probeweisen Einführung des Gesundheitspasses abgesehen und die Priorität dahin verlagert, zunächst wissenschaftlich alle als Probleme erkannten Sachverhalte zu untersuchen.

3.3 Autobahngebührenerfassung

Im November 1995 wurde in der Presse bekannt, daß es keine elektronisch einzuziehende Autobahngebühren für Personenkraftwagen geben würde. Damit wurde der Schlußstrich unter ein datenschutzrechtlich, aber wohl auch in manch anderer Hinsicht höchst fragwürdiges Projekt gezogen.

Der Ergebnisbericht des TÜV Rheinland zum Feldversuch auf der Bundesautobahn A 555 zwischen Bonn und Köln machte deutlich, daß es Verfahren zur automatisierten Autobahngebührenerfassung (AGE) gab, die das Problem der automatischen Erhebung der Autobahngebühren zufriedenstellend lösen dürften, daß jedoch die *automatische Kontrolle der ordnungsgemäßen Zahlung* von keinem Ansatz hinreichend gelöst werden konnte. Der Bericht machte ferner deutlich, daß die in Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder formulierten „Anforderungen des Datenschutzes" prinzipiell erfüllt werden können. Voraussetzung sei die Gebührenerhebung durch ein anonymes Zahlungsverfahren und die Sicherstellung, daß Zahlungswillige und Nicht-Zahlungspflichtige bei Kontrollen nicht registriert werden.

Der Schlußbericht kommt zum Ergebnis, daß die Einführung eines AGE-Systems nur für Lastkraftwagen mit einem zulässigen Gesamtgewicht von mindestens 12 t in Erwägung gezogen werden soll. Die Kontrolle soll dabei nach dem Muster herkömmlicher Kontrollen erfolgen.

Da frühzeitig Konsens darüber bestand, daß der Datenschutz und die Datensicherheit bei der Bewertung des Feldversuches eine entscheidende Rolle spielen würden, sind die Datenschutzbeauftragten des Bundes und der Länder unter Federführung des Bundesbeauftragten bereits frühzeitig in die Diskussion eingebunden worden. Zunächst wurden die datenschutzrechtlichen Anforderungen an die AGE-Verfahren formuliert. Danach sollten die Verfahren gewährleisten, daß

- die Erhebung anonym erfolgt und damit anonyme Zahlungsverfahren verwendet werden. Dies hätte zur Konsequenz, daß die Gebühren im voraus zu entrichten wären *(Prepaid-Verfahren)*;
- eine Speicherung der Benutzerdaten für einen eventuellen Nachweis der ordnungsgemäßen Zahlung nur dezentral beim Benutzer erfolgen solle;
- die Kontrolle die *Anonymität* für diejenigen erhält, die ordnungsgemäß zahlen oder zahlen wollen oder von den Gebühren befreit sind;
- die Kontrolldichte so gering wie möglich gehalten wird;
- die Vertraulichkeit auftretender personenbezogener Daten durch fortschrittliche technische Maßnahmen (gegenseitige Authentifizierung aller miteinander kommunizierenden Komponenten, kryptographische Verschlüsselung, Zugriffscodes für den Zugang an Daten auf dezentralen Speichern [z. B. Chipkarten im Fahrzeug]);
- die Datenintegrität sichergestellt wird, das heißt die richtigen Daten nur den richtigen Benutzern zugeordnet und alle sicherheitsrelevanten Daten gegen Manipulation geschützt werden;
- das gesamte Verfahren für den Benutzer *transparent* gestaltet wird, das heißt, er muß stets nachvollziehen können, welche Entgelte wann wo abgebucht wurden, wann sein Guthaben erschöpft oder nicht mehr ausreichend ist und wann sein Fahrzeug im Falle einer Kontrollmaßnahme identifiziert worden ist. Abbuchungen, Funktionsstörungen und Manipulationsversuche müssen dem Benutzer angezeigt werden und dezentral, z. B. auf einer Chipkarte im Fahrzeug, protokolliert werden können. Für die Protokolle müssen Druckmöglichkeiten, z. B. in Tankstellen, bereitgehalten werden.

Besonders bedeutsam ist die ergänzende Forderung nach *Stabilität gegen die Rücknahme* von Maßnahmen, die zur Erfüllung der obengenannten Forderungen getroffen werden. Sie dürfen nicht einseitig durch den Systembetreiber oder durch Dritte zurückgenommen werden können. Zum Beispiel bedeutet dies, daß eine generelle Videoüberwachung des fließenden Verkehrs ausgeschlossen sein muß, weil diese mit geringen Modifikationen auf eine Vollkontrolle umgestellt werden kann.

Im Januar 1995 fand in Berlin ein *Workshop* statt, bei dem alle zehn am Feldversuch beteiligten Unternehmen und Konsortien ihre Konzepte präsentierten und sich den Datenschutzbeauftragten zur Diskussion stellten. Grundlage war ein Fragenkatalog, der den Unternehmen zur Verfügung gestellt worden war.

Die Verfahren unterschieden sich in der technischen Konzeption der verschiedenen Phasen Positionsbestimmung, Kontrolle und Abrechnung teilweise sehr wesentlich, so daß aus datenschutzrechtlicher Sicht zwangsläufig sehr unterschiedliche Bewertungen zu erwarten waren:

Die meisten Verfahren ermittelten die *Position von Fahrzeugen* mittels fester Einrichtungen (Baken, Brücken) am Rande der Autobahn. Beim Passieren der Einrichtungen wird festgestellt, daß ein Fahrzeug zahlungspflichtig wird. Durch Mustererkennungsverfahren oder durch Kommunikation mit dem im Fahrzeug befindlichen Gerät (On-Bord-Unit – OBU –) wird die Fahrzeugklasse erkannt. Andere Verfahren verzichten auf solche Einrichtungen und verwenden das Global Positioning System (GPS), damit die OBU *satellitengestützt* die genaue Position des Fahrzeuges ermitteln kann. Durch Vergleich mit digital abgespeicherten Autobahnkarten kann dann festgestellt werden, ob sich das Fahrzeug auf einer kostenpflichtigen Autobahn befindet oder nicht.

Zur *Abrechnung* boten die meisten Verfahren wahlweise die Vorauszahlung *(prepaid)* oder die spätere Bezahlung nach Abrechnung *(postpaid)* an. Da beim Postpaid-Verfahren personenbezogene Daten über die Autobahnnutzung zur späteren Abrechnung gesammelt werden müssen, entsprachen diese Verfahren nicht den Anforderungen der Datenschutzbeauftragten, da die Anonymität der Straßennutzung nicht sichergestellt werden konnte. Die Wahl zwischen beiden Zahlungsarten stellt nicht sicher, daß die Rücknahme der datenschutzgerechten Maßnahme ausgeschlossen ist. Da die Einrichtungen zur Datenerhebung vorhanden waren, konnten sie auch so eingestellt werden, daß sie auch bei vorausbezahlenden Fahrern in Betrieb genommen werden konnten. Nur jene Verfahren konnten deshalb die ungeteilte Billigung der Datenschutzbeauftragten finden, die die vorauszahlende Abrechnungsweise (Abbuchung auf einer Prepaid-Chipkarte – vergleichbar mit der Telefonkarte – in der OBU) technisch erforderlich machten. Dies gilt z. B. für jene Verfahren, die auf straßenseitige Einrichtungen verzichten und daher keine fahrzeugbezogenen Daten während der Fahrt erfassen können.

Bei den *Kontrollverfahren* ging es um Methoden, Fahrzeuge zu erkennen, die nicht ordnungsgemäß bezahlt hatten. Dies erfolgte grundsätzlich durch Funkkommunikation zwischen der Kontrolleinrichtung und der OBU im Fahrzeug. Bei einigen Verfahren waren diese Kontrolleinrichtungen in die Baken bzw. Brücken zur Positionsbestimmung und Abbuchung eingebaut, bei einigen gab es spezielle Kontrolleinrichtungen, die ständig oder stichprobenweise eingesetzt werden konnten. Die ersteren eigneten sich für Vollkontrollen, das heißt, jedes vorbeifahrende Fahrzeug wird kontrolliert. Häufig wurden alle Fahrzeuge auch durch Videokameras zumindest kurzfristig erfaßt. Wenn die Kontrolle ergab, daß für ein Fahrzeug nicht ordnungsgemäß bezahlt wurde, wurden *Standfotos* mit den Kennzeichen gespeichert und zur weiteren Verfolgung verwendet. Vollkontrollen wurden von den Datenschutzbeauftragten schon deshalb abgelehnt, weil keine Sicherheit dafür bestand, daß sie – zumindest fallweise – nicht für die totale Überwachung und Aufzeichnung des Autobahnverkehrs mißbraucht werden können. Akzeptabel waren daher nur solche Verfahren, die auf eine stichprobenhafte Kontrolle zurückgriffen.

Nachdem der Workshop die Bandbreite der erprobten Möglichkeiten aufzeigte, verabschiedete die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Entschließung zur automatischen Erhebung von Straßennutzungsgebühren, in der die Anforderungen noch einmal schlaglichtartig zusammengefaßt wurden.[26]

26 vgl. Anlage 2.4

- Gewährleistung des Grundsatzes der *„datenfreien Fahrt“*,
- technische und rechtliche Ausschließung flächendeckender Kontrollen,
- Anonymität bei korrektem Verhalten,
- Transparenz und Kontrollierbarkeit der Abläufe für den Fahrer,
- keine Rücknehmbarkeit der Datenschutzmaßnahmen,
- gesetzliche Regelung des Verfahrens und Sicherstellung der Datenschutzmaßnahmen.

Der Feldversuch hat gezeigt, daß es mit gutem Willen Verfahren geben kann, die diesen Anforderungen genügen.

Allerdings war die technische Reife der Verfahren nicht so weit gediehen, daß der Versuch zu einer Entscheidung für die Einführung der elektronischen Autobahnmaut für Personenkraftwagen führen konnte. So mußte der gute Wille keinem Test unterzogen werden!

Insgesamt läßt sich aus dieser Diskussion aber ein positives Fazit für den Datenschutz ziehen: Erstmals kam es rechtzeitig vor der Entscheidung über die Einführung eines Datenschutzverarbeitungsverfahrens zu einem Dialog zwischen den Datenschutzbeauftragten und den Herstellern, an dessen Ende die Erkenntnis stand: datenschutzgerechte Technik ist möglich. An den Anforderungen des Datenschutzes ist jedenfalls – entgegen den Äußerungen mancher Verantwortlicher – das Projekt Automatische Gebührenerfassung nicht gescheitert.

3.4 Persönlichkeitsrechte im Knast

Datenschutz ist ein Menschenrecht.[27] Es gilt auch im besonderen Gewaltverhältnis und endet nicht vor Gefängnismauern. Wir haben versucht, durch eine *Querschnittsprüfung* in der größten Berliner Justizvollzugsanstalt, der *JVA Tegel*, festzustellen, wie es um den Datenschutz der Strafgefangenen bestellt ist.

Zum Prüfungszeitpunkt saßen ungefähr 1 500 Strafgefangene in den sechs Teilanstalten ein. Es gibt eine zentrale Vollzugsgeschäftsstelle, die Hausbüros der Teilanstalten haben jedoch wichtige Aufgaben – wie z. B. das Führen der Gefangenenpersonalakten – übernommen. Auch der Ärztliche Dienst ist dezentral in den Teilanstalten untergebracht. In die Prüfung waren die Vollzugsgeschäftsstelle, die Telefonzentrale, die Einweisungsabteilung, ein Hausbüro, eine Hauskammer, die Arbeitsverwaltung, Werkstätten, die Abteilung für Zentrale Aufgaben, die Pädagogische Abteilung, Arztgeschäftsstellen, die Sozialpädagogische Abteilung, Teilanstalten und das Haupttor einbezogen.

Nach dem neuen § 6 Abs. 2 BlnDSG finden für die Verarbeitung personenbezogener Daten im Strafvollzug die §§ 13 bis 15 des BDSG Anwendung, soweit im *Strafvollzugsgesetz* keine Datenverarbeitungsbefugnisse existieren. Die übrigen Vorschriften des Berliner Datenschutzgesetzes gelten uneingeschränkt.

Hintergrund dieser Regelung ist, daß in vielen Bundesgesetzen – so auch im Strafvollzugsgesetz – die erforderlichen bereichsspezifischen Datenverarbeitungsbefugnisse noch immer fehlen.[28] Sie darf jedoch nicht von der Tatsache ablenken, daß spezielle datenschutzrechtliche Regelungen vom Bundesverfassungsgericht gefordert wurden und dies nur eine befristete Notlösung sein kann. Es sind deshalb erhöhte Anforderungen an die Erforderlichkeit der Verarbeitung personenbezogener Daten im Strafvollzug zu stellen.

Einige gravierende Mängel waren zu beanstanden:

Ein *internes Dateienregister*, das alle in der JVA Tegel geführten Dateien mit Zweckangabe und Inhaltsbeschreibung aufführt, fehlt. Nur wenn ein Überblick über die vorhandenen Dateien besteht, ist die nach dem Berliner Datenschutzgesetz[29] vorgesehene Sicherstellung des Datenschutzes durch den behördlichen Datenschutzbeauftragten und die Kontrolle durch den Berliner Datenschutzbeauftragten[30] möglich. Das gilt insbesondere bei einer nahezu unübersichtlichen Menge von Datensammlungen, wie wir sie in der JVA Tegel vorgefunden haben. Allein bei den 22 geprüften Stellen werden 1 7 Sammlungen mit personenbezogenen Daten geführt.

In der Vollzugsgeschäftsstelle läuft seit Mitte 1994 eine als „Testphase“ bezeichnete automatisierte Datenverarbeitung. Sie dient der Erstellung von Gefangenenkarteikarten, der Lohnkontenverwaltung, der Arbeitsverwaltung und statistischen Zwecken. Obwohl bereits Echt-Daten gespeichert werden, erfolgte keine *Anmeldung zum Dateienregister* und keine hinreichende *Zugangs-, Speicher-, Benutzer-, Zugriffs-, Eingabe- und Organisationskontrolle*. Unter den vorgefundenen Umständen sind weder die Vertraulichkeit der Daten noch die Integrität und Verfügbarkeit der Daten, Programme und Systeme auch nur annähernd gewährleistet.

In der Querschnittsprüfung wurden auch einige Probleme von grundsätzlicher Bedeutung erkennbar:

Es fehlen Regelungen dafür, welche Stelle welche Datensammlungen führt. Zahlreiche *Daten werden mehrfach bei den verschiedensten Stellen gespeichert*, und bei Stellen mit identischen Aufgabenbereichen haben wir völlig unterschiedliche Datensammlungen vorgefunden.

Bundeseinheitliche Vorgaben der Vollzugsgeschäftsordnung, welche Datensammlungen zu führen sind, werden nicht hinreichend beachtet. Obwohl nach Nr. 63 Vollzugsgeschäftsordnung (VGO) nur die Vollzugsgeschäftsstelle ein Namensverzeichnis (Nr. 66 VGO) und ein Zugangs- und Abgangsbuch (Nr. 67 VGO) führt, haben wir beispielsweise sechsmal ein Namensverzeichnis und fünfmal ein Zugangs- und Abgangsbuch vorgefunden.

Die *Doppelspeicherungen* und der Datenumfang sind kritisch zu überprüfen. Ein Teil der Datensammlungen ist verzichtbar. Der von der Vollzugsgeschäftsordnung aufgestellte Grundsatz, daß die Vollzugsgeschäftsstelle bzw. die Hausbüros die Datensammlungen führen, sollte weitgehend wieder aufgegriffen werden. Eine Reduzierung der Datensammlungen und ihres Umfanges trägt nicht nur dem Grundsatz der Erforderlichkeit Rechnung, sondern stellt auch eine Arbeitsentlastung zugunsten anderer Vollzugsaufgaben dar.

Die *Automatisierung* eröffnet vielfältige Möglichkeiten für einen datenschutzgerechteren Umgang mit den Daten der Gefangenen. Die in der Vollzugsgeschäftsordnung vorgesehenen Bücher können von der Vollzugsgeschäftsstelle bzw. einer zentralen Stelle automatisiert erfaßt werden. Dabei ist die Einführung unterschiedlicher Zugriffsrechte und -beschränkungen, die sich an den Aufgaben der Mitarbeiter orientieren, vorzusehen. Auch der Datenumfang könnte vor einer Automatisierung noch einmal kritisch auf seine Erforderlichkeit für die Aufgabenerfüllung überprüft werden. Gerade bei der Größe einer Anstalt wie der JVA Tegel kann die Automatisierung entscheidend zur Arbeitsentlastung der Mitarbeiter und zur Verwirklichung des Schutzes des informationellen Selbstbestimmungsrechtes der Gefangenen beitragen. Die begonnene Automatisierung der Datenverarbeitung hat bereits jetzt gezeigt, daß sich hierdurch der Datenumfang der an andere Stellen innerhalb der JVA zu übermittelnden Daten verringert hat.

Der Inhalt der *Gefangenenpersonalakten* ist in mehrfacher Hinsicht problematisch: wegen des Umfanges der zum Teil höchst persönlichen Daten, wegen der Art der Aufteilung der Akte und im Hinblick auf die Zugriffsrechte Dritter.

In die Gefangenenpersonalakte sollten nur Unterlagen aufgenommen werden, die mit der Erreichung des Vollzugszieles in einem unmittelbaren Zusammenhang stehen. Die Aufnahme von für den Vollzug nicht relevanten Banalitäten (wie z. B. dienstliche Meldungen über zerbrochenes Geschirr) sollte unterbleiben. Auch bei den sogenannten *„Vormeldern“* (Anträge von Gefangenen) ist kritisch zu prüfen, ob eine Aufbewahrung in der Gefangenenpersonalakte tatsächlich erforderlich ist. Vormelder, mit denen die Gefangenen beispielsweise um einen Arztbesuch bitten, dienen nicht dem Vollzug, sondern stehen im Zusammenhang mit dem Arztbesuch, so daß der Vormelder – falls er aufbewahrt werden muß – wegen der besonderen Sachnähe in der Kranken- bzw. Gesundheitsakte abgeheftet werden sollte.

27 Jahresbericht 1990, 1.1
28 vgl. Jahrsbericht 1994, 4.8 und Anlage 2.10
29 § 19 Abs. 1 BlnDSG
30 § 24 Abs. 1 BlnDSG

Die derzeit bestehende Möglichkeit jedes Mitarbeiters des Vollzugsdienstes, Gefangenenpersonalakten einzusehen, ist mit dem Recht auf informationelle Selbstbestimmung nicht zu vereinbaren. Nur soweit es für die Aufgabenerfüllung tatsächlich erforderlich ist, darf die Personalakte eingesehen werden. Zur nachträglichen Überprüfung der Rechtmäßigkeit der Einsichtnahme ist eine Protokollierung vorzusehen.

Um einen am Erforderlichkeitsgrundsatz orientierten Zugriff auf die in der Gefangenenpersonalakte enthaltenen Daten zu gewährleisten, sollte eine *getrennte Aktenführung* eingeführt werden, die sich an den bereits vorhandenen drei Heftnadeln und den besonders sensiblen Daten über sozialtherapeutische oder ärztliche Behandlungen und Maßnahmen orientieren sollte.

Die JVA Tegel erhält vor der Aufnahme eines Gefangenen aus der JVA Moabit eine vollständig angelegte Personalakte mit einer *Aufnahmemitteilung* über den Gefangenen. Die Vollzugsgeschäftsstelle der JVA Tegel erstellt im automatisierten Verfahren eine neue Aufnahmemitteilung, die weniger Daten enthält. Die positiv zu bewertende Reduzierung des Datensatzes verliert bei der Abheftung der Aufnahmemitteilung in der Gefangenenpersonalakte durch die weitere Aufbewahrung der Moabiter Mitteilung ihre Wirkung, da bei Einsichtnahmen in die Akte die Möglichkeit besteht, auch die umfassendere Aufnahmemitteilung, deren Inhalt überholt ist, einzusehen. Diese inhaltlich überholten Daten, die auch in Gefangenenkarteien und anderen Datensammlungen wieder auftauchen, sollten vernichtet werden, da sie zur Aufgabenerfüllung nicht mehr erforderlich sind.

Die *Aufbewahrungsdauer* der Datensammlungen unterliegt offensichtlich keiner besonderen Kontrolle.

Soweit für Datensammlungen keine Aufbewahrungsfristen existieren, ist die Erforderlichkeit der Speicherungsdauer im Einzelfall zu prüfen. Für die Beurteilung der Erforderlichkeit sind nur Vollzugsaufgaben heranzuziehen. Die Aufbewahrung darf nicht mit der Begründung, die wir häufiger erhalten haben – „Die Erfahrung zeige, daß die meisten Gefangenen nach ihrer Entlassung wiederkommen“ –, zu einer Vorratsdatenverarbeitung führen.

Die zum Teil über viele Jahre *fortlaufende Führung der Bücher* führt zu unterschiedlich langen Aufbewahrungszeiten der personenbezogenen Daten. Sie sollten künftig jahrgangsweise und – wo möglich – als Kartei geführt werden. Nur so können unverhältnismäßig lange Speicherzeiten für einzelne Betroffene verhindert und die Fristenkontrolle erleichtert werden.

Probleme bereiten auch die *bundeseinheitlichen Bestimmungen über die Aufbewahrungsfristen* für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizbehörden, in denen auch Aufbewahrungsfristen für die in der Vollzugsgeschäftsordnung geregelten Buchwerke, die Gefangenenpersonalakte und die Gefangenenkarteikarten enthalten sind. Die Fristen reichen von fünf Jahren bis zu 30 Jahren.

Problematisch ist bereits der Anknüpfungspunkt für den Fristbeginn. Die Frist beginnt mit dem auf das Jahr der Weglegung folgenden Jahr zu laufen. Als Jahr der Weglegung z. B. bei Gefangenenbüchern gilt das Jahr, in dem der Vollzug aller darin aufgeführten Gefangenen beendet ist. Das bedeutet, daß Bücher, in denen Daten über einen zu lebenslänglicher Freiheitsstrafe verurteilten Gefangenen gespeichert sind, unter Umständen länger als 45 Jahre aufbewahrt werden. Die Regelung stellt einen krassen Verstoß gegen den Grundsatz der Verhältnismäßigkeit und das Recht auf informationelle Selbsbestimmung dar und erschwert die Fristenkontrolle. Es muß ständig kontrolliert werden, welcher Gefangene die längste Freiheitsstrafe verbüßt. Dies dürfte nur sehr schwer durchführbar sein, zumal die Länge der Haftdauer in den Büchern nicht vermerkt ist.

Die uns häufig auf unsere Frage nach der Aufbewahrungsdauer von Unterlagen gegebene Antwort – „Wir sammeln so lange, bis der Raum/Schrank (in dem die Altakten aufbewahrt werden) voll ist“ – zeigt, daß die Aufbewahrungsvorschriften nicht ausreichend bekannt sind. Erst recht unbekannt ist der Anknüpfungspunkt für den Fristbeginn, an den sich demzufolge niemand zu halten scheint. Der Beginn der Aufbewahrungsfristen sollte praxisgerechter und am Erforderlichkeitsgrundsatz orientiert festgelegt werden.

Die bundeseinheitlichen Aufbewahrungsvorschriften sind vor dem Hintergrund der Schwierigkeiten in der Anwendung und der dort geregelten Fristen dringend zu überarbeiten. Für die nicht in den bundeseinheitlichen Aufbewahrungsvorschriften geregelten Datensammlungen sind Aufbewahrungsvorschriften möglichst einheitlich für alle Justizvollzugsanstalten des Landes Berlin festzulegen.

Es gibt eine nahezu unübersichtliche Anzahl von *Fotos von den Gefangenen* zu den verschiedensten Zwecken und bei den verschiedensten Stellen.

Nach § 86 Abs. 1 Strafvollzugsgesetz (StVollzG) ist die Aufnahme von Lichtbildern zur erkennungsdienstlichen Behandlung des Gefangenen zur „Sicherung des Vollzuges“ zulässig. Danach dürfen Lichtbilder nur gefertigt werden, wenn konkrete Hinweise für eine Fluchtgefahr bestehen. Der Gesetzgeber schreibt eine Entscheidung in jedem Einzelfall vor und hält die Anfertigung von Lichtbildern von *jedem* Gefangenen nicht für angezeigt. Als eine das Ermessen bindende Regelung sieht in Nr. 23 Abs. 2 VGO darüber hinaus vor, daß nur bei Strafgefangenen mit einer Vollzugsdauer von einem Jahr und mehr Lichtbilder aufzunehmen sind.

Wir haben Zweifel, daß die Vielzahl von Fotos, die wir in der Anstalt vorgefunden haben, unter Beachtung dieser Anforderungen gefertigt wurde.

Nach § 86 Abs. 3 StVollzG kann der Gefangene beantragen, daß die erkennungsdienstlichen Unterlagen nach seiner Entlassung aus dem Vollzug vernichtet werden. Hierfür ist erforderlich, daß feststellbar ist, ob von dem Gefangenen Fotos gefertigt wurden, wie viele Abzüge existieren, an welche Stellen sie weitergegeben wurden und wo sich die Negative befinden. Die Verantwortlichkeit für die *Aufbewahrungs- und Dokumentationspflichten* ist klar zu regeln und sollte bei der Stelle liegen, die die Gefangenenpersonalakte führt. Nach § 86 Abs. 2 StVollzG sind die erkennungsdienstlichen Unterlagen zu den Gefangenenpersonalakten zu nehmen und nach Nr. 23 VGO dort in einem besonderen Umschlag aufzubewahren. In der Gefangenenpersonalakte sind auch das Negativ und sämtliche Abzüge sowie alle anderen Fotos, die zur Sicherung des Vollzuges gefertigt wurden, aufzubewahren. Hier ist die Zahl der Abzüge und jede Weitergabe von Abzügen zu dokumentieren.

Die in der JVA Tegel gewählte Verfahrensweise bei dem Umgang mit Fotos ist äußerst unübersichtlich. Nur in wenigen Gefangenenpersonalakten haben wir überhaupt ein Foto gefunden, so daß die gesetzliche Regelung hier zur Ausnahme gemacht worden ist. Fotos befinden sich bei den verschiedensten Stellen der Anstalt, auf Karteien oder anderen Unterlagen; eine Dokumentation, an welche Stellen Fotos weitergegeben wurden, existiert nicht. Nicht nur der Fotograf fertigt Fotos von Gefangenen an, sondern auch andere Stellen besitzen Polaroid-Kameras für Fotos von Gefangenen. Eine Kontrolle des Umganges mit den Fotos und eine Überprüfung der Zulässigkeit von Übermittlungen sowie die Durchsetzung des Anspruches der Gefangenen, daß *alle* ihre Fotos vernichtet werden (§ 86 Abs. 3 StVollzG), ist so nicht sichergestellt.

Es ist bedenklich, daß die Gefangenen über ihr Recht, die Vernichtung der Fotos zu verlangen, nur bei der Aufnahme durch einen Hinweis im Formular informiert werden, im übrigen offenbar für Ausländer nicht in ihrer Muttersprache. Bis zur Entlassung aus der Haft ist dieser Hinweis – wenn er denn auf dem umfangreichen Formular überhaupt gelesen wurde – in der Regel vergessen. Um den Betroffenen die Durchsetzung ihres Rechtes zu ermöglichen, sollte auch bei der Entlassung ein ausdrücklicher Hinweis hierauf erfolgen. Da die Fotos nach der Entlassung nicht mehr für Vollzugszwecke benötigt werden, wäre auch eine Vernichtung zu diesem Zeitpunkt ohne Antrag des Betroffenen sachgerecht und entspräche dem Erforderlichkeitsgrundsatz. Auf jeden Fall sind den Betroffenen die in ihrem Auftrag gefertigten Paß- und Ausweisfotos einschließlich der Negative bei ihrer Entlassung auszuhändigen.

3.5 Parkraumbewirtschaftung

Seit dem 6. März 1995 läuft in Berlin eine zweijährige Testphase zur Parkraumbewirtschaftung. Als Parkraumbewirtschaftungs-

zonen sind die Spandauer Altstadt, die westliche Innenstadt sowie Stadtmitte eingerichtet worden. Offensichtlich einmalig im Bundesgebiet übernehmen private Firmen in den drei Parkraumbewirtschaftungszonen nicht nur die Aufstellung und Unterhaltung der Parkscheinautomaten, sondern auch die Kontrolle der Parkberechtigungen im jeweiligen Bewirtschaftungsgebiet. Die Senatsverwaltung für Verkehr und Betriebe hat zu diesem Zweck für das Land Berlin mit verschiedenen Firmen einen *Vertrag über die Bewirtschaftung von Anwohnerparkzonen* in Berlin abgeschlossen.

Der Vertrag verpflichtet die Firmen zum einen zur Beschaffung, zum Aufbau und zur Unterhaltung der Parkscheinautomaten; zum anderen überträgt er den Firmen auch die *Überwachung des ruhenden Verkehrs* in Abstimmung mit der Polizei. Die privaten Firmen kontrollieren in den vertraglich vereinbarten Gebieten und zu vertraglich vereinbarten Zeiten den ruhenden Verkehr. Die Entscheidung, wo und wann kontrolliert wird, obliegt dem Polizeipräsidenten. Dieser kann den Mitarbeitern der privaten Firmen jederzeit Weisungen erteilen. Wenn die Privaten bei ihrer Kontrolltätigkeit einen Verstoß gegen das Halten und Parken feststellen, erfassen sie mittels *Handcomputer* die Daten und übermitteln diese nach Ablauf eines Arbeitstages an die Bußgeldstelle. Am kontrollierten Fahrzeug hinterlassen die Kontrolleure einen Hinweiszettel, mit dem der Fahrzeuginhaber darauf hingewiesen wird, daß er sein Fahrzeug verkehrswidrig abgestellt habe und die weitere Bearbeitung unter Einsatz der automatischen Datenverarbeitung der Bußgeldbehörde beim Landespolizeiverwaltungsamt erfolgen werde.

Bei dem Einsatz privater Firmen zur Kontrolle des ruhenden Verkehrs stellt sich aus datenschutzrechtlicher Sicht die Frage, ob es sich hierbei um eine Funktionsübertragung oder um *Auftragsdatenverarbeitung* nach § 3 BlnDSG handelt. Besonders problematisch ist in diesem Zusammenhang die Frage, in welchem Umfang Private im Bereich der hoheitlichen Aufgabenerfüllung eingesetzt werden dürfen.

Die Polizei übernimmt die erhobenen Daten über Parkverstöße zunächst zwar ohne weitere Prüfung zum Erlaß von Verwarnungs- und Bußgeldbescheiden. Nach dem mit den privaten Firmen abgeschlossenen Vertrag sind dem Polizeipräsidenten aber die Entscheidungen über das Ob, Wo und die Dauer der Kontrollen und damit der Datenerhebungen durch die Privaten vorbehalten. Bei den Datenerhebungen steht den Privaten kein Ermessensspielraum zu, da sie bei ihrer Tätigkeit weisungsabhängig vom Polizeipräsidenten sind.

Wir sehen den Einsatz der Privaten gerade noch als Auftragsdatenverarbeitung an, weil die Privaten bei ihrer Aufgabenerfüllung in jeder Hinsicht von den Weisungen des Polizeipräsidenten abhängig sind. Ob der Verzicht der Polizei auf eine Ermessensausübung vor Ort verfassungsrechtlich zulässig ist, ist allerdings umstritten und liegt dem Verwaltungsgericht zur Entscheidung vor.

Der mit den privaten Firmen geschlossene Vertrag, in dem auch die Auftragsdatenverarbeitung geregelt ist, zitiert speziell zur Datenerfassung und -speicherung mit *mobilen Datenerfassungsgeräten*, zur Zusammenführung der erfaßten Daten auf einem Datenträger und zum Transport der Datenträger bzw. Übertragung der Daten zur Bußgeldstelle lediglich § 5 Abs. 3 BlnDSG. Eine Präzisierung dieser Maßnahmen zur Erfüllung der zitierten Kontrollanforderungen erfolgt ebensowenig wie eine durchgängige, präzise Darstellung der in Auftrag gegebenen Datenverarbeitungsschritte.

Gerade wegen der besonderen Risiken mobiler IuK-Technik hätten jedoch Mindestanforderungen an Maßnahmen zur Benutzer- und Speicherkontrolle bei den mobilen Datenerfassungsgeräten und zur Transportkontrolle bei Datenträgeraustausch bzw. Datenübertragung an die Bußgeldstelle formuliert werden müssen.

Auch die *Umsetzung des Parkraumbewirtschaftungskonzeptes* warf bereits vor Beginn der Testphase zahlreiche Probleme auf.

Nachdem uns die Senatsverwaltung für Verkehr und Betriebe Ende November 1994 durch Übersendung einer Mitteilung zur Kenntnisnahme für das Abgeordnetenhaus über ein Parkraumbewirtschaftungskonzept unterrichtet hatte, erfuhren wir Anfang des Jahres 1995 aus der Presse sowie durch zahlreiche Bürgerbeschwerden, daß bereits private Firmen mit der Parkraumbewirtschaftung beauftragt worden waren und die Ausgabe von Anwohnervignetten etwa Ende Januar 1995 beginnen sollte. Ein Datenschutzkonzept lag nicht vor. Erst nach einer Beanstandung und einem weiteren halben Jahr hat uns die Senatsverwaltung für Verkehr und Betriebe den zwischen dem Land Berlin und den privaten Firmen geschlossenen Vertrag zur Verfügung gestellt. Auch eine Meldung zum Dateienregister war mit Beginn der Testphase des Parkraumbewirtschaftungskonzeptes noch nicht erfolgt. Nach Auffassung der Senatsverwaltung für Verkehr und Betriebe handelt es sich bei dem Notieren des Kraftfahrzeugkennzeichens, des Kraftfahrzeugtyps sowie der Angaben, wie und wo falsch geparkt wurde, durch die Privaten nicht um eine Datenspeicherung. Nach § 4 Abs. 2 Nr. 2 BlnDSG bedeutet Speichern jedoch das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger. Diese Voraussetzungen liegen hier zweifelsfrei vor.

Die Mitarbeiter der privaten Firmen fertigen in Ausnahmefällen auch *Fotos zu Beweiszwecken*. Die Filme bleiben bei den Firmen und werden erst im Rahmen einer etwaigen Zeugenanhörung durch die Bußgeldbehörde entwickelt und dieser übersandt. Der Verbleib der Negative bei den privaten Firmen ist bedenklich. Die zu Beweiszwecken gefertigten Negative sind der Bußgeldbehörde zu übermitteln, denn auch bei den Fotos handelt es sich um personenbezogene Daten, die für das Ordnungswidrigkeitenverfahren erhoben wurden. Nach Erledigung des jeweiligen Bußgeldverfahrens sind die Negative der zu Beweiszwecken aufgenommenen Fotos zu vernichten.

Auch die Datenerhebung zur *Erteilung eines Anwohnerparkausweises* war problematisch. Aus den Informationsmaterialien zur Antragstellung ergab sich für den Bürger, daß dem Antrag eine *Ablichtung des Personalausweises* und in Einzelfällen eine Bescheinigung aus dem Melderegister sowie eine Ablichtung der Seite des *Kraftfahrzeugscheines*, aus der sich der Name und die Anschrift des Halters sowie das amtliche Kennzeichen des Fahrzeuges ergeben, beigefügt werden mußte. Die Erhebung personenbezogener Daten ist nur zulässig, wenn sie zur Erfüllung der durch Gesetz der datenverarbeitenden Stelle zugewiesenen Aufgaben und dem jeweils damit verbundenen Zweck erforderlich ist.[31] Wie die Senatsverwaltung für Verkehr und Betriebe eingeräumt hat, enthält eine Ablichtung des Personalausweises personenbezogene Daten, die für die Antragsbearbeitung nicht benötigt werden. Erforderlich sind lediglich der Name und die Anschrift des Antragstellers, nicht jedoch die Augenfarbe und die Größe oder das Foto. Auch von dem Kraftfahrzeugschein sind nach Angaben der Verkehrsverwaltung für die Antragsbearbeitung nur der Name und die Anschrift des Halters sowie das amtliche Kennzeichen für die Erteilung der Vignette erforderlich, nicht aber das Datum der nächsten Hauptuntersuchung.

Die meisten Antragsteller dürften ihrem Antrag komplette Kopien ihrer Ausweise und Fahrzeugscheine beigefügt haben. Von der ursprünglich von der Senatsverwaltung für Verkehr und Betriebe angekündigten *Schwärzung der nicht erforderlichen Daten* wurde wieder abgerückt. Nunmehr soll nur dann geschwärzt werden, wenn ein Vorgang anläßlich eines Änderungsantrages neu bearbeitet wird. Änderungsanträge dürften jedoch nur in wenigen Fällen gestellt werden, so daß in der Mehrzahl der Fälle auch weiterhin unzulässig personenbezogene Daten gespeichert bleiben werden und für die Bewohner der Parkraumbewirtschaftungsbereiche eine bedenkliche Personalausweissammlung bei der Polizei entstanden ist.

Ausnahmegenehmigungen für das Parken in einer Parkraumbewirtschaftungszone werden in Form eines Bescheides durch den Polizeipräsidenten in Berlin erteilt, der den Bereich der Ausnahmegenehmigung, den Zeitraum der Wirksamkeit der Ausnahmegenehmigung, das Kraftfahrzeugkennzeichen des Antragstellers sowie den Zweck der Ausnahmegenehmigung enthielt. Da der Bescheid immer in Briefform verfaßt wird, enthält er auch die vollständige Adresse des Antragstellers. In den Nebenbestimmungen zu der Ausnahmegenehmigung wurden die Bürger darauf hingewiesen, daß sie – sofern sie ihr Fahrzeug verlassen – die erste Seite der Ausnahmegenehmigung im Fahrzeuginnern nach

31 § 18 Abs. 1 Satz 2 ASOG, § 9 Abs. 1 BlnDSG

außen hin lesbar anzubringen hätten. Diese erste Seite enthält die Adresse des Antragstellers, das Kraftfahrzeugkennzeichen sowie auch die Angabe des Zweckes für die Ausnahmegenehmigung.

Nach § 46 Abs. 3 Straßenverkehrsordnung (StVO) dürfen Ausnahmegenehmigungen und Erlaubnisse unter dem Vorbehalt des Widerrufes sowie mit Nebenbestimmungen erteilt werden. Die Vorschrift regelt auch, daß die Bescheide vom Betroffenen mitzuführen und auf Verlangen den zuständigen Personen auszuhändigen sind. Da bei einem Auslegen der ersten Seite des Bescheides im Kraftfahrzeug jedermann diese Daten lesen kann, dürfen nur die für die Aufgabenerfüllung tatsächlich erforderlichen Daten auf der Ausnahmegenehmigung auch für Dritte zu lesen sein. Dies ergibt sich aus dem Erforderlichkeitsgrundsatz des § 9 Abs. 1 BlnDSG. Nicht erforderlich ist danach die Angabe der vollständigen Adresse des Betroffenen. Dies hat auch der Polizeipräsident eingeräumt. Er hat uns mitgeteilt, daß in Zukunft der Genehmigungsinhaber beim Auslegen der Ausnahmegenehmigung im Fahrzeug nicht mehr sichtbar sein müsse.

Für nicht erforderlich halten wir auch das Auslegen des *Zweckes der Ausnahmegenehmigung*. Die Angabe des Zweckes der Ausnahmegenehmigung ermöglicht bei Abwesenheit des Fahrers nicht die Kontrolle, ob der angegebene Zweck tatsächlich in Anspruch genommen wird. Die in den Parkraumbewirtschaftungszonen tätigen privaten Firmen sind zudem nicht befugt, eigene Ermittlungen darüber anzustellen, ob der Fahrer des Fahrzeuges dem auf der Ausnahmegenehmigung angegebenen Zweck tatsächlich nachgeht. Da eine Kontrolle des Zweckes nach unserer Auffassung tatsächlich nicht möglich ist, halten wir die Angabe des Zweckes auf dem ausgelegten Teil des Bescheides für nicht erforderlich. Die Senatsverwaltung für Verkehr und Betriebe hat uns auf unsere Frage, warum der Zweck der erteilten Ausnahmegenehmigung sichtbar im Fahrzeug ausliegen müsse, keine befriedigende Antwort gegeben. Sie hat lediglich darauf hingewiesen, daß die Kontrollkräfte zweifelsfrei feststellen können müßten, daß zwar eine Ausnahmegenehmigung vorliege, diese jedoch zu anderen als den dort genannten Zwecken – und damit unzulässig – genutzt worden sei. Dies setze voraus, daß bei einer Verkehrsüberwachung der Zweck der Ausnahmegenehmigung ohne weiteres aus der im Fahrzeug ausgelegten Urkunde festgestellt werden könne. Dies ist unserer Auffassung nach jedoch gerade nicht möglich. Wir haben daher eine Beanstandung gegenüber der Senatsverwaltung für Verkehr und Betriebe wegen ihrer Forderung, auch den Zweck der Ausnahmegenehmigung für jedermann sichtbar durch Auslegen des Bescheides mit anzugeben, ausgesprochen.

Die Frage, wann eine *Löschung der Antragsdaten* erfolgen soll, ist nicht abschließend geklärt. Hier sind klare Löschungsfristen vorzusehen, die – wenn schon überflüssige Daten nicht geschwärzt werden – so bald wie möglich greifen sollten.

Da die *Informationsmaterialien und Antragsunterlagen* unzureichende Angaben über die zur Antragsbearbeitung erforderlichen Daten enthalten, ist eine Änderung dieser Unterlagen notwendig. Es müssen die erforderlichen datenschutzrechtlichen Hinweise – insbesondere auf die Schwärzungsmöglichkeit – gegeben werden. Eine Überarbeitung dieser Unterlagen soll „voraussichtlich“ nicht erfolgen. Dies ist um so bedauerlicher, als die Testphase für das Parkraumbewirtschaftungskonzept noch nicht einmal zur Hälfte abgelaufen ist, Erweiterungen offenbar geplant sind und sicherlich noch weitere Ausnahmegenehmigungen beantragt werden. Bei künftig eingehenden Anträgen, die für die Antragsbearbeitung nicht erforderliche personenbezogene Daten enthalten, sind diese Daten durch die Mitarbeiter der Polizei gleich zu schwärzen.

Der Vertrag zwischen dem Land Berlin und den Parkraumbewirtschaftungsfirmen enthält auch Regelungen über den Einsatz von Mitarbeitern bei den Firmen. Danach soll der Polizeipräsident seine Zustimmung zum Einsatz der Kontrolleure erteilen. Das setzt eine *Überprüfung der privaten Arbeitnehmer* und Datenerhebungen durch die Polizei voraus. Eine solche Datenerhebung würde ohne Rechtsgrundlage erfolgen. Das Allgemeine Sicherheits- und Ordnungsgesetz (ASOG) sieht hierfür keine Befugnis vor, und die Regelung des § 13 BDSG für die Datenerhebung, auf die das Berliner Datenschutzgesetz verweist, ist nur für die Personaldatenverarbeitung durch den öffentlichen Arbeitgeber anwendbar. In dieser Funktion wird die Polizei aber nicht tätig. Auch die in dem Vertrag vorgesehene Möglichkeit des Auftraggebers (Land Berlin), in die Personalakten der bei dem Auftragnehmer (private Firmen) beschäftigten Überwachungskräfte Einsicht zu nehmen und zu diesem Zweck die Einverständniserklärung des Betroffenen einzuholen, ist nicht zulässig. Die Einwilligung der Mitarbeiter in die *Einsichtnahme in ihre Personalakten* erfolgt in diesen Fällen nicht freiwillig. Im übrigen wäre auch eine Einsichtnahme in die vollständige Personalakte unzulässig, weil sie gleichzeitig zur Offenbarung von Personalinformationen führen würde, die für eine Überprüfung nicht erforderlich sind. Für eine ebenfalls in dem Vertrag vorgesehene Einholung von *„Gauck“-Auskünften* bei Mitarbeitern aus dem Westteil Berlins fehlt es ebenfalls an einer Rechtsgrundlage.[32]

3.6 Verwaltungsreform: Gläserne Verwaltung statt gläserner Bürger?

Mit Beschlüssen von August 1993 und Mai 1994 hat der Senat die Verwaltungsreform als Projekt *„BERLIN Unternehmen Verwaltung“* auf den Weg gebracht und ihr gleichzeitig eine hohe politische Priorität beigemessen. Die Berliner Verwaltung soll von einer bürokratischen Organisation zu einem modernen Anbieter von Dienstleistungen werden. Die rechtlichen Voraussetzungen wurden durch die Änderung der Verfassung von Berlin (Verkleinerung des Senats und der Bezirksämter) und durch die Verabschiedung des *Verwaltungsreformgesetzes* im Juni 1994[33] geschaffen. Das Verwaltungshandeln wurde in einem Katalog von „Dienstleistungsprodukten“ erfaßt, der seinerseits Grundlage für die Einführung der Kostenrechnung anstelle der herkömmlichen Kameralistik sein soll. Mit Hilfe der Kostenrechnung wird der *„gläserne Haushalt“* angestrebt.[34] Auch das Bild der „gläsernen Verwaltung“ wird als Zielvorstellung genannt, die vor allem durch die Veröffentlichung jährlicher Geschäftsberichte der Dienstleistungsbereiche und Serviceeinheiten verwirklicht werden soll. Dagegen greift das Projekt „Unternehmen Verwaltung“ nicht die von uns seinerzeit begrüßten und schon sehr weit gediehenen Vorbereitungen für ein *Informationsfreiheitsgesetz* auf, das zu einer noch größeren Transparenz des Verwaltungshandelns führen würde.

Angesichts knapper werdender öffentlicher Kassen und der möglicherweise bevorstehenden Fusion mit Brandenburg ist das Grundkonzept der Verwaltungsreform sicherlich zu begrüßen. Aus datenschutzrechtlicher Sicht muß aber klar sein, daß der Bürger, wenn er dem neuen „Unternehmen Verwaltung“ gegenübertritt, in seiner Rechtsstellung nicht schlechter gestellt sein darf als bisher. Auch die reformierte Berliner Verwaltung setzt sich weiterhin aus öffentlichen Stellen zusammen. Sie kann sich den sich daraus ergebenden rechtlichen Bindungen nicht dadurch entziehen, daß sie ihr Handeln stärker nach betriebswirtschaftlichen Kriterien organisiert. Auch das informationelle Selbstbestimmungsrecht des Bürgers darf durch die neue Organisations- und Handlungsform der Verwaltung nicht beeinträchtigt werden. Was dies im Zusammenhang mit einem wichtigen Projekt der Verwaltungsreform, dem Modellbezirksamt, bedeutet, haben wir im letzten Jahresbericht erläutert.[35]

Aber auch die *Rechtsstellung der Mitarbeiter* im „Unternehmen Verwaltung“ darf durch die Verwaltungsreform und den mit ihr verbundenen neuen Personalführungsstil nicht beeinträchtigt werden. Mit Problemen der Personaldatenverarbeitung vor dem Hintergrund der Verwaltungsreform hatten wir uns im vergangenen Jahr mehrfach auseinanderzusetzen.

Erhebung einer Zeit- und Mengenstatistik

Bei der Zeit- und Mengenstatistik handelt es sich um ein Instrument zur Datenerhebung für die Kosten- und Leistungsrechnung. Ziel der Zeitstatistik ist es, die Personalkosten den *„Produkten“* einer *Kostenstelle* unter Zugrundelegung von Durchschnittswerten zuzuordnen. Zweck der Mengenstatistik ist es, die Anzahl der erstellten Produkte zu erfassen. Über die Produktmengen und die durchschnittlichen Personalkosten werden die Produktstückkosten einer Kostenstelle ermittelt.

32 Jahresbericht 1993, 4.5.5
33 GVBl. 1994, 241
34 so die vom Presse- und Informationsamt des Landes Berlin herausgegebene Broschüre „Berlin Unternehmen Verwaltung – Mut zur Reform – Auf dem Weg zu einer neuen Unternehmenskultur des öffentlichen Dienstes“, S. 8
35 Jahresbericht 1994, 3.4

Laut Dienstvereinbarung zwischen der Senatsverwaltung für Inneres und dem Hauptpersonalrat soll für diese Erhebung der Zeitstatistik kein festes Verfahren vorgeschrieben werden. Entscheidend sei vielmehr, daß eine realitätsnahe Aufteilung der Stellen, z. B. des Amtes, einer Abteilung oder des Bürgermeisterbereiches, auf die Produkte geliefert wird. Die Leitung der Kostenstelle soll dabei entscheiden, ob eine Schätzung der Stellenverteilung auf Produkte durch die Leitung der Kostenstelle, eine repräsentative Zeitaufschreibung durch einige Beschäftigte der Kostenstelle oder eine separate Zeitaufschreibung durch alle Beschäftigten einer Kostenstelle durchgeführt werden soll, um verläßliche Daten für die Kostenrechnung zu ermitteln.

In der Dienstvereinbarung wurde ferner festgelegt, daß die *Erfassung von Zeiten und Mengen getrennt voneinander* und *anonym* erfolgen soll, um sicherzustellen, daß mit diesen Daten keine individuellen Leistungs- und Verhaltenskontrollen der Beschäftigten erfolgen können und keine Stellenbewertung damit verbunden ist.

Die Ausfüllanleitung der Zeitstatistik für die Beschäftigten (Anlage zur Dienstvereinbarung) sieht dabei die Eingabe der Kostenstelle, der Besoldungs-/Vergütungs-/Lohngruppe sowie des Stellenumfangs (Stammdaten) vor.

Wir haben den Bezirksverwaltungen vor Erhebung dieser Statistiken mitgeteilt, daß in kleineren Ämtern, wie z. B. dem Rechtsamt, eine separate Zeitaufschreibung durch alle Beschäftigten der Kostenstelle ausscheide, da sie wegen einer möglichen bzw. nicht auszuschließenden Deanonymisierbarkeit gegen die Dienstvereinbarung verstoßen würde. Für kleinere Verwaltungseinheiten, insbesondere mit unterschiedlichen Gehaltsgruppen, kommt daher nur die erste Alternative in Betracht, die eine Schätzung der Stellenverteilung auf Produkte durch die Leitung der Kostenstelle vorsieht. Sollte auch diese aus Praktibilitätsgründen ausscheiden, müßte die Rücksendung des Meldebelegs nicht über den Vorgesetzten, sondern direkt an die EDV-/Geschäftsstelle Berliner Verwaltungsreform des jeweiligen Bezirksamts erfolgen.

Assessment Center

Ebenfalls im Rahmen des Verwaltungsreformprozesses befaßt sich derzeit eine Arbeitsgruppe – bestehend aus Mitarbeitern aus zwei Bezirken, des Hauptpersonalrats, der ÖTV sowie des Projektbüros Price Waterhouse bei der Senatsverwaltung für Inneres – mit der Entwicklung eines Assessment Centers (Beurteilungszentrum). Hierunter wird ein *systematisches Verfahren zur Personalauswahl und -entwicklung* verstanden. Dabei beurteilen mehrere Beobachter gleichzeitig mehrere Bewerber um eine konkret ausgeschriebene Stelle.

Das Assessment Center führt eine Kombination verschiedener Übungen durch, die zukünftige Aufgaben der zu besetzenden Stellen simulieren. Das Verfahren endet mit einer gemeinsam zu treffenden Entscheidung, wer der beste Bewerber ist. Dabei ist beabsichtigt, daß die jeweilige Bezirksverwaltung durch gemeinsamen Beschluß bestimmen soll, daß das Votum des Beobachtergremiums grundsätzlich als eigene Entscheidung übernommen wird.

Zumindest in einer Übergangszeit ist geplant, daß im Beobachtergremium externe Beratungsfirmen mitarbeiten. Dies bedingt zwingend, daß Auskünfte aus der Personalakte der Bewerber diesen Dritten offenbart werden. Ein solches Verfahren verstößt gegen das Personalaktengeheimnis nach § 56 Landesbeamtengesetz (LBG).

Nach der ständigen Rechtsprechung des Bundesarbeitsgerichts und des Bundesverwaltungsgerichts in den letzten zehn Jahren genießen Personalakten sowohl im dienstlichen als auch schutzwürdigen persönlich-privaten Interesse des Beschäftigten einen besonderen Schutz, der sich auch auf den Verkehr der Behörden untereinander erstreckt. Deshalb gebietet es die Fürsorgepflicht des Dienstherrn, den Kreis der mit Personalakten befaßten Beschäftigten möglichst begrenzt zu halten und auch Teilakten, Auszüge oder einzelne Angaben nicht ohne zwingenden Grund – je nach dem Maße ihrer Schutzwürdigkeit – anderen Beschäftigten zur Kenntnis zu geben. Diese Auffassung hat sich sowohl im neuen Bundesbeamtengesetz als auch im Landesbeamtengesetz niedergeschlagen.

Nach § 56 Abs. 3 LBG dürfen danach Zugang zur Personalakte nur Beschäftigte der jeweiligen Dienstbehörde haben, die im Rahmen der Personalverwaltung mit der Bearbeitung der Personalangelegenheiten betraut sind und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Insoweit ist die vorgesehene Einsichtnahme in Personalaktendaten von Mitarbeitern der Beratungsfirmen unzulässig und obendrein auch nicht erforderlich.

Wünscht der Dienstherr ein Beobachtergremium, das sich ausschließlich aus kompetenten und sachkundigen Mitgliedern zusammensetzt, so steht es ihm frei, seine eigenen mit der Personalauswahl befaßten Mitarbeiter vorab z. B. durch geeignete Beratungsfirmen entsprechend zu schulen.

Zwar dürfen nach § 56 d Abs. 2 LBG Auskünfte an Dritte mit Einwilligung des Beschäftigten erteilt werden, jedoch setzt die Selbstbestimmung des Betroffenen eine „Entscheidungsfreiheit“ über die vorzunehmende Handlung voraus. Eine Einwilligung unter Zwang oder Täuschung widerspricht dem Selbstbestimmungsrecht. Davon geht auch die Europäische Datenschutzrichtlinie aus, nach der eine wirksame *Einwilligung „ohne Zwang“* und ohne jeden Zweifel freiwillig erteilt worden sein muß. (Art. 2 h, 7 a). Gerade im Bewerbungsverfahren hat der Bewerber jedoch *keine tatsächliche Entscheidungsfreiheit*. Vielmehr wird er, um das Ziel seiner Bemühungen nicht zu gefährden, in die Verarbeitung seiner Personalaktendaten durch Externe einwilligen.

Wir haben den Bezirken daher mitgeteilt, daß das oben ausgeführte Vorhaben gegen Datenschutzbestimmungen verstößt und daher unzulässig ist.

Teilprojekt Personalmanagement; Personalplanung

Im Rahmen eines neuen Führungs- und Steuerungssystems in der Berliner Verwaltung sind mehrere Teilprojekte gebildet worden, darunter das Teilprojekt „Personalmanagement“. Ziel dieses Teilprojekts ist die Erarbeitung eines Personalplanungs-, Führungs- und Personalentwicklungskonzepts auf der Grundlage einer Bestands- und Bedarfsanalyse.

Die Unterarbeitsgruppe „Personalplanung“ bei der Senatsverwaltung für Inneres beschäftigt sich mit den derzeitigen und zukünftigen notwendigen Möglichkeiten quantitativer und qualitativer Personalbedarfsplanung. Hierzu hat die Unterarbeitsgruppe ein Planungskonzept entwickelt, das im Hinblick auf seine Praktikabilität, Plausibilität und Generalisierbarkeit im Praxisbeispiel erprobt werden soll. Als Praxisbeispiel wurde unter anderem die Personalplanung im Amt für Kindertagesstätten in einem Bezirksamt ausgewählt.

Da für die weitere Arbeit eine konkrete Datengrundlage benötigt wurde, hatte die Arbeitsgruppe einen *Fragebogen* erarbeitet, der an alle in den Kindertagesstätten dieses Bezirks tätigen Dienstkräfte verteilt werden sollte. Die Betreuung und Auswertung vor Ort sollte dabei durch den dortigen Amtsleiter, der Mitglied der Arbeitsgruppe ist, erfolgen. Obwohl der Fragebogen ausdrücklich klarstellte, daß alle Angaben freiwillig sind, war ein Verstoß gegen das Recht der informationellen Selbstbestimmung der betroffenen Beschäftigten festzustellen.

Selbstbestimmung setzt *„Entscheidungsfreiheit“* über die vorzunehmenden oder zu unterlassenden Handlungen voraus. Der Betroffene muß, ohne einen Nachteil befürchten zu müssen, die Einwilligung auch verweigern können. Die Selbstbestimmung des Betroffenen ist daher durch entsprechende Vorkehrungen gegen Fremdbestimmung zu sichern. Aus diesem Grund konnte eine auf Freiwilligkeit basierende Umfrage nicht so erfolgen, daß die ausgefüllten Fragebögen beim Amtsleiter abgegeben und dort auch aufbewahrt werden sollten. Gleichgültig, wie der Amtsleiter selbst zu der Befragung und der Teilnahme seiner Mitarbeiterinnen und Mitarbeiter steht, entsteht eine Situation, in der die Betroffenen nicht mehr frei entscheiden können, ohne Nachteile befürchten zu müssen.

Wir haben der Senatsverwaltung für Inneres daher mitgeteilt, daß als Ort der Datenverarbeitung die Personalwirtschaftsstelle als künftige Serviceeinheit in Betracht kommt. Damit würde der gesetzlichen Vorgabe des § 56 Abs. 3 LBG Rechnung getragen werden, wonach Personalaktendaten lediglich Beschäftigten zugänglich zu machen sind, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten betraut sind. Eine dezentrale Verarbeitung dieser empfindlichen Daten sollte in jedem Fall vermieden werden.

Inhaltlich wurde der *Fragenkatalog* mit unserer Mithilfe auf das erforderliche Maß reduziert, um eine sinnvolle Personalplanung durchführen zu können.

Modellbezirksamt

Im vergangenen Jahr haben wir ausführlich die datenschutzrechtlichen Rahmenbedingungen für die Verarbeitung personenbezogener Daten im *Bürgerbüro* dargestellt.[36] In den wesentlichen Punkten bestand Einvernehmen darüber mit der Senatsverwaltung für Inneres.[37]

Im Berichtsjahr wurde uns ein mit den Bezirken erarbeiteter *Entwurf einer Dienstanweisung* vorgelegt, der allerdings diesen Anforderungen nicht entsprach. Der Zweck einer Geschäftsanweisung besteht darin, den Beschäftigten unter Berücksichtigung der Rechtslage einen schriftlichen Leitfaden als Entscheidungshilfe für ihr Verhalten in bestimmten Situationen an die Hand zu geben. Dieses Ziel erreicht der vorgelegte Entwurf nur unzureichend. Wir haben die Defizite ausführlich dargelegt und erwartet, daß die Senatsverwaltung die Einwände mit uns erörtert. Statt dessen wurde uns mitgeteilt, daß unsere Schreiben an die Bezirksämter weitergeleitet worden seien und wir weiteren Schriftwechsel direkt führen mögen, weil das Projekt „Modellbezirksamt“ mit dem Abschlußbericht an das Abgeordnetenhaus beendet sei.

Bis dahin bestand mit der Senatsverwaltung für Inneres Einvernehmen darüber, daß die Projektgruppe eine Mustergeschäftsanweisung entwirft, die von den Bezirken wegen möglicher Besonderheiten oder Abweichungen modifiziert oder angepaßt wird. Dabei sollte es nicht nur wegen der besonderen Bedeutung der Einrichtung von Bürgerbüros und der damit einhergehenden Lösungen datenschutzrechtlicher Fragen bleiben. Das Umsetzen des *Unternehmens Berlin* – wozu auch die Bürgerbüros zählen – und der Verwaltungsreform sind Ziele des Senates. Hierzu gehört auch die Schaffung einer Mustergeschäftsanweisung zum Datenschutz für Bürgerbüros.

3.7 Informationstechnische Sicherheit und Datenschutz

Informationstechnische Sicherheit zielt darauf ab, informationstechnische Systeme so zu entwerfen, herzustellen und einzusetzen, daß gegen alle Formen unerwünschter Beeinflussung der Datenverarbeitungsprozesse ein optimaler Schutz besteht. Auch alle technischen und organisatorischen Maßnahmen des Datenschutzes fallen darunter, denn diese sollen einen optimalen Schutz vor unbefugter Kenntnisnahme, Veränderung, Verarbeitung und Löschung personenbezogener Daten bei der Anwendung informationstechnischer Prozesse sicherstellen. Die Verarbeitung personenbezogener Daten ist in der öffentlichen Verwaltung die Regel. Wenn es also darum geht, informationstechnische Sicherheit in der öffentlichen Verwaltung zu erreichen, so dient dies der Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten, von Programmen, die personenbezogene Daten verarbeiten und von Systemen, auf denen diese Programme laufen, und damit dem Datenschutz.

Zur Erreichung informationstechnischer Sicherheit sind weltweit Instrumentarien entwickelt worden, die in verschiedener Weise wirken. In Deutschland hat das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) die Aufgabe, solche Instrumentarien zu entwickeln oder zu erschließen und Studien zur IT-Sicherheit in verschiedenen sensitiven Anwendungsbereichen zu erstellen. Die Ergebnisse der Arbeit des BSI werden regelmäßig veröffentlicht und für die öffentliche Verwaltung nutzbar gemacht.

Zu den wichtigsten Instrumenten gehören *gestufte IT-Sicherheitskriterien*, an denen die Sicherheit informationstechnischer Produkte evaluiert werden kann, so daß eine Zertifizierung von Produkten anhand der erreichten Sicherheitsstufen möglich ist. Das bekannteste Kriterienwerk ist das *Orange Book* des amerikanischen Verteidigungsministeriums.[38] Nach einer kurzen Phase der Anwendung eigener deutscher IT-Sicherheitskriterien[39] erfolgt nunmehr die Evaluierung in Deutschland nach den in der Europäischen Union harmonisierten *Information Technology Security Evaluation Criteria (ITSEC)* (Version 1.2, 1991).

Das auf dieser Basis erarbeitete *IT-Sicherheitshandbuch* des BSI[40] dient der Erarbeitung von IT-Sicherheitskonzepten auf der Grundlage differenzierter Bedrohungs- und Risikoanalysen.[41] Nicht nur unsere kritischen Äußerungen zum häufig unangemessenen methodischen Aufwand bei der Verwendung des IT-Sicherheitshandbuchs haben das BSI bewogen, mit dem *IT-Grundschutzhandbuch*[42] eine einfachere Methode zu entwickeln. Es zeigt sich, daß gerade im Zusammenwirken beider Handbücher eine in Aufwand und Ertrag optimale Methode zur Erarbeitung von IT-Sicherheitskonzepten gesehen werden kann.

IT-Sicherheits-Zertifizierung

Weil es bei der Beratung zu technischen Datenschutzfragen, insbesondere im Zusammenhang mit der Projektierung von IT-Anwendungen, häufig darum geht, Standardprodukte, die in größeren Stückzahlen regional, national oder sogar weltweit verbreitet werden, nach einheitlichen Kriterien zu bewerten und zu vergleichen, besteht ein Bedarf nach amtlichen und damit interessenungebundenen und allgemein anerkannten *Zertifikaten für die IT-Sicherheit.*

Ihre Bedeutung für den Datenschutz relativiert sich allerdings, wenn man überlegt, welche Einflußsphären auf die Sicherheit von konkreten IT-Anwendungen tatsächlich einwirken:

- die informationstechnische Sicherheit der eingesetzten Hard- und Softwareprodukte, d.h. die Eigenschaften der Systeme, sich verläßlich zu verhalten, gegen unabsichtliche und absichtliche Angriffe auf die IT-Sicherheit resistent zu sein, sie erkennen, abwehren und nachvollziehbar machen zu können *(technische Sicherheit);*
- die sorgfältige und an der IT-Sicherheit orientierte Nutzung der zur der Sicherheit dienenden Leistungsmerkmale und Systemkomponenten *(Anwendungssicherheit);*
- die an Sicherheit und Datenschutz orientierte Gestaltung der Informations- und Datenflüsse in einer Organisation *(organisatorische Sicherheit);*
- die Fähigkeit und Bereitschaft der beteiligten Personen, im Sinne der informationstechnischen Sicherheit zu handeln *(personelle Sicherheit).*

Nach unseren Prüferfahrungen steigt die Bedeutung dieser Einflußsphären für die erzielte Sicherheit in der Reihenfolge der hier gewählten Darstellung. Nicht umsonst weisen alle uns bisher in der Berliner Verwaltung bekanntgewordenen IT-Sicherheitsuntersuchungen unter Verwendung des IT-Sicherheitshandbuches nicht hinnehmbare Restrisiken im personellen Bereich auf. Daß dies ein Spezifikum der öffentlichen Verwaltung ist, kann bezweifelt werden.

Obwohl der Bereich, der einer Zertifizierung unterliegen kann, begrenzt ist, werden die Zertifikate aber nicht unbedeutend, denn gerade die Sicherheit der eingesetzten Hard- und Softwareprodukte ist am allerwenigsten von den Anwendern beeinflußbar und beurteilbar. Anhaltspunkte für die Auswahl sicherer Systeme sind daher für Anwender und Berater von großer Bedeutung. Wenn man auf amtliche Zertifikate unbesehen zurückgreifen

36 Jahresbericht 1994, 3.4
37 Stellungnahme des Senats, Drs. 12/5784

38 US-Department of Defense: Trusted Computer Systems Evaluation Criteria, DOD 5200.28-STD
39 Zentralstelle für die Sicherheit in der Informationstechnik: IT-Sicherheitskriterien i. d. F. v. 11. Januar 1989, Bonn 1989
40 Bundesamt für Sicherheit in der Informationstechnik: IT-Sicherheitshandbuch. Handbuch für die sichere Anwendung der Informationstechnik. Bonn 1992
41 Jahresbericht 1991, 1.2, Jahresbericht 1992, 2.2
42 Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch. Maßnahmeempfehlungen für den mittleren Schutzbedarf. Schriftenreihe zur IT-Sicherheit. Band 3. Ingelheim 1995

kann, kann man aufgrund der jeweiligen Bedrohungssituationen zu klaren Aussagen kommen und sich auf Empfehlungen konzentrieren, die die Anwendungssicherheit sowie die organisatorische und personelle Sicherheit betreffen.

Anzustreben wäre, auf der Grundlage einer fundierten *Bedrohungs- und Risikoanalyse* mit der zu beratenden Stelle einen Konsens über die notwendigen Sicherheitsstufen nach dem Orange-Book oder ITSEC zu erzielen, so daß entsprechende Forderungen im Pflichtenheft formuliert werden können, um sich anschließend auf das zu konzentrieren, was in der Organisation von innen heraus für die informationstechnischen Sicherheit getan werden muß.

Leider ist dies kaum möglich, denn es gibt zu wenige zertifizierte Produkte. Häufig entsprechen diese nicht mehr dem neuesten Stand der Technik, weil spätere Versionen auf dem Markt sind, die nicht oder noch nicht zertifiziert worden sind. Es sollten daher Wege gefunden werden, die Zertifizierungsverfahren zu beschleunigen, billiger zu machen und damit abzuspecken. Zivile Anwendungen haben andere Anforderungen als solche, die geheimdienstlichen Ansprüchen genügen müssen, stellen aber sicher mehr als 95 % aller sicherheitsbedürftigen Anwendungen. Die heute verwendeten IT-Sicherheitskriterien umfassen jedoch ein Spektrum, das für zivile Anwendungen nur im unteren Drittel erschlossen ist. Soweit die Sicherheitsstufen hierfür relevant sind, besteht daher auch das Bedürfnis, eine stärkere Differenzierung zu finden. Dazu wäre eine neue Erfassung ziviler Anforderungen geboten, die nach unserer Auffassung auf der Grundlage anderer Bedrohungs- und Risikolagen definiert werden sollten. In der Regel brauchen wir dort keinen Schutz vor ausgeklügelten, von langer Hand vorbereiteten kriminellen oder geheimdienstlichen Angriffen, sondern Schutz vor den Folgen menschlicher Fehler oder organisatorischer Pannen.

Nur dann, wenn das Sicherheitszertifikat die aktuell zu beschaffende Hard- oder Software betrifft, wenn es den Herstellern zumutbar ist, solche Zertifikate beizubringen und für die anwendenden Organisationen nachvollziehbar ist, daß das Zertifikat etwas zusichert, für das sie selbst einen Bedarf sehen, dann kann es in diesem Bereich, in dem die eigentliche Masse der Systeme abgesetzt wird, zum Verkaufsargument werden. Erst dann kann die Empfehlung ausgesprochen werden, bei den Ausschreibungen Zertifikate bestimmter Sicherheitsstufen als Ausschlußkriterium zu fordern.

IT-Sicherheitshandbuch und IT-Grundschutzhandbuch

Das *IT-Sicherheitshandbuch* beschreibt ein Verfahren zur Gewährleistung der IT-Sicherheit. Dabei kann es sich um Rechenzentren, spezielle Anwendungen mit ihren Anwendungsumgebungen, um Netze beliebiger Ausdehnung, um IT-Anwender insgesamt oder auch nur um Teile davon handeln.

Die Erstellung eines IT-Sicherheitskonzepts durchläuft vier Phasen, wobei Rückkopplungen zwischen Phasen durchaus beabsichtigt, ja sogar zu empfehlen sind:

- Zunächst ist die *Schutzbedürftigkeit zu ermitteln*, in dem die IT-Anwendungen und zu verarbeitenden Informationen erfaßt und hinsichtlich ihrer Schutzbedürftigkeit bewertet werden. Jeder erfaßten IT-Anwendung und Information werden Werte für den Schaden zugeordnet, der entsteht, wenn sich Bedrohungen der Vertraulichkeit, Integrität und Verfügbarkeit realisieren.
- Danach werden in einer *Bedrohungsanalyse* bedrohte Objekte differenziert erfaßt. Schwachstellen und Schutzmaßnahmen werden beschrieben und die relevanten Bedrohungen aufgelistet und den Grundbedrohungen zugeordnet.
- Es erfolgt eine *Risikoanalyse*, bei der eine Bewertung der bedrohten Objekte, von denen die Durchführung der IT-Anwendungen und die Verarbeitung der Informationen abhängt, vorgenommen wird. Den Bedrohungen der Objekte werden Schadenswerte zugeordnet. Die Häufigkeit, mit der ein Schaden eintritt, wird in einer Skala abgeschätzt, so daß schließlich eine Übersicht von Bedrohungen und Objekten einerseits sowie Schadens- und Häufigkeitswerten andererseits entsteht. Festzulegen ist, welche Schadenshöhe bei welchem Häufigkeitswert als tragbar oder untragbar anzusehen sind. Dann kann mit einer Entscheidungstabelle festgestellt werden, wo durch zusätzliche Maßnahmen die Risiken einzudämmen sind.
- In der letzten Phase ist das *IT-Sicherheitskonzept* zu erstellen. Maßnahmen zur Reduzierung der Risiken werden ausgewählt und hinsichtlich ihrer Wirkung auf Schadenshöhe und Häufigkeitswert bewertet. Es werden Kosten-Nutzen-Betrachtungen angestellt und die Angemessenheit von Maßnahmen auch aus dieser Sicht geprüft. Gegebenenfalls sind alternative Maßnahmen auszuwählen. Das Ergebnis der Auswahl der Maßnahmen wird dann einer Restrisikoanalyse unterzogen, um festzustellen, ob die vorher als untragbar erkannten Risiken durch die Maßnahmen auf ein akzeptables Maß reduziert werden können. Unter Umständen wären weitere oder verschärfende Maßnahmen zu treffen.

Am Ende des Prozesses darf es keine untragbaren Risiken mehr geben.

Der Prozeß enthält viele Schritte, bei denen subjektive Betrachtungen eine Rolle spielen, so bei der Definition von Bewertungsskalen, der Festlegung von Entscheidungstabellen und bei der Bewertung selbst. Um hier der Gefahr vorzubeugen, daß einseitige Ausrichtungen der Meinungsbildung, z. B. die Überbetonung wirtschaftlicher Restriktionen oder ein übertriebenes Sicherheitsbedürfnis das Ergebnis verfälschen, wird zu den einzelnen Schritten ausdrücklich festgelegt, wer sich an diesen Betrachtungen zu beteiligen hat.

Erste Erfahrungen in der Berliner Verwaltung haben gezeigt, daß es ratsam ist, die Meinung von neutralen Sicherheitsexperten nicht zu vernachlässigen, da sonst der „Rotstift“ beim Sicherheitskonzept regiert, vornehmlich dann, wenn er bei den übrigen Investitionen nicht wirksam genug eingesetzt wurde.

Das IT-Sicherheitshandbuch ist in der Berliner Verwaltung bisher im Rahmen von Großprojekten wie MAN, ISDN-Vernetzung oder AHW eingesetzt worden. In allen Fällen wurden die Untersuchungen von Beratungsfirmen durchgeführt. Diese Anwendungen haben zu wesentlich mehr Klarheit über die Risiken, Schwachstellen und Maßnahmenschwerpunkte geführt und wegen des methodischen Vorgehens auch das Vertrauen gestärkt, daß die Erkenntnisse als einigermaßen lückenlos angesehen werden können. Entscheidend ist jedoch in allen Fällen, daß die von neutraler Stelle empfohlenen Maßnahmen auch umgesetzt werden. Vorschläge für Sicherheitskonzepte von spezialisierten Unternehmen stehen noch nicht für sichere Systeme und Anwendungen!

Der große zeitliche und fachliche Aufwand bei der Anwendung des IT-Sicherheitshandbuches macht seinen Einsatz nur dort sinnvoll, wo es schon von der Bedeutung und Größe eines Projektes her angemessen erscheint. Wenn Millionenbeträge in neue Systeme und Verfahren investiert werden, von deren Sicherheit die Funktionsfähigkeit ganzer Verwaltungszweige abhängt und die informationelle Selbstbestimmung der Bürger gravierend tangiert wird, darf an einer systematischen Erarbeitung und Umsetzung von IT-Sicherheitskonzepten nicht gespart werden.

Andererseits ist zu akzeptieren, daß eine konsequente Anwendung des IT-Sicherheitshandbuchs für das Gros der Systeme und Verfahren die Verwaltung überfordern würde. Diese Kritik am IT-Sicherheitshandbuch wurde von der Fachwelt bald nach seiner Veröffentlichung erhoben. Einige Beratungsunternehmen entwickelten vereinfachte Analyseverfahren. Aber auch das BSI nahm die Kritik auf und entwickelte mit dem *IT-Grundschutzhandbuch* eine Alternative mit einem vereinfachten Verfahren für den sogenannten mittleren Schutzbedarf.

Das IT-Grundschutzhandbuch verzichtet auf aufwendige Risikoanalysen und auf differenzierte Fallunterscheidungen bei den Systemkonfigurationen. Auf der Grundlage überschlägiger Risikobetrachtungen werden Maßnahmenbündel für typische Systemkonfigurationen, Umfeld- und Organisationsbedingungen

vorgeschlagen. Derzeit erfaßt das IT-Grundschutzhandbuch den IT-Grundschutz übergeordneter Komponenten wie Organisation, Personal, Notfallvorsorge und Datensicherung, der Infrastruktur wie Gebäude, Verkabelung Büro- und Funktionsräume, von nichtvernetzten Systemen (DOS-PCs, UNIX-Mehrplatzsysteme, tragbare Systeme), von vernetzten Systemen (servergestützte PC-Netze, vernetzte UNIX-Systeme), von Datenübertragungseinrichtungen (Datenträgeraustausch, Modems), von Telekommunikationsystemen (digitale TK-Anlage, Telefax, Anrufbeantworter). Die IT-Grundschutzhandbuch ist auf die Erweiterung um weitere Standardkonfigurationen ausgelegt.

Für diese verschiedenen Gegenstandsbereiche bietet das IT-Grundschutzhandbuch Maßnahmen- und Gefährdungskataloge an und stellt Gefährdungen und Maßnahmen in tabellarische Beziehungen. Diese Kataloge stellen auch außerhalb der Anwendung des Handbuches eine lehrreiche Lektüre für alle dar, die Anregungen dafür benötigen, was in Standardkonfigurationen und -situationen an Unvorhergesehenem passieren und was man dagegen tun kann.

Aus Sicht des technisch-organisatorischen Datenschutzes ist allerdings zu betonen, daß

- der IT-Grundschutz Grenzen unterliegt und nicht für IT-Systeme ausreichend ist, die eines hohen Schutzes bedürfen,
- das einmalige Erstellen eines IT-Sicherheitskonzeptes nicht ausreicht, sondern einem ständigen Regelkreislauf aus Konzeption, Realisierung und Kontrolle der Maßnahmen unterliegen muß. Dies sicherzustellen ist eine Leitungsaufgabe.

Allerdings vereinfacht das IT-Grundschutzhandbuch auch den IT-Sicherheitsprozeß bei hochschutzbedürftigen Systemen und Anwendungen. Wenn die bedrohten Objekte nach dem IT-Sicherheitshandbuch bestimmt worden sind, kann geprüft werden, welche Objekte besondere Gefährdungen für das hochschutzbedürftige System aufweisen und daher der differenzierten Analyse nach dem IT-Sicherheitshandbuch bedürfen und für welche Objekte die pauschalen Betrachtungen des IT-Grundschutzhandbuchs ausreichend sind. Auch dort, wo die Maßnahmenempfehlungen nicht ausreichend sind, können sie zumindest zur Grundlage weitergehender Maßnahmen gemacht werden *(Hochschutz = Grundschutz + X)*.

Nachdem mit dem zumindest vorläufigen Scheitern des Projektes BROSiA[43] berlinweit *verbindliche Rahmensetzungen* für die Sicherstellung der informationstechnischen Sicherheit trotz der gewaltigen Anstrengungen zur Informatisierung der Berliner Verwaltung nicht zu erhoffen sind, begrüßen wir, daß die Senatsverwaltung für Inneres die Verwendung des IT-Grundschutzhandbuchs in einem Rundschreiben der Verwaltung unter den vom BSI vorgeschlagenen Einschränkungen empfiehlt.

4. Telekommunikation und Medien

4.1 Vernetzung der Gesellschaft

Verkehrsregeln auf der Datenautobahn

1995 ist als das Jahr der Netze bezeichnet worden. Tatsächlich schreitet die Vernetzung der Datenverarbeitung massiv voran. Im vergangenen Jahr hatten wir über die *Vernetzung im öffentlichen Bereich* und die rapide Zunahme von Online-Zugriffen durch Behörden berichtet.[44] Die Vernetzung der Datenverarbeitung im privaten Bereich ist demgegenüber noch weiter vorangeschritten. Zudem verwischen sich die Grenzen zwischen öffentlichem und privatem Bereich zunehmend.

Der Aufbau von Datennetzen, die gerne mit Datenautobahnen verglichen werden, ist auf vier Ebenen unterschiedlich weit gediehen:

In verschiedenen deutschen Großstädten, darunter auch in Berlin, werden gegenwärtig *digitale Stadtautobahnen* gebaut. Berlin gehört mit dem MAN als Träger des Verwaltungsnetzes dazu.[45] Diese Netze sollen zumindest teilweise in *privater Rechtsform* als Transportmedium für Unternehmen und Behörden angeboten werden. So ist in Berlin die Gründung einer privaten *BerlinNet GmbH* in Vorbereitung, die Trägerin eines vorhandenen Glasfasernetzes werden soll, das bereits jetzt den Datenverkehr innerhalb der Bankgesellschaft Berlin abwickelt. Dieses Unternehmen soll dem Land Berlin als Konkurrent zur Telekom zusätzliche Einnahmen verschaffen, indem es als Dienstleister für in Berlin ansässige Großunternehmen (Siemens, Schering) tätig wird. Diese Entwicklung wird beschleunigt zum einen durch den Umstand, daß sich dieses Glasfasernetz schon bisher im Eigentum des Landes Berlin und nicht der Telekom befand, zum anderen dadurch, daß die Liberalisierung des Telekommunikationsmarkts und damit das Ende des Monopols der Telekom bei den Datendiensten bereits jetzt beginnt, während der Sprachtelefondienst noch bis Ende 1997 allein der Telekom vorbehalten bleibt.

Bundesweit bieten dementsprechend bereits sogenannte private Unternehmensnetze *(Corporate Networks)* ihre Dienste als Datentransporteur für jeden an. Diese privaten Datenautobahnen werden ebenfalls in erster Linie von großen Anwendern (Unternehmen) genutzt, die auf diese Weise kostengünstiger kommunizieren können, als wenn sie die Dienste des ehemaligen Monopolisten Telekom in Anspruch nehmen würden. Die von der Telekom selbst betriebene *bundesweite digitale Datenautobahn* ist das *ISDN-Netz*, das bis Ende 1997 flächendeckend ausgebaut sein soll. Das ISDN-Netz wird zugleich mit den digitalen Datennetzen der europäischen Nachbarländer zu einem transeuropäischen Netz, also einer europäischen Datenautobahn weiterentwickelt.

Diese zunehmende Vernetzung auf lokaler, nationaler und europäischer Ebene ist im vergangenen Jahr jedoch weit in den Schatten gestellt worden von dem fast atemberaubenden Wachstum einer *globalen Informations-Infrastruktur* in Gestalt des *Internet*.[46]

Diese weltweite Datenautobahn, die auch im Land ihres Ursprungs, den Vereinigten Staaten, häufig als *„Infobahn“* oder *„Information Superhighway“* bezeichnet wird, zwingt dazu, die Frage nach den Verkehrsregeln auf derartigen Datenautobahnen völlig neu zu stellen. Die Datenautobahnen auf kommunaler, Landes- und Bundesebene unterliegen immerhin noch Verkehrsregeln, die ein Mindestmaß an Datenschutz gewährleisten sollen.[47]

Dagegen ändert sich die Situation beim grenzüberschreitenden Datenverkehr schlagartig. Die Europäische Datenschutzrichtlinie enthält zwar erstmals detaillierte Regelungen über den Datenverkehr innerhalb der Europäischen Union und über den Datenexport in Drittländer. Die Bundesrepublik wie auch die anderen Mitgliedstaaten der Europäischen Union sind verpflichtet, ihr innerstaatliches Recht innerhalb von drei Jahren an diese Richtlinie anzupassen.[48]

Spezielle Verkehrsregeln und Leitplanken für die europäische Telekommunikation fehlen demgegenüber, da die *ISDN-Richtlinie* der Europäischen Gemeinschaft noch immer nicht verabschiedet ist.[49]

Die Frage, ob auf der weltweiten Datenautobahn, im Internet, überhaupt Verkehrsregeln gelten sollen, wenn ja, welche und insbesondere wie diese durchgesetzt werden sollen, ist bisher nicht befriedigend gelöst.

Die Presse berichtete vor kurzem über die Absicht eines katholischen Geistlichen in Wien, im Internet eine Art *elektronischen Beichtstuhl* zu installieren, also weltweit die Möglichkeit zu eröffnen, mit Hilfe der elektronischen Post gegenüber diesem unsichtbaren Ansprechpartner die Beichte abzulegen. Zwar rechnet der findige Pater offenbar damit, daß der Vatikan ihm dieses Vorhaben alsbald untersagen wird; zugleich sieht er einen wesentlichen Vorteil in seinem Angebot gerade darin, daß die Person, die die Beichte ablegen will, dies in der „elektronischen Anonymität“ des Netzes tun kann und dem Geistlichen nicht persönlich gegenübertreten muß.

43 vgl. 2.2
44 Jahresbericht 1994, 3.2
45 vgl. 2.2
46 Jahresbericht 1994, 2.1
47 zur Neufassung des Telekommunikationsrechts im einzelnen unten 4.3
48 vgl. dazu im einzelnen 1.1
49 vgl. dazu unten 4.4

Schon jetzt erlaubt das Internet im Bereich der *Telemedizin*, Ferndiagnosen durch ausländische Spezialisten einzuholen oder diese sogar bei Teleoperationen über tausende von Kilometern hinweg mitwirken zu lassen. Der betroffene Patient liegt nicht mehr, wie zu Zeiten Rudolf Virchows, in einem Operationssaal, in dem eine begrenzte Zahl von Medizinstudenten dem Operateur zusehen können. Der Eingriff in seinen Körper ist vielmehr weltweit im Netz zu verfolgen.

Das *Beichtgeheimnis* wie auch die *ärztliche Schweigepflicht* gehören zu den ältesten Verschwiegenheitspflichten (Berufsgeheimnissen), die die Rechtsordnung kennt. Demgegenüber ist das Grundrecht auf informationelle Selbstbestimmung in der deutschen Verfassungsordnung vergleichsweise jungen Datums. In seinem Urteil zur Volkszählung hat das Bundesverfassungsgericht 1983 formuliert:

„Mit dem Recht auf informationelle Selbstbestimmung wären 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. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten“.[50]

Diese Sätze erhalten im Zeitalter des Internet einen ganz neuen Klang. Das Internet ist nämlich auch ein wichtiges *politisches Instrument der Kommunikation.* Es wird beispielsweise benutzt von britischen Bürgerrechtlern, die sich für eine geschriebene Verfassung in ihrem Lande einsetzen. Die mexikanischen Zapatisten nutzen es ebenso für ihre Zwecke wie chinesische Oppositionelle, die Informationen aus dem Ausland abrufen und elektronische Mitteilungen verschicken. Nicht umsonst versucht die chinesische Regierung gegenwärtig, den Zugang zum Internet in ihrem Land strikt zu kontrollieren.

Damit stellt sich die Frage, ob das *Menschenrecht auf informationelle Selbstbestimmung,* das den Einzelnen gerade auch vor der Registrierung von Verhaltensprofilen schützen soll, auf der globalen Datenautobahn überhaupt noch eine Chance hat. Es scheint, als könne man diese Frage guten Gewissens aus folgenden Gründen nur verneinen:

1. Eine *unbeobachtete Kommunikation* ist jedenfalls im Internet nicht möglich. Alles was unverschlüsselt über das Netz geht, seien es Netzadressen, Paßwörter oder Kreditkartennummern, kann von Dritten gelesen, gespeichert und natürlich auch für betrügerische Zwecke verwendet werden.

   Selbst wenn aber Techniken der *Ende-zu-Ende-Verschlüsselung* eingesetzt werden, kann gleichwohl der Datenverkehr zwischen verschiedenen Nutzern registriert werden. In den USA stehen Rechner, die ausschießlich dieses tun, die also Nutzerprofile jedes einzelnen „Netsurfers“ erstellen können, falls dies aus irgendwelchen Gründen interesssant erscheinen sollte. Und es wird in dem Maße interessanter, wie kommerzielle Unternehmen das Internet nutzen, die ihre Werbung und Angebote gewissermaßen am Rande der Datenautobahn postieren und die sich für das Nutzungsverhalten Einzelner interessieren, um diese wiederum gezielt mit elektronischer oder konventioneller Werbung einzudecken.

   Wohlgemerkt: den Inhalt der Kommunikation kann der einzelne Netzbürger („Netizen“) durch den Einsatz von Verschlüsselungs-Software schützen, die er bisher aus dem Netz auf seinen Rechner herunterladen kann. Damit wird aber noch nicht seine Adresse geheimgehalten, von der aus er Nachrichten absendet oder Informationen abfragt. Die einzige Möglichkeit, dies zu erreichen, ist die Benutzung von Pseudonymen oder Namen real existierender dritter Personen, hinter denen man sich verstecken kann. Dies wirft aber neue Probleme für den Schutz der Persönlichkeitsrechte des Dritten auf, der regelmäßig gar nicht weiß, daß und für welche Zwecke sein Name verwendet wird. Dazu muß man wissen, daß die benutzerfreundliche Software des *World-WideWeb (WWW-„weltweites Netz“)* mit Hilfe von Querverweisen (links) in Sekundenschnelle den Zugriff auf beliebige andere Datenbestände im globalen Netz ermöglicht. Damit können Dritte die Informationen, die ein Betroffener in das Netz eingestellt hat, in einen neuen – möglicherweise negativen – Zusammenhang bringen oder auch inhaltlich verändern. Wer etwa seine elektronische Visitenkarte im Internet (die sogenannte home page) mit einem Foto versieht, muß damit rechnen, daß dieses Foto von anderen Nutzern kopiert und verfremdet wird, was im Zeitalter von Multimedia kein Problem darstellt. Bekannt geworden ist auch der drastische Fall eines Teilnehmers an einem virtuellen Spiel im Netz, der die Identität eines anderen Mitspielers ohne dessen Wissen annahm und als solcher die Figur einer Mitspielerin vergewaltigte. Diese *Vergewaltigung im Cyberspace* hat in den USA dazu beigetragen, daß im Kongreß Vorschläge für gesetzliche Regelungen zur Unterbindung solcher Praktiken im Internet gemacht worden sind, die inzwischen – zumindest teilweise – auch Gesetzeskraft erlangt haben.
2. Wer also seine eigenen personenbezogenen Daten in das Internet einstellt, muß wissen, daß er sich auf einen globalen elektronischen Marktplatz begibt. Er veröffentlicht seine Daten nicht nur weltweit (und schon das ist qualitativ etwas anderes als ein Abdruck im örtlichen Anzeigenblatt oder einer überregionalen Tageszeitung), sondern er stellt sie auch für beliebige Verknüpfungen und vielfältige Manipulationen durch die Millionen von Netz-Teilnehmern zur Verfügung. Auch die Adressierung einer elektronischen Nachricht kann von Dritten unbemerkt verändert und das Datenpaket damit umgeleitet werden. Das sollte gerade auch derjenige berücksichtigen, der von dem eingangs erwähnten Angebot eines elektronischen Beichtstuhls Gebrauch machen will. Schon im Mittelalter stand auf dem Marktplatz auch der *Pranger.* Auf dem elektronischen Marktplatz der Neuzeit ist dies nicht anders. Der einzige Unterschied besteht darin, daß man heutzutage auf diese Weise weltweit in seiner Menschenwürde verletzt werden kann.
3. Das Hauptproblem auf der weltweiten Datenautobahn, dem Internet, ist das Fehlen einer zentralen verantwortlichen Instanz, also einer globalen *„Autobahnmeisterei“*. In seinen Anfängen war der Vorläufer des Internet vom amerikanischen Verteidigungsministerium gerade deshalb dezentral organisiert worden, um es gegen Angriffe auf einzelne Netzknoten unempfindlich zu machen. Daraus hat sich ein weitgehend unreguliertes (anarchisches) Netz zum Austausch von Informationen zunächst zwischen Wissenschaftlern und heute zwischen Millionen privater PC-Nutzer und zunehmend auch kommerziellen Unternehmen entwickelt. Das Fehlen einer zentralen verantwortlichen Instanz im Internet, das zunächst gerade ein Element der Sicherheit war und heute auch noch ist, schließt gleichzeitig die Kontrolle und Regulierung des Netzes „von oben“ und damit auch die einheitliche Durchsetzung eines weltweiten Datenschutzstandards aus.

Ob die Schaffung einer solchen zentralen Kontrollinstanz und die Entwicklung international verbindlicher rechtlicher Regelungen, also Leitplanken für die globale Datenautobahn, realistisch oder auch nur wünschenswert ist, wird sehr kontrovers diskutiert. Jedenfalls ist damit kurzfristig nicht zu rechnen. Unter den gegenwärtigen Bedingungen bedeutet das aber noch nicht, daß der *Zugang zum Internet* (die Auffahrt auf die Datenautobahn) z. B. für Berliner Behörden ohne weiteres möglich ist. Sie müssen vielmehr die Regelungen des Berliner Datenschutzgesetzes auch bei den Nutzungen dieses Netzes beachten, insbesondere müssen sie Vorkehrungen gegen die erheblichen Gefährdungen der Datensicherheit treffen.[51]

Allerdings muß das deutsche Datenschutzrecht möglicherweise in einem wichtigen Punkt angesichts der wachsenden Bedeutung der globalen Datenautobahnen geändert werden. Das Bundesdatenschutzgesetz regelt bisher nur die Datenverarbei-

50 BVerfGE 65, 1, 43

51 vgl. S. 22 f.

tung durch Bundesbehörden und durch private Unternehmen und Einzelpersonen, soweit sie geschäftsmäßig für berufliche oder gewerbliche Zwecke stattfindet. Dagegen unterliegt die *Datenverarbeitung Privater für persönliche Zwecke* keinen datenschutzrechtlichen Vorschriften. Da jeder PC-Benutzer mit Hilfe eines Modems personenbezogene Daten Dritter in die globalen Netze einspeisen kann, ist zu prüfen, ob er jedenfalls insoweit als „Verantwortlicher für die Datenverarbeitung" auch dann datenschutzrechtlichen Pflichten unterliegen sollte, wenn er die Datenautobahn für private Zwecke nutzt.

An diesem Beispiel wird deutlich, daß die Veränderungen in der Informationsgesellschaft weg von zentralen Datenbanken in öffentlicher oder privater Hand hin zu Millionen von Netzbewohnern, von denen jeder in die Persönlichkeitsrechte anderer eingreifen kann, grundlegende Änderungen in der Struktur des Datenschutzrechts notwendig machen.

Nur ein Bruchteil der Verkehrsteilnehmer auf der Datenautobahn unterliegt bisher ausreichenden datenschutzrechtlichen Regeln. Die *Leitplanken auf dem globalen Highway* reichen bei weitem noch nicht aus.

Um eins klarzustellen: Es geht nicht um Zensur des Netzverkehrs. Der Fall des Internet-Anbieters *CompuServe,* der auf Druck der Münchner Staatsanwaltschaft den Zugang zu bestimmten Newsgroups (schwarzen Brettern) im Internet gesperrt hat, weil dort Kinderpornographie angeboten wird, zeigt deutlich, daß die Versuche nationaler Strafverfolgungsbehörden, die Inhalte des Internets zu kontrollieren, untauglich sind. Zu Recht hat der Bundesminister für Bildung, Wissenschaft, Forschung und Technologie es als wenig erfolgversprechend bezeichnet, den einzelnen Anbieter für das verantwortlich zu machen, was im Internet stattfindet. Die Anbieter haben keine Möglichkeit, die Angebotsinhalte weltweit zu kontrollieren. Selbst wenn sie den Zugang sperren, kann jeder Nutzer – wenn auch mit höherem Aufwand – eine andere Auffahrt nehmen, um zu dem inkriminierten Angebot zu gelangen. Dasselbe gilt für laufende Ermittlungsverfahren gegen andere Internet-Provider in Deutschland, gegen die wegen der Verbreitung nationalsozialistischer Propaganda ermittelt wird, weil im globalen Netz auch Rechtsradikale ihre Parolen streuen.

Der Datenschutz steht in der Diskussion um das Internet vor einem prinzipiellen Dilemma: Einerseits muß es ihm darum gehen, dem Einzelnen wie bei allen anderen begrenzteren Netzen die anonyme Nutzung dieses immer wichtiger werdenden Mediums zu ermöglichen. Andererseits muß es gerade auch aus Sicht des Datenschutzes Grenzen dafür geben, wie mit personenbezogenen Daten auf der Datenautobahn umgegangen werden darf. Eine Lösung dieses Dilemmas steht noch aus. Sie muß auf verschiedenen Ebenen gesucht werden:

- Jeder Nutzer, der sich ins Internet begeben will, muß unmißverständlich über die Risiken dieses weltweiten Netzes aufgeklärt werden. Er muß wissen, daß er sich in eine *„Wildnis"* begibt, in der es neben vielfältigen Informationen und Chancen eben auch „Löwen und Giftschlangen" gibt.[52]
- Die *nationalen Rechtsordnungen* einschließlich der Regelungen für Fälle mit Auslandsberührung sollten angesichts des Internet ihren Geltungsanspruch nicht von vornherein aufgeben, sondern auf die Einhaltung der Bedingungen dringen, die sie für die Auffahrt auf den Information Superhighway für öffentliche und private Stellen vorsehen.
- Die *technischen Bedingungen* der Nutzung des Internet müssen datenschutzgerecht sein. Sie müssen sowohl die Identität des einzelnen Nutzers jedenfalls so lange effektiv schützen, wie er nicht in Rechte Dritter eingreift. Auch müssen nicht überwindbare Verschlüsselungsverfahren verfügbar bleiben.
- Für den Umgang im Internet selbst hat sich in der weltweiten „Netzgemeinde" bereits ein Verfahren der *Selbstregulierung* entwickelt, das unterhalb rechtlicher Regeln zum Entstehen einer Netzethik *(Netiquette)* führen könnte. Auch dieser Prozeß sollte für den Persönlichkeitsschutz nutzbar gemacht und unterstützt werden.

52 so der anschauliche Vergleich von Dr. Waltraut Kotschy, Österreichische Datenschutzkommission

Öffnung zum Internet – Gefahren für die öffentliche Verwaltung?

Auch Behörden haben zunehmend den Wunsch nach einem Zugang zu globalen Datennetzen, insbesondere dem Internet. Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe erarbeitet, die den für den Betrieb von Netzen der öffentlichen Verwaltung Verantwortlichen deutlich machen soll, mit welchen Risiken für die Sicherheit der Verwaltungsnetze bei einem Anschluß an das Internet zu rechnen ist und wie diese begrenzt werden können.

Der Anschluß an das Internet ist nur vertretbar, wenn zuvor eingehende Analysen und Bewertungen erfolgt sind und die Gefahren durch technische und organisatorische Maßnahmen beherrscht werden können. Eine hundertprozentige Sicherheit gegen Angriffe aus dem Internet kann jedoch auch bei Beachtung sämtlicher Maßnahmen nicht erzielt werden, da ständig neue unerwartete Sicherheitsprobleme entdeckt werden. Die Problematik ist mit der der Virensuchprogramme vergleichbar. Es können im Normalfall nur bekannte Sicherheitsprobleme beachtet werden, zukünftige Probleme müssen umgehend nach Bekanntwerden durch geeignete Maßnahmen behoben werden.

Die *Sicherheitsrisiken im Internet* lassen sich grob in zwei Kategorien einteilen.

Zum einen hat jeder im Internet zur Verfügung stehende Dienst, wie z. B. Electronic Mail oder das WorldWideWeb (WWW), eigene dienstespezifische Sicherheitsrisiken; zum anderen beinhaltet die Nutzung der Kommunikationsprotokolle TCP/IP (Transmission Control Protocol/Internet Protocol) unabhängig vom genutzten Internet-Dienst bestimmte Risiken.

So werden bei den üblichen Diensten die *Nutzerkennung* und das *Paßwort* unverschlüsselt im Klartext übertragen. Mit Programmen, die unter dem Namen *„Packet Sniffer"* bekannt sind, kann der Datenverkehr im Netz bzw. auf den Netzknoten belauscht und nach interessanten Informationen durchsucht werden. Dadurch können diese Abhörprogramme zahlreiche Nutzerkennungen mit den dazugehörigen Paßworten ausspähen, mit deren Hilfe sich ein Angreifer einen unberechtigten Zugriff auf andere Rechner verschaffen kann. Datenpakete können jedoch nicht nur abgehört, sondern auch manipuliert werden. Ein Angreifer kann sich dies zunutze machen, indem er IP-Pakete mit gefälschten Absenderadressen an fremde Rechnersysteme schickt und sich so Zugang, unter Umständen sogar mit Administratorrechten, verschafft.

Um ein Netz vor Angriffen aus dem Internet zu schützen, werden in letzter Zeit in zunehmendem Maße *Firewalls* eingesetzt. Eine Firewall ist eine Schwelle zwischen zwei Netzen, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen. Eine Firewall stellt nach außen hin nur eine kleine Anzahl gut gesicherter und streng überwachter Dienste zur Verfügung. Jede Kommunikation zwischen dem zu schützenden Netz und dem unsicheren Netz (hier das Internet) wird durch die Firewall überwacht.

Eine Firewall kann durch verschiedene Grundkonzepte realisiert werden. Generell sollte es eine zentrale Firewall geben, über die die Anbindung vom Verwaltungsnetz zum Internet realisiert wird. Diese zentrale Firewall muß den Mindestschutz gewährleisten, der für den Großteil der angeschlossenen Teilnetze ausreichend ist. Teilnetze mit höheren Sicherheitsanforderungen sind durch eine eigene Firewall innerhalb des Verwaltungsnetzes abzuschotten, das heißt, das Gesamtkonzept sollte durch das Zusammenwirken gestaffelter Firewalls realisiert werden. Das Konzept der gestaffelten Firewalls ist auch geeignet, der Gefährdung der *informationellen Gewaltenteilung* innerhalb des Verwaltungsnetzes entgegenzuwirken. Auch innerhalb des Verwaltungsnetzes muß natürlich eine *Abschottung der Teilnetze* gegeben sein.

Folgende *Empfehlungen* für den Anschluß von Netzen der öffentlichen Verwaltung an das Internet können aus Datenschutzsicht gegeben werden:

- Verwaltungsnetze sollten nur an das Internet angeschlossen werden, wenn dies unbedingt erforderlich ist. Die Kommunikationsmöglichkeiten müssen sich dabei am Kommunikationsbedarf orientieren. Dazu ist die Durchführung einer Kommunikationsanalyse notwendig.
- Voraussetzung für die Anbindung eines Verwaltungsnetzes an das Internet ist das Vorliegen eines schlüssigen Sicherheitskonzeptes und dessen konsequente Umsetzung. Die Internet-Anbindung darf nur erfolgen, wenn die Risiken durch technische und organisatorische Maßnahmen beherrscht werden können.
- Die Sicherheit des Verwaltungsnetzes ist durch geeignete Firewall-Systeme sicherzustellen. Diese müssen eine differenzierte Kommunikationssteuerung und Rechtevergabe unterstützen. Dabei müssen die Anforderungen, die von den Firewall-Komponenten zu erfüllen sind, im Sicherheitskonzept integriert sein.
- Um der Gefahr von Maskeraden und der Ausforschung der Netzstrukturen des Verwaltungsnetzes entgegenzuwirken, sollte eine gesonderte interne Adreßstruktur verwendet werden. Die internen Adressen müssen dann durch eine zentrale Firewall in externe Internet-Adressen umgesetzt werden.
- Der ausschließliche Einsatz einer zentralen Firewall-Lösung ist nur dann vertretbar, wenn eine Orientierung am höchsten Schutzbedarf erfolgt, auch wenn dies Nachteile für weniger sensible Bereiche mit sich bringt. Die Frage der Kontrolle interner Verbindungen bleibt jedoch bei einer solchen Lösung offen. Das Konzept der gestaffelten Firewalls kommt den Datenschutzanforderungen an Verwaltungsnetze entgegen, die aus einer Vielzahl verschiedener Teilnetze bestehen, in denen Daten unterschiedlicher Sensibilität von verschiedenen Stellen für unterschiedliche Aufgaben verarbeitet werden und in denen dementsprechend jeweils unterschiedliche Sicherheitsanforderungen bestehen.
- Der personelle und sachliche Aufwand für Firewall-Lösungen ist generell sehr hoch. Es ist dabei unverzichtbar, hochspezialisierte Kräfte einzusetzen, um gegen mindestens ebenso spezialisierte Angreifer gewappnet zu sein.
- Auch beim Einsatz von Firewalls bleiben Restrisiken bestehen, denen anwendungsbezogen begegnet werden muß. Es bleibt daher notwendig, personenbezogene Daten nur verschlüsselt zu übertragen, wobei hierzu auch Paßwörter und sonstige Authentifikationsdaten zu zählen sind.
- Bei einem unvertretbaren Restrisiko muß auf einen Anschluß an das Internet verzichtet werden. Der Zugriff auf Internet-Dienste muß in diesem Fall auf Systeme beschränkt werden die nicht in das Verwaltungsnetz eingebunden sind.
- Firewall-Konzepte entlasten die dezentralen Systemverwalter und Netzadministratoren nicht von ihrer Verantwortung zur Gewährleistung des Datenschutzes. Durch die Vernetzung erhöhen sich vielmehr die Anforderungen an die lokale Systemverwaltung, da Administrationsfehler ungleich schwerwiegendere Konsequenzen haben können.

Für die Anbindung des Berliner Verwaltungsnetzes MAN an das Internet wurden bereits erste Schritte unternommen. Die Notwendigkeit einer sicheren Abschottung gegenüber dem Internet wurde bereits sehr frühzeitig erkannt und die *Konzeption eines Security Servers*, der diese Funktionen übernehmen soll, in Auftrag gegeben. Hierbei wurde aufgrund der guten Erfahrungen bei der Erstellung der Risikoanalyse und dem darauf aufbauendem Datenschutz- und Datensicherheitskonzept für das MAN wiederum auf externen Sachverstand zurückgegriffen. Das Konzept enthält gute Ansätze für die technische Anbindung des MAN an das Internet. Problematisch erscheint die Tatsache, daß entgegen den oben erwähnten Empfehlungen nicht mit einer Kommunikationsanalyse begonnen wurde. Zur Zeit existiert im Land Berlin keine Planung für eine mögliche Nutzung des Internet bzw. der Dienste im Internet. Eine detaillierte Kommunikationsanalyse ist jedoch unbedingte Voraussetzung für die Festlegung, wer in welcher Art und Weise welche Internet-Dienste benutzen muß bzw. für den eine Nutzung sinnvoll erscheint. Ein Firewall-Konzept kann jedoch nicht nach Art und Weise eines Kochrezeptes erstellt werden, sondern muß sehr genau den Anforderungen und Gegebenheiten angepaßt werden, um die Risiken auf ein vertretbares Minimum zu reduzieren.

Um es noch einmal zu betonen: Auch ein gut durchdachtes Firewall-Konzept kann keine hundertprozentige Sicherheit gegen Angriffe aus dem Internet bieten. Es sollte daher sehr gut überlegt werden, ob eine Anbindung an das Internet für einen Großteil der Berliner Verwaltung wirklich notwendig ist oder ob es einfach nur die allgemeine Zeiterscheinung ist, auf den Modezug – Internet – unter allen Umständen aufzuspringen. Als sicherste Lösung bietet sich an, den Internet-Zugang über Systeme zu schaffen, die vom Verwaltungsnetz getrennt sind.

4.2 Multimedia

Die Einführung digitalisierter Übertragungsverfahren im Medienbereich eröffnet neue Möglichkeiten für das Angebot von Telekommunikationsdiensten. Wurde zunächst mit der Umstellung auf ISDN der Telefondienst digitalisiert, so werden gegenwärtig auch Verfahren zur *digitalen Übertragung von Rundfunk- und Fernsehdiensten* entwickelt und eingeführt.

Während bei herkömmlichen analogen Übertragungsverfahren der Umfang des Angebotes durch die Anzahl der zur Verfügung stehenden Frequenzen begrenzt war, wird in Zukunft durch den Einsatz von Multiplex- und Kompressionsverfahren ein Vielfaches an Kanälen zur Verfügung stehen. Auf der Übertragungsebene wird durch die Digitalisierung die Übertragung beliebiger Informationen über eine *einheitliche Netzinfrastruktur* möglich; die traditionelle Bindung verschiedener Medien an unterschiedliche Netze (z. B. Telefonnetz, besondere Datenübertragungsnetze und das Kabelfernsehnetz) ist damit technisch nicht mehr notwendig. Gleichzeitig findet eine Integration verschiedener Informationsformen (Text, Sprache, Stand- und Bewegtbilder) unter *einheitlichen Benutzeroberflächen* statt.

Diese Entwicklungen haben unter den Schlagworten *„Datenautobahn“*, *„Multimedia“* und *„Interaktive Dienste“* im Berichtszeitraum eine erhebliche Publizität erlangt. Zwar sind die Begriffe noch unscharf, doch lassen sich bereits jetzt einzelne Angebote identifizieren, mit deren flächendeckendem Angebot in naher Zukunft gerechnet werden muß. Diesen Diensten ist gemeinsam, daß bei ihrer Nutzung Daten über das *Mediennutzungsverhalten* des Betroffenen in bisher nicht bekanntem Ausmaß anfallen können.

Telekommunikationsdienste und Medienangebote waren bisher überwiegend dadurch gekennzeichnet, daß Informationen für eine unbestimmte Anzahl von Nutzern verbreitet werden, wobei der Veranstalter oder Anbieter keine Rückmeldung erhält, wer welche Angebote in Anspruch genommen hat (sogenannte *„Verteildienste“*). Hier war es für den Betroffenen möglich, Informationsangebote wahrzunehmen, ohne sich dem Anbieter gegenüber identifizieren zu müssen. Ein Beispiel hierfür ist die terrestrische Ausstrahlung von Fernsehprogrammen.

Im Gegensatz dazu stehen „vermittelte“ Dienste, bei denen der Nutzer für die Inanspruchnahme eines bestimmten Informationsangebotes *Gebühren* zu entrichten hat (z. B. der deutsche Bildschirmtext/T-Online-Dienst). Bei diesen Diensten fallen in der Regel *für Abrechnungszwecke Verbindungsdaten* darüber an, wer welche Angebote in Anspruch genommen hat. Die Einführung von Multimediadiensten wird aller Voraussicht nach zur Folge haben, daß zahlreiche Informationsangebote, die gegenwärtig als Verteildienste ausgestaltet sind, zukünftig als vermittelte Dienste angeboten werden (dies gilt insbesondere für die derzeit im Rahmen des Pilotprojekts *„Interaktive Videodienste“* von der Telekom in Berlin erprobten Dienste).[53]

Bei einer entsprechenden Ausgestaltung der Systeme würde es in Zukunft in zahlreichen Fällen daher nicht mehr möglich sein, einzelne Informationsangebote *anonym*, also ohne Preisgabe der eigenen Identität, wahrzunehmen.

Dies könnte zur Speicherung von personenbezogenen Daten über das *Konsum- und Medienverhalten* des einzelnen in bisher

53 vgl. S. 24

nicht bekanntem Ausmaß führen. Es würden detaillierte Informationen z. B. darüber vorliegen, wer wann welche Fernsehsendungen gesehen hat, wer welche Artikel aus der elektronischen Zeitung oder ähnlichen Medienangeboten abgerufen hat, wer welche Abrufe in kommerziell verfügbaren Datenbanken getätigt hat und wer welche Konsumangebote außerhalb des Medienbereiches (z. B. *„elektronische Kaufhäuser")* in Anspruch genommen hat. Gleichzeitig liegt auf der Hand, daß die Anbieter derartiger Telekommunikationsdienstleistungen ein großes Interesse daran haben müssen, im Hinblick auf die Optimierung ihrer eigenen Programmangebote möglichst detaillierte und umfassende Daten über die einzelnen Nutzer ihrer Dienste zu erheben und zu verarbeiten.

Aus Sicht des Datenschutzes kommt es daher entscheidend auf die *Ausgestaltung der Nutzungs- und Abrechnungsverfahren* bei solchen Diensten an. Es ist zu fordern, daß auch weiterhin die anonyme Nutzung von Informations- und sonstigen Dienstleistungsangeboten möglich sein muß, selbst wenn diese gebührenfrei sind. Darüber hinaus sind geeignete Verfahren mit anonymen Abrechnungsmöglichkeiten bei gebührenpflichtigen Angeboten zu entwickeln.

Grundsätzlich sollte die Verarbeitung personenbezogener Daten durch Systembetreiber und Programmanbieter auf ein möglichst geringes Maß reduziert werden. Nicht für die Erbringung eines Dienstes erforderliche Daten dürfen gar nicht erst erhoben werden. Gleichzeitig müssen die verbleibenden zu verarbeitenden personenbezogenen Daten einem strengen *Zweckbindungsgebot* unterworfen werden, das eine Verwendung der Daten für andere Zwecke als die Erbringung der gewünschten Dienstleistung explizit ausschließt. Diese Auffassung habe ich bei einer Anhörung des Bundestagsausschusses für Post- und Telekommunikation am 20. September 1995 zu „Multimedialer Kommunikation" in Bonn vertreten. Im gleichen Sinne habe ich mich auch auf eine Anfrage der Senatskanzlei, die das Land Berlin in der Bund-Länder-Arbeitsgruppe „Multimedia" vertritt, geäußert.

Pilotprojekt „Interaktive Videodienste Berlin"

Am 15. Februar 1995 hat das Multimedia-Pilotprojekt „Interaktive Videodienste Berlin" der Deutschen Telekom AG als bisher einziges von insgesamt sechs in Deutschland geplanten Pilotprojekten den Betrieb aufgenommen. Die angeschlossenen fünfzig Teilnehmer bestehen zur Hälfte aus Privathaushalten, die übrigen Terminals sind an öffentlich zugänglichen Plätzen (z. B. in Kaufhäusern) und in der öffentlichen Verwaltung installiert. Auch der Berliner Datenschutzbeauftragte nimmt am Pilotprojekt teil.

Die angebotenen Informationen sind auf einem von der Telekom betriebenen *Video-Server* gespeichert. Für die Übertragung an die Teilnehmer wird das Kabelnetz der Telekom benutzt. Dabei wird ein sonst nicht genutzter Frequenzbereich („Hyperband") verwendet, der in fünfzig Kanäle aufgeteilt ist. Jeder Kanal ist eindeutig einem Teilnehmer zugeordnet. Bei den Teilnehmern ist eine *„Set Top Box"* installiert, die die über das Kabelnetz empfangenen Signale zur Wiedergabe auf dem Fernsehgerät dekodiert und dekomprimiert. Die Set Top Box ist durch eine Chipkarte gegen unbefugte Benutzung gesichert. Für den *„Rückkanal"* – das heißt die Übertragung von Signalen vom Teilnehmer zur Telekom – wird in Berlin das Telefonnetz genutzt. An anderen Standorten im Bundesgebiet sollen verschiedene andere Rückkanaltechniken wie das Breitbandkabelnetz oder sogar Glasfaserkabel eingesetzt werden. Der Benutzer kann das System durch eine Fernbedienung beeinflussen.

Zu den bisher angebotenen Diensten gehören:

- *Video on Demand:* Ermöglicht den jederzeitigen Abruf entgeltpflichtig angebotener Filme. Dabei kann der Film wie auf einem Videorecorder vor- und zurückgespult werden.
- *Near Video on Demand:* Auch hier kann der Benutzer unter einem bestimmten Angebot von Filmen auswählen, diese werden jedoch nur in bestimmten Zeitabständen (z. B. alle fünfzehn Minuten) gestartet. Hier sollen ebenfalls Gebühren für das Ansehen des einzelnen Films erhoben werden.
- *Pay per Channel:* Hier wird für einen bestimmten Zeitraum (z. B. für einen Monat) das Programm eines bestimmten Fernsehsenders angemietet. Derartige Angebote sind bereits jetzt – wenn auch in einer anderen technischen Realisierung – verfügbar.
- *Home-Shopping:* Ermöglicht den Einkauf verschiedener Waren bei verschiedenen Anbietern „vom Wohnzimmersessel aus". Die Bestellungen werden an die Versandhäuser weitergegeben und dort bearbeitet.
- *Pay-Radio:* Einzelne Radioprogramme werden für einen bestimmten Zeitraum gemietet.

Daneben besteht das Pilotprojekt aus zahlreichen *Informationsangeboten,* die so unterschiedliche Bereiche wie Öffnungszeiten von Stellen der Berliner Verwaltung bis hin zu Kleinanzeigen abdecken. An dem Pilotprojekt sind neben der Telekom öffentliche und private Rundfunksender und andere Unternehmen aus dem Medienbereich beteiligt.

Ziel des Pilotprojekts in der gegenwärtigen Phase ist in erster Linie die Erkundung verschiedener Möglichkeiten zur technischen Realisierung derartiger Dienste. Der Berliner Datenschutzbeauftragte hat sich entschlossen, an dem Pilotversuch teilzunehmen, um bereits bei der Entwicklung solcher Technologien auf eine Berücksichtigung des Datenschutzes zu dringen.

Die aus unserer Sicht zentrale Gestaltung der Abrechnungsverfahren ist bislang noch völlig offen. Das liegt vordergründig daran, daß im Berliner Pilotprojekt alle Angebote gebührenfrei sind. Aber auch der Umstand, daß jeder Tastendruck der einzelnen Teilnehmer an diesem Projekt anschlußbezogen registriert wird, ist allenfalls für die jetzt zu Ende gehende Versuchsphase, nicht aber für den späteren flächendeckenden Echtbetrieb akzeptabel. Notwendigkeit ist eine datenschutzfreundliche Gestaltung der Nutzung und Abrechnung derartiger Dienstleistungsangebote.

Unterdessen ist zwischen dem Datenschutzbeauftragten der Telekom, dem Bundesbeauftragten für den Datenschutz und den Landesdatenschutzbeauftragten derjenigen Länder, in denen Pilotprojekte der Telekom stattfinden, ein regelmäßiger Erfahrungsaustausch vereinbart worden.

4.3 Entwicklung des Telekommunikationsrechts

Postreform III – Schlußstein der Liberalisierung im Telekommunikationsbereich

Obwohl die Arbeiten zur Umsetzung der Postreform II in einzelnen Bereichen noch nicht abgeschlossen sind[54], sind die Vorbereitungen für die nächste und letzte Stufe der Liberalisierung im Telekommunikationsbereich („Postreform III") bereits in vollem Gange. Kern dieses Reformabschnitts ist die *Liberalisierung des Sprachtelefondienstes* im Festnetz zum 1. Januar 1998, der bisher als letzter Monopoldienst ausschließlich der Deutschen Telekom AG vorbehalten ist. Gleichzeitig soll die Möglichkeit geschaffen werden, eine gleichmäßige Versorgung der Bevölkerung mit Basistelekommunikationsdiensten zu angemessenen Preisen durch die Verpflichtung aller oder bestimmter Wettbewerber zum Angebot eines *„Universaldienstes"* sicherzustellen.

Bereits im März 1995 hat das Bundesministerium für Post- und Telekommunikation sogenannte „Eckpunkte eines künftigen Regulierungsrahmens im Telekommunikationsbereich"[55] vorgelegt. Danach sollten sich die im Rahmen der Postreform III zu treffenden Regelungen zu Fernmeldegeheimnis und Datenschutz „. . . an den einschlägigen europarechtlichen Regelungen und darin festgelegten Mindestanforderungen orientieren." In meiner Stellungnahme als Vorsitzender des Arbeitskreises Telekommunikation und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder habe ich gegenüber dem Bundespostministerium darauf hingewiesen, daß das Datenschutzniveau für die Bürger bei der Liberalisierung des Telefondienstes auf keinen Fall weiter abgesenkt werden darf.

Schon in zurückliegenden Berichtsjahren hatten wir auf die Notwendigkeit der Erhaltung einer einheitlichen *unabhängigen Datenschutzkontrolle für den Telekommunikationsbereich* hingewiesen. Zwar sieht der Entwurf für ein Telekommunikationsgesetz die Übertragung der Kontrollkompetenz für den Bereich der

54 vgl. S. 25 f.
55 Amtsblatt des BMPT 7/95, S. 525

Telekommunikation auf eine neu zu schaffende *Regulierungsbehörde* vor. Aufgrund ihrer voraussichtlichen organisatorischen Gestaltung kann jedoch nicht davon ausgegangen werden, daß diese Stelle eine dem Bundesbeauftragten für den Datenschutz vergleichbare Unabhängigkeit bei der Erfüllung ihrer Aufgaben besitzt. Darüber hinaus sind aufgrund einiger der zahlreichen weiteren Aufgaben, die dieser Stelle übertragen werden sollen (z. B. im Zusammenhang mit der technischen Umsetzung von Überwachungsmaßnahmen), Interessenkonflikte zu befürchten. Daher haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 50. Konferenz in einer Entschließung gefordert, die zentrale Funktion des Bundesbeauftragten für den Datenschutz für die Kontrolle im Telekommunikationsbereich zu erhalten. Gleichzeitig bedürfen die Aufgaben, die die Landesbeauftragten für den Datenschutz und Aufsichtsbehörden im Rahmen ihrer Zuständigkeit zu erfüllen haben (etwa bei lokalen [Stadt-]Netzen und Nebenstellenanlagen), einer klaren gesetzlichen Regelung.

Bereits jetzt werden auch Überlegungen zur Ausgestaltung des Universaldienstes angestellt. Hierzu hat das Bundesministerium für Post und Telekommunikation den Entwurf einer *Universaldienstleistungsverordnung* vorgelegt. Dieser Entwurf enthält keinerlei Bestimmungen zum Datenschutz. Wir halten es allerdings für erforderlich, die entsprechenden Dienstleistungsunternehmen im Rahmen des Universaldienstes auch zum kostengünstigen Angebot entsprechender *datenschutzfreundlicher Leistungsmerkmale* zu verpflichten. Es darf nicht soweit kommen, daß die Betroffenen wegen zu hoher Kosten auf die Inanspruchnahme von Leistungsmerkmalen zum Schutz ihres informationellen Selbstbestimmungsrechts verzichten.

Telekommunikationsdienstunternehmen-Datenschutzverordnung

Bereits im letzten Jahresbericht hatten wir über die *Postreform II*[56] berichtet. Mit dem Inkrafttreten des Gesetzes zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz – PTNeuOG)[57] war unter anderem der Erlaß einer Datenschutzverordnung erforderlich geworden, die die bisherige TELEKOM-Datenschutzverordnung (TDSV) und die Teledienstunternehmen-Datenschutzverordnung (UDSV) in einer einzigen Rechtsvorschrift zusammenfassen und ersetzen soll. Ein entsprechender Entwurf einer Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen *(Telekommunikationsdienstunternehmen-Datenschutzverordnung – TDSV)* liegt nunmehr vor.[57 a] Die Verordnung soll den Schutz personenbezogener Daten der am Fernmeldeverkehr beteiligten Bürger unabhängig von der Rechtsform des Dienstleistungsunternehmens einheitlich regeln.

Leider ist festzustellen, daß der Entwurf das Datenschutzniveau für die Betroffenen keinesfalls verbessert; in einigen Punkten bleiben die Regelungen der neuen Verordnung sogar hinter denen von TDSV und UDSV zurück:

Im Bereich des Sprachtelefondienstes soll nach dem Entwurf die Speicherung der um die letzten *drei Stellen gekürzten Rufnummer* des angerufenen Teilnehmers bis zu achtzig Tagen nach Rechnungsversand zur Regel werden. Bislang war dies nur vorgesehen, wenn der Anrufer einen *Einzelverbindungsnachweis* beantragt hatte. Für die Erteilung eines Einzelverbindungsnachweises reicht nunmehr die schriftliche Erklärung des Kunden aus, daß er alle zum Haushalt gehörenden Mitbenutzer des Anschlusses über die Bekanntgabe der Verbindungsdaten an ihn zur Erteilung des Nachweises informiert hat. Die Regelungen der TDSV/UDSV setzten demgegenüber eine ausdrückliche Einverständniserklärung der zum Haushalt gehörenden Mitbenutzer des Anschlusses voraus.

Abweichend von der gegenwärtigen Praxis der Deutschen Telekom AG läßt der Verordnungsentwurf die Erstellung von Einzelverbindungsnachweisen mit vollständigen Zielnummern ohne Einflußmöglichkeit der angerufenen Kunden zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit darauf hingewiesen, daß dem Schutz des *informationellen Selbstbestimmungsrechts des Angerufenen* am besten entsprechen würde, wenn jeder inländische Anschlußinhaber selbst entscheiden könnte, ob und gegebenenfalls wie seine Rufnummer auf Einzelverbindungsnachweisen erscheinen soll. Obwohl ein entsprechendes Verfahren in den Niederlanden bereits erfolgreich praktiziert wird, hat der Bundesminister für Post und Telekommunikation diesen Vorschlag wiederum nicht aufgegriffen.

Über die Problematik der Aufnahme von Anrufen bei *telefonischen Beratungsstellen* in Einzelverbindungsnachweise hatten wir schon früher berichtet.[58] Während solche Anrufe nach den Regelungen der TDSV/UDSV weder im Fest- noch im Mobilfunknetz auf Einzelentgeltnachweisen ausgewiesen werden dürfen, sieht die neue Datenschutzverordnung eine Ausnahme für Mobilfunknetze vor. Die Netzbetreiber brauchen hier ihre Kunden lediglich auf die fehlende Anonymität bei Anrufen bei Beratungsstellen hinzuweisen. Sollte diese Regelung so in Kraft treten, wäre das Beratungsgeheimnis bei der Nutzung von Mobiltelefonen nicht mehr gegeben.

Bereits früher haben die Datenschutzbeauftragten gefordert, daß *datenschutzfreundliche Leistungsmerkmale*, die eine datenschutzgerechte Nutzung der digitalisierten Telefonnetze zu ermöglichen, nicht mit zusätzlichen Kosten belastet werden dürfen. Solche Merkmale müssen vielmehr kostenfrei angeboten werden. Auch diese Anregung ist bezüglich der Unterdrückung der Rufnummernanzeige des Anrufers beim Angerufenen in der TDSV nicht aufgegriffen worden. Bereits jetzt erhebt die Telekom Gebühren für die *Rufnummernunterdrückung* im Einzelfall.

Der Charakter der *Telefonauskunft* soll völlig verändert werden. War bisher nur die Auskunft über die Rufnummer zu einem bekannten Namen möglich, so soll jetzt über den gesamten in den Teilnehmerverzeichnissen enthaltenen Datensatz (also z. B. auch die Adresse) Auskunft gegeben werden. Abweichend von den Regelungen der TDSV/UDSV, die dies nur nach Einwilligung des Betroffenen ermöglichten, räumt die neue TDSV den Betroffenen lediglich ein Widerspruchsrecht ein.

In einem wichtigen Punkt verbessert die neue Datenschutz-Verordnung allerdings die Rechte des Telefonkunden: Seit billige elektronische Telefonverzeichnisse reißenden Absatz finden, die qualitativ weitergehende Verarbeitungsmöglichkeiten bieten (z. B. *CD-ROM* oder Abruf aus Online-Diensten mit *Adreß-Selektion*, bundesweiter Recherchemöglichkeit und umgekehrter Rufnummernsuche), kann niemand, dessen Adresse zusammen mit der Rufnummer im herkömmlichen Telefonbuch steht und der eine Zeitungsannonce ausschließlich mit seiner Rufnummer aufgegeben hat, darauf vertrauen, daß er von Interessenten nur angerufen wird. Er muß vielmehr damit rechnen, daß sie plötzlich vor seiner Wohnungstür stehen, weil sie anhand seiner Telefonnummer mit Hilfe einer Telefon-CD-ROM seine Adresse durch Knopfdruck ermittelt haben.

> *Ein elfjähriges italienisches Mädchen gab im Rahmen eines Telefonkontaktes auf einer „chat line" (eine Art Konferenzschaltung zum Schwatzen) zwar weder ihr richtiges Alter noch ihre richtige Adresse, wohl aber ihre richtige Telefonnummer an. Ein Mitschwätzer fand auf Grund der Telefonnummer die Adresse heraus, besuchte die Kleine – und vergewaltigte sie.*[59]

Die Datenschutzbeauftragten hatten seit dem ersten Erscheinen derartiger elektronischer Kundenverzeichnisse gefordert, daß jeder Telefonkunde das Recht haben sollte, sich zwar für einen Eintrag im herkömmlichen Telefonbuch, aber gegen eine Übernahme in elektronische Teilnehmerverzeichnisse zu entscheiden.[60] Die bisherige Rechtslage war insofern nicht ganz eindeutig, und die Telekom hatte es bis jetzt abgelehnt, von sich aus den Kunden ein solches differenziertes Widerspruchsrecht einzuräumen. Zur Begründung verwies sie auch auf die technische Möglichkeit für jeden, mit Hilfe der Scannertechnologie herkömmliche Telefonbücher in elektronische Datenbanken umzuwandeln und zu vermarkten. Auch die datenschutzrechtliche Zulässigkeit dieses Verfahrens wurde bisher unterschiedlich beurteilt.

56 Jahresbericht 1994, 5.1
57 BGBl. I, S. 2325 ff.
57 a Bundesrats-Drucksache 60/96
58 Jahresbericht 1994, 5.1
59 FAZ v. 28. 12. 95, S. 23
60 Jahresberichte 1991, 2.3; 1994, 5.1

Der Entwurf für eine neue Telekommunikationsdienstunternehmen-Datenschutzverordnung sieht jetzt vor, daß jeder Telefonkunde der Aufnahme seiner Daten in elektronische Verzeichnisse auch dann *widersprechen* kann, wenn er ihre Aufnahme in das herkömmliche Telefonbuch wünscht. In diesem Fall ist sein Eintrag in das Telefonbuch entsprechend zu kennzeichnen. Damit wird zugleich dokumentiert, daß der Kunde es als Beeinträchtigung seiner schutzwürdigen Belange betrachtet, wenn Dritte seine Daten aus dem Telefonbuch in elektronische Verzeichnisse einlesen.

Allerdings würde diese Neuregelung dem Kunden die Initiative aufbürden, der Aufnahme seiner Daten auf elektronische Datenträger ausdrücklich zu widersprechen. Schweigt er, weil er die Information des Netzbetreibers nicht versteht, für Werbung hält, oder einfach weil er im Urlaub ist und sie erst nach Ablauf der Widerspruchsfrist vorfindet, so wird dies als Zustimmung gewertet. Das ist weder datenschutzgerecht noch kundenfreundlich. Das wirtschaftliche Interesse der Netzbetreiber an einer elektronischen Vermarktung der Kundendaten darf nicht höher bewertet werden als das Persönlichkeitsrecht der Telefonkunden. Die Aufnahme seiner Daten in elektronische Kundenverzeichnisse sollte nur mit *ausdrücklicher Einwilligung* des Kunden zulässig sein.

Daneben erlauben die Regelungen der neuen Datenschutzverordnung auch die regelmäßige Herausfilterung von Daten solcher Verbindungen, für die tatsächlich Anhaltspunkte den Verdacht eines strafbaren Mißbrauchs von Fernmeldeanlagen oder der mißbräuchlichen Inanspruchnahme von Telekommunikationsdienstleistungen begründen. Dies kommt einer *präventiven Rasterfahndung* der dem Fernmeldegeheimnis unterliegenden Verbindungsdaten gleich, in die bereits im Vorfeld eines konkreten Verdachts sämtliche Teilnehmer einbezogen werden. Darüberhinaus wird den Dienstleistungsunternehmen unter bestimmten Voraussetzungen auch die Verarbeitung von Nachrichteninhalten gestattet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung zur zweiten TDSV[61] die mit diesen Regelungen verbundene Absenkung des Datenschutzstandards im Bereich der Telekommunikation kritisiert. In der Entschließung wird insbesondere die Aufweichung des Zweckbindungsgrundsatzes für die Verarbeitung von Kundendaten kritisiert. Diese muß auch in Zukunft ausdrücklich auf Telekommunikationszwecke beschränkt bleiben.

Fernmeldeverkehr-Überwachungs-Verordnung (FÜV)

Häufig waren in der Vergangenheit der Presse Berichte zu entnehmen, nach denen die *Abhörbarkeit* insbesondere der *Mobilfunknetze durch die Sicherheitsbehörden* nicht in vollem Umfang sichergestellt ist. Die Bundesregierung hat dies zum Anlaß genommen, in einer Rechtsverordnung die technische Umsetzung bereits jetzt materiell rechtlich zulässiger Fernmeldeüberwachungsmaßnahmen zu regeln.[61 a] Diese Verordnung verpflichtet die Betreiber für den öffentlichen Verkehr bestimmter Fernmeldeanlagen – also nicht nur die Betreiber von Mobilfunknetzen –, den dazu berechtigten Stellen („Bedarfsträgern", d. h. Strafverfolgungsbehörden und Nachrichtendiensten) neben den übermittelten Nachrichteninhalten auch zahlreiche Verbindungsdaten in einem definierten Verfahren zur Verfügung zu stellen. Dazu zählt auch die Verpflichtung, Nachrichten, die mit vom Betreiber zur Verfügung gestellten Verschlüsselungsmöglichkeiten geschützt sind, im Klartext zur Verfügung zu stellen. Die Betreiber sind verpflichtet, ein entsprechendes Konzept über die Umsetzung der Verpflichtung beim Bundesamt für Post- und Telekommunikation vorzulegen.

Besonders kritisch erscheint aus Datenschutzsicht in diesem Zusammenhang die explizite Verpflichtung der Betreiber, über die Gesprächsinhalte hinaus einen umfangreichen *Katalog an Verbindungsdaten* (z. B. über die „Funkzelle", in der sich der Mobilfunkteilnehmer gerade aufhält) zur Verfügung zu stellen. Dies könnte die Einführung datenschutzfreundlicher Techniken behindern, die ohne die Erhebung der genannten Daten auskämen.

4.4 Zur Regulierung der Telekommunikation in Europa und den Vereinigten Staaten

Telekommunikation wird zunehmend ein weltweites Geschäft. Europäische Telekommunikationsorganisationen wie die Deutsche Telekom und France Télécom beteiligen sich an der amerikanischen Telefongesellschaft Sprint und wollen einen weltweiten Telekommunikationskonzern unter dem Namen *„Global One"* bilden[62]. Rechtliche Regelungen der Telekommunikation auf dem internationalen Markt können sich daher nicht auf die nationale Gesetzgebung beschränken, sondern müssen auf der europäischen und der internationalen Ebene getroffen werden. Um so wichtiger ist es, daß die vorhandenen Ansätze in der Europäischen Union und dem *Europarat zügig* weiter entwickelt werden.

Der *Entwurf der ISDN-Richtlinie* lag unter der französischen Ratspräsidentschaft in der Europäischen Union im ersten Halbjahr 1995 noch auf Eis, weil die Verabschiedung der allgemeinen Datenschutzrichtlinie abgewartet werden sollte. Die Konferenz der Europäischen Datenschutzbeauftragten kritisierte diese Verzögerung bei ihrer Sitzung in Lissabon[63] und setzte sich für eine zügige Verabschiedung bei gleichzeitiger Anhebung des Datenschutzniveaus ein. Außerdem kritisierte sie, daß der Entwurf der Richtlinie in der Ratsarbeitsgruppe „Telekommunikation" und nicht in der für die allgemeine Datenschutzrichtlinie zuständigen Ratsarbeitsgruppe behandelt werde. Nach der Verabschiedung der allgemeinen Datenschutzrichtlinie im Juli 1995 wurde die inhaltliche Diskussion der ISDN-Richtlinie in der Arbeitsgruppe des Ministerrats wieder aufgenommen und unter der spanischen Präsidentschaft beschleunigt. Um in dieser Phase noch Verbesserungen im gegenwärtigen Richtlinienentwurf zu erreichen, haben die Europäischen Datenschutzbeauftragten in einer zweiten gemeinsamen Erklärung detaillierte Verbesserungsvorschläge gemacht[64]. Seit Anfang 1996 führt Italien den Vorsitz im Ministerrat und dringt offensichtlich auf eine schnelle abschließende Beratung der ISDN-Richtlinie. Die italienische Ratspräsidentschaft hat die Anregung der Datenschutzbeauftragten aufgegriffen und die Erörterungen über den Entwurf wieder in die Arbeitsgruppe „Datenschutz" des Rates zurückverlagert. Es soll versucht werden, im ersten Halbjahr 1996 zu einem Gemeinsamen Standpunkt zu gelangen. Eine weitere Verzögerung der europäischen Rechtssetzung in diesem wichtigen Bereich wäre allerdings nicht länger hinnehmbar, zumal die technische Entwicklung und die Bildung neuer Unternehmensallianzen ständig fortschreitet.

Mit wesentlich höherer Priorität als den Datenschutz bei der Telekommunikation behandelt die Europäische Union die Liberalisierung und Deregulierung der Telekommunikationsmärkte. Das wird deutlich an der zügigen Beratung der *Richtlinie über den offenen Netzzugang im Sprachtelefondienst*[65], die gegen Ende des Berichtszeitraumes kurz vor der endgültigen Verabschiedung stand, obwohl sie jüngerem Datums als die ISDN-Richtlinie ist und bereits einmal am Widerstand des Europäischen Parlaments gescheitert war. An diesem Richtlinienvorschlag wurden auch keine datenschutzrechtlichen Verbesserungen vorgenommen, die wir stets gefordert hatten. Der Zug in Richtung „Liberalisierung" zum Stichtag 1. Januar 1998 ist so schnell, daß der Datenschutz droht, unter die Räder zu kommen, wenn nicht die ISDN-Richtlinie in verbesserter Form alsbald beschlossen wird.

Auch zum *Grünbuch der Europäischen Kommission über die Liberalisierung der Telekommunikationsinfrastruktur und der Kabelfernsehnetze*[66] hat die Europäischen Konferenz der Datenschutzbeauftragten auf unseren Vorschlag hin Stellung genommen.[67] Während die Europäische Kommission zu Recht die Not-

61 Anlage 2.15. Der ursprüngliche Verordnungsentwurf, zu dem sich die Konferenz geäußert hat, bezog noch die Informationsdienstleistungen mit ein und war deshalb mit „Telekommunikations- und Informationsdienstleistungunternehmen – Datenschutzverordnung" überschrieben.

61a Verordnung über die technische Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs in Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, v. 18. 5. 1995, BGBl. I, S. 722 ff.

62 Frankfurter Allgemeine Zeitung vom 2. Februar 1996

63 vgl. Anlage 3.2

64 vgl. Anlage 3.7; siehe bereits Jahresbericht 1994, Anlage 3.4

65 vgl. Jahresbericht 1994, 5.1

66 Teil I KOM (94) 440 endg.; Teil II KOM (94) 682 endg.

67 vgl. Anlage 3.1

wendigkeit betont hat, eine Spaltung der Informationsgesellschaft in „Informationsbesitzer“ und „Informationshabenichtse“ zu verhindern, haben wir darauf hingewiesen, daß eine solche Spaltung auch in einem anderen Sinne verhindert werden muß: Es darf keinen Unterschied geben zwischen denen, die sich Datenschutz und Datensicherheit leisten können, und denen, die dies nicht können. Möglichkeiten des anonymen Netzzugangs und der Nutzung von Diensten ohne identifizierbare elektronische Spuren im Netz anzubieten, muß für alle Betreiber und Anbieter obligatorisch sein. Schließlich haben wir uns im Auftrag der Europäischen Datenschutzkonferenz auch an der Konsultation beteiligt, die die Europäische Kommission mit Mitgliedern des Europäischen Parlaments zu *Fragen des Universaldienstes* durchgeführt hat.[68]

Während im Rahmen der Europäischen Union der Datenschutz bei der Telekommunikation noch ungeregelt ist, hat der *Europarat* inzwischen gehandelt: Am 7. Februar 1995 beschloß der Ministerausschuß eine *Empfehlung über den Schutz personenbezogener Daten im Bereich der Telekommunikationsdienste unter besonderer Berücksichtigung des Telefondienstes.*[69] Dieser Empfehlung, an deren Erarbeitung wir zeitweise als Sachverständige beteiligt waren, enthält wichtige Leitlinien etwa zum anonymen Zugang zu Telekommunikationsnetzen und -diensten, aber auch zu Risiken der Netzsicherheit und Möglichkeiten zu ihrer Begrenzung, die dem Kunden zur Verfügung gestellt werden sollten. Die Empfehlung hat zwar nicht wie die geplante ISDN-Richtlinie eine verpflichtende Wirkung auf die Mitgliedstaaten des Europarats (zu denen inzwischen auch Rußland zählt); dennoch ist die Empfehlung ein bedeutsamer Schritt zur Entwicklung des bereichsspezifischen Datenschutzes in der europäischen Telekommunikation.

Bedeutsam ist schließlich eine weitere *Empfehlung des Europarats zu Problemen des Strafverfahrensrechts im Zusammenhang mit der Informationstechnik,* die am 1 . September 1995 beschlossen wurde.[70] Dieses Dokument enthält Richtlinien zur Beschlagnahme von Computern und Durchsuchungen von Datenbanken für strafprozessuale Zwecke ebenso wie Bestimmungen zur Überwachung des Fernmeldeverkehrs und zur Nutzung von Verschlüsselungstechniken.

Auch aus europäischer Sicht immer bedeutender wird die Entwicklung des Telekommunikationsrechts in den *Vereinigten Staaten.* Die von Präsident Clinton zur Begleitung der entstehenden *National Information Infrastructure („NII“)* gebildete Information Infrastructure Task Force setzte eine Arbeitsgruppe zum Datenschutz (Privacy Working Group) ein, die im Juni 1995 *„Prinzipien für die Bereitstellung und für den Gebrauch personenbezogener Informationen“* veröffentlichte. Diese Richtlinien sollen einen fairen Umgang mit personenbezogenen Informationen nicht nur im öffentlichen, sondern auch im privaten Bereich fördern. Sie sind auch vor dem Hintergrund der jetzt verabschiedeten Europäischen Datenschutzrichtlinie formuliert worden und könnten zu einem Baustein für ein neues Datenschutzrecht in den Vereinigten Staaten werden, auch wenn die Prinzipien sehr allgemein gehalten sind und eine öffentliche Instanz zur Überwachung ihrer Einhaltung bisher völlig fehlt. Bemerkenswert an diesen Prinzipien ist aber gleichwohl die Grundaussage, daß jeder, also auch der private Datenverarbeiter, in der modernen Informationsgesellschaft bestimmte Regeln einzuhalten hat, wenn er mit personenbezogenen Informationen umgeht. Dieser Ansatz ist auch von besonderer Bedeutung im Zusammenhang mit dem Internet und könnte dort die Diskussion über eine notwendige Netiquette positiv beeinflussen.

Gerade in den Vereinigten Staaten ist die *Direkt-Marketing-Industrie* fast allgegenwärtig. Sie hat insbesondere großes Interesse an einer Nutzung der massenhaft anfallenden Daten über das Kommunikationsverhalten von Telefonkunden. Aus diesem Grund hält es das US-Handelsministerium inzwischen für notwendig, daß private Netzbetreiber und die Diensteanbieter sich stärker als bisher auf den Schutz der Persönlichkeitsphäre ihrer Kunden verpflichten, diese über die Verarbeitung ihrer Daten informieren und ihre Einwilligung einholen. In seinem entsprechenden Weißbuch[71] sieht das Handelsministerium allerdings davon ab, neue bundesgesetzliche Regelungen vorzuschlagen. An den Anfang seiner Überlegungen stellt das Ministerium ein Zitat eines Mitglieds des Obersten Gerichtshofs der Vereinigten Staaten, das auch Europäern zu denken geben sollte:

„Die Nummern, die von einem privaten Telefonanschluß aus angewählt werden, – auch wenn sie sicherlich sehr viel prosaischer sind als der Inhalt des Telefongesprächs selbst – sind nicht ohne Inhalt. Die meisten privaten Telefonkunden werden ihre Nummern in einem Telefonbuch veröffentlichen lassen, aber ich bezweifele, daß irgend jemand einverstanden wäre, wenn eine Liste der von ihm angewählten Nummern weltweit abrufbar wäre. Dies liegt nicht daran, daß so eine Liste in irgendeiner Weise belastend wäre, sondern daran, daß mit ihrer Hilfe leicht die Identität der angerufenen Personen und Einrichtungen und damit höchst intime Details des persönlichen Lebens des Anrufers offengelegt werden können.“[72]

4.5 Datenschutz und Medien

Die unabhängige und unzensierte Berichterstattung durch Presse, Rundfunk und Film dient der freien individuellen und öffentlichen Meinungsbildung. Das Bundesverfassungsgericht hat die freie Meinungsbildung als Voraussetzung sowohl der Persönlichkeitsentfaltung als auch der demokratischen Ordnung bezeichnet. Allerdings sind mit der rasanten Entwicklung der Medientechnik, der Zunahme interaktiver Teledienste und der verstärkten kommerziellen Nutzung von Pressedatenbanken neben neuen Informationsmöglichkeiten für den Bürger auch verstärkte Gefährdungen des Rechts auf informationelle Selbstbestimmung verbunden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer 46. Konferenz am 26./27. Oktober 1993 in Berlin den Arbeitskreis Medien beauftragt, über Fragen des Persönlichkeitsschutzes im Medienbereich der Konferenz zu berichten. Dieser Bericht wurde der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen vorgelegt und von ihr zustimmend zur Kenntnis genommen.

Der Bericht behandelt verschiedene Aspekte des Verhältnisses von Persönlichkeitsschutz und Medien. Im Bereich des *Electronic publishing und der Medienarchive* führen neue Formen der Verbreitung von Informationen über Netze und auf elektronischen Datenträgern in bisher unbekanntem Maß zu großen Informationsbeständen, in denen potentiell jedermann gezielt auf personenbezogene Daten zugreifen kann. Medienarchive, die bislang ausschließlich für journalistische Zwecke genutzt wurden, öffnen ihre riesigen Datensammlungen zunehmend auch für medienfremde Nutzer. Im Hinblick auf diese Entwicklung muß die Reichweite des datenschutzrechtlichen „Medienprivilegs“ neu bestimmt werden, das Presseunternehmen bisher weitgehend von datenschutzrechtlichen Verpflichtungen freistellt. Mindestens ist eine gesetzliche Klarstellung erforderlich, daß die geschäftsmäßige Verwendung personenbezogener Daten – z. B. durch kommerzielle Pressedatenbanken – außerhalb des eigentlichen Medienbereiches nicht unter das Medienprivileg fällt.

Der Ausbau *Interaktiver Dienste und anderer neuer digitaler Kommunikationsformen* kann zu einer Gefährdung der Persönlichkeitsrechte der Nutzer führen. Bei der Gestaltung dieser Dienste sollten Techniken zum Einsatz kommen, bei denen personenbezogene Verbindungs- und Nutzungsdaten gar nicht erst entstehen. Von besonderer Bedeutung sind hier anonyme Zahlverfahren.

Auch die *Rechte der Betroffenen gegenüber den Medien* bedürfen einer Verbesserung. Während ein Betroffener, der durch die Berichterstattung von Rundfunkveranstaltern in seinem Persönlichkeitsrecht beeinträchtigt wird, in den meisten Fällen nach der Publikation Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen kann, besteht gegenüber der Presse bisher kein entsprechendes Auskunftsrecht. Im Gegensatz zu den Rundfunkveranstaltern sind

68 vgl. Anlage 3.6
69 Empfehlung Nr. R (95) 4
70 Empfehlung R. (95) 13

71 Privacy and the NII:Safeguarding Telecommunikations-Related Personal Information, U.S. Dep. of Commerce, Oktober 1995
72 Justice Potter Stewart in seiner abweichenden Meinung in Smith v. Maryland, 442 U.S. 735, 748 (1979)

Presseunternehmen auch nicht verpflichtet, etwaige Gegendarstellungen zu den gespeicherten Daten zu nehmen, auf die sie sich beziehen (Mitspeicherungspflicht). Da ein sachlicher Grund für diese unterschiedliche Behandlung der Betroffenen nicht erkennbar ist, sollte das Presserecht insofern dem bestehenden Rundfunkrecht angeglichen werden. Darüber hinaus sollte den Betroffenen gegenüber Pressedatenbanken, die nicht nur dem eigenen internen Gebrauch dienen, ein Auskunftsrecht bezüglich des zu seiner Person gespeicherten, veröffentlichten Materials eingeräumt werden.

Auch personenbezogene Veröffentlichungen, die im Rahmen der Öffentlichkeitsarbeit der Behörden erfolgen, können das Recht auf informationelle Selbstbestimmung erheblich beeinträchtigen. Mindestens bei der Weitergabe von Daten aus Strafermittlungsverfahren an die Medien sollte daher besonders zurückhaltend verfahren werden. Gleichzeitig müssen für den Umfang des Anspruchs der Medien auf Weitergabe personenbezogener Daten durch Behörden gesetzliche Regelungen geschaffen werden, die den Behörden eine Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und der Freiheit der Berichterstattung durch Rundfunk und Presse besser als bisher ermöglichen.

Der ausführliche Bericht des Arbeitskreises Medien an die Konferenz der Datenschutzbeauftragten wird demnächst im Rahmen der Reihe „Materialien zum Datenschutz“ des Berliner Datenschutzbeauftragten veröffentlicht werden. Die Broschüre kann beim Berliner Datenschutzbeauftragten kostenlos bezogen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer Sitzung am 9./10. März 1995 eine Entschließung zu Anforderungen an den Persönlichkeitsschutz im Medienbereich gefaßt.[72 a] Dabei sind die Datenschutzbeauftragten auch den in jüngster Zeit zunehmend erhobenen Forderungen nach einer Aufhebung des Verbots der *Hörfunk- und Fernsehberichterstattung aus Gerichtsverhandlungen* entgegengetreten. Mit unserer Verfassung wäre es unvereinbar, wenn Strafverfahren vor deutschen Gerichten nach dem Vorbild des Simpson-Prozesses in den USA den Charakter eines *massenmedial vermittelten Prangers* annehmen würden. Die herkömmliche Öffentlichkeit von Gerichtsverfahren, bei der Zuschauer im Saal der Verhandlung oder Interessierte der indirekten Berichterstattung durch Journalisten in den Medien folgen können, ist etwas qualitativ anderes als die Wiedergabe jeder einzelnen Bewegung und sichtbaren Gefühlsregung des Angeklagten durch Fernsehkameras.

Datenschutz beim Bildschirmtext (T-Online)

Der Bildschirmtext-Dienst der Deutschen Telekom (zwischenzeitlich „Datex-J“ genannt) wird jetzt unter dem neuen Namen „T-Online“ angeboten und gewinnt in letzter Zeit gerade deshalb immer mehr Kunden, weil er – wie die meisten Online-Dienste – einen Zugang zum Internet ermöglicht. Die Deutsche Telekom hat als Trägerin dieses Dienstes inzwischen eine eigene Betreibergesellschaft, die T-Online GmbH, gegründet.

> *Bereits seit den achtziger Jahren wird im Bildschirmtext-Dienst von einem privaten Verein über das Verkehrsamt Berlin ein Programm mit der Bezeichnung „Berliner Bettenbörse“ auf einem externen Rechner des Vereins angeboten. Das Angebot enthält Angaben über freie Zimmer in Berliner Hotels, die nach Preis und Ausstattung in verschiedene Kategorien eingeteilt sind. Die Zimmer können über das System gebucht werden. Das bloße „Blättern“ in dem entsprechendem Datenbestand ist kostenfrei, die Buchungen hingegen gebührenpflichtig.*

Das Angebot war durch den Anbieter derart ausgestaltet worden, daß personenbezogene Daten der Interessenten bereits mit dem Zugang zum externen Rechner – das heißt, noch bevor eine gebührenpflichtige Buchung ausgelöst wurde – erhoben wurden. Dagegen gestattet Artikel 9 Abs. 6 Satz 1 des Btx-Staatsvertrages[73] die Erhebung und Speicherung personenbezogener Daten nur, soweit dies für die Erbringung einer Leistung, den Abschluß oder die Abwicklung eines Vertragsverhältnisses erforderlich ist. Allein aus der Tatsache, daß ein externer Rechner angewählt wird, kann jedoch nicht auf das Zustandekommen eines Vertrags geschlossen werden, da es durchaus denkbar ist, daß der anwählende Teilnehmer sich lediglich einen Überblick über das Angebot verschaffen will. Eine Erhebung personenbezogener Daten bereits in diesem Stadium ist daher nach dem Btx-Staatsvertrag unzulässig.

Die seinerzeit für die Kontrolle des Datenschutzes beim Bildschirmtext zuständige Senatsverwaltung für Inneres untersagte dem Anbieter mit Bescheid vom 15. August 1989, personenbezogene Daten von Teilnehmern bereits auf der Zugangsseite des externen Rechners abzufragen. Gegen diesen Bescheid erhob der Anbieter Klage vor dem Verwaltungsgericht. Der Rechtsstreit ist erst im zurückliegenden Berichtszeitraum rechtskräftig entschieden worden. Das Oberverwaltungsgericht Berlin hat die Berufung des Anbieters zurückgewiesen und die Rechtsauffassung der Senatsverwaltung für Inneres und des Berliner Datenschutzbeauftragten insoweit bestätigt.[74]

Die begehrten Höreradressen

> *Ein Berliner Privatsender hatte im Berichtszeitraum bei einem Marktforschungsinstitut eine Umfrage zur Bewertung des Hörfunkprogramms durch Berliner Bürger in Auftrag gegeben. In diesem Zusammenhang hatte sich ein Petent an uns gewandt und um datenschutzrechtliche Überprüfung gebeten.*
>
> *Auf dem Begleitbogen und der Antwortkarte fehlte der Hinweis auf die Freiwilligkeit der Umfrage. Unklar blieb für den Bürger auch, in wessen Auftrag das Marktforschungsinstitut die Umfrage durchgeführt hat. Darüber hinaus war nicht transparent, wie mit den personenbezogenen Daten weiter verfahren werden sollte.*

Die Stellungnahme des Senders ergab, daß neben der Erhebung von anonymen Zahlen zu Hörgewohnheiten auch diejenigen Hörer, die unter Angabe ihrer Adresse geantwortet hatten, in eine Marketing-Datei des Senders für spätere Werbung aufgenommen werden sollten. Eine solche Verarbeitung personenbezogener Daten ist nur mit Einwilligung der Betroffenen möglich. Dies ist den Hörern allerdings nicht hinreichend klar gemacht worden. Ich habe insoweit im Einvernehmen mit dem brandenburgischen Landesbeauftragten für den Datenschutz einen datenschutzrechtlichen Mangel festgestellt. Der Sender hat sich bereit erklärt, all diejenigen Hörer, die unter Angabe ihrer Adresse an der Umfrage teilgenommen haben, erneut anzuschreiben und um Einverständnis für die Aufnahme in die Marketing-Datei zu bitten. Die Daten der Hörer, die diese Anfrage nicht positiv beantworten, werden umgehend gelöscht. Darüber hinaus habe ich angeregt, auf der Antwortkarte unmißverständlich klarzustellen, daß die Daten nicht an Dritte weitergegeben werden und daß die Betroffenen jederzeit die Löschung ihrer Daten veranlassen können. Auch dieser Empfehlung ist der Sender gefolgt.

5. Aus den Geschäftsbereichen der Verwaltung

5.1 Senatskanzlei

Geheimniskrämerei um den Verdienstorden der Bundesrepublik Deutschland oder: Der gläserne Ordensempfänger

> *Jeder kann einen Vorschlag machen, wem der Verdienstorden der Bundesrepublik Deutschland – insbesondere das **Bundesverdienstkreuz** – vom Bundespräsidenten verliehen werden sollte. Diese Vorschläge werden in Berlin von der Senatskanzlei als zuständiger Ordensbehörde gesammelt und überprüft. Vor einer Weiterleitung der Vorschläge werden umfangreiche **Ermittlungen über die vorgeschlagenen Personen** angestellt, insbesondere werden unbeschränkte Auskünfte beim Bundeszentralregister über etwaige Vorstrafen, Auskünfte beim Polizeipräsidenten über laufende Ermittlungsverfahren, die im Informationssystem Verbrechensbekämpfung gespeichert sind, sowie Auskünfte beim Bundesarchiv über mögliche belastende Informatio-*

72 a vgl. Anlage 2.5

73 Die Angabe bezieht sich auf die im Jahre 1989 gültige Fassung des Btx-Stv, jetzt: Art. 10 Abs. 6 Satz 1 Btx-Stv 1991

74 Urteil v. 19. 4. 1995 (OVG 7 B 33.92)

nen im ehemaligen Berlin Document Center aus der Zeit des Nationalsozialismus eingeholt. Diese Ermittlungen werden ohne Wissen und ohne Einwilligung des Vorgeschlagenen angestellt.

Die Senatskanzlei, die bisher in dieser Weise verfahren war, bekam Zweifel an der datenschutzrechtlichen Zulässigkeit dieser Vorgehensweise und wandte sich an uns mit der Bitte um Rat. Dabei wies sie zusätzlich darauf hin, daß auch überlegt werde, ob bei der Vorprüfung von Ordensvorschlägen Auskünfte beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR, bei den Verfassungsschutzämtern des Landes und des Bundes, beim Militärischen Abschirmdienst und beim Bundesnachrichtendienst eingeholt werden könnten.

Das *Bundesgesetz über Titel, Orden und Ehrenzeichen* enthält selbst keinerlei Bestimmungen über die Erhebung und weitere Verarbeitung personenbezogener Daten. Bei der Durchführung von Bundesgesetzen durch die Berliner Landesverwaltung sind in derartigen Fällen die einschlägigen Bestimmungen des Bundesdatenschutzgesetzes zur Lückenschließung heranzuziehen. Grundsätzlich sind personenbezogene Daten danach beim Betroffenen zu erheben. Ausnahmen von diesem Grundsatz läßt das Bundesdatenschutzgesetz nur zu, wenn entweder eine Rechtsvorschrift die Datenerhebung ohne Mitwirkung des Betroffenen zwingend voraussetzt oder die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen erforderlich macht und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Das Gesetz über Titel, Orden und Ehrenzeichen sieht weder die *Datenerhebung ohne Mitwirkung des Betroffenen* ausdrücklich vor, noch setzt es sie zwingend voraus. Man kann sich zwar auf den Standpunkt stellen, daß die zu erfüllende Verwaltungsaufgabe (Vorbereitung einer Ordensverleihung) ihrer Art nach eine Erhebung bei anderen Personen erforderlich macht, weil der vorgeschlagene Bürger sich möglicherweise in einem zu positivem Licht darstellt. Sehr zweifelhaft ist aber, ob nicht überwiegende schutzwürdige Interessen des Betroffenen durch diese Form der Datenerhebung beeinträchtigt werden. Diese Frage läßt sich nicht pauschal, sondern nur bezogen auf die Art der Informationen beantworten, die die Ordensbehörde bei dritten Stellen erhebt. Genauer gesagt: Es hängt im Einzelfall davon ab, welche Daten im Bundeszentralregister oder beim Polizeipräsidenten über den vorgeschlagenen Bürger gespeichert sind, ob durch die Übermittlung dieser Daten an die Ordensbehörde schutzwürdige Belange des Betroffenen beeinträchtigt werden. Letztlich kann nur der Betroffene selbst entscheiden, ob seine Daten der Ordensbehörde zur Verfügung gestellt werden sollen, nachdem er von diesen Daten Kenntnis erhalten hat. Die Senatskanzlei ist damit nicht berechtigt, hinter seinem Rücken Informationen zur Vorbereitung eines Ordensvorschlages zu erheben.

Zusätzlich zur – fehlenden – Erhebungsbefugnis der Ordensbehörde müßte außerdem immer auch eine korrespondierende *Übermittlungsbefugnis* der datenverarbeitenden Stelle vorliegen, bei der die Ordensbehörde Auskünfte einholen will.

Die Ausführungsbestimmungen zum Statut des Verdienstordens der Bundesrepublik Deutschland sehen vor, daß nur eine Verurteilung wegen eines Verbrechens eine Auszeichnung mit dem Verdienstorden generell ausschließt, eine Verurteilung wegen eines Vergehens jedoch lediglich unter bestimmten Voraussetzungen. Diesen Bestimmungen ist nicht zu entnehmen, daß andere gerichtliche Entscheidungen und Entscheidungen von Verwaltungsbehörden (z. B. Ausweisungen, Paßversagungen und -entziehungen), die ebenfalls im Bundeszentralregister eingetragen sind, Einfluß auf die Auszeichnung haben können. Die bisher übliche Einholung einer *unbeschränkten Auskunft aus dem Bundeszentralregister* ist deshalb unverhältnismäßig. Sie sollte – auch mit Einwilligung des Vorgeschlagenen – in Zukunft auf Verurteilungen wegen Verbrechen und Vergehen beschränkt werden.

Auch die Polizei hat keine gesetzliche Befugnis, ohne Einwilligung des Betroffenen über laufende Ermittlungsverfahren der Ordensbehörde Auskünfte zu erteilen. Über Informationen, die nach den Ausführungsbestimmungen zum Statut des Verdienstordens einer Auszeichnung entgegenstehen könnten, verfügt die Polizei nicht. Eine Information über laufende Ermittlungsverfahren gegen eine für die Auszeichnung vorgeschlagene Person ist auch nicht zur Abwehr erheblicher Nachteile für das Gemeinwohl erforderlich.

Eine Einholung von Auskünften bei der Polizei über etwaige laufende Ermittlungsverfahren gegen Personen, die für eine Auszeichnung vorgeschlagen worden sind, verstieße auch gegen die *Unschuldsvermutung* nach der Europäischen Menschenrechtskonvention. Es ist zwar nicht zu bestreiten, daß die Öffentlichkeit mit Unverständnis reagieren könnte, wenn rechtskräftige Verurteilungen eines mit dem Verdienstorden ausgezeichneten Bürgers später in der Öffentlichkeit bekannt würden. Diese Gefahr besteht jedoch auch dann, wenn zum Zeitpunkt der Ordensverleihung nicht einmal ein Ermittlungsverfahren eingeleitet worden ist oder der Betroffene erst später straffällig wird.

Auch das *Bundesarchivgesetz*, das auf die früher unter amerikanischer Hoheit stehenden Unterlagen des *Berlin Document Center* anzuwenden ist, läßt Auskünfte zur Prüfung der Ordenswürdigkeit nur in engen Grenzen zu. Insgesamt ist die Anwendung des Bundesarchivgesetzes auf Auskünfte aus dem Document Center nicht befriedigend, weil dieses Gesetz nur die Verwendung von Unterlagen für Forschungszwecke, nicht aber für Zwecke des Verwaltungsvollzuges regeln soll. Wir haben deshalb angeregt, auf Bundesebene die Ergänzung des Bundesarchivgesetzes um eine spezielle Vorschrift zur Nutzung der Unterlagen des Document Center für Verwaltungszwecke vorzuschlagen.

Schließlich enthalten weder das Stasi-Unterlagen-Gesetz noch die gesetzlichen Grundlagen für die Verfassungsschutzämter des Bundes und des Landes Berlin, des Militärischen Abschirmdienstes und des Bundesnachrichtendienstes Befugnisse zur Auskunftserteilung an Ordensbehörden.

Die Senatskanzlei hat zunächst – unserem Vorschlag entsprechend – die Einwilligung von Bürgern, die für den Verdienstorden der Bundesrepublik Deutschland vorgeschlagen wurden, in eine Überprüfung durch Einholung von Auskünften bei dem Landeseinwohneramt, dem Bundeszentralregister und dem Polizeipräsidenten in Berlin eingeholt. Wer diese Einwilligung verweigerte, kam für einen Vorschlag des Regierenden Bürgermeisters zur Verleihung des Verdienstordens nicht in Betracht. Hierauf wurde er ausdrücklich hingewiesen. Dieses Verfahren ist datenschutzgerecht.

Nach etwa einem halben Jahr teilte uns die Senatskanzlei allerdings mit, sie sehe sich durch Stellungnahmen des Bundespräsidialamtes und des Bundesministeriums des Innern, die mit dem Bundesministerium der Justiz abgestimmt worden sei, daran gehindert, weiterhin die Einwilligung des vorgeschlagenen Bürgers einzuholen, und werde deshalb zum bisherigen Verfahren der Überprüfung ohne Beteiligung der vorgeschlagenen Person zurückkehren.

Das Bundesministerium des Innern war der Auffassung des Bundesbeauftragten für den Datenschutz entgegengetreten, der eine bereichsspezifische Ergänzung des Gesetzes über Titel, Orden und Ehrenzeichen empfohlen hatte, um das bisherige Überprüfungsverfahren auf eine datenschutzgerechte Grundlage zu stellen. Dabei vertrat das Bundesministerium des Innern die erstaunliche Auffassung, die Ordensverleihung sei eine Aufgabe, die ihrer Art nach Vertraulichkeit auch bereits hinsichtlich der Einleitung des Verfahrens auf Prüfung der Ordenswürdigkeit erfordere. Würde man den Betroffenen vor Prüfung seiner Ordenswürdigkeit über den Vorgang informieren und seine Einwilligung einholen, hätte dies zur Folge, daß die notwendige Vertraulichkeit nicht mehr gewahrt würde und beim Betroffenen „eine konkrete Erwartungshaltung geweckt würde“. Die vorgeschlagene Person müsse insoweit Einschränkungen ihres informationellen Selbstbestimmungsrechtes im überwiegenden Allgemeininteresse hinnehmen. In die erforderliche Abwägung sei auch einzubeziehen, zu welchen Zwecken Angaben verlangt werden und welche Verknüpfungs- und Verwendungsmöglichkeiten bestehen. Die Vergabe von Orden erfolge als Anerkennung besonderer Verdienste für das Gemeinwohl. Die Datenerhebung diene also ausschließlich der *„Vorbereitung eines Gunsterweises“*. Daher bestünden keine Anhaltspunkte dafür, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt würden.

Das Bundesinnenministerium ging noch einen Schritt weiter und äußerte sich auch zu der Frage, ob der vorgeschlagene Bürger einen *Auskunftsanspruch* gegen das Bundespräsidialamt über die zu seiner Person gespeicherten Daten habe. Es lehnte diesen Auskunftsanspruch mit der schwer nachzuvollziehenden Begründung ab, die ordnungsgemäße Erfüllung der Aufgaben der Ordnungsbehörden würde durch die Auskunftserteilung gefährdet. Nur wenn darauf vertraut werden könne, daß Angaben in Ordensangelegenheiten vertraulich behandelt und nicht offenbart würden, seien offene und umfassende Auskünfte über den Vorgeschlagenen zu erwarten, ohne die die Ordenswürdigkeit nicht beurteilt werden kann.

Wir haben der Senatskanzlei mitgeteilt, daß das Bundesinnenministerium bei seiner Bewertung völlig übersehen hat, daß bei der Vorprüfung in Ordensangelegenheiten höchst sensible Informationen über den Betroffenen zusammengezogen werden, die möglicherweise fehlerhaft oder veraltet sind. Allein dieser Umstand führt zu einer schwerwiegenden Beeinträchtigung der schutzwürdigen Belange des Betroffenen, unabhängig davon, ob es später zu einem Vorschlag oder sogar zu einer Ordensverleihung kommt. Völlig unvertretbar ist insbesondere die Auffassung des Bundesinnenministeriums, der Betroffene habe noch nicht einmal ein Auskunftsrecht gegenüber dem Bundespräsidialamt über die zu seiner Person dort gespeicherten Daten. Daß durch eine Auskunftserteilung an den Betroffenen die ordnungsgemäße Erfüllung der Aufgaben der Ordensbehörden gefährdet werden sollen, ist in keiner Weise nachvollziehbar. Wir verkennen nicht, daß Ordensverleihungen wesentlich darauf beruhen, daß Vorschläge von Dritten gemacht und glaubwürdige Beurteilungen des Betroffenen bei Dritten eingeholt werden können. Diese Überlegung rechtfertigt es jedoch nicht, zum Zwecke der Ordensverleihung *geheime Dossiers* über den Betroffenen zu erstellen, von deren Inhalt dieser auch auf Verlangen keine Kenntnis erhält. Statt eines „Gunsterweises" wird das Verfahren der Ordensverleihung dadurch insgesamt zu einer massiven Beeinträchtigung des informationellen Selbstbestimmungsrechts derjenigen Personen, deren Vorschlagswürdigkeit die Senatskanzlei überprüft. Die Senatskanzlei hat sich unseren Rechtsstandpunkt zu eigen gemacht und ihn dem Bundesministerium des Innern und dem Bundespräsidialamt mitgeteilt. Inzwischen teilt auch das Bundesministerium der Justiz die Auffassung der Datenschutzbeauftragten, daß die gegenwärtige Rechtslage unzureichend ist. Gegenwärtig wird versucht, eine datenschutzgerechte Lösung zu finden. Jetzt schon gilt: In einem republikanischen Staatswesen darf das Verfahren zur Ordensverleihung nicht länger geheim betrieben werden.

Begnadigung von Straftätern

Eine Boulevardzeitung berichtete darüber, daß der Senat nach kontroverser Diskussion es abgelehnt habe, einen zu lebenslänglicher Haft verurteilten Straftäter zu begnadigen. In dem Artikel wurden Einzelheiten über den betroffenen Strafgefangenen und die Opfer seiner 20 Jahre zurückliegenden Straftat in teilweise personenbezogener Form genannt.

Wir haben den Vorfall zum Anlaß genommen, das *Verfahren in Gnadensachen* datenschutzrechtlich zu überprüfen. Nach der Verfassung von Berlin übt der Senat das Recht der Begnadigung aus (Art. 81). Er hat in bestimmten gesetzlich geregelten Fällen den vom Abgeordnetenhaus gewählten *Ausschuß für Gnadensachen* zu hören. Bei Verurteilungen zu lebenslanger Freiheitsstrafe und Sicherungsverwahrung liegt die Gnadenentscheidung stets beim Senat, im übrigen ist sie auf die Senatorin für Justiz übertragen. Will diese bei ihrer Entscheidung von der Stellungnahme des Gnadenausschusses abweichen, so ist wiederum die Entscheidung des Senats herbeizuführen.

Senatsvorlagen in Gnadensachen werden vertraulich außerhalb der Tagesordnung behandelt. Die Vorlagen betreffend Gnadensachen wurden bisher in personenbezogener Form den einzelnen Senatsmitgliedern im verschlossenen Umschlag und in der Senatskanzlei zusammen mit dem übrigen Sitzungsmaterial allen an der Vorbereitung einer Senatssitzung beteiligten Stellen zugeleitet. Nach der Entscheidung im Senat wurde der entsprechende Beschluß in das förmliche *Protokoll über die Senatssitzung* aufgenommen.

Es konnte nicht festgestellt werden, auf welche Weise in dem beschriebenen Fall Informationen an die Presse gelangt waren. Auf Vorschlag der Senatorin für Justiz hat der Senat allerdings aus diesem Anlaß beschlossen, das Verfahren in Gnadensachen in Zukunft so zu ändern, daß Vorlagen der Senatsverwaltung für Justiz künftig nur noch *anonymisiert*, d. h. ohne Nennung des Namens und des Geburtsdatums des Betroffenen, in den Senat einzubringen sind. Nur der Regierende Bürgermeister wird auf seinen Wunsch ein Exemplar der Senatsvorlage mit vollständigen Personalangaben verschlossen erhalten. Ferner soll die Anzahl der Exemplare verringert werden. Schließlich wird von der Aufnahme des Wortlauts der Senatsentscheidung in das Senatsprotokoll zukünftig abgesehen; statt dessen wird lediglich ein (nachrichtlicher) Hinweis in das Protokoll aufgenommen, daß der Senat über die Gnadensache „Aktenzeichen . . ." entschieden hat.

Der Regierende Bürgermeister hat zudem öffentlich erklären lassen, er lege Wert darauf, daß auch weiter die Behandlung der Gnadensachen nicht durch Indiskretionen aus dem Senat und reißerische Darstellungen in der Öffentlichkeit gestört wird.

Auch wenn die praktische Verfahrensweise in Gnadensachen im Anschluß an diesen Vorfall aus Sicht des Datenschutzes deutlich verbessert worden ist, bleibt festzustellen, daß die vorhandenen Regelungen über Gnadenentscheidungen (Gesetz über den Ausschuß für Gnadensachen vom 19. Dezember 1968[75], die Anordnung des Senats vom 29. September 1987 über die Ausübung des Begnadigungsrechts[76] und die von der Senatorin für Justiz erlassene Gnadenordnung vom 23. Juli 1990[77] in datenschutzrechtlicher Hinsicht unzureichend sind.

Sicherheitsüberprüfungen – Rechtsgrundlage fehlt noch immer

Das Fehlen hinreichender Rechtsvorschriften für die Durchführung der Sicherheitsüberprüfung ist derzeit der bedeutendste Mangel der Berliner Gesetzgebung.[78] Es war deshalb zu begrüßen, daß gegen Ende der Legislaturperiode endlich der Entwurf eines „Gesetzes über den Geheim- und personellen Sabotageschutz im Land Berlin – *Geheimschutzgesetz* –" vorlag. Allerdings wies der Gesetzentwurf erhebliche datenschutzrechtliche Defizite auf, wobei die weitgehende Anlehnung an das Sicherheitsüberprüfungsgesetz des Bundes (SÜG-Bund) datenschutzfreundlichere Detailregelungen auf Landesebene nicht ausschließt.

So wird der von Sicherheitsüberprüfungen *betroffene Personenkreis* sehr weit gefaßt. Angesichts der sichernden Verfahrensregelungen beim Umgang mit Verschlußsachen sollten hiervon nicht Personen erfaßt werden, bei denen nur die Möglichkeit besteht, daß sie sich Zugang zu Verschlußsachen verschaffen können.

Soweit Sicherheitsüberprüfungen zum Schutz von *„lebens- oder verteidigungswichtigen Einrichtungen"* vorgesehen sind, dürfen sie nur Personen betreffen, die dort an „sicherheitsempfindlichen Stellen" tätig sind. Die Datenschutzkonferenz hat hierzu gefordert, daß Sicherheitsüberprüfungen auf die Bereiche beschränkt bleiben müssen, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß.[79] Es muß konkreter gefaßt werden, was „lebens- und verteidigungswichtige Einrichtungen" sind, und die betroffenen öffentlichen oder privaten Einrichtungen sollten in einer Rechtsverordnung bestimmt werden.[80] Nur so ist für die betroffenen Mitarbeiter erkennbar, unter welchen Voraussetzungen sie von diesen erheblich in ihr Persönlichkeitsrecht eingreifenden Maßnahmen betroffen werden können.

Es ist für den Betroffenen nicht hinreichend erkennbar, mit welcher Verarbeitung welcher Daten er im Zusammenhang mit der Sicherheitsüberprüfung konkret zu rechnen hat. Nach dem Wortlaut des Gesetzentwurfes wäre nicht ausgeschlossen, daß medizinische Daten, die Vermögensverhältnisse, sexuelles Verhalten und andere sensible Angaben aus seiner Privat- und Intimsphäre erfaßt werden. Es muß sichergestellt werden, daß die Erkenntnisgewinnung für die Sicherheitsüberprüfung nicht in die

75 GVBl. S.1767; zuletzt geändert durch Gesetz vom 11. Januar 1979, GVBl. S. 58
76 Senatsbeschluß Nr. 2265.87
77 Amtsblatt 1990, S. 1660
78 Jahresbericht 1994, 4.1
79 vgl. Anlage 2.2
80 vgl. Sicherheitsüberprüfungsgesetz Nordrhein-Westfalen – SÜG NRW – vom 7. März 1995, GVBl. S. 210

Kernbereiche des Rechtes auf informationelle Selbstbestimmung eingreift. Zu begrüßen ist, daß Informationen über persönliche, dienstliche und arbeitsrechtliche Verhältnisse der Betroffenen zur Sicherheitsakte nur zu nehmen sind, soweit sie für die sicherheitsmäßige Beurteilung erforderlich sind. Im Hinblick auf die Erfahrungen anderer Datenschutzbeauftragter, die eine „große Sammelwut der Landesämter für Verfassungsschutz" festgestellt haben, ist der Beachtung des *Erforderlichkeitsgrundsatzes* bei der Speicherung personenbezogener Daten besondere Bedeutung beizumessen.

Es sollte klargestellt werden, welcher Art die tatsächlichen Anhaltspunkte für ein *Sicherheitsrisiko beim Ehegatten oder Lebenspartner* sein müssen. Wie ursprünglich im Sicherheitsüberprüfungsgesetz des Bundes vorgesehen, sollte das Vorliegen eines Sicherheitsrisikos bei diesen Personen auf besondere Gefährdungen wegen Anbahnungs- oder Werbungsversuchen fremder Nachrichtendienste beschränkt werden.

Der Ehegatte, Lebenspartner oder Referenzpersonen sind vor Erteilung ihrer Einwilligung darüber aufzuklären, daß auch bei einfachen Sicherheitsüberprüfungen Datenabfragen zu ihrer Person bei anderen Landesämtern und dem Bundesamt für Verfassungsschutz erfolgen. Auch weitere Überprüfungsmaßnahmen des Ehegatten oder Lebenspartners dürfen nur mit ihrer Zustimmung erfolgen und wenn sich aus der Sicherheitserklärung oder aufgrund der Abfrage im nachrichtendienstlichen Informationssystem NADIS sicherheitserhebliche Erkenntnisse ergeben.[81]

Die *Befragung Dritter* soll bereits möglich sein, wenn „die Erhebung beim Betroffenen nicht ausreicht". Durch diese großzügige Möglichkeit der Ausdehnung der Befragungen können die Grenzen zwischen den einzelnen Stufen der Sicherheitsüberprüfung zerfließen und die Dreiteiligkeit der Prüfungsstufen, mit der dem Grundsatz der Verhältnismäßigkeit Rechnung getragen werden soll, ins Leere laufen.

Die im Vorentwurf noch vorgesehene Zustimmung des Betroffenen zu der Befragung Dritter ist leider wieder entfallen. Damit büßt die Sicherheitsüberprüfung, die schließlich nur mit Kenntnis und Einwilligung des Betroffenen in alle zu ergreifenden Maßnahmen erfolgen soll, erheblich an Transparenz ein.[82] Für den Betroffenen bleibt unklar, welche Befragungen konkret bei „geeigneten Personen und Stellen" vorgenommen werden dürfen. Kriterien, nach denen diese Personen oder Stellen auszuwählen sind, fehlen.

Besonders bedenklich ist die *Nutzung* der im Rahmen der Sicherheitsüberprüfung *erlangten Daten für fast alle Aufgaben des Verfassungsschutzes.* Damit würde das Landesamt für Verfassungsschutz durch seine mitwirkende Tätigkeit bei der Sicherheitsüberprüfung in den Besitz von Daten gelangen, die es nach dem Verfassungsschutzgesetz in der Regel nicht hätte erheben dürfen.

Nicht nachvollziehbar ist auch, warum die Unterlagen über die Sicherheitsüberprüfung beim Landesamt für Verfassungsschutz doppelt so lange aufbewahrt werden sollen wie bei der Dienstbehörde. Beim Ausscheiden des Betroffenen aus der sicherheitsempfindlichen Tätigkeit bedeutet das eine *Aufbewahrungsfrist* von bis zu zehn Jahren beim Landesamt für Verfassungsschutz.

Auskunfts- und die *Akteneinsichtsrechte* des Betroffenen werden zu weitgehend eingeschränkt. Die Regelungen des Berliner Datenschutzgesetzes sollten uneingeschränkt Anwendung finden.

Wenn der Betroffene keine Auskunft erhält, muß zumindest ein uneingeschränktes Prüfungsrecht des Datenschutzbeauftragten bestehen. Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung seiner Daten unter den Bedingungen der automatisierten Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechtes auf informationelle Selbstbestimmung.[83] Nicht akzeptabel sind die vorgesehenen *Einschränkungen der Kontrollbefugnis* des Berliner Datenschutzbeauftragten. Die Möglichkeit, nur eine persönliche Kontrolle zuzulassen, ist auch im Sicherheitsüberprüfungsgesetz des Bundes nicht für notwendig erachtet worden. Die weitere Einschränkung des Kontrollrechtes durch Widersprüche der Betroffenen sollte entfallen. Sie hat sich in der Anwendung als völlig unpraktikabel erwiesen und erschwert die datenschutzrechtlichen Querschnittsprüfungen nicht unerheblich.

Bei Sicherheitsüberprüfungen von *Mitarbeitern in Unternehmen* oder anderen privaten Organisationen ist die Befugnis zur Speicherung personenbezogener Daten in automatisierten Dateien auf die Daten der Betroffenen zu beschränken (vgl. § 31 SÜG-Bund). Die für entsprechend anwendbar erklärten *Aufbewahrungsfristen* des öffentlichen Dienstes sind für Privatunternehmen zu lang. Es ist nicht ersichtlich, warum Unternehmen für Mitarbeiter, die dort lange nicht mehr tätig sind oder die keine sicherheitsrelevante Tätigkeit aufgenommen haben, die Sicherheitsakten aufbewahren sollen. Zu den datenschutzrechtlichen Anforderungen, die bei Sicherheitsüberprüfungen in Unternehmen zu beachten sind, hat die Datenschutzkonferenz Mindestanforderungen formuliert.[84] Der Gesetzentwurf entspricht diesen Anforderungen in wesentlichen Punkten nicht.

Verwaltungsvorschriften – nur wenig Verbesserungen für den Datenschutz

Für die *Auswertungsbereiche* beim Landesamt für Verfassungsschutz wurde eine *Arbeitsanweisung* vorgelegt. Leider beschränkt sie sich darauf, die bestehende Praxis festzuschreiben, wonach Sachakten mit einer Fülle nicht erforderlicher personenbezogener Daten gefüllt werden.[85] Es wird nicht hinreichend berücksichtigt, daß es dem Wesen der Sachakte entspricht, daß der Anteil personenbezogener Daten möglichst gering gehalten wird. Sollen Informationen zu bestimmten Personen dennoch aufbewahrt werden, weil sie auch ohne Bezug zur Bestrebung eigene, verfassungsschutzrelevante Bedeutung haben, ist eine Akte zur Person anzulegen, die regelmäßig überprüft und insgesamt vernichtet werden kann, wenn sie nicht mehr erforderlich ist.

In *Sachakten* dürfen nur personenbezogene Daten aufgenommen werden, die für die Bestrebung als solche relevant sind. Dies ist bei Personen der Fall, die das Beobachtungsobjekt nachhaltig unterstützen (z. B. Personen, die Führungs- und Funktionärsaufgaben wahrnehmen). Nur diese Verhaltensweisen sind nach § 6 Abs. 1 Satz 2 Landesverfassungsschutzgesetz (LfVG) verfassungsschutzrelevant. Die Angaben müssen für die Beurteilung der Bestrebung erforderlich sein und dürfen nicht nur dazu dienen, die Persönlichkeit einzelner Verdächtiger zu umschreiben. Derartige Unterlagen stellen einen problematischen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar.

Eine *Arbeitsanweisung,* die u. a. Datenübermittlungen an *ausländische Nachrichtendienste* regelt, wurde in Kraft gesetzt. Einige unserer Empfehlungen wurden aufgegriffen. Erhebliche Bedenken bestehen aber noch gegen die Übermittlung sogenannter „weicher Daten" (Verdächtigungen, Denunziationen u. ä.). Sie sollten nicht an ausländische Stellen weitergegeben werden, da ihr Wahrheitsgehalt nicht nachprüfbar ist und dies zu erheblichen Eingriffen in das Persönlichkeitsrecht der Betroffenen führen kann.

Die Schranken für die Übermittlung personenbezogener Daten, die dem Landesamt für Verfassungsschutz aus einem *Asylverfahren* zur Kenntnis gelangen, sind enger zu fassen. Derartige Angaben dürfen weder direkt noch indirekt an Behörden, Sicherheitsdienststellen und sonstige ausländische Stellen weitergeleitet werden. Die Betroffenen offenbaren hier sehr sensible Daten in einer Schutz verdienenden Notlage. Dies gilt auch für Fälle, in denen konkrete Anhaltspunkte dafür bestehen, daß einem Betroffenen im Ausland rechtsstaatswidrige Behandlung (z. B. Folter) widerfährt. Nur in dem Ausnahmefall, wenn dies im Einzelfall zur Abwehr einer konkreten Gefahr für Leib oder Leben anderer Personen erforderlich ist, kann eine Datenübermittlung in diesen Fällen akzeptiert werden.

Wir hatten kritisiert, daß in der *Auskunftsanweisung* die Unterlagen, die von der Polizei an das Landesamt für Verfassungsschutz übermittelt worden sind, von der Akteneinsicht ausge-

81 vgl. § 13 Abs. 2 Satz 4 SÜG-Bund
82 Beschluß der Konferenz der Datenschutzbeauftragten vom 13. September 1985, Jahresbericht 1985, Anlage 4
83 BVerfGE 65, 1, 46
84 vgl. Anlage 2.2
85 vgl. Jahresbericht 1989, 2.1

nommen werden sollen.[86] Nachdem der Polizeipräsident nunmehr in Einzelfällen auch Akteneinsicht nach dem ASOG gewährt, wurde die von uns kritisierte Regelung in der Auskunftsanweisung gestrichen.

Kontrollfreier Raum

Die Einsichtnahme der *G 10-Kommission* in Abschriften von *Kontrollaufträgen des MfS* hatten wir zum Anlaß genommen, auf die bestehenden Kontrollücken beim Landesamt für Verfassungsschutz aufmerksam zu machen.[87]

Die Kontrollücken bestehen auch bei der Speicherung, Nutzung und Übermittlung personenbezogener Daten, die auf Maßnahmen beruhen, die von den *Westalliierten* vor der Wiedervereinigung Berlins vorgenommen wurden, und bei der weiteren Verwendung der durch *Telefonüberwachungen und Postkontrollen* vom Landesamt für Verfassungsschutz selbst erlangten personenbezogenen Daten.

Der Verfassungsschutzausschuß des Abgeordnetenhauses ist zwar unserer Empfehlung, besondere Kontrollkompetenzen für die G 10-Kommission vorzusehen, nicht gefolgt, hat aber für die Datenspeicherungen beim Landesamt für Verfassungsschutz aufgrund westalliierter Maßnahmen eine Nutzungssperre, die in einer Arbeitsanweisung festzulegen ist, gefordert.

Eine *Arbeitsanweisung über die Nutzung und Übermittlung von personenbezogenen Informationen, die erkennbar aus Maßnahmen der Telefonüberwachung oder Briefkontrolle vor dem 30. Oktober 1990 stammen,* wurde inzwischen vom Landesamt für Verfassungsschutz erlassen. Die Nutzungsbeschränkungen orientieren sich an den Vorschriften des G 10. Nicht geregelt wurde der Umgang mit den Daten, die aus anderen Maßnahmen der Alliierten stammen.

Das Landesamt für Verfassungsschutz hat in diesem Zusammenhang mitgeteilt, daß eine *Kontrollbefugnis auch des Berliner Datenschutzbeauftragten* nicht in Betracht komme. Da weder eine Kontrolle des Umganges mit diesen Daten durch eine andere unabhängige Stelle erfolgt, noch Betroffene Auskunft über diese Datenspeicherungen beim Verfassungsschutz erhalten, bleibt als Konsequenz nur die umgehende Löschung dieser Daten. Denn eine Speicherung, Nutzung und Weitergabe dieser sehr sensiblen Daten durch den Verfassungsschutz kann nur hingenommen werden, wenn als Korrektiv eine Kontrolle hierüber möglich ist.

Datenaustausch: Kein Hinderungsgrund für das Auskunftsrecht des Landesamtes für Verfassungsschutz

> *Eine Bürgerin hatte beim Landesamt für Verfassungsschutz Auskunft über die zu ihrer Person gespeicherten Daten und Einsicht in die vorhandenen Unterlagen beantragt. Das Landesamt für Verfassungsschutz teilte mit, daß ihre Daten in Dateien gespeichert seien und sie im Verdacht stehe, der linksextremistischen Szene anzugehören. Weitergehende Auskunft und Akteneinsicht wurden wegen überwiegender Geheimhaltungsinteressen abgelehnt.*

Unsere Prüfung hat ergeben, daß der Petentin nicht nur weitergehende Auskunft und Aktensicht zu erteilen sind, sondern die gesammelten Daten auch zu löschen sind. Die Unterlagen enthalten keine aktuellen verfassungsschutzrelevanten Informationen mehr und sind deshalb für die Aufgabenerfüllung nicht mehr erforderlich. Die Erkenntnisse stammen überwiegend aus öffentlich zugänglichen Quellen wie Zeitungsartikeln. Geheimhaltungsinteressen, die einer Akteneinsicht entgegenstehen, sind nicht erkennbar.

Das Landesamt für Verfassungsschutz ist unserer Einschätzung schließlich gefolgt und hat zugesagt, die Daten zu löschen und der Petentin vor der Löschung Einsichtnahme in die Unterlagen zu gewähren und ihr auch die in der Akte befindlichen *Presseartikel* vorzulegen.

Ein Problem waren die *Daten, die von einer anderen Stelle übermittelt wurden.* Das Landesamt für Verfassungsschutz erteilt mangels *„Verfügungsberechtigung“* hierüber grundsätzlich keine Auskunft.

Unser Vorschlag, bei der übermittelnden Stelle um Zustimmung zur Auskunftserteilung nachzusuchen, wenn die Petentin mit dieser Verfahrensweise einverstanden ist (denn es können dann Daten bei der übermittelnden Stelle anfallen, die dort längst gelöscht wurden), lehnte das Landesamt für Verfassungsschutz als undurchführbar ab: Es liege eine Auskunftssperre vor, so daß die Betroffene nicht einmal in allgemeiner Form unterrichtet werden könne. Ein Einverständnis mit der Verfahrensweise könne sie aber nur erteilen, wenn sie zuvor konkret über Art und Herkunft der Daten informiert werde. Später stellte das Landesamt für Verfassungsschutz fest, daß die Datenspeicherungen über die Betroffene bei der anderen Stelle nicht mehr vorhanden sind und kündigte an, aufgrund dieser Tatsache die Unterlagen, die von dort stammen, umgehend zu vernichten. Dies haben wir zunächst verhindert.

Bei dieser Vorgehensweise würde den Betroffenen jede Möglichkeit genommen werden, von derartigen Datenspeicherungen und -übermittlungen zu erfahren und sie gegebenenfalls überprüfen zu lassen. Dies widerspricht dem Recht auf informationelle Selbstbestimmung, dessen unmittelbarer Ausfluß das Auskunftsrecht ist.

Nach § 31 Abs. 1 Satz 2 LfVG erstreckt sich die Auskunftsverpflichtung nicht auf Informationen, die nicht der alleinigen Verfügungsberechtigung des Landesamtes für Verfassungsschutz unterliegen, sowie die Herkunft von Informationen.

Eine Auskunft durch das Landesamt für Verfassungsschutz wird hierdurch jedoch nicht ausgeschlossen. Zweck dieser Norm ist es, das möglicherweise bestehende Geheimhaltungsinteresse der übermittelnden Stelle zu gewährleisten. Dem ist hinreichend Rechnung getragen, wenn bei der übermittelnden Stelle um Zustimmung zur Auskunftserteilung nachgesucht wird. Dies wurde – mit Zustimmung des Betroffenen – in einem anderen Fall so praktiziert.

Wenn die Daten bei der übermittelnden Stelle bereits gelöscht, aber beim Landesamt für Verfassungsschutz noch vorhanden sind, kann das nicht dazu führen, daß das Auskunftsrecht des Betroffenen leerläuft, indem die Daten auch hier gelöscht werden.

Es gibt in diesem Fall folgende Möglichkeiten:

- Das Landesamt für Verfassungsschutz entscheidet eigenverantwortlich über die Auskunftserteilung, da die Verfügungsberechtigung über die Daten nach der Löschung bei der übermittelnden Stelle allein beim Landesamt für Verfassungsschutz liegt,

  oder

- das Landesamt für Verfassungsschutz sieht die übermittelnde Stelle nach wie vor als verfügungsberechtigt an und holt dort unter Mitteilung des Sachverhaltes die Zustimmung zur Auskunftserteilung ein, wenn der Betroffene hiermit einverstanden ist. In diesem Fall ist es auch möglich, eine Prüfung der Datenübermittlung und der Auskunftserteilung durch den für die übermittelnde Stelle zuständigen Datenschutzbeauftragten zu veranlassen.

Das Landesamt für Verfassungsschutz hat schließlich die übermittelnde Stelle um Freigabe der Daten gebeten. Nachdem diese eine Auskunft und Akteneinsicht abgelehnt hat, haben wir die zuständige Datenschutzkontrollbehörde eingeschaltet. Diese wird die Ablehnung überprüfen.

Wir gehen davon aus, daß künftig an dieser Verfahrensweise festgehalten wird und die Auskunftsrechte der Betroffenen auch bei übermittelten Daten gewährleistet werden.

86 Jahresbericht 1994, 4.1
87 Jahresbericht 1993, 4.5.2

5.2 Bau- und Wohnungswesen

Automatisierter Abruf und Datenübermittlung aus dem Liegenschaftskataster

Am 31. Dezember 1995 sind die Verordnungen über die Benutzung des Liegenschaftskatasters mit Hilfe automatisierter Abrufverfahren *(LikaAbrufVO)*[88] und über die Abgabe digitaler Angaben aus dem Liegenschaftskataster *(LikaAbgabeVO)*[89] in Kraft getreten. Damit sind – wenngleich mit einiger Verzögerung – alle im Artikelgesetz von 1993 enthaltenen Verpflichtungen zum Erlaß bereichsspezifischer Rechtsverordnungen erfüllt. Unsere Empfehlungen, die Datenempfänger bzw. Abrufberechtigten, die Übermittlungszwecke sowie die zu übermittelnden Daten im Verordnungstext möglichst konkret zu benennen und zu prüfen, ob stets die Angaben über die Eigentümer, Erbbauberechtigte und andere Personen bei der Übermittlung erforderlich sind,[90] wurden von der Senatsverwaltung für Bau- und Wohnungswesen im wesentlichen aufgegriffen und in den Rechtsverordnungen umgesetzt.

Für alle Behörden, sonstigen öffentlichen Stellen und Unternehmen – soweit sie öffentliche Aufgaben erfüllen – kann auf Antrag eine Erlaubnis für die *Einrichtung eines automatisierten Verfahrens zum Abruf von Flurstücks- und Gebäudeangaben* erteilt werden. Eine Erlaubnis für den Abruf von Eigentümerangaben kann dagegen nur für die in der Anlage zur Verordnung abschließend genannten Stellen für den dort bezeichneten Verwendungszweck erteilt werden. Weiter setzt die Erlaubnis zum *Abruf von Eigentümerdaten* voraus, daß die Einrichtung des Verfahrens unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen wegen der Vielzahl der voraussichtlichen Zugriffe oder wegen der besonderen Eilbedürftigkeit angemessen ist.[91] Eine ausführliche Protokollierung jedes Datenabrufes ist verbindlich festgeschrieben. Die Erlaubnis zur Einrichtung des automatisierten Abrufverfahrens ist zu widerrufen, wenn die erforderlichen Datenschutzmaßnahmen nach § 5 BlnDSG nicht getroffen werden.[92]

Für die *Abgabe von Daten aus dem Liegenschaftskataster auf maschinenlesbaren Datenträgern* ist ebenfalls ein differenziertes Verfahren, bei dem auf die Art der zu übermittelnden Daten abgestellt wird, vorgesehen. Danach dürfen Flurstücks- und Gebäudeangaben ohne weitere Voraussetzungen an pauschaliert benannte Stellen – auf deren Antrag – abgegeben werden. Demgegenüber dürfen auch hier Eigentümerangaben nur an die Betroffenen für die Verwaltung ihrer Liegenschaften sowie an die abschließend in der Anlage 1 zur LikaAbgabeVO genannten Stellen abgegeben werden. Auch der Kreis von Datenempfängern, an die die Eigentümerangaben zum Aufbau bzw. zur Aktualisierung von Informationssystemen abgegeben werden dürfen, ist abschließend bezeichnet.

Durch die Differenzierung der verschiedenen Datenarten entsprechend ihrer Sensibilität sowie die darauf abgestimmten unterschiedlichen Voraussetzungen für die Datenübermittlung wird dem Persönlichkeitsrecht der Betroffenen Rechnung getragen. Die konkrete und abschließende Auflistung der Datenempfänger und der Übermittlungszwecke in den Anlagen zu den Verordnungen schafft die erforderliche Transparenz.

Die beiden Rechtsverordnungen setzen die datenschutzrechtlichen Vorgaben vorbildlich um. Die Schaffung von Rechtsverordnungen in anderen Bereichen sollte sich an diesen Beispielen orientieren.

Datenschutzrechtliche Stellung der vom Land Berlin eingesetzten Sanierungsbeauftragten

Das Land Berlin setzt für Sanierungsgebiete nach § 157 Baugesetzbuch (BauGB) Sanierungsbeauftragte ein und beauftragt sie damit, die notwendigen städtebaulichen Sanierungsmaßnahmen vorzubereiten und durchzuführen. Zu beurteilen war, ob die dabei von den Sanierungsbeauftragten durchgeführte Verarbeitung von personenbezogenen Daten im Rahmen einer Auftragsdatenverarbeitung für die Senatsverwaltung für Bau- und Wohnungswesen oder in eigener Verantwortung erfolgt.

Den Sanierungsbeauftragten werden umfangreiche Aufgaben übertragen. Dazu zählen die Durchführung der vorbereitenden Untersuchungen und die Verhandlungen mit den Beteiligten.[93] Sie erörtern mit den Eigentümern, Mietern und sonstigen Sanierungsbetroffenen die erforderlichen baulichen Maßnahmen. Sie sind mit der Durchführung der erforderlichen Befragungen[94], den Vorarbeiten für das Sanierungskonzept[95] bis hin zur Entwicklung von Bebauungsplanentwürfen[96], der Erarbeitung und Fortschreibung des Sozialplanes[97] und der Durchführung von bestimmten Ordnungsmaßnahmen[98] befaßt. Ihre Grenzen findet die Übertragbarkeit der Aufgaben an den Sanierungsbeauftragten dort, wo hoheitliche Befugnisse des Landes Berlin betroffen sind. Eine derartig weitreichende Übertragung von Aufgaben der öffentlichen Verwaltung ist daher nicht mehr als *Auftragsdatenverarbeitung* i. S. d. § 3 BlnDSG anzusehen.

Die Senatsverwaltung für Bau- und Wohnungswesen hat sich dieser Auffassung angeschlossen und wird zukünftig in den mit den Sanierungsbeauftragten zu schließenden Verträgen klarstellen, daß die Sanierungsbeauftragten – soweit sie zur Erfüllung der ihnen übertragenen Aufgaben personenbezogene Daten verarbeiten – als eigenständige und -verantwortliche datenverarbeitende Stelle i. S. d. § 4 Abs. 3 Nr. 1 BlnDSG handeln. Sie haben die Bestimmungen des Berliner Datenschutzgesetzes zu beachten[99] und unterstehen der direkten Kontrolle des Berliner Datenschutzbeauftragten.

Bekämpfung der Zweckentfremdung von Wohnraum

Gegen einen Vermieter wurde vom Wohnungsamt wegen Wohnungsleerstands ermittelt. Als Nachweis für die Beseitigung des Leerstandes wurde er aufgefordert, Kopien der vollständigen Mietverträge an das Wohnungsamt zu übersenden. Beim Bezirkseinwohneramt hat das Wohnungsamt angefragt, ob die Mieter sich auch tatsächlich angemeldet haben, also der Wohnungsleerstand auch tatsächlich beseitigt wurde.

Von einem anderen Wohnungsamt wurde festgestellt, daß ein Petent seine Wohnung auch gleichzeitig als Geschäftssitz nutzt. Im Rahmen der Prüfung, ob eine Zweckentfremdung von Wohnraum vorlag, hat das Wohnungsamt den Petenten mehrfach vergeblich – allerdings unter der Meldeanschrift seiner von ihm getrennt lebenden Ehefrau – um Stellungnahme gebeten. Die vom Wohnungsamt durchgeführten Ermittlungen führten zu umfangreichen Datenspeicherungen zur Person des Petenten und weiterer unbeteiligter Dritter. In der zur Person des Petenten beim Wohnungsamt geführten Akte befanden sich u. a. ein Auszug aus dem Liegenschaftskataster mit Eigentümernachweisen für das gesamte Wohnhaus, ein Auszug aus dem Wohnungskataster, in dem – ebenfalls das gesamte Haus betreffend – eine Vielzahl von Daten Dritter enthalten war, Anfragen an das Bezirkseinwohneramt zur Klärung der Meldeverhältnisse des Petenten und seiner von ihm getrennt lebenden Ehefrau sowie ein Schriftwechsel mit der Deutschen Post AG über die vergebliche Zustellung von Poststücken an den Petenten unter der Adresse seiner Ehefrau.

In beiden Fällen haben wir einen Verstoß gegen datenschutzrechtliche Bestimmungen festgestellt.

Das Wohnungsamt darf zur Klärung eines bestimmten Sachverhaltes die in § 2 a *Zweckentfremdungsbeseitigungsgesetz* (ZwBesG) genannten personenbezogenen Daten (von Eigentümern, Verwaltern, beauftragten Rechtsanwälten, Mietern, sonstigen Wohnraumnutzern und Wohnungssuchenden, deren Familienname, Vorname, akademischen Grad, Telefonnummer, gegenwärtige Anschrift sowie die Anschrift, Lage, Fläche, Ausstattung und Nutzungsart der Wohnung) erheben, soweit dies zur Erfüllung der Aufgaben erforderlich ist.[100]

88 GVBl. S. 847 ff.
89 GVBl. S. 840 ff.
90 Jahresbericht 1994, 4.3
91 vgl. § 2 Abs. 2 Satz 2 LikaAbrufVO
92 vgl. § 5 Abs. 1 LikaAbrufVO
93 §§ 137, 139 BauGB
94 § 138 BauGB
95 § 140 Nr. 3 BauGB
96 § 140 Nr. 4 BauGB
97 § 140 Nr. 6 BauGB
98 § 147 BauGB
99 § 2 Abs. 1 Satz 2 BlnDSG
100 § 18 Abs. 1 ASOG

Dieser *Datenkatalog* ist abschließend. Die Erhebung und Speicherung darüber hinausgehender Daten (z. B. aus den Mietverträgen die Höhe der Mietkaution bzw. Miete sowie Geburtsdaten der Vertragspartner usw.) ist unzulässig. Die Daten sind grundsätzlich beim Betroffenen selbst und mit seiner Kenntnis zu erheben.[101] Eine Erhebung der Daten bei Dritten – ohne Kenntnis des Betroffenen – (z. B. aus dem Liegenschaftskataster und durch Anfragen beim Bezirkseinwohneramt) ist gemäß § 18 Abs. 4 Nr. 1 bis 3 ASOG nur zulässig, wenn sie beim Betroffenen selbst nicht oder nicht rechtzeitig möglich ist, einen unverhältnismäßig hohen Aufwand erfordern würde und schutzwürdige Belange des Betroffenen nicht entgegenstehen oder die Erfüllung der Aufgaben gefährden würde. Keine der genannten Tatbestandsalternativen lag hier vor.

Mit einer Umfrage in den Bezirken untersucht die Senatsverwaltung für Bau- und Wohnungswesen derzeit, inwieweit der Datenkatalog des § 2 a ZwBesG für die Aufgabenerfüllung der Wohnungsämter bei der Bekämpfung der Zweckentfremdung von Wohnraum ausreichend ist bzw. erweitert werden sollte.

Strafurteil für Bewilligung von Wohngeld

Ein Bürger, der zur Zeit als Freigänger eine Haftstrafe in einer Justizvollzugsanstalt verbüßt, hat einen Antrag auf Wohngeld für die von ihm zusammen mit seiner Verlobten bewohnte Wohnung gestellt. Er beschwert sich darüber, daß das Wohnungsamt die Übersendung seines Strafurteiles verlangt, obwohl er bereits eine Haftbescheinigung der Justizvollzugsanstalt vorgelegt hatte, aus der sich das voraussichtliche Haftende entnehmen läßt. Wir konnten zunächst klären, daß nicht das gesamte Strafurteil, sondern nur der Tenor, aus dem sich die Haftstrafe ergibt, für die Antragsbearbeitung vom Wohnungsamt für erforderlich gehalten wird.

Die Datenerhebung wird vom Wohnungsamt auf § 12 Abs. 4 Wohngeldsondergesetz gestützt. Das Wohnungsamt führt dazu aus, daß die Angabe der *Haftdauer* im Urteil erforderlich sei, um eine eventuell mißbräuchliche Inanspruchnahme von Wohngeld beurteilen zu können.

Das ist unzutreffend. Die vom Petenten vorgelegte Haftbescheinigung ist für diesen Zweck geeignet und ausreichend. Hier ist die konkrete Bemessung des Haftzeitraumes angegeben, während dieser im Strafurteil selbst nur abstrakt benannt ist. Die Formulierung in der Haftbescheinigung „in Haft vom . . . bis voraussichtlich . . .“ ist deshalb sachlich richtig und unvermeidbar, weil eine Haftverkürzung möglich ist. Eine Prognose über eine mögliche Aussetzung der Vollstreckung einer Freiheitsstrafe im vorhinein kann nicht abgegeben werden. Sie ist nach den Voraussetzungen der §§ 57, 57 a StGB zu einem späteren Zeitpunkt möglich, so daß die Angabe zur Haftdauer nur eine voraussichtliche sein kann.

Die Angabe der im Urteil aufgeführten Haftstrafe enthält demnach nicht ein Mehr an Informationen, es mangelt ihr vielmehr an der Aussage über den konkreten Haftbeginn. Das Urteil ist nicht geeignet für die hier zu treffende Entscheidung, und durfte zur Vorlage nicht verlangt werden.

Datenerhebungen für kommunales Vorkaufsrecht

Unter bestimmten Voraussetzungen stehen dem Land Berlin kommunale Vorkaufsrechte bei Grundstücksverkäufen zu.[102]

Ein Petent hat sich bei uns darüber beschwert, daß ein Bezirksamt von Berlin zur Durchführung des Verfahrens ohne Ausnahme die Vorlage vollständiger Urkundsabschriften der Kaufverträge verlangt, ohne zuvor geprüft und festgestellt zu haben, ob überhaupt ein kommunales Vorkaufsrecht in Betracht kommt.

Dieses Verfahren ist weder erforderlich noch verhältnismäßig.

Zwar hat nach § 28 Abs. 1 BauGB der Verkäufer eines Grundstückes der Gemeinde den Inhalt des Kaufvertrages unverzüglich mitzuteilen. Die Bestimmung ist restriktiv dahingehend auszulegen, daß nur die erforderlichen Inhaltsangaben des Kaufvertrages mitzuteilen sind. Eine Übersendung des vollständigen Inhaltes des Kaufvertrages ist dagegen nicht erforderlich, da für die Prüfung des Bestehens oder Nichtbestehens eines kommunalen Vorkaufsrechtes vertragsunabhängige, objektive Kriterien, die der Gemeinde bekannt oder für sie ermittelbar sind, maßgeblich sind.

Für die Erteilung eines sogenannten *Negativ-Zeugnisses* ist es ausreichend, wenn der Gemeinde die Tatsache des Kaufes, die Kaufvertragsparteien, die genaue Bezeichnung des Grundstückes und die Tatsache, ob das Grundstück bebaut oder unbebaut ist, mitgeteilt werden. Erst wenn die Gemeinde aufgrund dieser Informationen feststellt, daß grundsätzlich ein Vorkaufsrecht besteht und nicht auszuschließen ist, daß dieses Vorkaufsrecht tatsächlich ausgeübt werden soll, kann die Vorlage der vollständigen Kaufvertragsurkunde verlangt werden.

Gegen ein derartiges *zweistufiges Verfahren* spricht nicht, daß in § 28 Abs. 2 BauGB bestimmt ist, daß das Vorkaufsrecht nur in einer Frist von zwei Monaten ausgeübt werden kann. Die zweimonatige Frist beginnt erst zu dem Zeitpunkt, zu dem die Gemeinde aus der Mitteilung des Verkaufsfalles ohne weiteres feststellen kann, was Gegenstand des Kaufvertrages ist. Durch die formblattmäßige Vorkaufsrechtsanfrage wird die Frist dagegen nicht in Gang gesetzt.

In Bayern wird dieses zweistufige Verfahren bereits seit mehreren Jahren angewandt. Die dortigen Erfahrungen haben gezeigt, daß es auch mit einem geringeren Arbeitsaufwand für die Gemeinden verbunden ist, da diese für ihre Entscheidung, ob die Voraussetzungen für ein kommunales Vorkaufsrecht gegeben sind, Daten erhalten, die bereits vom Verkäufer nach einheitlichen Vorgaben aufgearbeitet worden sind. Dadurch werden überflüssige Aktenvorgänge bereits im Vorfeld vermieden.

Wir haben die Bezirksämter aufgefordert, das Verfahren entsprechend zu ändern.

Zugriff auf Bauakten

Mehrfach wurde uns im vergangenen Jahr die Frage gestellt, unter welchen Voraussetzungen andere Behörden (z. B. das Amt für Umweltschutz oder die Denkmalschutzbehörde), aber auch private Dritte (z. B. Nachfolger des Bauherrn, Alteigentümer, Forscher) Einsicht in Bauakten nehmen dürfen, die bei den Bauaufsichtsämtern der Bezirke lagern. Die Einsichtnahme durch Alteigentümer in den östlichen Bezirken wird noch dadurch kompliziert, daß es dort ein eigenständiges Gebäudeeigentum gibt und der Gebäudeeigentümer häufig nicht damit einverstanden ist, daß der Grundstückseigentümer Informationen über ihn den Bauakten entnimmt und zu Maßnahmen gegen den Gebäudeeigentümer verwendet.

Die Rechtslage in diesem Bereich stellt sich als sehr unübersichtlich dar. Das beruht auch darauf, daß die Bauaufsichtsämter ihre Bauakten ständig um neue Unterlagen, die in bezug auf das jeweilige Gebäude entstehen, ergänzen. Damit sind Bauakten zu historischen Gebäuden, die später verändert werden, praktisch nie abgeschlossen. Sie werden aus diesem Grund häufig auch nicht dem Landesarchiv angeboten, wie es das *Archivgesetz* des Landes Berlin an sich vorschreibt, weil das Bauaufsichtsamt auf diese Akten möglicherweise auch vor Ablauf der archivrechtlichen Sperrfristen noch zugreifen will.

Zunächst ist zwischen Unterlagen in Bauakten zu unterscheiden, die *jünger als 30 Jahre* sind, und solchen Unterlagen, die vor *30 Jahren und früher* entstanden sind. Soweit noch keine 30 Jahre seit Entstehung der jeweiligen Unterlagen vergangen sind, findet das Berliner Datenschutzgesetz mit den sonstigen bereichsspezifischen Datenschutzvorschriften im Landesrecht, insbesondere dem ASOG, Anwendung. Die Übermittlung an andere Ordnungsbehörden ist dann zulässig, wenn die Daten zur rechtmäßigen Erfüllung ordnungsbehördlicher Aufgaben erforderlich sind (§ 44 Abs. 1 ASOG). Dies trifft für die Auswertung von Bauakten durch die Denkmalschutzbehörde zu. Auch wenn die in Bauakten enthaltenen personenbezogenen Daten vordergründig zunächst nicht zum Zwecke des Denkmalschutzes erhoben worden sind, zumal das betreffende Gebäude häufig erst nach einer bestimm-

101 § 18 Abs. 4 ASOG
102 §§ 24, 25 BauGB, § 3 BauGB-Maßnahmengesetz, § 45 Abs. 5 Naturschutzgesetz oder § 7 Abs. 5 Landeswaldgesetz

ten Zeit die Denkmalseigenschaft erwirbt, sind die Belange des *Denkmalschutzes* und der Denkmalpflege nach dem Denkmalschutzgesetz Berlin in die städtebauliche Entwicklung, Landespflege und Landesplanung einzubeziehen und bei öffentlichen Planungen und Maßnahmen angemessen zu berücksichtigen. Insofern verfolgt die Denkmalschutzbehörde bei der Erfüllung ihrer gesetzlichen Aufgaben (vgl. § 11 Nr. 6 OrdZG i. V. m. Denkmalschutzgesetz Berlin) die gleichen Zwecke wie die Baugenehmigungsbehörde, die die Bauakte ursprünglich angelegt hat. Die Erhaltung und der Schutz des Gebäudes schließen sich an seine Genehmigung und Errichtung an.

Sind dagegen 30 Jahre und mehr seit Entstehung der jeweiligen Unterlage in den Bauakten vergangen, ist das Archivgesetz des Landes Berlin sinngemäß auch auf dezentral bei den Bau- und Wohnungsaufsichtsämtern in den Bezirken lagernde Bauakten anzuwenden. *Nach Ablauf von 30 Jahren* seit Entstehung werden die entsprechenden Bauakten bzw. deren Teile Archivgut im Sinne des Landesarchivgesetzes. Es gelten dann für die Nutzung die *Sperrfristen* dieses Gesetzes. Auch für die Auswertung von so alten Bauakten für *wissenschaftliche Zwecke* gilt statt des Berliner Datenschutzgesetzes das Archivgesetz. Zu Lebzeiten der betroffenen Personen dürfen deren Daten nur mit ihrer Einwilligung Dritten zugänglich gemacht werden. Nach dem *Tod der Betroffenen* bedarf die Nutzung des Archivguts bis zum Ablauf von 10 Jahren der Einwilligung der Angehörigen. Ist der Todestag der Betroffenen nicht bekannt, endet die Schutzfrist 90 Jahre nach der Geburt. Ist auch der Geburtstag nicht bekannt, endet die Schutzfrist 70 Jahre nach der Entstehung der Unterlagen. Vor Ablauf dieser Fristen dürfen auch öffentliche Stellen des Landes Berlin, also z. B. die Denkmalschutzbehörde oder das Bauaufsichtsamt, in dem die Unterlagen entstanden sind und lagern, diese nicht ohne weiteres nutzen.

Allerdings können die Archive der bezirklichen Bau- und Wohnungsaufsichtsämter diese *Schutzfristen verkürzen*, wenn und soweit dies im überwiegenden öffentlichen Interesse liegt. Dies ist in der Regel dann gegeben, wenn die Person oder der historische Vorgang, auf die in dem gesperrten Archivgut Bezug genommen wird, von besonderer oder exemplarischer Bedeutung für die Erforschung der Geschichte oder das Verständnis der Gegenwart ist. Dies wird man entsprechend auch auf *historisch bedeutsame Baudenkmäler* anwenden können.

Auch ohne Vorliegen eines überwiegenden öffentlichen Interesses ist die Verkürzung der Sperrfristen zulässig, wenn die Betroffenen oder – falls sie verstorben sind – ihre Angehörigen eingewilligt haben. Kann die Einwilligung nicht eingeholt werden, ist eine Verkürzung nur zulässig, wenn durch geeignete Maßnahmen gegenüber dem Nutzer sichergestellt ist, daß die schutzwürdigen Belange der Betroffenen nicht beeinträchtigt werden. Dies bedeutet, daß vor Ablauf der archivrechtlichen Sperrfristen Auskünfte an Dritte aus Bauakten regelmäßig nur in *anonymisierter Form* gegeben werden dürfen. Die Übermittlung personenbezogener Daten aus diesen älteren Bauakten an die Denkmalschutzbehörde ist dagegen nicht geeignet, schutzwürdige Belange zu beeinträchtigen, so daß an sie im erforderlichen Umfang auch vor Ablauf der Schutzfristen personenbezogene Auskünfte gegeben werden dürfen, nicht jedoch an private Dritte.

Eine uneingeschränkte Bauakteneinsicht durch den Nachfolger des Bauherrn oder Grundstückseigentümers ist erst dann möglich, wenn sämtliche archivrechtlichen Sperrfristen abgelaufen sind oder wenn die Betroffenen, deren Informationen sich in den Bauakten befinden, eingewilligt haben. Solange diese Voraussetzungen nicht erfüllt sind, sind jeweils nur *differenzierte (anonymisierte) Auskünfte* und Einsichten zulässig.

Soweit die jeweilige Bauakte noch nicht älter als 30 Jahre und deshalb kein Archivgut ist, gilt für die Akteneinsicht durch am Verfahren Beteiligte zudem das *Verwaltungsverfahrensgesetz* mit der Folge, daß personenbezogene Daten nur dann eingesehen werden dürfen, wenn eine Abwägung durch die Behörde ein überwiegendes Interesse des Einsicht Begehrenden gegenüber dem ergibt, dessen Daten offenbart würden.

Zusätzlich ist der Anspruch auf Information nach § 4 Abs. 1 des *Umweltinformationsgesetzes* zu berücksichtigen. Der Umweltbegriff wird hier weit ausgelegt.[103] Dieser Anspruch auf Information kann durch Erteilung einer Auskunft, Akteneinsicht oder in sonstiger Form erfüllt werden. Der Anspruch besteht allerdings nicht, soweit durch das Bekanntwerden der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden. Häufig werden die Belange der Bauherren, Architekten, Voreigentümer oder Besitzer nicht entgegenstehen, weil sie mit dem Grundstück nicht mehr befaßt sind. Andererseits können in den Akten enthaltene Daten über Zwangsmaßnahmen gegen Personen, Bußgeldbescheide oder ähnliche Unterlagen durchaus deren schutzwürdige Interessen berühren. Solche Unterlagen wären dann aus den Akten zu entfernen, bevor sie zur Einsichtnahme bereitgestellt werden. Auch ist der Betroffene, also der, dessen Daten offenbart werden sollen, zuvor anzuhören.

Auch der Grundstückseigentümer kann in dem beschriebenen Umfang ein Einsichtsrecht haben, wenn auf seinem Grundstück fremdes Gebäudeeigentum steht. Bei den erforderlichen Interessenabwägungen ist einerseits sein gesteigertes Interesse aufgrund seiner Eigentümerstellung zu berücksichtigen. Andererseits ist auch das gesteigerte Interesse des Gebäudeeigentümers zu berücksichtigen: Eventuelle Unterlagen über Ordnungsmaßnahmen gegen diesen in der Vergangenheit bergen naturgemäß ein verstärktes Risiko in sich, daß der Grundstückseigentümer sich dieser Informationen bedient, um den Gebäudeeigentümer von seinem Grundstück zu entfernen (soweit dies rechtlich unter den besonderen in den östlichen Bezirken geltenden Bedingungen zulässig ist).

Insgesamt ist die datenschutzrechtliche Situation hinsichtlich der Bauakten und Bauarchive allerdings so unzureichend, daß wir vorgeschlagen haben, die Bauordnung um normenklare gesetzliche Regelungen zur Verarbeitung personenbezogener Daten in Bauakten zu ergänzen, die dort bisher fehlen. Die Antwort der Bauverwaltung steht noch aus.

5.3 Finanzen

Vermögensrechtsdatenverarbeitungsgesetz

Mit dem am 12. Juli 1995 in Kraft getretenen Vermögensrechtsdatenverarbeitungsgesetz (VermDVG)[104] sind endlich die notwendigen datenschutzrechtlichen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im Regelungsbereich des Vermögensgesetzes in Berlin geschaffen worden.

Das VermDVG regelt den Umfang der Verarbeitung personenbezogener Daten und führt abschließend die Zwecke auf, zu denen die Daten verarbeitet werden dürfen. Der Grundsatz der *Datenerhebung beim Betroffenen* gilt auch im VermDVG. Ausnahmen von diesem Grundsatz sind möglich, wenn die Einreichung der erforderlichen Belege durch den Antragsteller oder eine Erteilung der erforderlichen Auskunft nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Eine für die Arbeit der Vermögensämter sehr wichtige Regelung ist die Regelung über Datenübermittlungen. Hier sind im Gesetz die Stellen benannt worden, denen auf Ersuchen von den Vermögensämtern bestimmte Daten aus den Anträgen für die Durchführung ihrer ebenfalls im Gesetz konkret benannten Aufgaben übermittelt werden dürfen. Schließlich ermöglicht das VermDVG auch einen *automatisierten Abruf* bestimmter gesetzlich geregelter Daten.

In Zukunft wird sowohl für den Bürger als auch für die Mitarbeiter der Vermögensämter Rechtssicherheit bei der Frage herrschen, ob die Datenverarbeitung im Einzelfall zulässig ist.

Abgabenordnung: Und immer noch fehlen die gesetzlichen Grundlagen

Nachdem das Bundesministerium für Finanzen Ende 1993 beschlossen hatte, den Entwurf eines *Abgabenänderungsgesetzes 1994* nicht weiterzuverfolgen, hatten wir gehofft, daß das Gesetzesvorhaben 1995 wiederaufgenommen werden würde. Unsere Hoffnung wurde auch in diesem Jahr enttäuscht; dabei werden

103 Jahresbericht 1994, 4.3
104 GVBl. 1995, 451

– wie der nachfolgende Fall zeigt – datenschutzrechtliche Regelungen im Bereich der *Abgabenordnung* dringend benötigt, um Diskussionen wie die folgende in Zukunft überflüssig zu machen.

Ungeliebte Bürgerrechte oder: Vorrang der Abgabenordnung vor dem Datenschutzgesetz

Ein Bürger wollte von uns wissen, ob ihm auch bei seiner „Steuerakte" ein Akteneinsichtsrecht zustehen würde. Das zuständige Finanzamt hatte seinen Antrag auf Akteneinsicht mit dem Hinweis auf die Regelungen der Abgabenordnung abgelehnt.

Nach § 16 Abs. 4 BlnDSG kann der Betroffene Einsicht in personenbezogene Daten, die in Akten über ihn gespeichert sind, verlangen. Die Abgabenordung (AO) enthält selbst keine Regelung über *Akteneinsicht* der Betroffenen. Sie trifft in § 91 AO lediglich eine Regelung über die Anhörung von am Steuerverfahren beteiligten Personen vor Erlaß eines Verwaltungsaktes. Nur dem Anwendungserlaß AO ist zu entnehmen, daß die Gewährung von Akteneinsicht im pflichtgemäßen Ermessen der Behörde steht und danach grundsätzlich auch möglich ist.

Die Senatsverwaltung für Finanzen hat sich gegen ein Akteneinsichtsrecht des Betroffenen nach dem Berliner Datenschutzgesetz im Bereich der Abgabenordnung gewandt. Sie ist der Auffassung, daß das Berliner Datenschutzgesetz im Bereich der Abgabenordnung nicht anwendbar sei bzw. daß es verfassungskonform entsprechend auszulegen sei. Schon im letzten Jahresbericht hatten wir uns zur Anwendbarkeit des Berliner Datenschutzgesetzes im Bereich der Steuerverwaltung geäußert[105] und dargelegt, warum das Berliner Datenschutzgesetz auch in diesem Bereich anwendbar ist. Auch der von der Senatsverwaltung für Finanzen zur Begründung herangezogene Grundsatz „Bundesrecht bricht Landesrecht" führt hier nicht zu einer Unanwendbarkeit des Berliner Datenschutzgesetzes. Die Abgabenordnung enthält gerade keine abschließenden datenschutzrechtlichen Regelungen für ihren Rechtsbereich, so daß dieser Grundsatz hier nicht herangezogen werden kann. Es handelt sich um zwei verschiedene Regelungsbereiche, und die Abgabenordnung hat die Anwendbarkeit des Berliner Datenschutzgesetzes nicht ausgeschlossen.

Zu der Frage der Anwendbarkeit des Berliner Datenschutzgesetzes im Bereich der Steuerverwaltung bleibt anzumerken, daß es auch Finanzämter gibt, die sich gegenüber anderen Verwaltungen auf Übermittlungsvorschriften des Berliner Datenschutzgesetzes berufen.

Datenübermittlung im Steuerstrafverfahren

Ein Bürger wurde wegen eines gegen ihn geführten steuerstrafrechtlichen Ermittlungsverfahrens in Untersuchungshaft genommen. Im Rahmen der Ermittlungstätigkeit wandte sich die zuständige Steuerfahndungsstelle der Finanzämter mit einem Schreiben an Geschäftspartner der von dem Bürger vertretenen Firma und bat diese um die Beantwortung einiger Fragen. Sie teilte den Firmen in ihrem Schreiben mit, daß sich der Bürger in Untersuchungshaft befinden würde und die Sache deswegen eilbedürftig sei.

Die Steuerfahndung hat durch den Hinweis auf die *Untersuchungshaft* des Bürgers personenbezogene Daten an Dritte übermittelt. Für eine solche Datenübermittlung fehlte es jedoch an der erforderlichen Rechtsgrundlage. Nach den Vorschriften der Strafprozeßordnung über die schriftliche Zeugenvernehmung dürfen dem Zeugen im Ermittlungsverfahren der Name des Beschuldigten sowie der Untersuchungsgegenstand mitgeteilt werden (§ 69 Abs. 1 StPO). Weitere Mitteilungen sehen die Vorschriften der Strafprozeßordnung nicht vor, so daß es für die Datenübermittlung an einer gesetzlichen Grundlage fehlte.

Die Senatsverwaltung für Finanzen hat sich nach längerer Diskussion unserer rechtlichen Bewertung des Falles angeschlossen. Wir gehen davon aus, daß die Tatsache, daß ein Beschuldigter sich in Untersuchungshaft befindet, in Zukunft den Zeugen im Zeugenanhörungsbogen nicht mehr mitgeteilt wird.

Steuererhebung mit Hilfe der I-Kennzeichendatei

Die Senatsverwaltung für Finanzen trat erstmals Ende des Jahres 1994 mit der Frage an uns heran, ob das Landeseinwohneramt verpflichtet sei, dem Finanzamt für Erbschaftssteuer und Verkehrssteuern die für die Festsetzung der Kraftfahrzeugsteuer insbesondere bei Fahrzeugabmeldungen und -stillegungen erforderlichen Daten aus der I-Kennzeichendatei zu übermitteln. Die I-Kennzeichendatei enthielt Daten aus dem Ostteil der Stadt, die von der Steuerverwaltung zur Überprüfung der zutreffenden Besteuerung der Kraftfahrzeuge benötigt wurden. Das Landeseinwohneramt hatte eine Übermittlung der Daten gegenüber der Senatsverwaltung für Finanzen mit dem Hinweis auf die Verpflichtung zur Löschung der Datei zum 31. Dezember 1994 abgelehnt.

Nach der Straßenverkehrsordnung dürfen Fahrzeug- und Halterdaten an die Finanzbehörden zur Sicherung des Steueraufkommens übermittelt werden. Der Einigungsvertrag hatte jedoch geregelt, daß für die nach dem bisherigen Recht der DDR erfolgten Zulassungen die örtlichen Fahrzeugregister, die die I-Kennzeichendatei darstellen, von den für die Zulassung zuständigen Behörden unter entsprechender Anwendung einiger Vorschriften des Straßenverkehrsgesetzes bis zum 31. Dezember 1993 weitergeführt werden durften. Unter den vom *Einigungsvertrag* für entsprechend anwendbar erklärten Vorschriften des Straßenverkehrsgesetzes (StVG) befand sich auch die Übermittlungsbefugnis an die Finanzbehörden.

Auch wenn man den Begriff „Weiterführen", der im Einigungsvertrag verwendet wird, nicht so versteht, daß damit bereits zwingend die Löschung der Daten verbunden ist, hätte die Löschung der Daten spätestens am 31. Dezember 1994 erfolgt sein müssen, denn auch nach den verkehrsrechtlichen Regelungen, auf die der Einigungsvertrag verweist, wären die Daten bei Fahrzeugen mit amtlichen Kennzeichen spätestens ein Jahr nach Eingang der vom Kraftfahrtbundesamt übersandten Abmeldemitteilung zu löschen gewesen. Da die I-Kennzeichendatei in jedem Fall am 31. Dezember 1994 hätte gelöscht sein müssen, durfte das Finanzamt für Erbschaftsteuer und Verkehrsteuern die Daten aus der noch vorhandenen I-Kennzeichendatei daher nicht mehr zu steuerlichen Zwecken nutzen. Die Datei ist inzwischen gelöscht worden.

5.4 Gesundheit

Krebsregister

Das *Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen, Sachsen-Anhalt und Thüringen* wird seit dem 1. Januar 1995 auf der Grundlage des Krebsregistergesetzes des Bundes und eines Verwaltungsabkommens der beteiligten Länder[106] in Berlin geführt. Wir haben das Register im Berichtszeitraum in Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz in Brandenburg (zugleich im Auftrag der Datenschutzbeauftragten der anderen beteiligten Länder) überprüft.

Schon bei dem Abschluß des Verwaltungsabkommens, erst recht aber bei den gegenwärtigen Beratungen über einen *Musterentwurf für ein Ausführungsgesetz der Länder zum Krebsregistergesetz* haben wir darauf gedrungen, das Krebsregister als organisatorische Einrichtung auf die Grundlage eines *Staatsvertrages* zwischen den beteiligten Ländern zu stellen. Bei der Einrichtung eines Krebsregisters muß durch bereichsspezifische Rechtsnormen geregelt werden, welche organisatorische Stelle zu welchem Zweck die erforderlichen Daten verarbeitet und wie das Krebsregister seine Aufgaben im einzelnen zu erfüllen hat. Dabei können allerdings auch unterschiedliche landesgesetzliche Regelungen in Betracht kommen, soweit die in Berlin gesammelten Datenbestände den Bundesländern, aus denen sie stammen, eindeutig zugeordnet werden können. Um das Gesetzgebungsvorhaben zügig voranzubringen, finden hierzu intensive Beratungen mit den beteiligten Gesundheitsverwaltungen statt.

Der Umzug des Krebsregisters von Karlshorst nach Kaulsdorf wurde zum Anlaß genommen, die technisch-organisatorischen Maßnahmen vor Ort zu überprüfen. Dabei haben wir festgestellt,

105 Jahresbericht 1994, 4.4

106 Jahresbericht 1994, 4.5

daß entgegen den Vorgaben des Bundeskrebsregistergesetzes ein großer Teil der Datenbestände nach wie vor nur in manueller Form vorliegt und daß es in absehbarer Zeit nicht zu bewerkstelligen ist, den Anforderungen des Gesetzes nach *Anonymisierung der Daten* zu entsprechen. Es ergibt sich daraus das grundsätzliche Problem, welche Nutzungen bei diesen Daten möglich sind und wie diese Daten in das Anonymitätsschema des Bundeskrebsregistergesetzes einzuordnen sind, das zwischen Vertrauensstelle und Registerstelle unterscheidet.

Lediglich die seit 1961 eingegangenen Einzelmeldungen sind überwiegend auf elektronische Datenträger übernommen worden. Dieser Bestand an Meldungen liegt dem mittlerweile erschienenen „Atlas zur Krebsinzidenz in der DDR von 1961 bis 1969“ zugrunde. Wir haben empfohlen, den restlichen Anteil der Meldungen ebenfalls auf elektronische Datenträger zu übernehmen, um bei künftigen Nutzungen die gebotene Anonymität gewährleisten zu können. Das Krebsregistergesetz läßt diesen Verarbeitungsschritt zu.

Altlasten Patientenakten

Mit den vorläufigen *Richtlinien zur Patientenaktenverwaltung* der Senatsverwaltung für Gesundheit vom 2. November 1995 wurde die Zuständigkeit für die Verwaltung der Patientenakten aus den aufgelösten ambulanten Einrichtungen des *ehemaligen staatlichen Gesundheitswesens* der DDR dem jeweiligen neu enstandenen Bezirksamt übertragen. Die Bezirksämter haben dafür Sorge zu tragen, daß die Unterlagen in gehöriger Obhut aufbewahrt werden. Dazu gehört insbesondere die Aufgabe, den zulässigen Zugriff im Eigeninteresse der Patienten zu gewährleisten. Jeder Patient soll das Recht auf Einsicht ausüben sowie Zugriff auf die Akten nehmen können, insbesondere wenn dies zur Nach- oder Weiterbehandlung erforderlich ist. Da die Bezirksämter hierfür nicht über die notwendigen finanziellen und personellen Mittel verfügen, wurde diese Aufgabe auf Empfehlung der Senatsgesundheitsverwaltung einer Beschäftigungs- und Qualifizierungsgesellschaft im Gesundheitswesen, dem Verein „Beschäftigungsinitiative für Verwaltungsdienstleistungen e. V.“ übertragen. Von den geschätzten vierzehn bis fünfzehn Millionen Patientenunterlagen in den Bezirken im Ostteil Berlins sind derzeit etwa fünf Millionen Akten medizinisch beurteilt, registriert und projektgerecht archiviert. Es war beabsichtigt, in Zusammenarbeit mit den Bezirksämtern den Aufbau und die Nutzung einer *„überbezirklichen Aktenfindungsdatei“* zu betreiben. Dazu war vorgesehen, aus den Bezirksdatenbanken den Namen, Vornamen und das Geburtsdatum des Patienten sowie Standort und Herkunftseinrichtung einer Akte zu doppeln und gesondert zu speichern. Dadurch sollte eine überbezirkliche Aktenfindung in bezug auf einen einzelnen Patienten ermöglicht werden. Den Patienten sollte es ermöglicht werden, durch eine einzige Abfrage alle verwalteten Patientenunterlagen auch aus anderen Bezirken aufzufinden.

Datenschutzrechtliche Bedenken bestehen hiergegen nicht, weil diese Datensammlung im Interesse der Patienten als Ersatz für die stillgelegten Einrichtungen verwaltet wird und ein Zugriff durch die Bezirksämter oder die Senatsverwaltung nicht besteht. Die Informationen aus den Patientenakten dürfen für die Aufgabenerfüllung öffentlicher Stellen nach wie vor nicht ohne Zustimmung der Patienten herangezogen werden. Auskünfte über den Ort und die Art von Patientenunterlagen sind daher nur den betroffenen Patienten selbst oder einem von ihm beauftragten Arzt oder einer anderen Person zu geben. Durch organisatorische und aufsichtsrechtliche Maßnahmen muß sichergestellt bleiben, daß nur mit Zustimmung und im ausdrücklichen Auftrag eines Patienten auf die Daten zugegriffen wird. Die Zustimmung muß auch im nachhinein nachweisbar sein, so daß die Schriftform unabdingbar ist.

> *Empörte Bürger machten darauf aufmerksam, daß Ärzte und medizinisches Fachpersonal in der DDR Meldungen erstatteten, wenn sie z. B. Kenntnis von geplanten Straftaten erhielten.*

Danach war auch jeder Arzt, vor allem bei dem berüchtigten Straftatbestand der „staatsfeindlichen Hetze“ (§ 106 Abs. 2 StGB der DDR), der glaubwürdig davon Kenntnis erlangt hatte, verpflichtet, an „die zuständigen Sicherheitsorgane (Ministerium für Staatssicherheit, Volkspolizei, Staatsanwalt)“ zu melden. Notfalls sollte die Anzeige auch an ein „anderes staatliches Organ gerichtet werden (Rat des Kreises, Rat der Gemeinde)“. Eine Anzeigepflicht bestand unverzüglich nach Bekanntwerden des anzeigepflichtigen Umstandes. Die Meldetechnik war „formlos – geeignete Form je nach Umständen (Telefon, persönliche Vorsprache)“. Die Verpflichtung zur Anzeige war zeitlich nicht begrenzt und wurde durch die Beendigung einer Straftat nicht aufgehoben. Durch diese Aussagepflicht wurden also die ärztliche Schweigepflicht und das Zeugnisverweigerungsrecht aufgehoben (§ 136 StGB der DDR). Die Verletzung der Anzeigepflicht war selbst strafbar und wurde mit Freiheitsstrafe oder mit Verurteilung auf Bewährung, Geldstrafe oder öffentlichem Tadel bedroht. Obwohl dieses Ergebnis unserem rechtsstaatlichen Empfinden widerstrebt, wird man wohl davon ausgehen müssen, daß die Übermittlung von DDR-Vorschriften gedeckt war.

Pflegeversicherung: Der unersättliche Informationshunger des fürsorglichen Staates

Die Einführung der *Pflegeversicherung* hat zu einer Fülle von Datenerhebungen in Formularen, Anträgen und Gutachten geführt. Dies wird von Behinderten und Behindertenverbänden vielfach abgelehnt. Deutliche Kritik wurde am *Begutachtungsverfahren* zwischen Medizinischem Dienst und Pflegekassen laut, weil hier erhebliche Datenmengen aus der medizinischen Begutachtung an die Pflegekasse fließen sollen. Die Datenschutzbeauftragten haben – leider vergeblich – auf die nicht immer gegebene Erforderlichkeit dieser Übermittlung hingewiesen. Während § 18 Abs. 5 Sozialgesetzbuch XI (SGB XI) die Regelung enthält, daß der *Medizinische Dienst der Pflegekasse* das „Ergebnis seiner Prüfung“ mitzuteilen und Maßnahmen zur Rehabilitation, Art und Umfang von Pflegeleistungen sowie einen individuellen Pflegeplan zu empfehlen hat, wird diese Vorschrift in der Praxis so angewendet, daß der wesentliche Gehalt der Gesamtbegutachtung an die Pflegekassen übermittelt wird, obwohl dort eine medizinische Bewertung der einzelnen Befunde nicht möglich ist. Wenngleich von den Bundesverbänden ein gemeinsames Formular eingeführt wurde, sollte weiterhin darüber nachgedacht werden, ob die *Übermittlung von „Ergebnissen“* beschränkt werden sollte, weil anderenfalls das Gesetz in einer widersprüchlichen Art und Weise ausgelegt würde. Denn das „Ergebnis“ einer Begutachtung schließt nicht die Darstellung der Untersuchungsbefunde ein.

> *Eine Pflegekasse verpflichtete einen Behinderten, ergänzend zur häuslichen Pflege regelmäßig einen Pflegeeinsatz durch eine von den Pflegekassen zugelassene Pflegeeinrichtung abzurufen. Der Betroffene befürchtete, daß dabei persönliche und sachliche Verhältnisse, der wirtschaftliche Status, sowie politische und religiöse Gesinnung offenbart werden. Während „in den vergangenen dreißig Jahren“ seit Eintritt der Körperbehinderung mit staatlicher finanzieller Unterstützung ein selbstbestimmtes Leben möglich gewesen sei, werde nun das Recht auf freie Arztwahl, das Freiheitsrecht als Patient, eingeschränkt und an „die von staatlicher Seite befohlene Vorgehensweise der Fürsorge“ früherer Zeiten erinnert.*

Nach dem Pflegeversicherungsgesetz ist jeder Pflegebedürftige, dem die Möglichkeit zur häuslichen Pflege zugestanden wurde, gleichwohl verpflichtet, in regelmäßigen Abständen den Besuch einer Pflegeeinrichtung zu dulden, die mit der Pflegekasse einen Versorgungsvertrag abgeschlossen hat *(Pflichtabruf)*. Es handelt sich um eine flankierende Maßnahme bei der Gewährung von Pflegegeld für selbstbeschaffte Pflegehilfen nach § 37 SGB XI. Zu prüfen war, ob dabei in unverhältnismäßigem Umfang personenbezogene Daten aus der Privatsphäre an die Pflegekasse oder eine andere Einrichtung übermittelt werden. Die Befürchtungen, die in der Beschwerde ausgesprochen waren, stellten sich allerdings als unbegründet heraus.

Aus § 37 Abs. 3 SGB XI ergibt sich vielmehr keine Befugnis der Pflegeeinrichtung und ihrer Mitarbeiter, Erkenntnisse über die Privatsphäre der Betroffenen der befürchteten Art an die Pflegekasse oder an den Medizinischen Dienst zu übermitteln. Die Datenübermittlung ist vielmehr auf das zu beschränken, worauf nicht verzichtet werden kann, wenn der Pflichtabruf überhaupt eine Bedeutung haben soll. Dies wird noch präzisiert in § 10 des

Rahmenvertrages zur ambulanten pflegerischen Versorgung der Spitzenverbände der Pflegekassen und der Spitzenverbände der freien Wohlfahrtspflege. Es soll verhindert werden, daß Angehörige der pflegebedürftigen Person Mittel aus der Pflegeversicherung unterschlagen oder nicht sachgerecht verwenden. Nach dieser Vorschrift findet eine Übermittlung von Informationen nur dann statt, wenn der Pflegebedürftige dies wünscht. Das *Einverständnis des Pflegebedürftigen* wird somit zwingend vorausgesetzt.

Um eine einheitliche Handhabung zu gewährleisten, ist zum Rahmenvertrag als Anlage ein Formular zum Nachweis des Pflegeeinsatzes erstellt worden. Auch das Formular weist eindeutig auf die Freiwilligkeit der Mitteilung über die Versorgungssituation hin und beschränkt die Datenübermittlung auf die Feststellung, daß die Versorgungssituation gesichert ist oder daß der Versicherte mit der Weitergabe einer Mitteilung über seine Versorgungssituation nicht einverstanden ist. Die Rechtsgrundlage dieser rahmenvertraglichen Vereinbarung findet sich im Sozialgesetzbuch. In § 75 Abs. 2 Nr. 4 SGB XI hat der Gesetzgeber die Verbände ermächtigt, Regelungen zur Überprüfung der Notwendigkeit und Dauer der Pflege vertraglich zu treffen. Der Schutz des informationellen Selbstbestimmungsrechts der Pflegebedürftigen ist durch § 17 (Datenschutz) dieses Rahmenvertrages sichergestellt. Dort werden die Leistungserbringer einer besonderen Schweigepflicht zum Schutze der Pflegebedürftigen unterworfen. Von der Schweigepflicht ausgenommen sind lediglich die gesetzlich geregelten Angaben. Wenn der Versicherte einer Weitergabe einer Mitteilung nicht zustimmt, kann allerdings der Medizinische Dienst einen Hausbesuch durchführen (§ 18 SGB XI). Dieser kann dabei die Versorgungssituation grundsätzlich neu beurteilen und eine neue Entscheidung durch die Pflegekasse herbeiführen.

5.5 Inneres

5.5.1 Polizei

Bundeskriminalamt

Noch immer entbehrt die Verarbeitung von personenbezogenen Daten durch das Bundeskriminalamt (BKA) einer *bereichsspezifischen Rechtsgrundlage,* die dem rechtstaatlichen Gebot der Normenklarheit genügt. In einem Fall, in dem ein Kläger die Löschung der zu seiner Person beim BKA gespeicherten Daten begehrte, hat der Hessische Verwaltungsgerichtshof diese Auffassung mittlerweile bestätigt.[107] Die §§ 1 Abs. 1, 2 Abs. 1 Nr. 1 BKA-G[108] genügen nach Auffassung des Gerichtes den Anforderungen an eine bereichsspezifische Regelung nicht. Sie stellen lediglich eine Aufgabenzuweisung an das Bundeskriminalamt dar. Die Voraussetzungen für die Befugnis zur Datenspeicherung bzw. für die Verpflichtung zur Datenlöschung personenbezogener Daten sind darin nicht geregelt. Auch auf den sogenannten *Übergangsbonus* könne die Datenverarbeitung beim BKA nicht mehr gestützt werden, da seit dem Volkszählungsurteil im Jahr 1983 bereits 12 Jahre vergangen sind, ohne daß der Gesetzgeber die erforderlichen bereichsspezifischen Regelungen erlassen hat. Dies hat zur Folge, daß die Betroffenen Eingriffe in ihr Recht auf informationelle Selbstbestimmung seit 12 Jahren hinnehmen müssen, ohne daß dafür eine Ermächtigungsgrundlage existiert. Die dem Gesetzgeber zustehende Übergangszeit soll diesem ausreichend Zeit für Beratung und Erlaß der entsprechenden Regelungen geben. Sie dient – so führt das Gericht aus – nicht dem Zweck, eine rechtswidrige Praxis zu legitimieren. Der Entwurf eines BKA-Gesetzes[109] wird zur Zeit im Bundestag beraten. Wann mit einer Verabschiedung eines entsprechenden Gesetzes zu rechnen ist, ist derzeit noch nicht absehbar.

Am 17. November 1995 hat das BKA die Errichtungsanordnung für eine *Arbeitsdatei PIOS-Osteuropäer (APOE)* erlassen und die Innenressorts der Länder gebeten, die nach Nr. 10 Abs. 2 Dateienrichtlinie erforderliche Zustimmung für die Einrichtung der Verbunddatei zu erteilen.

Gegen die Einrichtung der APOE haben wir Bedenken geäußert und dabei insbesondere auf die Unbestimmtheit des Dateizweckes hingewiesen. Im Gegensatz zu den bereits eingerichteten PIOS-Dateien wird mit der APOE nicht die Verfolgung oder Vorbeugung von Straftaten in konkret bestimmten Kriminalitätsbereichen bezweckt. Als Abgrenzungskriterium wird vielmehr allein auf die geographische Herkunft der Täter (Osteuropa) abgestellt. Darüber hinaus ist bereits die Erforderlichkeit zu bezweifeln. Zur Bekämpfung der Bereiche „organisierte Kriminalität“ und „Drogenkriminalität“ existieren bereits die PIOS-Dateien APOK und APR, auf die auch im Zusammenhang mit der Bekämpfung osteuropäischer Tätergruppen zurückgegriffen werden kann. Demgegenüber hat die Senatsverwaltung für Inneres der Einrichtung von APOE durch Verstreichenlassen der Einwendungsfrist zugestimmt und dazu ausgeführt, es sei aus kriminalpolizeilicher Sicht unverzichtbar, „jedes Mittel zu nutzen, das zu einer besseren Bekämpfung der Kriminalität osteuropäischer Tätergruppierungen beitragen kann“.

Probleme mit dem ASOG

Auf Antrag eines Bürgers wurde ein Sonderparkplatz für Schwerbehinderte mit außergewöhnlicher Gehbehinderung vor seinem zukünftigen Wohnhaus eingerichtet. Im nachhinein wurden der Polizei Umstände bekannt, die darauf hinwiesen, daß die im Antrag benannten Wohnräume als Gewerberäume genutzt werden. Daraufhin befragte die Polizei den Vermieter, der der Polizei Einzelheiten aus dem Mietvertrag mitteilte.

Die Polizei stützte die Datenerhebung beim Vermieter auf § 18 Abs. 3 ASOG und erklärte, daß die Befragung Dritter schon dann möglich sei, wenn Tatsachen vorliegen, daß diese sachdienliche Angaben machen können, die für die Erfüllung einer polizeilichen Aufgabe erforderlich sind. Das ist unzutreffend. § 18 Abs. 3 ASOG enthält lediglich die grundsätzlichen Voraussetzungen für die Durchführung einer Befragung. Die *Befragung Dritter ohne Kenntnis des Betroffenen* wird vielmehr durch § 18 Abs. 4 ASOG eingeschränkt. Darin sind abschließend deren Voraussetzungen geregelt, wenn die Befragung der betroffenen Person

- nicht oder nicht rechtzeitig möglich ist,
- einen unverhältnismäßig hohen Aufwand erfordern würde und schutzwürdige Belange der betroffenen Person nicht entgegenstehen,
- die Erfüllung der Aufgaben gefährden würde.

Keine der drei Tatbestandsalternativen war im vorliegenden Fall gegeben. Hier hätte beim Betroffenen selbst zum Inhalt des Mietvertrages nachgefragt werden müssen.

Die Senatsverwaltung für Inneres hat in einem weiteren Fall ausgeführt, daß auch Befragungen Dritter erfolgen können, ohne daß die Bedingungen des § 18 Abs. 4 ASOG vorliegen müssen, wenn der Betroffene kurz und formlos über die Befragung unterrichtet wird. Diese Rechtsauffassung entspricht weder dem Sinn noch dem Zweck der Regelungen in § 18 Abs. 4 ASOG. Der einzelne kann sein Recht, selbst über die Preisgabe und Verwendung seiner Daten bestimmen zu dürfen,[110] nur ausüben, wenn ihm die Behörde auch Gelegenheit dazu gibt. Dementsprechend verpflichtet § 18 Abs. 4 ASOG Ordnungsbehörden und die Polizei, Angaben über den Betroffenen grundsätzlich unmittelbar bei diesem einzuholen. Nur dadurch erhält der Betroffene die Möglichkeit, selbst zu entscheiden, welche Informationen er über sich preisgibt und zu welchem Zweck sie verwendet werden sollen. Im Rahmen des § 18 Abs. 4 ASOG ist daher ausschließlich zwischen dem Grundsatz, Befragungen an den Betroffenen selbst zu richten, und der Ausnahme, unter besonderen Voraussetzungen auch Dritte befragen zu können, zu differenzieren. Eine weitergehende Auslegung des Wortlautes der Bestimmungen dahingehend, daß Befragungen mit Kenntnis des Betroffenen an Dritte gerichtet werden können, ohne daß die weiteren Voraussetzungen vorliegen müssen, entspricht dem nicht.

In unserem letzten Jahresbericht hatten wir kritisiert, daß die Polizei das *Akteneinsichtsrecht* des ASOG „nur als Möglichkeit zur Arbeitserleichterung“ ansah.[111] Demgemäß erteilt die Polizei

107 Urteil vom 22. Juni 1995 – 6 UE 152/92 (nicht rechtskräftig)
108 Gesetz über die Einrichtung des Bundeskriminalamtes vom 29. Juni 1973, BGBl. I S. 704
109 BR-Drs. 94/95; Jahresbericht 1994, 4.6.1
110 § 1 Abs. 1 Nr. 1 BlnDSG
111 Jahresbericht 1994, 4.1; siehe auch Rede des Berliner Datenschutzbeauftragten vor dem Abgeordnetenhaus am 15. September 1994, Jahresbericht 1994, Anlage 1

regelmäßig nur Auskunft aus den Akten statt dem Betroffenen Akteneinsicht zu gewähren. Das Akteneinsichtsrecht ist Ausfluß des Rechtes auf informationelle Selbstbestimmung, und § 50 Abs. 6 ASOG ist im Lichte dieses Grundrechtes auszulegen, das heißt, in jedem Einzelfall ist zu prüfen, ob die Gewährung von Akteneinsicht möglich ist. Dabei ist zu berücksichtigen, daß es für den Betroffenen ein fundamentaler Unterschied ist, ob ihm über den Inhalt der Akte Auskunft erteilt wird oder ob er die Gelegenheit hat, die Unterlagen einzusehen. Zwischenzeitlich hat der Polizeipräsident zwar klargestellt, daß bei jedem Akteneinsichtsantrag eine Einzelfallprüfung erfolge; sind wir davon ausgegangen, daß hierbei das Recht auf informationelle Selbstbestimmung der Betroffenen häufig hinreichend berücksichtigt wird. Dies ist offenbar aber nach wie vor nicht der Fall. Im Zusammenhang mit der Auskunftsanweisung des Landesamtes für Verfassungsschutz[112] hat die Polizei wiederum darauf hingewiesen, daß es nur in wenigen Einzelfällen zweckmäßig sein könne, von der vom Gesetzgeber im ASOG „aus Gründen der Verwaltungsvereinfachung eingeräumten Möglichkeit, Akteneinsicht zu gewähren“ Gebrauch zu machen. Die von der Polizei vorgenommene Auslegung der Norm stellt weiterhin einseitig die Interessen der Polizei in den Vordergrund und ist somit rechtswidrig.

Anhörung der Polizei bei Namensänderungsverfahren

Eine Bürgerin beantragte beim zuständigen Bezirksamt die Änderung ihres Vornamens. Sie war überrascht, als ihr im Rahmen der Antragsbearbeitung vorgehalten wurde, daß über sie wegen mehrerer Strafverfahren (z. B. wegen Körperverletzung und Beleidigung) Daten bei der Polizei gespeichert sind. Von den Datenspeicherungen hatte die Petentin selbst zuvor keine Kenntnis. Die Polizei hat nach unserer Prüfung die Daten der Bürgerin gelöscht.

Die Polizei übermittelt den Bezirksämtern auf deren Anfrage die Aktenzeichen und Verfahren, zu denen Antragsteller auf *Namensänderung* als Beschuldigte in kriminalpolizeilichen Datensammlungen gespeichert sind.

Eine Rechtsgrundlage hierfür fehlt. Insbesondere kann die Datenübermittlung nicht auf § 3 Abs. 2 Namensänderungsgesetz gestützt werden. Danach sind die für die Entscheidung über die Namensänderung erheblichen Umstände von Amts wegen festzustellen und die zuständige „Ortspolizei“ zu hören. Eine Befugnis zur Übermittlung von Daten der Betroffenen durch die Polizei an die den Namensänderungsantrag bearbeitende Stelle ist darin nicht zu sehen.

Im Rahmen der Anhörung ist es nicht erforderlich mitzuteilen, ob über den Antragsteller Vorgänge bei der Polizei gespeichert sind. Keinesfalls ist die Übermittlung von konkreten Aktenzeichen für die Aufgabenerfüllung der den Namensänderungsantrag bearbeitenden Stelle erforderlich. Vielmehr ist für die vorgesehene Anhörung der Polizei die Mitteilung ausreichend, ob generell Bedenken gegen die Namensänderung bestehen.

Datenübermittlungen an die Jugendgerichtshilfe

Die Polizei unterrichtet in jedem Strafermittlungsverfahren, das gegen Jugendliche oder Heranwachsende geführt wird, bereits vor Abgabe des Verfahrens an die Staats- bzw. Amtsanwaltschaft die zuständige Jugendgerichtshilfe. Als Rechtsgrundlage für das Verfahren verweist die Polizei auf § 38 Abs. 3 Jugendgerichtsgesetz (JGG) und führt dazu aus, daß anders die Verpflichtung der Strafverfolgungsorgane, die Jugendgerichtshilfe im gesamten Verfahren heranzuziehen, nicht erfüllt werden könnte.

Zutreffend ist, daß § 38 Abs. 3 JGG grundsätzlich zur Datenübermittlung an die Jugendgerichtshilfe berechtigt bzw. sogar verpflichtet. Nicht geregelt ist jedoch in § 38 Abs. 3 JGG, welche Stelle die Jugendgerichtshilfe zu unterrichten hat. Herr des Ermittlungsverfahrens ist die Staatsanwaltschaft. Nur sie – und nicht die Polizei, die für die Staatsanwaltschaft als Hilfsbeamte tätig wird – hat über die Einschaltung der Jugendgerichtshilfe zu entscheiden.

Die Beteiligung der Jugendgerichtshilfe am gesamten Strafverfahren soll in erster Linie Schutz und Hilfe für den Jugendlichen bieten. Dies darf nicht in sein Gegenteil verkehrt werden. Bei einer pauschalen undifferenzierten Mitteilung über geführte Ermittlungsverfahren an die Jugendgerichtshilfe besteht die Gefahr unnötiger *Bloßstellung* oder *Stigmatisierung* des Betroffenen. Dies widerspricht dem Erziehungsgedanken des Jugendgerichtsgesetzes. Dem entspricht auch, daß die Arbeit für den Ermittlungsbericht durch die Jugendgerichtshilfe grundsätzlich erst nach Eingang der Anklageschrift bzw. des Antrages auf Erlaß eines Haftbefehles einzusetzen hat, da die Jugendgerichtshilfe selbst nicht über die Begründung des Verdachtes über einen bloßen Anfangsverdacht hinaus entscheiden kann.

Nach § 70 Satz 1 JGG wird die Jugendgerichtshilfe von der Einleitung und dem Ausgang des Verfahrens unterrichtet. Entsprechend der Regelung in Nr. 6 der Anordnung über Mitteilungen in Strafsachen (MiStra) ist davon auszugehen, daß nach dieser spezialgesetzlichen Übermittlungsbefugnis nur Verfahren mitgeteilt werden dürfen, bei denen ein begründeter Tatverdacht gegeben ist. Ob dies der Fall ist, ist von der Staatsanwaltschaft zu prüfen. Dementsprechend hat auch die Mitteilung nach § 70 Satz 1 JGG – ebenso wie die Mitteilung nach Nr. 6 MiStra – durch die Staatsanwaltschaft zu erfolgen. Über die bloße Mitteilung hinausgehende Daten dürfen aus den genannten Gründen erst dann an die Jugendgerichtshilfe übermittelt werden, wenn die Anklageschrift bzw. der Antrag auf Erlaß eines Haftbefehles vorliegen. Dies hat insbesondere den Sinn, unschuldig in Verdacht geratene Jugendliche bzw. Heranwachsende vor voreiligen Eingriffen in ihre Privatsphäre zu schützen.

Unsere Fortsetzungsgeschichte: Prostituiertenkartei

Nachdem Ende 1994 vom Berliner Datenschutzbeauftragten und dem Polizeivizepräsidenten ein gemeinsames Positionspapier zu der Kartei erarbeitet worden war, gingen wir davon aus, daß die Kartei künftig in datenschutzgerechter Weise geführt wird. In dem Positionspapier wird hervorgehoben, daß künftig Kontrollen auf dem Straßenstrich oder in bordellähnlichen Betrieben nur noch gezielt nach *Vorgabe der Fachdienststellen* durchgeführt werden und die Vorgabe *dokumentiert* wird. Weiterhin soll auf absehbare Zeit eine inhaltliche, nicht auf Fristen beschränkte Durchsicht der Kartei im Hinblick auf die Erforderlichkeit für die Bekämpfung des Menschenhandels und der ausbeuterischen Zuhälterei erfolgen.

Eine inhaltliche Gesamtdurchsicht der Kartei ist nach wie vor nicht erfolgt. Inhaltliche Prüfungen beschränken sich auf die Einzelfallbearbeitung. Die (ohnehin übliche) jährliche Gesamtdurchsicht erfolgte nur im Hinblick auf die Aufbewahrungsfristen. Es wurden keine Maßnahmen ergriffen, die sicherstellen, daß die Gründe für die Erfassung einer Person in der Datei nachvollziehbar dokumentiert werden. Die Verwendung andersfarbiger Karteikarten, aus welchen textlich der Erfassungsgrund (z. B. „angetroffen als Prostituierte“) hervorgeht, reicht hierfür nicht aus. Daß das „Antreffen als Prostituierte“ nach wie vor als Erfassungsgrund genannt wird, ist befremdlich, da schon vor Jahren der Konsens erzielt wurde, daß diese Tatsache allein für eine Speicherung nicht ausreichend ist.[113]

5.5.2 Meldewesen und Wahlen

Novellierung des Meldegesetzes

Schon 1988[114] hatten wir ausführlich über die Probleme mit dem Meldegesetz berichtet und Klarstellungen angeregt. Das betrifft beispielsweise die Speicherung von Daten nichtehelicher Kinder, des Rufnamens und des Wohnungsgebers bei Untermietverhältnissen, die Hotel- und Krankenhausmeldepflicht, die Möglichkeit der Angabe einer zu benachrichtigenden Person, die Protokollierung von Übermittlungen an Behörden, die Zuständigkeiten bei der Änderung der Konfessionszugehörigkeit sowie den Zugriff der Bezirksämter auf den gesamten Meldedatenbestand. Seitdem hat uns die Senatsverwaltung für Inneres immer

112 vgl. Ziff. 5.1

113 Stellungnahme des Senats zum Jahresbericht 1993, 4.5.1; AbghsDrs. 12/4655, S. 50

114 Jahresbericht 1988, 4.5

wieder zugesagt, daß alles bei einer Änderung berücksichtigt werde. Trotz der Änderung des Melderechtsrahmengesetzes im Jahr 1994, die ohnehin eine Novellierung erforderlich macht, liegt noch immer kein Konzept vor.

Speicherung des Wohnungsgebers als Adressierungszusatz

Alle Jahre wieder erreichen uns im Zusammenhang mit der Verteilaktion der neuen Lohnsteuerkarten Beschwerden darüber, daß bei Untermietverhältnissen im Adreßfeld der Name des Hauptmieters als Wohnungsgeber ausgedruckt ist.

Die bei der Anmeldung erhobenen Daten des Wohnungsgebers dürfen nach § 2 Abs. 2 Nr. 6 Meldegesetz nur für den dort genannten Zweck – nämlich die Feststellung der Mitwirkungspflichtigen nach § 13 Meldegesetz – erhoben und gespeichert werden. Die weitergehende Verwendung des Namens des Wohnungsgebers als Adressierungszusatz ist dagegen nicht durch § 2 Abs. 1 Nr. 11 Meldegesetz abgedeckt, da danach lediglich gegenwärtige und frühere Anschriften sowie die Haupt- und Nebenwohnung gespeichert werden dürfen, nicht aber, in welchem privatrechtlichen Verhältnis der Betroffene zum Wohnungsgeber steht.

Die Senatsverwaltung für Inneres war seinerzeit lediglich bereit, in den Erläuterungen zu den Feldern des *Meldescheines* die Erhebung selbst näher zu erklären, ohne aber von der bisherigen Praxis des Speicherns des Adressierungszusatzes Abstand zu nehmen. Das hat zur Folge, daß nicht nur bei Melderegisterauskünften an Private nach §§ 28, 29 Meldegesetz oder Datenübermittlungen an andere öffentliche Stellen nach §§ 25 bis 27 Meldegesetz, sondern auch in Lohnsteuerkarten diese Adressierungszusätze unzulässigerweise ausgedruckt werden; sie erlauben den Empfängern der Melderegisterauskünfte oder den Arbeitgebern Rückschlüsse auf die persönlichen und sachlichen Verhältnisse des Betroffenen.

Zwar löscht die Meldebehörde auf Antrag den Namen des Wohnungsgebers, den Ärger aber hat der Bürger, der erst nach der Löschung durch das Landeseinwohneramt beim Bezirkseinwohneramt eine neue Lohnsteuerkarte ausgestellt bekommt. Hier ist durch technisch-organisatorische Maßnahmen sicherzustellen, daß bei den Altfällen der Adressierungszusatz sowohl bei den Melderegisterauskünften oder den Übermittlungen an andere öffentliche Stellen als auch bei der Erstellung der Lohnsteuerkarten beim Ausdruck weggelassen wird.

Kommunales Wahlrecht für Unionsbürger

Anläßlich der Wahlen zum Europäischen Parlament, zum Abgeordnetenhaus und den Bezirksverordnetenversammlungen sind eine Reihe datenschutzrechtlicher Probleme aufgetreten. Insbesondere gab es Schwierigkeiten mit der erstmaligen *Teilnahme von Bürgern der Europäischen Union an den Wahlen* zu den Bezirksverordnetenversammlungen:

Nach dem Vertrag von Maastricht waren die Mitgliedstaaten verpflichtet, das Kommunalwahlrecht für Unionsbürger einzuführen. Für Berlin bedeutete das die Einführung des aktiven und passiven Wahlrechtes für die Wahlen zu den Bezirksverordnetenversammlungen. Dazu mußten die Verfassung, das Wahlgesetz und die Wahlordnung geändert werden.

Die erforderlichen *Datenverarbeitungsbefugnisse* wurden jedoch nicht geschaffen. Eine Speicherungsbefugnis für die Angabe, daß Unionsbürger vom Wahlrecht oder der Wählbarkeit ausgeschlossen sind, fehlt. Das Meldegesetz sieht bisher eine Speicherung dieses Merkmales nur bei deutschen Einwohnern vor. Auch für die Mitteilung strafgerichtlicher Wahlausschlußgründe für Unionsbürger existiert keine Rechtsgrundlage. Nach § 29 Abs. 2 AGGVG i. V. m. Nr. 12 MiStra dürfen nur die rechtskräftigen Verurteilungen von deutschen Staatsangehörigen der zuständigen Verwaltungsbehörde mitgeteilt werden. Art. 2 des Dritten Änderungsgesetzes zum Europawahlgesetz, mit dem eine Übergangsregelung für Mitteilungen der Justiz zum Wählerverzeichnis für Unionsbürger geschaffen wurde, bezieht sich nur auf die Europawahl und sieht außerdem keine Speicherungsbefugnis für das Wahlamt vor.

Die Unionsbürger sind in ein besonderes Verzeichnis einzutragen, das Bestandteil des *Wählerverzeichnisses* wird (§ 40 a Landeswahlordnung). Damit kein gesondertes „Ausländerverzeichnis“ entsteht, haben wir für die Wahlen zu den Bezirksverordnetenversammlungen die Schaffung eines gesonderten, gemeinsamen Wählerverzeichnisses für Deutsche und Unionsbürger angeregt. Die Unionsbürger wären dann im Wählerverzeichnis für die Abgeordnetenhauswahl nicht enthalten, könnten im Verzeichnis der Bezirksverordnetenversammlungen alphabetisch integriert werden und sind als solche nicht mehr erkennbar. Die in das Wählerverzeichnis Einsichtnehmenden könnten zwar weiterhin durch einen Abgleich der verschiedenen Verzeichnisse feststellen, ob jemand Deutscher oder Unionsbürger ist, dies wäre jedoch mit einem erheblichen Aufwand verbunden und bei einer Einsichtnahme allenfalls auf Einzelfälle beschränkt. Diese Anregung wurde für die Wahlen im Oktober 1995 nicht mehr berücksichtigt. Die Senatsverwaltung für Inneres will jedoch für künftige Wahlen Überlegungen hinsichtlich der Auslegung der Wählerverzeichnisse anstellen.

Nach der gleichen Vorschrift können sich die Wahlbenachrichtigungskarten und die Wahlscheine für Unionsbürger *farblich* von *Formblättern* für Deutsche unterscheiden. Zweck dieser Regelung ist, daß beim Betreten des Wahllokales die Ausgabe von Stimmzetteln für die Abgeordnetenhauswahlen verhindert werden soll. Durch die farblich unterschiedliche Gestaltung ist allerdings im Wahllokal für jeden deutlich sichtbar, ob ein Deutscher oder Unionsbürger von seinem Wahlrecht Gebrauch macht. Gleiches gilt für die Zustellung der Wahlbenachrichtigungskarten. Bei ordnungsgemäßer Handhabung ist auch bei einheitlicher Farbgebung die Gefahr einer unzulässigen Stimmabgabe keineswegs größer als bei dem praktizierten Verfahren. Nur die Verwaltungsvereinfachung rechtfertigt dieses Verfahren nicht.

Zweckentfremdung der Wahlbenachrichtigung

Vor den Wahlen erhält jeder Wahlberechtigte eine Wahlbenachrichtigungskarte, die aufgrund des Meldedatenbestandes erstellt wurde. Nach der Europawahl hatte die Senatsverwaltung für Inneres die bezirklichen Wahlämter gebeten, nicht zugestellte Wahlbenachrichtigungskarten („unbekannt verzogen“, „verstorben“) auch nach dem Wahltag an das Landeseinwohneramt weiterzuleiten, soweit eine neue oder andere Anschrift bekannt ist.

Meldebehörden für die Speicherung der erforderlichen Daten einschließlich der zum Nachweis ihrer Richtigkeit erforderlichen Hinweise sind die Bezirkswahlämter.[115] Ihnen obliegt es, unrichtig gespeicherte Daten zu berichtigen, um ihren wahlrechtlichen Verpflichtungen nachkommen zu können. Dabei sind die Erkenntnisse über offensichtlich veränderte Meldeverhältnisse, die sich aus dem Rücklauf unzustellbarer Wahlbenachrichtigungskarten ergeben, wesentliche Anhaltspunkte.

Die Senatsverwaltung für Inneres räumt ein, daß in diesen Fällen die Überprüfung rechtzeitig vor dem Wahltag hätte erledigt werden müssen, um die erneute Wahlbenachrichtigung der Betroffenen vornehmen zu können. Da dies in einem Wahlkreis nicht in vollem Umfang geschehen ist, bestehe nunmehr – vor dem Hintergrund der melderechtlichen Vorschriften – die Verpflichtung zur Aufarbeitung. Es bestehen dort keine Bedenken, wenn die Wahlämter als Meldebehörde die Überprüfung der in Rede stehenden Fälle selbst übernehmen. Da für das Landeseinwohneramt die Verpflichtung zur Speicherung und Berichtigung derselben Daten besteht, sei die Bereitschaft der Übernahme der Arbeiten zu begrüßen und rechtlich nicht in Frage zu stellen.

Diese Auffassung teilen wir sowohl hinsichtlich der Nutzung der an die Wahlämter zurückgelaufenen unzustellbaren Wahlbenachrichtigungskarten zur Fortschreibung des Melderegisters als auch der Durchführung dieser Aufgabe durch das Bezirkseinwohneramt nicht. Zwar ist es zutreffend, daß die Bezirkseinwohnerämter (Wahlämter) die Wählerverzeichnisse führen. Die hierfür übermittelten Daten aus dem Melderegister dürfen jedoch nur für den Zweck genutzt werden, zu dem sie übermittelt wurden, d. h. zur Wahlbenachrichtigung.[116]

115 § 1 Abs. 4 MeldeG
116 § 25 Abs. 6 MeldeG, § 11 Abs. 1 BlnDSG

Das Bezirkseinwohneramt nimmt unterschiedliche Aufgaben wahr. Bei der Vorbereitung und Durchführung von allgemeinen Wahlen[117] handelt es sich um eine andere Aufgabe als die der Meldebehörde.[118] Als Meldebehörde darf das Bezirkseinwohneramt für die Vorbereitung und Durchführung von allgemeinen Wahlen die Tatsache des Ausschlusses vom Wahlrecht oder der Wählbarkeit speichern.[119] Für die Weitergabe der als unzustellbar an das Bezirkseinwohneramt zurückgelaufenen Wahlbenachrichtigungskarten fehlt jedoch eine Übermittlungsbefugnis. Unberührt davon bleiben die Einzelanfragen des Wahlamtes, um beispielsweise bei einem unzustellbaren Rücklauf einer Wahlbenachrichtigungskarte noch vor der Wahl rechtzeitig durch die Klärung der Meldeverhältnisse dafür sorgen zu können, daß der Wahlberechtigte benachrichtigt werden kann. Auch die Änderung der Wohnanschrift im Melderegister durch das Bezirkseinwohneramt ist unzulässig.[120] Das darf nur das Landeseinwohneramt.[121]

Es ist auch ohne Vorlage der Wahlbenachrichtigungskarte möglich, an der Abstimmung teilzunehmen, wenn die Identität des Betroffenen anhand anderer Unterlagen festgestellt werden kann. Dies sollte nach Auffassung der Senatsverwaltung für Inneres möglichst die Ausnahme bleiben. Da die Überprüfung von Meldeverhältnissen durch die Bezirkswahlämter vor der Wahl aus Zeitgründen nicht optimal sein könne, werde sich die Zahl der nicht zustellbaren Wahlbenachrichtigungskarten erheblich vergrößern. Um die amtliche Berichtigung des Registers zu ermöglichen, ist eine Änderung des Meldegesetzes erforderlich.

Keine öffentliche Auslegung des Wählerverzeichnisses mehr!

Wahlberechtigte Personen, die in Krankenhäusern, Pflegeheimen und sonstigen Einrichtungen, die der Betreuung pflegebedürftiger oder behinderter Menschen dienen, leben, sind noch immer in den zur allgemeinen Einsicht öffentlich ausliegenden Wählerverzeichnissen aufgeführt.

Die Wählerverzeichnisse sind für jeden Stimmbezirk auf der Grundlage des Melderegisters nach den Straßennamen in alphabetischer Reihenfolge aufzustellen (§ 13 Landeswahlordnung). Innerhalb der Straßen sind die Häuser nach ihren Nummern und innerhalb der Häuser die Wahlberechtigten alphabetisch mit laufender Nummer, Familiennamen, Vornamen und Geburtsdatum einzutragen. Die Wählerverzeichnisse werden ohne Angabe des Geburtsdatums in festgelegten Zeiträumen zur allgemeinen Einsicht öffentlich ausgelegt (§ 16 Landeswahlordnung). In diesen öffentlich ausliegenden Verzeichnissen waren bisher auch Personen aufgeführt, für deren Daten eine melderechtliche Auskunftssperre besteht. Somit war ein *Umgehen der melderechtlichen Auskunftssperre* durch eine Einsichtnahme in das Wahlverzeichnis möglich. Aufgeführt sind auch Personen, die in Krankenhäusern, Pflegeheimen oder sonstigen Einrichtungen leben, die der Betreuung pflegebedürftiger oder behinderter Menschen dienen. Die öffentliche Auslegung beeinträchtigt die Persönlichkeitsrechte dieser Personen erheblich.

Die Aufnahme wird damit begründet, daß den Wahlberechtigten die Feststellung ermöglicht werden soll, ob sie im Wählerverzeichnis eingetragen sind und ob andere Personen zu Unrecht eingetragen sind. Wegen des überragenden Allgemeininteresses an der Öffentlichkeit der Wahl sei eine öffentliche Auslegung des Wählerverzeichnisses und die Aufnahme aller Wahlberechtigten mit Ausnahme der in Justizvollzugsanstalten gemeldeten Personen erforderlich. Im übrigen sei ein Auffinden von gesuchten Personen nur dann möglich, wenn die Anschrift bekannt ist, weil das Wahlverzeichnis nach Straßen und Hausnummern geordnet ist. Darüber hinaus würde von der Möglichkeit der Einsichtnahme in das Wählerverzeichnis nur noch selten Gebrauch gemacht und der technische Aufwand sei unverhältnismäßig, verschiedene Gruppen aus den öffentlich ausliegenden Wahlverzeichnissen herauszunehmen.

Die öffentliche Auslegung des Wählerverzeichnisses sollte *abgeschafft* werden. Wegen der außerordentlich geringen Inanspruchnahme ist der Hinweis auf die Transparenz des Wahlverfahrens, zumal im Hinblick auf die Beeinträchtigungen schutzwürdiger Belange von Bürgern, die in einer speziellen sozialen Situation leben (Pflegeheime, Krankenhäuser, Frauenhäuser), nicht mehr zeitgemäß. Wenn man dennoch auf die öffentliche Auslegung nicht verzichten will, sollte zumindest der Beschluß der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder[122] umgesetzt werden und nur noch Name, Vorname und Geburtsdatum (also ohne Anschrift) der Wahlberechtigten aufgeführt oder aber nur noch Auskünfte zu bestimmten Personen erteilt werden.

Bisher ist uns die Senatsverwaltung für Inneres insoweit gefolgt, daß bei den Wahlen im Oktober 1995 in den Wählerverzeichnissen nicht mehr Personen mit einer melderechtlichen *Auskunftssperre* enthalten waren. Die Wahlberechtigten, die in Pflegeheimen oder sonstigen Einrichtungen gemeldet sind, wurden bei dieser Wahl aus den öffentlich ausliegenden Wählerverzeichnissen noch nicht herausgenommen, weil der technische Aufwand für zu groß gehalten wurde. Es müßten dazu alle in Betracht kommenden Einrichtungen nach Straßen und Hausnummern aufgelistet und im Einwohnerdatenbestand gekennzeichnet werden. Darüber hinaus müßte festgestellt werden, wer nicht pflegebedürftig ist, aber in einer solchen Einrichtung gemeldet ist (z. B. Personal). Die Senatsverwaltung für Inneres will dennoch Überlegungen anstellen, wie unsere Empfehlung bei künftigen Berliner Wahlen realisiert werden kann. Das wird sie auch müssen, weil es nicht hinnehmbar ist, daß mit dem bloßen Hinweis auf technische Schwierigkeiten möglichen Beeinträchtigungen der schutzwürdigen Belange hingenommen werden.

Politische Meinungen im Melderegister

*Sofern **Unterstützungsunterschriften für einen Wahlvorschlag** erforderlich sind, müssen sich die Parteien oder Einzelbewerber darum bemühen. Sie haben die Formulare dem Wahlamt einzureichen, das anhand des Meldedatenbestandes die Wahlberechtigung der Unterstützenden prüft. Sofern sie wahlberechtigt sind, wird dies auf dem Vordruck bestätigt und die Tatsache der Unterstützung und der Name der Partei im Melderegister gespeichert. Auf diesem Weg soll eine mehrfache Unterstützung verhindert werden.*

Die Senatsverwaltung für Inneres hält die Speicherung des Namens der Partei für zulässig und notwendig, um die gesetzlichen Erfordernisse des Landeswahlgesetzes und der Landeswahlordnung zu erfüllen. Hat ein Wahlberechtigter mehrere Wahlvorschläge derselben Art unterstützt, so sind alle Unterschriften ungültig. Hat er gleichartige Wahlvorschläge derselben Partei mehrfach unterstützt, so ist jeweils eine Unterstützungsunterschrift gültig; die Doppelunterschriften werden nicht mitgerechnet. Nach § 2 Abs. 2 Nr. 1 Meldegesetz dürfen Daten mit Hinweisen gespeichert werden, die die wahlrechtlichen Bestimmungen erfordern. Dies ist für die Senatsverwaltung für Inneres die Rechtsgrundlage für die Speicherung der unterstützten Partei. Sie will bei Zweifeln an der Zulässigkeit jedoch für eine Klarstellung im Meldegesetz sorgen.

Die *Speicherung des Namens der unterstützten Partei* ist von der geltenden Rechtslage nicht gedeckt. Nach § 2 Abs. 2 Nr. 1 Meldegesetz darf lediglich die Tatsache, daß eine Unterstützungsunterschrift geleistet wurde, gespeichert werden. Als Hinweis für die Richtigkeit kommt der Zusatz der Partei nicht in Betracht. Bei den Hinweisen handelt es sich um die Benennung von Urkunden und Nachweisen mit der Bezeichnung der ausstellenden Behörde oder des Gerichtes sowie den Tag des Ereignisses, die Rechtswirksamkeit der Änderung oder die Angabe von Fristen. Die Speicherung des Namens der Partei, die unterstützt wird, geht weit darüber hinaus; sie enthält einen eigenen, besonders sensiblen Informationsgehalt. Zwar mag diese zusätzliche Information der Verwaltung das Auffinden von Unterlagen im Zusammenhang mit den Wahlen erleichtern, das rechtfertigt jedoch nicht eine Speicherung im Melderegister. Sofern weiter so verfahren werden

117 Nr. 3 Abs. 18 Anlage zu § 4 Abs. 1 Allgemeines Zuständigkeitsgesetz
118 § 33 Nr. 2 Gesetz über die Zuständigkeit der Ordnungsbehörden (OrdZG)
119 § 1 Abs. 4 i. V. m. § 2 Abs. 2 Nr. 1 Meldegesetz
120 vgl. Jahresbericht 1989, 4.4
121 § 1 Abs. 2 Meldegesetz
122 vgl. Anlage 2.9

soll, ist eine Klarstellung bei der Novellierung des Meldegesetzes zwingend erforderlich, wobei allerdings fraglich ist, ob dies mit der EU-Datenschutzrichtlinie vereinbar ist. Diese verpflichtet die Mitgliedstaaten, die Verarbeitung personenbezogener Daten über politische Meinungen zu untersagen (Art. 8 Abs. 1).

Irritierende Parteiwerbung

Die unendliche Geschichte mit der Wahlwerbung beschäftigte uns auch im Berichtsjahr wieder. Vor allem wurden wir gefragt, wie die Parteien an die Adressen gelangt sind.

Nach dem Meldegesetz darf die *Meldebehörde* Parteien im Zusammenhang mit den Wahlen zum Abgeordnetenhaus in den sechs Monaten vor der Wahl die Namen und Anschriften der Wahlberechtigten mitteilen. Die Listen dürfen nach Altersgruppen sortiert werden, wobei das Geburtsdatum nicht übermittelt werden darf. Der Betroffene kann der Weitergabe seiner Daten an die Partei zur Wahlwerbung widersprechen. Auf dieses Recht ist er bei der Anmeldung und durch öffentliche Bekanntmachung hinzuweisen.

Der Inhalt verschiedener Werbebriefe hat allerdings Empfänger daran zweifeln lassen, ob dieser Weg immer eingehalten wurde. So hat eine Partei ausführlich ihre Positionen zum Rentenüberleitungsgesetz dargelegt, so daß bei Empfängern der Eindruck entstand, hier seien die Datenbestände der Bundesversicherungsanstalt für Angestellte genutzt worden. Ursache war, daß die Meldebehörde Listen nach Altersgruppen sortieren darf – es gab eine Gruppe der 60- bis 70jährigen und eine weitere der über 70jährigen. Mit einem Hinweis auf die Rechtslage und einer kurzen Erläuterung, woher die Daten stammen, hätten die Befürchtungen vermieden werden können.

Ein Kandidat einer anderen Partei sprach die Empfänger darauf an, daß er von Ihnen schon mehrfach ins Abgeordnetenhaus gewählt worden sei und erweckte damit den Eindruck, daß er *Zugang zu Wahlunterlagen* hätte. Den hatte er natürlich nicht, denn der Brief richtete sich an alle Wählerinnen und Wähler des Wahlkreises, aber auch hier hätte das Mißverständnis mit einer kurzen Erklärung vermieden werden können.

Auch die *kommerzielle Werbung* hat eine bisher unbekannte Dimension erreicht. Ein Braunschweiger Münzhandelsunternehmen hat Werbebriefe verschickt, die in ihrer Aufmachung sehr den Wahlbenachrichtigungskarten ähnelten. Mit der Verwendung des Berliner Bären als Wappen und des Hinweises „Benachrichtigung für Wahlberechtigte“ wurde ein amtlicher Anschein erweckt. Darüber hinaus ließ die Werbung den Eindruck entstehen, daß Wahlunterlagen verwandt wurden. Auch hier wurden der Firma keine Daten aus Wahlunterlagen zur Verfügung gestellt. Die Firma hatte sich die Anschriften (auch von Insassen von Justizvollzugsanstalten) vom Adressenhandel beschafft. Die Senatsverwaltung für Inneres hat wegen der unzulässigen Verwendung des Berliner Landeswappens Strafantrag gestellt.

Repräsentative Wahlstatistik

Bei der Bundestagswahl 1994 wurde aufgrund einer kurzfristigen Änderung des *Bundeswahlgesetzes* die repräsentative Wahlstatistik als Bundesstatistik ausgesetzt. Gegenwärtig wird eine Novellierung des Bundeswahlgesetzes vorbereitet, die auch eine Neufassung der entsprechenden Bestimmungen beinhalten soll.

Aus diesem Anlaß verabschiedete die Konferenz der Datenschutzbeauftragten im März 1995 eine Entschließung.[123] Darin wird gefordert, daß Wahlberechtigte, in deren Bezirk eine repräsentative Statistik durchgeführt werden soll, bereits in der Wahlbenachrichtigung darüber zu informieren sind. Auch ein gut sichtbar angebrachter Hinweis im Wahllokal sollte diese Information unterstützen. Des weiteren wird eine *Mindestbesetzung der Geschlechts- und Altersgruppen* in den Wahlbezirken gefordert, um das Wahlgeheimnis mit Sicherheit zu wahren. Dieses Kriterium ist vom jeweiligen Landeswahlleiter zu prüfen. Wahlbezirke mit nur geringen Einwohnerzahlen in einzelnen Altersgruppen sollten ausgetauscht werden. Der Wahlvorstand, so empfahlen die Datenschutzbeauftragten, sollte nur das Wahlergebnis feststellen, während die statistische Auszählung durch eine gesonderte, für die Durchführung der Statistik zuständige Stelle vorzunehmen ist. Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- oder personenbezogen zusammengeführt werden, gefährden, so stellt die Entschließung fest, das Wahlgeheimnis und sind daher unzulässig. Die Entschließung beinhaltet also keine generelle Ablehnung einer Wahlstatistik.

Bei den der Wahlen zum Abgeordnetenhaus und zu den Bezirksverordnetenversammlungen von Berlin sowie zum Volksentscheid über die Verfassung Berlins gelten die entsprechenden Regelungen des *Landeswahlgesetzes*. Bereits im Jahresbericht 1992 informierten wir über eine Änderung der Landeswahlordnung, die unseren Forderungen Rechnung trug. Danach dürfen in Berlin nur solche Stimmbezirke in die Wahlstatistik einbezogen werden, in denen in jeder Alters- und Geschlechtsgruppe mindestens 20 Wahlberechtigte im Wahlverzeichnis eingetragen sind. Wahlberechtigte, die durch Briefwahl wählen, werden nicht in die repräsentative Wahlstatistik einbezogen. Durch vorbereitende statistische Auswertungen schafft der Landeswahlleiter darüber hinaus weitere Sicherheiten zur Wahrung des Wahlgeheimnisses. Zunächst wird versucht, eine Mindestbesetzung von 30 Wahlberechtigten je Altersgruppe durch eine stimmbezirksbezogene Auszählung der Meldedatei zu erreichen. Das Auszählen der Stimmzettel nach den Merkmalen der repräsentativen Wahlstatistik erfolgt erst nach Feststellung des endgültigen Wahlergebnisses durch das Statistische Landesamt. Im Wahllokal wird lediglich die Altersstruktur der Wähler am Wahltag selbst durch eine Strichliste erfaßt. Diese kann jedoch dadurch, daß sie im Moment des Wahlaktes bei der Ausgabe des Stimmzettels erhoben wird, nicht mit dem beim geheimen Wahlakt manifestierten Wählerwillen des einzelnen in Zusammenhang gebracht werden. Auch ist die Altersgruppierung auf den *Stimmzetteln* selbst wesentlich gröber als diejenige, die im Wahllokal durch das Ausstricheln der Wähler im Wählerverzeichnis erfaßt wird. Eine weitere Maßnahme zur Sicherung des Wahlgeheimnisses besteht darin, daß auf Stimmbezirksebene keine Wahlstatistikdaten veröffentlicht werden. Die Ergebnisse selbst werden lediglich als repräsentative Statistik zu Prozentangaben vorgenommen. Absolute Zahlen sind nicht enthalten. Aus datenschutzrechtlicher Sicht bietet das in Berlin angewandte Verfahren keine Möglichkeiten, das Wahlverhalten einzelner Bürger auszuspähen.

Um dem Bürger jedoch hinreichende Informationen über die zwangsweise Kopplung seiner Stimmabgabe an eine statistische Erhebung zu geben, empfehlen wir, die betreffenden Bürger bereits mit der Wahlbenachrichtigung über die anstehende Wahlstatistik zu informieren.

5.5.3 Ausländerwesen

Aufnahmemitteilungen der Justizvollzugsanstalten an die Ausländerbehörde

Aufgrund einer im Jahr 1984 zwischen der Senatsverwaltung für Inneres und der Senatsverwaltung für Justiz getroffenen Vereinbarung erhält die Ausländerbehörde von den Berliner Justizvollzugsanstalten eine Kopie der Aufnahmemitteilung jedes Ausländers, der inhaftiert wird. Die Aufnahmemitteilungen enthalten eine Vielzahl von personenbezogenen Daten des Ausländers; u. a. sind darin auch Angaben über das gerichtliche Aktenzeichen und den Tatvorwurf vermerkt.

Die Strafvollzugsbehörden haben den Ausländerbehörden den Antritt der Auslieferungs-, Untersuchungs- und Strafhaft, die Verlegung in eine andere Justizvollzugsanstalt und den vorgesehenen und festgesetzten Entlassungstermin mitzuteilen.[124] Dieser Katalog ist abschließend. Weitergehende Angaben auf den Aufnahmemitteilungen (z. B. gerichtliches Aktenzeichen, Angaben zum Tatvorwurf) dürfen ohne ein konkretes Ersuchen der Ausländerbehörde im Einzelfall nicht mitgeteilt werden. Auch in diesem Fall müssen die Daten für die Aufgaben der Ausländerbehörde erforderlich sein.

Dies ist bei einer Reihe weiterer Daten auf der Aufnahmemitteilung (z. B. Tatbeteiligte, erlernter Beruf, Bekenntnis) und bei Daten, die nach § 42 MiStra bereits von der Staatsanwaltschaft

123 vgl. Anlage 2.9

124 § 76 Abs. 5 Ausländergesetz (AuslG) i. V. m. § 4 Abs. 2 Ziff. 1–3 Ausländerdatenübermittlungsverordnung (AuslDÜV)

übermittelt werden, nicht ersichtlich. Die Rechtsauffassung der Ausländerbehörde, daß die Datenübermittlung auf die Bestimmung des § 75 Abs. 2 Satz 2 Nr. 3, 2. Alternative Ausländergesetz (AuslG) gestützt werden kann, geht fehl. Diese Vorschrift regelt lediglich, unter welchen Voraussetzungen die Ausländerbehörde vom Grundsatz der Datenerhebung beim Betroffenen abweichen darf. Eine Legitimation für die Übermittlung von personenbezogenen Daten durch andere Behörden an die Ausländerbehörde kann daraus nicht abgeleitet werden. Dies stellen im übrigen auch die vorläufigen Anwendungshinweise zu den §§ 75 bis 77 AuslG klar, die von der Senatsverwaltung für Inneres am 27. September 1994 verbindlich in Kraft gesetzt worden sind.[125]

Interesse der Polizei am ehelichen Beischlaf

Wenn die Polizei meint, ein Ausländer habe seine Aufenthaltsgenehmigung durch eine Scheinehe erschlichen, führt sie strafrechtliche Ermittlungen durch. Bei den Vernehmungen werden auch Daten zur Praxis des ehelichen Beischlafs erhoben. Die Polizei erachtet derartige Fragen für zulässig. Sie stützt dies auf § 1353 BGB und hält den ehelichen Beischlaf für ein Merkmal des Ehebegriffs. Eine klare Abgrenzung zwischen dem „Führen einer ehelichen Gemeinschaft" und dem „ehelichen Beischlaf" sei nicht möglich. Die Frage nach dem Vollzug des Geschlechtsverkehrs sei sachdienlich, da dies ein Aspekt für die Existenz einer Ehe sei.

Bei einer strafprozessualen Beschuldigtenvernehmung sind auch persönliche Fragen erlaubt, während bei einer rein behördlichen Befragung Fragen nach dem Intimbereich von vornherein unzulässig wären.[126] Jedoch erlauben selbst überwiegende Interessen der Allgemeinheit – auch im Strafprozeß – keinen Eingriff in den *absoluten Kernbereich privater Lebensgestaltung*.[127] Das Sexualverhalten gehört grundsätzlich in den Bereich der besonders geschützten Intimsphäre. Eine Einschränkung ist nur dann möglich, wenn die Befragung das einzige Mittel zur Überführung des Täters einer schweren Straftat darstellt.[128]

Es ist bereits zweifelhaft, ob in den hier vorliegenden Fällen so schwerwiegende Straftaten vorliegen, daß ein derartiger Eingriff in die Grundrechte Art. 1 Abs. 1, Art. 2 Abs. 1 GG gerechtfertigt ist. Außerdem ist die Frage nach dem ehelichen Beischlaf nicht das einzige Mittel zur Feststellung einer „Scheinehe". Sie ist darüber hinaus auch nicht geeignet, zuverlässige Rückschlüsse auf das Führen einer eheähnlichen Gemeinschaft zuzulassen. Der Begriff „Eheliche Lebensgemeinschaft" gemäß § 1353 BGB beinhaltet nach Auffassung des Gesetzgebers[129] eine Partnerschaft gleichen Rechts und gleicher Pflichten mit besonderen Anforderungen auf gegenseitige Rücksichtnahme und Selbstdisziplin, auf Mitsprache und Mitentscheidung. Der Vollzug des Geschlechtsverkehrs ist somit nicht konstituierend für die eheliche Lebensgemeinschaft, wenn auch ein diesbezüglicher Anspruch unter den Eheleuten selbst bestehen mag.

Besonders deutlich wird die Irrelevanz geschlechtlicher Beziehungen in einer Ehe durch § 7 Personenstandsgesetz, der ausdrücklich die Eheschließung auf dem Sterbebett regelt. Außerdem sind auch Abreden über dauernde Enthaltsamkeit (sog. *Josephsehe*) zulässig. Dies gilt selbstverständlich auch für binationale Ehen. Da also eine Ehe weder den Beischlaf erfordert noch geschlechtliche Beziehungen an eine Ehe gebunden sind, läßt die Beantwortung dieser Frage keine Rückschlüsse hinsichtlich einer „Scheinehe" zu.

Im übrigen hat auch eine Ehe ohne Herstellung einer ehelichen Lebensgemeinschaft nach dem bürgerlichen Recht Bestand. Sie führt nur nicht zu einer aufenthaltsrechtlichen Begünstigung, da getrennt lebende Eheleute auch in unterschiedlichen Ländern getrennt leben können. Auch hieraus ergibt sich, daß es für das Bestehen einer ehelichen Lebensgemeinschaft in aufenthaltsrechtlicher Sicht allein auf das Bestehen einer *häuslichen Gemeinschaft* ankommt. Für das Aufenthaltsrecht ist somit lediglich der Wunsch ehelichen Zusammenlebens maßgeblich, während die sexuelle Ausgestaltung der Ehe allein eine Sache der Ehepartner ist. Derartige Fragen sind unzulässig und haben zu unterbleiben.

Datenerhebungen bei der Einbürgerung

Wenn ein Ausländer einen Antrag auf Einbürgerung stellt, werden viele Angaben von ihm verlangt und viele Überprüfung vorgenommen. Spezialgesetzliche Befugnisse, die diese Datenerhebungen erlauben, fehlen. Sie werden auf die Einwilligung des Betroffenen gestützt. Die Antragsteller sollen z. B. Fotokopien von ***Scheidungsurteilen*** *vorlegen, obwohl das gesamte Urteil, das höchstpersönliche Angaben enthalten kann, für die Einbürgerungsentscheidung nicht erforderlich ist.*

Es erfolgen weiterhin Anfragen beim Finanzamt, dem Sozialamt, beim Landesamt für Verfassungsschutz, bei der Ausländerbehörde, beim Landeskriminalamt, bei der Staatsanwaltschaft, beim Polizeilichen Staatsschutz und beim Bundeszentralregister.

Zur Überprüfung der *wirtschaftlichen Verhältnisse* werden neben Anfragen beim Finanzamt und Sozialamt auch „bei verschiedenen Stellen Ermittlungen durchgeführt und auch Akten eingesehen". In dieser pauschalen Form ist eine wirksame Einwilligung des Betroffenen die Datenerhebung nicht möglich. Bei Anspruchseinbürgerungen *junger Ausländer* dürfen derartige Ermittlungen zudem nicht erfolgen, da es hier auf die *wirtschaftlichen Verhältnisse* nicht ankommt. Auch insoweit soll nach Mitteilung der Senatsverwaltung für Inneres eine Änderung des Verfahrens erfolgen.

Anfragen beim *Landeskriminalamt* sind auf laufende Ermittlungsverfahren zu beschränken, da Verurteilungen sich bereits aus der Bundeszentralregisteranfrage ergeben. Die Erforderlichkeit der Anfrage beim polizeilichen Staatsschutz neben der Verfassungs- und ISVB-Anfrage ist zweifelhaft.

Bedenken bestehen auch gegen die Praxis, die *gesamte Ausländerakte* anzufordern, da nur bestimmte Angaben aus der Ausländerakte für die Entscheidung über die Einbürgerung relevant sind. Die relevanten Informationen können durch Auskünfte eingeholt werden.

Beim *Landesamt für Verfassungsschutz* wird bei Anspruchseinbürgerungen nur angefragt, wenn konkrete Hinweise auf eine politisch-extremistische Betätigung bestehen. Bei Einbürgerungen, in denen ein Ermessensspielraum besteht, erfolgt hingegen eine *Regelanfrage.* Voraussetzung für die Einbürgerung ist, daß keine Gefährdung für die freiheitliche demokratische Grundordnung oder die Sicherheit der Bundesrepublik Deutschland vorliegt. Dem kann hinreichend Rechnung getragen werden durch Anfragen im Einzelfall. Die Regelanfrage – unabhängig vom Einzelfall – ist unverhältnismäßig, da nicht bei jedem Antragsteller eine Erforderlichkeit für diese Datenerhebung unterstellt werden kann. Die Anfragen sind ohnehin seit 1990 überflüssig, da das Ausländergesetz auch den Verfassungsschutz verpflichtet, Daten, die eine Ausweisung rechtfertigen, an die Ausländerbehörde zu übermitteln. Wie in anderen Bundesländern sollte deshalb auf die Regelanfrage auch bei Ermessenseinbürgerungen verzichtet werden und Anfragen von den konkreten Umständen des Einzelfalls abhängig gemacht werden.

5.5.4 Statistik

Umzugswirren

Mit besonderer Aufmerksamkeit verfolgen wir die Entwicklung der technisch-organisatorischen und datenschutzrechtlichen Gegebenheiten im *Statistischen Landesamt.* Im Jahresbericht 1994 legten wir die Ergebnisse einer umfangreichen Prüfung dar.[130] Damals wurden erhebliche datenschutzrechtliche Mängel festgestellt, die wir beanstandet haben. In der Erwartung, daß mit dem Umzug des Statistischen Landesamtes nach Alt-Friedrichsfelde die Situation hinsichtlich der Einhaltung der datenschutzrechtlichen und technisch-organisatorischen Vorschriften eine

125 Jahresbericht 1994, 4.6.3; vgl. 4.10
126 vgl. BVerfGE 76, 1, 61
127 BVerfGE 34, 238, 245
128 BVerfGE 34, 239, 250
129 BT-Drs. 7/4371 S. 7

130 Jahresbericht 1994, 4.6.4

qualitative Verbesserung erfahren wird, begleiteten wir diesen Umzug. Zwar wurde die technische Infrastruktur auf den modernsten Standard gebracht. Leider wurden die darin liegenden Chancen jedoch unzureichend genutzt.

Als erhebliches Manko erwies sich, daß weder eine *Risikoanalyse* noch ein *Datenschutz- und Sicherheitskonzept* erstellt worden war. Auch fehlten klare Regelungen in der Administration des neuen PC-Netzes. Wir stellten unter anderem fest, daß neunzehn Berechtigungen für Systemverwalter (Super-User) eingetragen waren. Weiter fehlt ein Nachweis der ordnungsgemäßen *Datenverarbeitung im Auftrag.* Weder für die Beziehung zwischen Statistischem Landesamt und dem Landesamt für Informationstechnik konnten ein Vertrag oder vertragsähnliche Unterlagen vorgelegt werden, noch waren Verträge bezüglich der Datenverarbeitung durch Dritte, insbesondere bei der Datenerfassung und zur Vernichtung auffindbar. Generell läßt sich aber feststellen, daß sich die Bedingungen für die Einhaltung datenschutzrechtlicher und technisch-organisatorischer Vorschriften im neuen Dienstgebäude wesentlich verbessern dürften.

Kampagnen 1995

Mit dem *Wohnungsstatistikgesetz* von 1993 legte der Bundesgesetzgeber fest, daß zum Stichtag 30. 9. 1995 für das Beitrittsgebiet, also auch die östlichen Bezirke Berlins, eine Totalzählung von Gebäuden und Wohnungen durchzuführen ist. Auskunftspflichtig sind Eigentümer, Verwalter, Erbbauberechtigte sowie Verfügungs- oder Nutzungsberechtigte. Entsprechend den Möglichkeiten, die der Bundesgesetzgeber einräumte, nutzte das Statistische Landesamt zum Bestimmen des Kreises der Auskunftspflichtigen Angaben der Grundbücher, der Ämter zur Regelung offener Vermögensfragen, der Wohnungsbaugesellschaften und Genossenschaften, der Meldebehörden sowie der Gebäudebrandversicherung. Durch ein Ankündigungsschreiben, das leider infolge einer verspäteten Adressübermittlung durch die Grundbuchstellen erst verzögert an die Betroffenen ging, wurden diese auf ihre Auskunftspflicht aufmerksam gemacht. Dies sorgte bei den Betroffenen für einige Verwirrung. Insgesamt läßt sich jedoch feststellen, daß bis Redaktionsschluß keine wesentlichen datenschutzrechtlichen Mängel erkennbar wurden.

Nachdem uns im Mai 1995 die *Erhebungsbögen* für die jährliche *Mikrozensuserhebung* zur Kenntnis gelangten, mußten wir feststellen, daß im Unterschied zu den Befragungen der Vorjahre eine wesentliche Veränderung vorgenommen wurde. Der Mikrozensus unterschied ausgehend von den Auflagen des Volkszählungsurteils zwischen Daten, für die Auskunftspflicht besteht, und freiwillig zu erhebenden Angaben. Diese freiwilligen Angaben wurden bislang auf einem gesonderten Erhebungsbogen erfaßt. Dabei war sowohl für den Auskunftspflichtigen als auch für den Interviewer diese Unterscheidung klar. Der *Mikrozensusbogen des Jahres 1995* hatte die *freiwillig zu erhebenden Angaben* inhaltlich unmittelbar dem jeweiligen Fragekomplex zugeordnet und die Freiwilligkeit lediglich durch eine gesonderte farbliche Markierung (hellblau statt dunkelblau) bzw. mit einem unter der laufenden Merkmalsnummer stehendem F vermerkt.

Dieses Verfahren birgt ein erhebliches datenschutzrechtliches Problem in sich. So haben die Interviewer vor Beginn des Interview zu klären, ob die Betroffenen bereit sind, auch über die Auskunftspflicht hinaus *freiwillige Fragen* zu beantworten. Es wird also die Einwilligung zu einem Zeitpunkt verlangt, zu dem die Betroffenen die Auswirkungen ihrer Einwilligung nur abschätzen können, wenn ihnen die freiwillig zu beantwortenden Fragen im einzelnen bekannt sind. In der Praxis müßte nun der Interviewer bei den einzelnen Fragen nochmals den Betroffenen auf die Freiwilligkeit hinweisen. Für die Selbstausfüller, das sind diejenigen Bürger, die zwar ihrer Auskunftspflicht nachkommen, jedoch auf die Unterstützung durch einen Interviewer verzichten wollen, wird das Verfahren auch *nicht hinreichend transparent.* Lediglich auf dem Deckblatt des Bogens wird auf die farbliche Unterscheidung und das F bei den freiwillig zu beantwortenden Fragen hingewiesen. Dies widersprach den Geboten von Normenklarheit und Transparenz. Der Entwurf für den *Erhebungsbogen im Jahre 1996* stellt insoweit wieder eine datenschutzrechtliche Verbesserung dar, als bei jeder freiwillig zu beantwortenden Frage explizit mit dem Wort „freiwillig“ auf die Situation hingewiesen wird.

Im Jahresbericht 1994 verwiesen wir auf das durch den Bundesgesetzgeber neu zu fassende Mikrozensusgesetz. Der gegenwärtig vorliegende Regierungsentwurf verzichtet darauf, die mit Auskunftspflicht zu erhebenden Merkmale zu erweitern. Unbeschadet dessen sind wir nach wie vor der Auffassung, daß sich der Umfang der freiwillig zu erhebenden Angaben wesentlich erweitern ließe, ohne den Zweck und die Aussagekraft des Mikrozensus zu gefährden. Einen diesbezüglichen Antrag hat auch das Land Nordrhein-Westfalen im Bundesrat eingebracht.

Mit dem Computer an der Wohnungstür

Zusammen mit dem Mikrozensusgesetz änderte der Bundesgesetzgeber das *Bundesstatistikgesetz.* Es wurde um eine Bestimmung zu *computergestützten Erhebungsverfahren* ergänzt. Danach können Bundesstatistiken mit derartigen Verfahren durchgeführt werden. Des weiteren wird den Betroffenen die Möglichkeit gegeben, ihre Antworten nicht unmittelbar in den Computer eingeben zu lassen, sondern sie auch schriftlich direkt an das Statistische Landesamt zu schicken. Im Jahresbericht 1991 verwiesen wir bereits auf einige beim Einsatz von *Laptops* durch Interviewer bei den Betroffenen möglicherweise auftretenden Probleme.[131] Zwar hat der Bundesgesetzgeber mit der neuen Regelung der Forderung nach Wahlmöglichkeiten, wenn diese nicht durch Gesetz eingeschränkt werden, Rechnung getragen. Doch scheint diese neue Regelung den Weg zu öffnen, auch alle künftigen technischen Erhebungsmittel zur statistischen Befragung der Bürger zu nutzen. Solche Erhebungsverfahren bergen eine erhebliche Gefährdung des informationellen Selbstbestimmungsrechtes in sich, insbesondere dann, wenn eine Bundesstatistik ausschließlich ein solches Verfahren vorsehen sollte und damit den Betroffenen keine Wahlmöglichkeit gegeben ist.

So können künftig alle nur denkbaren Möglichkeiten der *Telekommunikation* zur Gewinnung personenbezogener Daten für die amtliche Statistik genutzt werden, da eine abschließende Aufzählung der technisch möglichen computergestützten Methoden nicht erfolgt. Möglich ist es damit auch, bei entsprechender elektronischer Legitimation des anrufenden Statistikers, *Telefoninterviews* bei Erhebungen mit Auskunftspflicht durchzuführen. Werden, wie beispielsweise beim Mikrozensus, Daten sowohl mit Auskunftspflicht als auch auf freiwilliger Grundlage erhoben, so dürften für den Betroffenen die Unterschiede bei aktiven Telefoninterviews kaum noch erkennbar sein. Es kommt hinzu, daß hier wie auch bei der kommerziellen Telefonwerbung jeder ungebetene Telefonanruf als Eingriff in die Privatsphäre anzusehen ist, der im Fall der amtlichen Statistik nur durch ein überwiegendes Allgemeininteresse gerade an dieser Form der „Fernbefragung“ zu rechtfertigen wäre. Daran wird es jedoch in der Regel fehlen. Ohne Zweifel zulässig sind nur passive Telefoninterviews, bei denen die Betroffenen selbst das Statistische Landesamt anrufen und ihre Daten diesem per Telefon übermitteln. Im Falle des Mikrozensus liegen dem Betroffenen dann im Regelfall die Erhebungsbogen vor, aus denen die Unterscheidung zwischen obligatorisch und freiwillig zu beantwortenden Fragen deutlich hervorgehen sollte.

5.5.5 Personalwesen

Neues Personalaktenrecht endlich verabschiedet

Mit Gesetz vom 21. September 1995[132] hat der Berliner Gesetzgeber das Personalaktenrecht grundlegend neu gestaltet. Er folgte damit dem Bundesgesetzgeber, der die rahmenrechtlichen Vorgaben gesetzt hatte.

Zur Personalakte gehören gemäß § 56 Landesbeamtengesetz (LBG) alle Unterlagen einschließlich der in Dateien gespeicherten, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen *(Personalaktendaten).* Andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden. Nicht Bestandteil der Personalakte sind daher Unterlagen, die besonderen, von der Person und dem Dienstverhältnis sachlich zu trennenden Zwecken dienen, insbesondere Prüfungs-, Sicherheits- und Kindergeldakten.

131 Jahresbericht 1991, 3.4.3

132 Gesetz zur Änderung des Landesbeamtengesetzes, des Berliner Richtergesetzes und des Berliner Hochschulgesetzes, GVBl. S. 608

Nebenakten dürfen nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für den Beamten zuständig sind. Sie dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde erforderlich ist und die sich auch in der Grundakte und Teilakten befinden. In die Grundakte ist dabei ein vollständiges Verzeichnis aller Teil- und Nebenakten aufzunehmen.

Erhebungs- und Verarbeitungsvoraussetzungen

Der Dienstherr darf gemäß § 56 Abs. 4 LBG personenbezogene Daten der Bewerber, Beamte und ehemalige Beamte nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt.

Der Unterausschuß „Datenschutz“ des Innenausschusses und auch dieser Ausschuß selbst hatten in der parlamentarischen Beratung des Gesetzentwurfs mehrheitlich unseren Vorschlag aufgegriffen, wonach der Senat durch *Rechtsverordnung* den Umfang und die Verarbeitung der zu erhebenden Personaldaten im einzelnen bestimmen sollte. Damit wäre zumindest im Land Berlin einer Forderung entsprochen worden, die die Datenschutzbeauftragte des Bundes und der Länder seit jeher erhoben haben: Für den Bewerber sollte transparent festgelegt werden,

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

Trotz der Beschlußlage im Innenausschuß wurde in der 2. Lesung des Gesetzentwurfs im Plenum des Abgeordnetenhauses die Streichung der Verordnungsermächtigung und damit die Wiederherstellung der ursprünglichen Entwurfsfassung beantragt. Dieses ungewöhnliche Verfahren veranlaßte mich, in der Plenardebatte vom 22. Juni 1995[133] das Wort zu ergreifen und für die Annahme der Ausschußvorlage zu plädieren. Nach Zurückverweisung des Entwurfs an den Innenausschuß rückte dieser von seinem früheren Beschluß ab und empfahl, die Verordnungsermächtigung zu streichen. In dieser – vom Abgeordnetenhaus schließlich verabschiedeten – Fassung des Landesbeamtengesetzes ist nur noch vorgesehen, daß *Personalfragebogen* ab dem 1. Januar 1996 der Genehmigung der zuständigen obersten Dienstbehörde bedürfen. Wir gehen davon aus, daß die obersten Dienstbehörden den Berliner Datenschutzbeauftragten beteiligen werden, bevor sie derartige Genehmigungen erteilen. Eine derartige Beteiligung wurde während der Beratungen im Unterausschuß „Datenschutz“ von allen Fraktionen für notwendig gehalten.

Diese Daten dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn der Beamte willigt in die anderweitige Verwendung ein. Bei automatisierter Verarbeitung dieser Daten dürfen Personalaktendaten in Dateien nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verarbeitet werden (Personalinformationssystem – § 56 g LBG –). Ein automatisierter Datenabruf durch andere Behörden ist unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist. Beihilfedaten dürfen automatisiert nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt verarbeitet und genutzt werden.

Eine Besonderheit gilt bei Unterlagen über medizinische oder psychologische Untersuchungen und Tests. Hier dürfen im Rahmen der Personalverwaltung nur die Ergebnisse automatisiert verarbeitet oder genutzt werden, soweit sie die Eignung betreffen und ihre Verarbeitung oder Nutzung dem Schutz des Beamten dient.

Zugang zur Personalakte

Zugang zur Personalakte dürfen gemäß § 56 Abs. 2 LBG 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.

Die Personalakte darf *ohne Einwilligung* des Beamten ferner für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde vorgelegt werden. Das gleiche gilt für Behörden desselben Geschäftsbereichs, sobald die Vorlage zur Vorbereitung oder Durchführung einer Personalentscheidung notwendig ist. Ärzten, die im Auftrag der personalverwaltenden Behörden ein medizinisches Gutachten erstellen, darf die Personalakte ebenfalls ohne Einwilligung vorgelegt werden (§ 56 d Abs. 1 LBG).

Dagegen dürfen *Auskünfte an Dritte* nur mit Einwilligung des Beamten erteilt werden, es sei denn, daß die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz Berechtigter höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert. Inhalt und Empfänger der Auskunft sind gemäß § 56 d Abs. 2 LBG dem Beamten schriftlich mitzuteilen.

Im übrigen haben der Beamte selber sowie sein Bevollmächtigter gemäß § 56 c LBG auch nach *Beendigung des Beamtenverhältnisses* jederzeit ein Recht auf Einsicht in die vollständige Personalakte. Der Zusatz „*jederzeit*“ wurde auf Wunsch des Unterausschusses „Datenschutz“ in den Entwurf aufgenommen. Dies gilt auch für Hinterbliebene, wenn ein berechtigtes Interesse glaubhaft gemacht wird.

Der Beamte hat darüber hinaus ein Recht auf Einsicht auch in *andere Akten*, die personenbezogene Daten über ihn enthalten und für sein Dienstverhältnis verarbeitet und genutzt werden, soweit gesetzlich nichts anderes bestimmt ist. Dies gilt nicht für Sicherheitsakten.

Fristen

Tilgungsfristen für Beschwerden, Behauptungen, Bewertungen Mitteilungen in Strafsachen sowie Aufbewahrungsfristen für Personalakten sind erstmals ebenfalls in diesem Gesetz in den §§ 56 e und 56 f LBG geregelt. Nach Ablauf dieser Fristen sind die jeweiligen Schriftstücke oder die gesamte Personalakte zu vernichten.

Auf unsere Initiative hin wurde die Frist, nach deren Ablauf der Beamte die Entfernung oder Vernichtung von Unterlagen über ihn betreffende Beschwerden, Behauptungen und Bewertungen, die sich zwar nicht als unbegründet oder falsch erwiesen haben, aber für den Beamten ungünstig sind oder ihm nachteilig werden können, auf ein Jahr verkürzt (§ 56 e Abs. 1 Nr. 2 LBG).

Eine entsprechende Verkürzung der Aufbewahrungsfrist für Mitteilungen in Strafsachen, die nicht Bestandteil einer Disziplinarakte sind, wurde in den Ausschußberatungen aus nicht nachvollziehbaren Gründen abgelehnt. Derartige Mitteilungen sind erst nach drei Jahren mit Zustimmung des Beamten zu entfernen und zu vernichten (§ 56 e Abs. 2 LBG).

Alarmpläne

Ein Berliner Krankenhausbetrieb beabsichtigte, von sämtlichen Mitarbeiterinnen und Mitarbeitern für die Erstellung des Alarmierungsplans die Angabe der privaten Telefonnummer zu verlangen und den Alarmierungsplan mit den entsprechenden Daten allen Beschäftigten zugänglich zu machen.

133 Protokoll der Sitzung, S. 7523

Voraussetzung für jede Art der Verarbeitung personenbezogener Daten ist sowohl nach dem Berliner Datenschutzgesetz als auch nach dem Bundesdatenschutzgesetz die Erforderlichkeit der Daten. Auch bei einer Katastrophe kann keineswegs davon ausgegangen werden, daß sämtliche Beschäftigte für eine Versorgung der Bevölkerung erforderlich sind. Sie würden sich höchstwahrscheinlich eher wechselseitig behindern.

Die Krankenhausleitung und der Sicherheitsbeauftragte sollten vielmehr auf der Grundlage des Personalstamms überlegen, welches Personal für welche Art von Katastrophe benötigt wird, und versuchen, diese Mitarbeiter *auf freiwilliger Basis* für eine Mithilfe zu gewinnen. Bei den im Krankenhaus beschäftigten Ärzten sowie bei bestimmten anderen Dienstkräften ergibt sich die Verpflichtung zur Hilfe bereits aus ihrem Dienst- und Arbeitsverhältnis. Im übrigen darf ein Katastrophenplan keineswegs jedem Mitarbeiter zugänglich gemacht werden, sondern lediglich dem Katastrophenschutzbeauftragten und den freiwilligen Helfern, damit eine Verständigung untereinander im Ernstfall reibungslos erfolgen kann. Der Plan ist von diesen verschlossen am Arbeitsplatz bzw. zu Hause aufzubewahren.

Teilnahme an Fortbildungsveranstaltungen

Anläßlich einer Anmeldung von Beschäftigten des Berliner Datenschutzbeauftragten für einen Kurs an der Verwaltungsakademie wurde uns mitgeteilt, daß eine Sammelmeldung unter anderem auch die *Vergütungs- bzw. Besoldungsgruppe* des jeweiligen Beschäftigten enthalten müsse.

Zur Erforderlichkeit dieser Angabe verwies die Verwaltungsakademie darauf, daß die Veranstaltungen regelmäßig zielgruppenbezogen seien. Die Besoldungs- bzw. Vergütungsgruppe gebe Aufschluß darüber, ob es sich um einen Gruppenleiter, Sachbearbeiter oder Zuarbeiter mit entsprechend unterschiedlichen Lernbedürfnissen und auch unterschiedlichen Bildungsvoraussetzungen handelt, so daß nur bei Kenntnis dieses Merkmals soweit wie möglich eine homogene Lerngruppe zusammengestellt werden könne. Wir haben der Verwaltungsakademie mitgeteilt, daß die Angabe der Laufbahn ausreichend sei, um eine an den unterschiedlichen Lernbedürfnissen der Dienstkräfte orientierte Einteilung der Gruppen zu ermöglichen. Im übrigen gibt die Besoldungs-/Vergütungsgruppe durchaus nicht immer Aufschluß über die konkrete Tätigkeit der Dienstkraft, da insbesondere Leitungsfunktionen auf Bezirksebene anders bewertet werden wie z. B. auf Landesebene. Mit Rundschreiben vom 6. 11. 1995 wurde nunmehr geregelt, daß diese Angabe freiwillig ist.

Beförderungsverfahren

Der Lehrerpersonalrat eines Bezirksamtes wies uns auf folgende Verwaltungspraxis der Schulaufsicht bei der Senatsverwaltung für Schule, Berufsbildung und Sport hin: In den Auswahlentscheidungen bei Beförderungsfällen, in deren Rahmen auch Fremdbeurteilungen herangezogen werden, kommt es zu wertenden Äußerungen der Schulaufsicht über die Arbeit von Lehrern, die im Bewerbungsvorgang nur als sog. „Medium" dienen. Diese wertenden Äußerungen werden den Betroffenen regelmäßig nicht zur Kenntnis gegeben und sie werden auch nicht in ihre Personalakten abgeheftet, sondern zu Bestandteilen von Sachakten gemacht, von denen die betroffenen Mitarbeiter keine Kenntnis und auf die sie auch keinen Zugriff haben.

Wir haben der Senatsverwaltung unsere datenschutzrechtlichen Bedenken mitgeteilt, woraufhin im November 1994 eine dienstliche Anweisung erging, die eine *Anonymisierung der Unterrichtsbewertungsvermerke* durch die prüfenden Referenten nunmehr vorschreibt. Anläßlich eines späteren Besuchs bei der Senatsschulverwaltung baten wir, die älteren Vorgänge ebenfalls zu anonymisieren. Wir verdeutlichten, daß die Bewerbungsvorgänge einschließlich der darin enthaltenen Bewertungsvermerke keinesfalls zu Zwecken der dienstlichen Beurteilung der „Medien" herangezogen werden dürfen, es sei denn, dies wird von diesen ausdrücklich gewünscht. Sollte letzteres der Fall sein, so kann der Bewertungsvermerk Teil des Beurteilungsvorganges hinsichtlich des „Mediums" werden, müßte jedoch vorher bezüglich des Bewerbers anonymisiert werden. Die Senatsverwaltung wird gemäß unseren Empfehlungen verfahren.

Personalüberhanglisten

In der Vergangenheit haben wir uns mehrfach zum Problem der Offenbarung von Personaldaten von Überhangkräften und zur Weitergabe von Personalakten dieses Personenkreises geäußert. Zuletzt hat die Senatsverwaltung für Inneres mit Rundschreiben vom 9. März 1989 Vorgaben für die Verwaltungen gemacht. Danach sollen die Dienstbehörden auf Anforderung von anderen Dienstbehörden in konkreten Stellenbesetzungsfällen schriftliche Informationen nach einem beigefügten *Formblatt* anstelle der Personalakten übersenden. Dieses Formblatt enthält folgende Angaben: Namen und Vornamen, Geburtsjahr, Wohnbezirk, Personalüberhanglistennummer, Telefonnummer, derzeitige Dienststelle, derzeitiges Arbeitsgebiet lt. Geschäftsverteilungsplan, Berufsausbildung, Studienabschluß, bisherige berufliche Tätigkeit, besondere fachliche Kenntnisse oder Teilnahme an Fortbildungsmaßnahmen. Dieses von der Senatsverwaltung für Inneres vorgegebene Verfahren halten wir datenschutzrechtlich für akzeptabel. Darüber hinausgehende Informationen über die betroffene Person dürfen ohne deren vorherige Einwilligung in keinem Fall an andere Dienstbehörden übermittelt werden. Dies ergibt sich für Beamte aus § 56 d Abs. 2 Landesbeamtengesetz, der auch für Angestellte im öffentlichen Dienst Anwendung findet.

Krankheiten und Fehltage

Von dem Lehrerpersonalrat eines Berliner Bezirkes erhielten wir den Hinweis, der Leiter einer dortigen Grundschule führe eine Datei mit den Fehlzeiten der an der Schule unterrichtenden Lehrkräfte über einen Zeitraum von 10 Jahren. Anläßlich von amtsärztlichen Untersuchungen werde dieser Fehlzeitenkatalog als Anhang zum Untersuchungsantrag der Personalvertretung vorgelegt.

Nach der ständigen Rechtsprechung des Bundesarbeitsgerichts ist eine Speicherung von Personalaktendaten, die einem erhöhten Schutz unterliegen, nur solange zulässig, wie es der Zweck des Arbeitsverhältnisses unbedingt erfordert. Lange *zurückliegende Fehlzeiten* sind in den seltensten Fällen geeignet, Aufschluß über den aktuellen Gesundheitszustand des Beschäftigten zu geben. Insoweit sind sie für die ärztliche Diagnose/Prognose wenig hilfreich. Wenn keine weiteren besonderen Gründe für die lange Aufbewahrungsdauer vorliegen, ist die Speicherung der Fehlzeiten über diesen Zeitraum unzulässig.[134] Die Zulässigkeit der Speicherdauer hängt dabei vorrangig von den Umständen des Einzelfalls ab, sollte jedoch einen Zeitraum von zwei Jahren nicht übersteigen.

Die BVG hatte einen Mitarbeiter, der bereits längere Zeit arbeitsunfähig erkrankt war, aufgefordert, sich von einem vom Betrieb unabhängigen Arzt untersuchen zu lassen und diesen „freiwillig" von der ärztlichen Schweigepflicht zu entbinden, um eine Auswertung der Diagnosedaten durchführen und eine Zukunftsprognose abgeben zu können.

Die dem Arzt anvertrauten Geheimnisse und Daten unterliegen der ärztlichen Schweigepflicht. Deren unbefugte Weitergabe ist nach § 203 Abs. 1 Nr. 1 Strafgesetzbuch mit Strafe bedroht. Deshalb wird bei ärztlichen Begutachtungen auch zwischen *Befund- und Bescheidbogen* differenziert. Der Befundbogen enthält eine Dokumentation der medizinischen Daten des Arbeitsnehmers und bleibt beim Arzt. Für ihn gilt § 203 Abs. 1 Nr. 1 StGB, der es dem Arzt bei Strafe untersagt, Dritten, also auch dem Dienstherren oder Arbeitgeber des Untersuchten, Geheimnisse zu offenbaren, die ihm im Rahmen seiner Berufsausübung bekanntgeworden sind. Demgegenüber ist der sog. Bescheidbogen, der die Umsetzung der medizinischen Erkenntnisse für die betriebliche Praxis enthält, für die Personalverwaltung bestimmt. Der Bescheidbogen enthält personenbezogene Daten, die dem Arbeitgeber als Entscheidungshilfe für das konkrete Beschäftigungsverhältnis dienen können, wie z. B. Angaben über die Tauglichkeit für einen bestimmten Arbeitsplatz.

134 Jahresbericht 1991, 2.4

Jede Mitteilung, die über das reine Untersuchungsergebnis (z. B. „tauglich, eingeschränkt tauglich, nicht tauglich“) hinausgeht, muß durch eine *ausdrückliche Einwilligung* des Betroffenen gedeckt sein. Allein der Umstand, daß sich der Betroffene möglicherweise „freiwillig“ einer (amts-)ärztlichen Untersuchung unterzogen hat, kann nicht als stillschweigende Einwilligung in weitergehende Offenbarungen betrachtet werden. Aber auch die ausdrückliche Einwilligung stellt den Arzt nicht von der Verantwortung frei, den Umfang der Offenbarung auf das erforderliche Maß zu reduzieren. Eine pauschale (formularmäßige) Mitteilung medizinischer Einzelangaben ist daher selbst dann unzulässig, wenn der Betroffene auf Verlangen seines Arbeitgebers darin eingewilligt hat. Vielmehr sind die medizinischen Angaben, die mit Einwilligung übermittelt werden, auf das für die Entscheidung der Dienstbehörde unerläßliche Ausmaß zu beschränken.

Auch für den Fall, daß die Dienstbehörde eine eigene ärztliche Stelle als Adressat der Daten bestimmen kann, gilt nichts anderes: Das ärztliche Berufsgeheimnis gilt auch dann, wenn *Ärzte untereinander* Daten offenbaren. Dies bringt auch die ärztliche Berufsordnung zum Ausdruck, die eine eingeschränkte Offenbarungsbefugnis mit Widerrufsrecht des Betroffenen lediglich bei Parallel- oder Nachbehandlung vorsieht.

Im Ergebnis führen diese Überlegungen zu einem gestuften Verfahren: Aufgrund der Übermittlung des Untersuchungsergebnisses, die keiner ausdrücklichen Einwilligung bedarf, kann die Dienstbehörde dann, wenn sie einen Bedarf an zusätzlichen Daten geltend machen kann (z. B. bei einer unterschiedlichen Bewertung der Diensttauglichkeit durch Dienstbehörde und Amtsarzt) den Betroffenen um die (ausdrückliche) Einwilligung in die Offenbarung weiterer Daten bitten, der dann vom Amtsarzt im erforderlichen Umfang entsprochen werden kann. Dies entspricht auch der gesetzlichen Regelung im Beamtenrecht (§ 77 LBG), über die wir im vergangenen Jahr berichtet haben.[135]

Immer noch: Gauck-Überprüfungen

Ein ehemaliger Mitarbeiter einer Bezirksschulverwaltung beschwerte sich darüber, daß an sämtlichen Schulen in dem betreffenden Bezirk eine von der Abteilung Volksbildung erstellte Statistik ausgehängt worden war, die über arbeitsrechtliche Konsequenzen auf der Grundlage der Prüfungsergebnisse durch die Gauck-Behörde bei den Beschäftigten Aufschluß gab. In zwei Fällen wurden Fallzahlen „kleiner 3“ angegeben.

Dieses Vorgehen verstieß gegen die *Geheimhaltungsgrundsätze* des § 16 Landesstatistikgesetz. Danach sind Einzelangaben über persönliche und sachliche Verhältnisse, die für eine Landesstatistik gemacht worden sind, von den Amtsträgern, die mit der Durchführung von Landesstatistiken betraut sind, geheimzuhalten, soweit durch Rechtsvorschrift nichts anderes bestimmt ist. Die Weitergabe *ausreichend anonymisierter Einzeldatensätze* wird dabei unter der Voraussetzung als zulässig erachtet, daß bei Anlegung vernünftiger Maßstäbe die Daten einem einzelnen Betroffenen nicht mehr zuzuordnen sind. Verlangt wird folglich keine absolute Anonymisierung in dem Sinne, daß jede theoretisch denkbare Wiederherstellung des Personenbezuges ausgeschlossen sein muß, sondern eine gesteigerte faktische Anonymisierung, die nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft durchbrochen werden kann. Dies war hier jedoch nicht der Fall, da das plötzliche Ausscheiden von Lehrern in der jeweiligen Schule bekannt sein dürfte. Nicht bekannt ist jedoch in aller Regel der *Grund für dieses plötzliche Ausscheiden.* Werden nun in einer Statistik Einzel- oder „Zweier“-fälle bekanntgegeben, in denen Lehrer aufgrund von Gauck-Bescheiden ausgeschieden sind, ist es den Empfängern der Information an einer Schule möglich, den Zusammenhang mit einem vor kurzem ausgeschiedenen Lehrer herzustellen. Das Statistikgeheimnis ist damit verletzt. Aufgrund unserer Intervention wurden die Aushänge aus den Schulen entfernt.

135 Jahresbericht 1994, 4.6.5

Schließt der Datenschutz die Heimarbeit aus?

Ein Berliner Bezirksamt ist an uns mit der Frage herangetreten, ob in Anbetracht des Datenschutzes und einer stark eingeschränkten Möglichkeit der Kontrolle und Dienstaufsicht in Privatwohnungen „Heimarbeit“ zugelassen und in den Forderungskatalog eines Frauenförderplans gemäß § 4 Landesgleichstellungsgesetz aufgenommen werden kann.

Wir haben der Bezirksverwaltung mitgeteilt, daß die Zulassung und Durchführung von Heimarbeit aus datenschutzrechtlicher Sicht nicht ausgeschlossen ist. Allerdings ist von entscheidender Bedeutung, daß innerhalb der datenverarbeitenden Stelle (möglicherweise auch einheitlich für das gesamte Bezirksamt) *organisatorische Regelungen* darüber zu treffen sind, wer Heimarbeit zu genehmigen hat und wer für den jeweiligen konkreten Heimarbeitsauftrag datenschutzrechtlich verantwortlich ist. Man wird insofern zu unterscheiden haben zwischen Aufgaben der *Texterfassung* (reine Schreibarbeiten) und selbständiger *Vorgangsbearbeitung* bis hin zur „Heimarbeit“ durch Leitungskräfte. Bei Mitarbeiterinnen und Mitarbeitern, die einen Dienstvorgesetzten haben, ist jeweils festzulegen, wer als ihr Dienstvorgesetzter Heimarbeit zulassen kann (so bei Texterfassung und Vorgangsbearbeitung) oder wer zumindest darüber zu informieren ist, wenn ein leitender Mitarbeiter einen Vorgang mit personenbezogenen Daten in seiner Privatwohnung bearbeiten will. Auch § 82 Abs. 3 Gemeinsame Geschäftsordnung für die Berliner Verwaltung (GGO I) sieht für die Mitnahme von Schriftgut eine derartige Zulassung durch den Dienstvorgesetzten vor.

Wir haben daher empfohlen, für die Zulassung von Heimarbeit in einer Dienstanweisung folgende *Prüfschritte* vorzusehen:

- Ist die Verarbeitung personenbezogener Angaben überhaupt zwingend erforderlich oder kann ein Vorgang auch ohne Personenbezug bzw. in anonymisierter Form zu Hause bearbeitet werden?

- Soweit die Texterfassung oder die Vorgangsbearbeitung ohne personenbezogene Angaben nicht möglich ist, muß dem Dienstvorgesetzten im einzelnen eine genaue Aufstellung der Vorgänge bzw. der Diktate vorgelegt werden, bevor dieser Heimarbeit zulassen kann.

- Die Person, die Heimarbeit leisten möchte, ist eindringlich darüber aufzuklären, daß sie sowohl beim Transport der Unterlagen zwischen Dienststelle und Privatwohnung als auch insbesondere im häuslichen Bereich wirksame Maßnahmen treffen muß, um den Zugriff Unbefugter (auch Familienangehöriger) auf diese Unterlagen zu verhindern.

Wenn daran gedacht ist, bei der Heimarbeit personenbezogene Daten mit automatisierten Verfahren zu bearbeiten, dann sind *die technischen und organisatorischen Maßnahmen* zu treffen, die dazu geeignet sind, die Vertraulichkeit und Integrität der Daten sowie die Ordnungsmäßigkeit der Datenverarbeitung sicherzustellen. Je nach der Sensitivität der zu verarbeitenden Daten, der Art der zu Hause auszuführenden Arbeitsprozesse und der eingesetzten IUK-Technik sind die Maßnahmen in einem Sicherheitskonzept festzulegen, dem realistische Risikobetrachtungen zugrunde liegen. Solche Sicherheitskonzepte sind stark vom Einzelfall abhängig, müssen aber geeignet sein, die Kentnisnahme der Daten durch Unbefugte und unzulässige Eingriffe in den Verarbeitungsprozeß wirksam zu verhindern.

Der für die Zulassung der Heimarbeit *verantwortlichen Person* (in der Regel dem Dienstvorgesetzten) ist mitzuteilen, welche Maßnahmen der Datensicherung nach § 5 Abs. 2 BlnDSG bei konventionellem Schriftgut bzw. nach § 5 Abs. 3 BlnDSG bei automatisierter Verarbeitung getroffen werden. Insofern empfiehlt sich insbesondere bei Schreibkräften, die Heimarbeit leisten, von der datenverarbeitenden Stelle eine Checkliste für technisch-organisatorische Maßnahmen vorzugeben, deren Einhaltung die Dienstkraft, die zu Hause arbeiten möchte, zusichern sollte.

Personenbezogene Daten, die *Berufs- und besonderen Amtsgeheimnissen* unterliegen (medizinische Daten, Personaldaten und Sozialdaten) sollten nicht in Heimarbeit verwendet werden.

5.6 Jugend und Familie

Defizite der Normsetzung

Seit zwei Jahren ist die Frist abgelaufen, innerhalb derer die Senatsverwaltung für Jugend und Familie gesetzlich verpflichtet war, durch Rechtsverordnung die Datenverarbeitung bei der Berechnung der *Kostenbeteiligung der Eltern* an der Betreuung ihrer Kinder in städtischen *Kindertagesstätten* und in *Tagespflege* zu regeln.[136] Es ist nicht nachvollziehbar, weshalb inzwischen alle anderen betroffenen Senatsverwaltungen dazu in der Lage waren, die vom Parlament vorgegebene Fristsetzung zum Erlaß bereichsspezifischer Rechtsverordnungen zum Datenschutz einzuhalten, nur die Senatsverwaltung für Jugend und Familie nicht.

Zur Begründung wies diese Verwaltung immer wieder auf bevorstehende „Umstrukturierungen" im Kita-Bereich hin, die die Ausarbeitung einer Rechtsverordnung noch nicht zugelassen hätten. Damit war wohl in erster Linie die Umsetzung des bundesrechtlich vorgeschriebenen *Anspruchs auf einen Kindergartenplatz* gemeint.

Es hätte sich also angeboten, bei den dazu erforderlichen landesgesetzlichen Regelungen auch das Problem der Datenverarbeitung für die Errechnung der Kostenbeteiligung mitzuregeln. Auch wenn der Gesetzgeber die Regelung zunächst auf den Verordnungsgeber verlagert hat, ist es ihm unbenommen, die Materie in einem späteren Gesetz selbst zu regeln.

Diese Möglichkeit bot sich der Jugendverwaltung bei der Vorbereitung des Gesetzes zur Förderung und Betreuung von Kindern in Tageseinrichtungen und Tagespflege (Kita-Gesetz), mit dem der im Kinder- und Jugendhilfegesetz (SGB VIII) garantierte Anspruch auf einen Kindergartenplatz landesrechtlich umgesetzt werden sollte. Die Chance wurde allerdings nicht genutzt. Ohne daß wir im Entwurfsstadium von der Verwaltung um Rat gefragt worden wären, wurde das Kita-Gesetz am 19. Oktober 1995 im Parlament verabschiedet und trat am 1. Januar 1996 in Kraft.[137]

Prompt führte dieses Gesetz zu datenschutzrechtlichen Problemen, weil versäumt worden ist, die *Datenverarbeitung bei der Feststellung des Bedarfs an Ganztagsplätzen* mit der gebotenen Klarheit zu regeln. Der Bundesgesetzgeber hat jedem Kind vom vollendeten dritten Lebensjahr an einen *Anspruch auf den Besuch eines Kindergartens* zugestanden. Nur für Kinder im Alter bis zu drei Jahren und für schulpflichtige Kinder sind *nach Bedarf* Plätze in Tageseinrichtungen vorbehalten (§ 24 SGB VIII). Kinder unter drei Jahren sollten außerdem halbtags in den Kindergarten aufgenommen werden, wenn ihre Zurückweisung eine *besondere Härte* bedeuten würde. Um den generellen Anspruch für alle Kinder ab drei Jahren auf einen Halbtagsplatz im Kindergarten ab dem 1. August 1996 verwirklichen zu können, war die Senatsjugendverwaltung bestrebt, „herauszufinden", welche Eltern die Ganztagsplätze, die sie für ihre Kinder bisher in Anspruch nahmen, auch tatsächlich voll oder nur teilweise nutzen und in welchen Fällen eine besondere Härte vorliegt, wenn ein Kind unter drei Jahren nicht einmal halbtags in den Kindergarten aufgenommen wird.

Dazu wurde ein umfangreicher *Fragebogen „Anmeldung zur Tagesbetreuung"* entwickelt, den die Eltern ausgefüllt an die Jugendämter zurückgeben sollten. Er sorgte unter den Befragten für erhebliche Unruhe.

Die Erhebung personenbezogener Daten im Zusammenhang mit der Anmeldung eines Kindes im Kindergarten erfolgt grundsätzlich auf der Basis des Sozialgesetzbuchs Zehntes Buch (§ 67 a), denn die Aufnahme in den Kindergarten ist eine Sozialleistung. Wer eine Sozialleistung in Anspruch nehmen will, ist zur *Mitwirkung* insofern verpflichtet, als er die erforderlichen Sozialdaten offenbaren muß, die die Behörde benötigt, um seine Berechtigung zu überprüfen. Die Angaben unterliegen dem *Sozialgeheimnis.* Verweigert er seine Mitwirkung, kann die Sozialleistung – unter bestimmten Voraussetzungen – in letzter Konsequenz versagt werden. Abgesehen davon, daß es versäumt worden war, im Erhebungsbogen der Jugendverwaltung auf diese Folge einer Auskunftsverweigerung hinzuweisen, bedarf die Rechtsgrundlage für die gesamte Datenerhebung der Präzisierung durch den Landesgesetzgeber. Es ist nach Bundesrecht Sache der Länder festzulegen, wie der Bedarf an Ganztagsbetreuung und das Vorliegen einer besonderen Härte ermittelt werden soll. Damit ist auch durch Landesrecht näher zu regeln, welche personenbezogenen Daten zu diesem Zweck erforderlich sind. Das Berliner Kita-Gesetz enthält solche Regelungen nicht, obwohl es ohne weiteres möglich gewesen wäre, einen entsprechenden Kriterien- und Datenkatalog in das Gesetz aufzunehmen. Da dies versäumt worden ist, muß es unverzüglich im Rahmen der *Rechtsverordnung* nachgeholt werden, die aufgrund des Kita-Gesetzes *zur Personalbemessung* noch ergehen muß. Auch in diesem Rahmen ist der Bedarf der Kinder ein wesentlicher Anknüpfungspunkt.

Auch einzelne Fragen im Anmeldungsbogen lösten verständlicherweise Mißtrauen bei den befragten Eltern aus. So wurde nach *Namen, Anschrift und Telefon der Arbeitsstätten* des Vaters und der Mutter gefragt. Wenn Zweck dieser Frage allein gewesen wäre, den Eltern – wenn möglich – einen Kindergartenplatz für ihr Kind in der Nähe des Arbeitsplatzes zuzuweisen, so hätte es ausgereicht, nach der Straße und dem Bezirk zu fragen. So aber entstand zwangsläufig der Eindruck, die Jugendämter würden die Angaben der Eltern hinter deren Rücken beim Arbeitgeber überprüfen. Wir haben deutlich gemacht, daß dies als rechtswidrig zu beanstanden gewesen wäre und hinsichtlich der Gestaltung des letzten bis zum Redaktionsschluß dieses Berichts vorliegenden Anmeldungsformulars einen datenschutzrechtlichen Mangel festgestellt.

Vertrauen in der Jugendhilfe

Von 1990 bis Juli 1994 wurde in einer Stelle des Jugendnotdienstes (JND) regelmäßig in Telefonbüchern festgehalten, welche hilfesuchenden Personen dort angerufen hatten. Im einzelnen wurden der Name des Anrufers, der Name des angerufenen Mitarbeiters sowie Datum und Uhrzeit der Verbindung notiert. Privatgespräche der Mitarbeiter wurden nicht aufgeschrieben.

Die Erhebung und Speicherung der Verbindungsdaten zwischen den hilfesuchenden Personen und dem Fachpersonal des JND im Zeitraum von 1990 bis Mitte 1994 und vermutlich noch über diesen Zeitraum stellt einen Verstoß gegen die Vorschriften des Sozialgesetzbuches (§ 67ff SGB X) dar. Jede Speicherung dieser Daten hätte nur auf gesetzlicher Grundlage oder aufgrund der Einwilligung des Anrufers erfolgen dürfen. Eine allgemeine Rechtsgrundlage für die Erhebung und Speicherung von Verbindungsdaten beim Telefonverkehr ist nicht ersichtlich. Auch eine konkludente Einwilligung wegen des Hilfewunsches konnte aufgrund der als vertraulich einzustufenden Anrufe nicht angenommen werden. Im Hinblick auf die besondere Vertrauensbeziehung zwischen den hilfesuchenden Personen zu dem Fachpersonal des JND (§ 203 Abs. 1 Nr. 4 oder 5 StGB) waren zudem alle Maßnahmen zu unterlassen, die das Fachpersonal in *Konflikt mit ihrer Geheimhaltungspflicht* bringen konnten. Hintergrund der Praxis war, daß die im Jugendnotdienst verwendete Telefonanlage in einem derart desolatem Zustand war, daß der Abbruch von Verbindungen zu befürchten war, da die technische Vermittlung sowie die Nebenstellenanlagen oft nicht funktionierten und deshalb die zuverlässige soziale Beratung nicht immer gewährleistet war. Mit den unzulässigen Datenspeicherungen versuchte man sich zu behelfen. Die Mitarbeiter hatten selbst den Mangel erkannt und auf Beseitigung gedrungen. Die Telefonanlage ist zwischenzeitlich erneuert, die Vernichtungsprotokolle der unzulässig erhobenen Daten wurden uns vorgelegt.

Eine Pflegemutter bewarb sich bei ihrem zuständigen Bezirksamt um eine Pflegestelle für Kinder. Aufgrund der Angabe eines früheren Wohnsitzes der Antragstellerin stellte das Bezirksamt Erkundigungen beim Jugendamt des früheren Wohnbezirkes an, um die Geeignetheit der Antragstellerin zu überprüfen. Dabei ergab sich, daß diese selbst in ihrem früheren Wohnbezirk Betreuungsdienste in Anspruch genommen hatte und daß aufgrund der besonderen Umstände nicht von einer Geeignetheit im Sinne des § 44 SGB VIII (Kinder- und Jugendhilfegesetz) ausgegangen werden konnte. Obwohl zur Zeit der Antragstellung bei der betroffenen Frau große Hoffnungen auf die Zustimmung des Amtes entstanden waren, erhielt sie zum Schluß eine Ablehnung mit Hinweis auf den früheren Betreuungstatbestand.

136 § 7 a Kita-Kostenbeteiligungsgesetz i.d.F. v. 27. 5. 1993, GVBl. S. 224; vgl. dazu bereits Jahresbericht 1994, 1.2

137 GVBl. 1995, S. 681

Die Irritation der Antragstellerin und ihre verständliche Enttäuschung wären vermeidbar gewesen, wenn sie von vornherein über die notwendige Prüfung der Geeignetheit durch eine Nachfrage beim früheren Wohnbezirk informiert worden wäre. Der Fall zeigt, daß nicht nur hier, sondern auch in anderen Bereichen der sozialstaatlichen Verwaltung Hilfeempfänger und Antragsteller mehr als früher über die gesetzlich geregelten und tatsächlich praktizierten Datenübermittlungen oder Datenabgleiche informiert werden müssen. Schon durch eine solche Information kann nicht nur erhebliche Verwaltungsarbeit vermieden werden, sondern auch der Bürger davor geschützt werden, sich leichtfertig in Situationen zu begeben, die ihn in einem ungünstigen Licht erscheinen lassen und zu einer weiteren Verbreitung nachteiliger Informationen, nämlich bei der ersuchten und bei der ersuchenden Stelle führen müssen.

5.7 Justiz

Lauschinformationen gestoppt

Ein Hochschulprofessor hatte Verfassungsbeschwerde sowie einen Antrag auf Einstweilige Anordnung beim Bundesverfassungsgericht gegen einige Regelungen des am 1. Dezember 1994 in Kraft getretenen Verbrechensbekämpfungsgesetzes[138] *eingelegt. Er hatte sich insbesondere gegen eine Regelung gewandt, nach der auf Antrag des Bundesnachrichtendienstes bei bestimmten Straftaten das Fernmeldegeheimnis aufgehoben werden und der Bundesnachrichtendienst (BND) zu diesem Zweck mit Suchbegriffen den Fernmeldeverkehr abhören darf. Durch seine beruflichen Kontakte in das Ausland befürchtete er, daß seine Ferngespräche mit ausländischen Kollegen vom BND aufgezeichnet werden würden.*

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 5. Juli 1995 über den Eilantrag[139] die Befugnis des BND zur Verwertung und Weitergabe von beim Abhören erlangten Daten auf die Fälle beschränkt, in denen der Verdacht einer Straftat besteht. Damit hat das Bundesverfassungericht klargestellt, daß es für die *Weiterleitung von Fernmeldeaufzeichnungen an die Staatsanwaltschaft* nicht – wie im Verbrechensbekämpfungsgesetz geregelt – ausreicht, daß tatsächliche Anhaltspunkte den Verdacht einer Straftat begründen, sondern diese nur dann übermittelt werden dürfen, wenn bestimmte Tatsachen den Verdacht einer Straftat begründen. In der Hauptsacheentscheidung wird das Bundesverfassungsgericht auch über die Frage entscheiden, inwieweit der Kläger durch die Fernmeldeaufzeichnung mit Hilfe von Suchbegriffen in seinen Grundrechten verletzt wird. Dabei wird das Bundesverfassungsgericht zu klären haben, inwieweit die im Verbrechensbekämpfungsgesetz geregelte Ausdehnung der Fernmeldeüberwachung auf Tatbestände, die auch die innere Sicherheit der Bundesrepublik berühren, noch mit der Verfassung vereinbar ist. Es wird insbesondere auch zu der Frage der Aufhebung des Trennungsgebotes von Nachrichtendienst und Polizei, das verfassungsrechtlichen Rang hat, Stellung nehmen.

Justiz: Schlußlicht der Datenschutzgesetzgebung

Das letzte Mal hatten wir in unserem Jahresbericht 1993 über den Entwurf eines *Justizmitteilungsgesetzes* berichtet.[140] Der Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (JuMiG)[141] war jedoch vom letzten Deutschen Bundestag nicht mehr beraten worden, so daß auch heute noch gesetzliche Regelungen der Mitteilungen im Justizbereich fehlen. Das Bundesjustizministerium sieht die Schaffung gesetzlicher Regelungen inzwischen als eilbedürftig an und hat einen neuen Gesetzentwurf vorbereitet. Gegenüber dem vorangegangenen Entwurf sollen zwei datenschutzrechtlich wesentliche Punkte geändert werden:

- Dem Betroffenen ist nur auf Antrag Auskunft über den Inhalt und den Empfänger der übermittelten Daten zu erteilen. Eine Unterrichtung von Amts wegen ist nur in gesetzlich geregelten Fällen vorgesehen, die lediglich einen kleinen Teil der Datenübermittlungen ausmachen.
- Die Mitteilungsbefugnisse sollen in einer Rechtsverordnung durch das Bundesministerium der Justiz geregelt werden.

Eine Regelung, die die *Unterrichtung des Betroffenen* von Amts wegen zur Ausnahme macht und eine konkrete Benennung der *Übermittlungspflichten durch Rechtsverordnung* vorsieht, wird dem Volkszählungsurteil nicht gerecht, nach dem jeder Bürger wissen können muß, „wer was wann und bei welcher Gelegenheit über ihn weiß“.[142] Der Bürger muß im Einzelfall wissen, ob personenbezogene Daten von der Justiz und an welche Stellen sie übermittelt worden sind. Eine Regelung der Übermittlungspflichten durch Rechtsverordnung würde diesem Erfordernis nur dann gerecht werden können, wenn die Voraussetzungen für eine Datenübermittlung dort ohne Verwendung unbestimmter Rechtsbegriffe geregelt würden. Aber auch dann bleibt die *Benachrichtigungspflicht* die datenschutzfreundlichste Lösung, da nur sie gewährleistet, daß der Betroffene überhaupt von Übermittlungen erfährt. Die eilige Wiederaufnahme des Gesetzgebungsvorhabens darf nicht dazu führen, daß den datenschutzrechtlichen Belangen nicht ausreichend Rechnung getragen wird. Nachdem das Justizmitteilungsgesetz schon so lange erwartet wird, darf es jetzt nicht zu einem „datenschutzrechtlichen Schnellschuß“ werden.

1994 hatten die Länder dem Bundesrat den Entwurf eines *Strafverfahrensänderungsgesetzes 1994*[143] zugeleitet, der die notwendigen datenschutzrechtlichen Regelungen im Strafverfahrensrecht schaffen sollte, aber zu weitgehende Eingriffe in das Recht auf informationelle Selbstbestimmung zuließ. Dieser Gesetzentwurf hat offensichtlich keine Aussicht, vom Parlament verabschiedet zu werden, da die Bundesregierung auf eine Stellungnahme verzichtet und stattdessen einen eigenen Gesetzentwurf angekündigt hat, der noch immer nicht vorliegt. Wir hoffen sehr, in unserem nächsten Jahresbericht über einen Fortschritt dieses dringenden Gesetzgebungsvorhabens berichten zu können.

Sensible Daten in Urteilen

Wenn das Familiengericht die Ehescheidung ausgesprochen hat, erhalten die Parteien ein Scheidungsurteil zugestellt, das in seinem Urteilstenor die einzelnen Entscheidungen des Gerichtes – wie beispielsweise den Scheidungsausspruch, die Entscheidung über die elterliche Sorge oder den Versorgungsausgleich – enthält. Das Urteil enthält außerdem den Tatbestand mit vielen persönlichen Daten und die Entscheidungsgründe. Nach der Scheidung verlangen zahlreiche Behörden und sonstige Stellen (Meldebehörde, Standesamt, Finanzamt, Arbeitgeber etc.) von den Betroffenen die Vorlage des Scheidungsurteils mit allen darin enthaltenen Daten.

Bei der Übersendung des vollständigen *„Ehescheidungsverbundurteils“* werden den einzelnen Stellen immer auch Daten übermittelt, die sie für die Erfüllung ihrer Aufgaben nicht benötigen. In den meisten Fällen würde der jeweiligen Stelle für ihre Aufgabenerfüllung auch ein Auszug aus dem Urteilstenor ausreichen. Die Parteien wissen dies jedoch in der Regel nicht und legen aus Unkenntnis immer wieder das vollständige Urteil vor. Da die Partei nach Beendigung des Ehescheidungsverfahrens nicht mehr anwaltlich vertreten ist, hatten wir bei der Senatsverwaltung für Justiz angeregt, den Parteien zusammen mit der Versendung des Urteils ein Merkblatt zuzusenden, das auf die Möglichkeit hinweist, daß für die verschiedenen Vorlagezwecke Auszüge aus dem Ehescheidungsverbundurteil angefertigt werden können.

Unsere Anregung ist von der Senatsverwaltung für Justiz leider nicht aufgegriffen worden. Sie hält ein solches Merkblatt für die Parteien nicht für erforderlich, da in vielen Fällen geschwärzte Kopien zur Vorlage bei den Stellen ausreichen würden und kein weiterer Nachweis verlangt würde. In anderen Bundesländern ist der Vorschlag eines Merkblattes für die Parteien im Scheidungsverfahren dagegen aufgegriffen worden.

Wenn eine gerichtliche Entscheidung über das Bestehen – oder Nichtbestehen – eines Eltern- oder Kindschaftsverhältnisses ergangen ist, wird dem zuständigen Standesamt immer dann ein vollständiges Urteil übermittelt, wenn eine Eintragung im Personenstandsbuch erforderlich ist. Durch die Übersendung des voll-

138 BGBl. I 3186; Jahresbericht 1994, 128 ff.
139 EuGRZ 1995, 353 – 1BvR 2226/94
140 Jahresbericht 1993, 4.7
141 BT-Drs. 12/1399
142 BVerfGE 65, 1, 43
143 Jahresbericht 1994, 4.8; Jahresbericht 1992, 4.3; Jahresbericht 1991, 3.6

ständigen Urteils erhält das zuständige Standesamt Daten, die weit über den erforderlichen Umfang hinausgehen und besonders sensibel sind, da sie den internen Bereich der Familie betreffen.

Eine vollständige *Urteilsübermittlung an das Standesamt* ist in diesen Fällen nicht erforderlich, da das Standesamt für seine Aufgabenerfüllung diesen Datenumfang nicht benötigt. Der Erforderlichkeitsgrundsatz ist auch bei der Anwendung der Verwaltungsvorschrift „Mitteilungen in Zivilsachen" heranzuziehen, die in Berlin übergangsweise einer gesetzlichen Regelung gleichgestellt sind[144] und in VIII/1 eine Datenübermittlung an die Standesämter vorsehen. Auch die Senatsverwaltung für Inneres hat uns bestätigt, daß bei der überwiegenden Zahl der mitzuteilenden Entscheidungen die Übersendung einer Urteilsausfertigung ohne vollständigen Tatbestand und ohne Entscheidungsgründe in Verbindung mit den Angaben im jeweiligen Mitteilungsvordruck für die Aufgabenerfüllung des Standesbeamten ausreichend sei. Damit reichen in den meisten Fällen die Angabe des Familiennamens, des Vornamens, der Anschrift, des Ortes und Tages der Geburt, des Familienstandes, der Staatsangehörigkeit und der Eheschließung der Mutter aus.

Die Senatsverwaltung für Justiz hat uns hierzu mitgeteilt, daß der von uns gewünschten Beschränkung der Mitteilungspflicht aus ihrer Sicht keine durchschlagenden Bedenken entgegenstehen würden. Wenn die Senatsverwaltung für Inneres ihre Zustimmung als zuständige Behörde für das Personenstandswesen erteilt, will die Senatsverwaltung für Justiz bei dem federführenden Bayerischen Justizministerium eine Änderung der bundeseinheitlichen Mitteilungen in Zivilsachen vorschlagen.

Unabhängig davon sollte aber bereits jetzt der Umfang der übermittelten Daten auf der erforderliche Maß reduziert werden.

Post von der Staatsanwaltschaft

Eine Hochschule wunderte sich, als sie von der Staatsanwaltschaft eine Anklageschrift erhielt, bei der die Angeklagte zum einen nicht Mitglied der Hochschule war. Die Anklageschrift enthielt außer den Daten der Angeklagten zum anderen auch Daten der Mitangeklagten und Zeugen. Aus einem Anschreiben zu der Anklageschrift konnte die Hochschule ersehen, daß es sich um eine Mitteilung nach der Anordnung über Mitteilungen in Strafsachen (MiStra) handeln sollte.

Im vorliegenden Fall war die Anklageschrift an die Hochschule übermittelt worden, ohne daß die Voraussetzungen für eine Übermittlung vorlagen. Nach Nr. 28 MiStra sind in *Strafsachen gegen Studierende* von Hochschulen nur bestimmte rechtskräftige Entscheidungen mitzuteilen. Eine Mitteilung der Anklageschrift war bereits deshalb unzulässig. Eine Mitteilung rechtskräftiger Entscheidungen in Strafsachen gegen Studierende von Hochschulen, Höheren Fachschulen oder Fachakademien ist darüber hinaus nur in den Ländern Baden-Württemberg, Bayern und Schleswig-Holstein zulässig. In Berlin hätte daher auch ein Urteil der Hochschule nicht übermittelt werden dürfen.

Auf unsere Beanstandung hin hat die Senatsverwaltung für Justiz bestätigt, daß die Datenübermittlung unzulässig war. Die Problematik, inwieweit Daten Dritter bei Mitteilungen nach MiStra übermittelt werden dürfen, wird wegen ihrer grundsätzlichen Bedeutung auch für andere Mitteilungstatbestände der MiStra bei der Senatsverwaltung für Justiz noch diskutiert.

Leider ist in diesem Zusammenang auch zu berichten, daß Mitteilungen in Strafsachen immer wieder offen versandt werden, obwohl die MiStra eine Versendung in einem *verschlossenen Umschlag* und unter Verwendung eines *grünen Klebezettels,* auf dem u. a. auch „Vertraulich, Verschlossen" zu stehen hat, zu erfolgen hat. Nach § 5 Abs. 2 BlnDSG sind zudem bei dem Transport auch von Schriftstücken die erforderlichen Maßnahmen zu treffen, um den Zugriff Unbefugter zu unterbinden. Auch Irrläufer sind bei der offenen Versendung keine Seltenheit gewesen.

Die Senatsverwaltung für Justiz hat uns als Maßnahmen gegen diese datenschutzrechtlichen Mängel mitgeteilt, daß in Zukunft bei der Versendung geheimhaltungsbedürftiger personenbezogener Daten mehr Stichproben, Untersuchungen und Kontrollen durchgeführt werden sollen. Daneben soll eine regelmäßige Belehrung der Mitarbeiter durchgeführt werden. Bei der Staatsanwaltschaft I sind die Kanzleien noch einmal darauf hingewiesen worden, daß bei Mitteilungen in Strafsachen der Hinweis „Verschlossen, Vertraulich" auf dem Schriftstück anzubringen und rot *zu unterstreichen* sei.

Opferschutz durch Zeugenschutz

Seit einiger Zeit erhalten wir vermehrt Anfragen von Bürgern und öffentlichen Bediensteten zu der Handhabung der Zeugenschutzregelungen der Strafprozeßordnung. Die Bürger fragen an, ob es zulässig ist, daß dem Angeklagten ihre Adresse (als Zeugen im Verfahren) mitgeteilt wird. Insbesondere bei Körperverletzungsdelikten besteht bei vielen Bürgern Angst vor Belästigungen oder Repressalien durch den Angeklagten.

Im Zusammenhang mit der Bekämpfung der organisierten Kriminalität sind in die Strafprozeßordnung (StPO) zusätzliche Zeugenschutzregelungen aufgenommen worden. Nach § 68 Abs. 2 StPO kann einem gefährdeten Zeugen generell im strafrechtlichen Verfahren (also auch bei staatsanwaltschaftlichen Vernehmungen[145]) gestattet werden, statt des Wohnortes seine *Dienst- oder Geschäftsanschrift* oder eine besondere, ladungsfähige Anschrift anzugeben, wenn Anlaß zu der Besorgnis besteht, daß durch die Angabe des Wohnortes der Zeuge oder eine andere Person gefährdet werden.

Eine Gefährdung ist nicht bereits dann zu besorgen, wenn bloße Belästigungen – wie Telefonanrufe oder fingierte Warensendungen – befürchtet werden. Sie ist z. B. gegeben, wenn schon ein früherer Anschlag auf den Zeugen oder einen Dritten erfolgt oder angedroht worden ist und dies mit den Bekundungen des Zeugen im gegenwärtigen Verfahren zusammenhängt. Die Gefährdung kann sich aber auch aufgrund kriminalistischer Anhaltspunkte, kriminologischer Erfahrungen oder der Lebenserfahrung ergeben. Dies dürfte insbesondere in Verfahren der organisierten Kriminalität der Fall sein. Ob eine Gefährdung vorliegt, ist jedoch immer im Einzelfall zu entscheiden.

Auch in der Anklageschrift (§ 200 Abs. 1 StPO) und der Namhaftmachung der Zeugen durch das Gericht gemäß § 222 Abs. 1 StPO genügt in den Fällen, in denen ein Zeuge konkret gefährdet ist, die Angabe einer ladungsfähigen Anschrift, die nicht die Wohnanschrift des Zeugen sein muß.

Die Möglichkeit, daß ein Täter die *Anschrift eines Zeugen* erfährt, kann dennoch nicht ausgeschlossen werden. Die Anschrift des Zeugen kann sich in der strafrechtlichen Ermittlungsakte befinden, in die der Verteidiger des Beschuldigten nach § 147 StPO einsehen kann. Der Angeklagte oder Beschuldigte könnte daher über seinen Verteidiger die Anschrift des Zeugen erfahren.

Auf die Angabe von *Vor- und Zunamen* eines Zeugen kann in der Regel nicht verzichtet werden. Hier ist zu bedenken, daß zur Verteidigung für einen Beschuldigten die Kenntnis der Beweismittel zur Prüfung der Glaubwürdigkeit der Zeugen notwendig ist, und hierzu gehören auch die Zeugen.

Eine *Geheimhaltung der Identität* des Zeugen, d. h. auch des Namens des Zeugen, ist unter den Voraussetzungen des § 68 Abs. 3 StPO möglich. Dies setzt einen Anlaß zur Besorgnis einer konkreten Gefährdung von Leib, Leben oder Freiheit des Zeugen oder einer anderen Person voraus. Der Gesetzgeber hat hier insbesondere an Verfahren der Betäubungsmittel- oder sonstigen organisierten Kriminalität gedacht. Liegt ein Anlaß zur Besorgnis einer konkreten Gefährdung vor, muß der Zeuge keine Angaben zu seiner Identität machen. Er muß in der Hauptverhandlung jedoch auf Befragen angeben, in welcher Eigenschaft ihm die Tatsachen, die er begründet, bekanntgeworden sind. In diesem Fall dürften auch die Angaben zur Identität des Zeugen nicht zu strafrechtlichen Ermittlungsakten genommen werden, so daß auch der Verteidiger des Beschuldigten bei der Akteneinsicht die Identität dieser erheblich gefährdeten Zeugen nicht erfährt.

Das Gericht kann zudem nach § 247 StPO anordnen, daß sich der Angeklagte während einer Vernehmung aus dem Sitzungszimmer entfernt, wenn zu befürchten ist, ein Mitangeklagter oder ein Zeuge werde bei seiner Vernehmung in Gegenwart des Angeklagten nicht die Wahrheit sagen. Das gleiche gilt, wenn bei der

144 § 29 Abs. 2 AGGVG

145 § 161 a Abs. 1 Satz 2 i. V. m. § 68 StPO

Vernehmung einer Person als Zeuge in Gegenwart des Angeklagten die dringende Gefahr eines schwerwiegenden Nachteils für die Gesundheit dieser Person besteht. Über die Anordnung der Entfernung des Angeklagten in der Hauptverhandlung entscheidet das Gericht.

Die Zeugenschutzregelungen regeln nicht den häufigen Fall, daß das Opfer eines Körperverletzungsdeliktes Angst vor Repressalien durch den Täter hat und deshalb bei Vernehmungen seine Wohnanschrift nicht angeben will. Bei den an uns gerichteten Anfragen handelte es sich oftmals auch um jugendliche Opfer. In diesen Fällen wäre es Sache des Gesetzgebers, eine Lösung des Konfliktes zwischen Opfer- bzw. Zeugenschutz und den Verfahrensrechten des Angeklagten zu finden. Die Senatsverwaltung für Justiz hält eine besondere *Regelung für jugendliche Opfer* für entbehrlich, da die bestehenden Zeugenschutzregelungen nicht an das Alter der zu schützenden Person anknüpfen.

Auf eine Zeugenschutzmöglichkeit, die in der Praxis auch genutzt wird, wollen wir an dieser Stelle noch einmal ausdrücklich hinweisen: *Bei Mitarbeitern des Landes Berlin,* die in ihrer Mitarbeiterfunktion als Zeuge vor Gericht aussagen sollen, besteht die Möglichkeit, statt des Wohnortes den Dienstort gegenüber der Polizei bzw. der Staatsanwaltschaft anzugeben (§ 68 Abs. 1 Satz 2 StPO). Wir haben den Polizeipräsidenten in Berlin gebeten, die Betroffenen hierauf hinzuweisen.

Zulassung von Rechtsanwälten

Ein Bürger beantragte bei der Senatsverwaltung für Justiz die Zulassung zur Rechtsanwaltschaft. Auf den Antragsunterlagen kreuzte er bei der Frage nach Vorstrafen das Feld „Nein“ an. Als der von der Senatsverwaltung angeforderte unbeschränkte Bundeszentralregisterauszug eintraf, stellte sich heraus, daß im Bundeszentralregister noch Vorstrafen eingetragen waren. Daraufhin forderte die Senatsverwaltung auch die Strafurteile bei den Gerichten an. Sowohl den Bundeszentralregisterauszug in Kopie als auch zwei Strafakten übersandte die Justizverwaltung an die Rechtsanwaltskammer, die im Rechtsanwaltszulassungsverfahren ein Gutachten abzugeben hat.

Im Rechtsanwaltszulassungsverfahren wird bei jedem Antragsteller eine *unbeschränkte Bundeszentralregisterauskunft* eingeholt. Auf dem Fragebogen des Antragsformulares wird der Antragsteller darauf hingewiesen, daß die Landesjustizverwaltung nach § 41 Abs. 1 Nr. 2 Bundeszentralregistergesetz (BZRG) ein Recht auf unbeschränkte Auskunft aus dem Bundeszentralregister hat. Da § 41 Abs. 1 Nr. 2 BZRG keine Erhebungsbefugnis für oberste Landesbehörden darstellt, kann die Datenerhebung allein an § 36 a Abs. 1 Bundesrechtsanwaltsordnung (BRAO) gemessen werden. Nach dieser Vorschrift sind nur die erforderlichen Beweismittel heranzuziehen, und der Bewerber hat sein Einverständnis in die Verwendung von Beweismitteln zu erklären, wenn sein Recht auf informationelle Selbstbestimmung betroffen ist. Die Einholung eines unbeschränkten BZR-Auszuges muß daher im Einzelfall für die Antragsbearbeitung erforderlich sein. Dies ist hier nicht der Fall, denn selbst für die Prüfung der Würdigkeit des Antragstellers (§ 7 BRAO) reicht die Einholung eines *Führungszeugnisses* aus, das die schwerwiegenden Straftaten enthält und das der Antragsteller nach § 30 BZRG selbst beantragen soll. Die Anforderung eines Führungszeugnisses stünde auch im Einklang mit einer Empfehlung der Senatsverwaltung für Inneres aus dem Jahr 1994, wonach die Einholung unbeschränkter Bundeszentralregisterauszüge auf Fälle mit erheblicher Bedeutung beschränkt und jedes Auskunftsersuchen entsprechend begründet werden sollte.

Auch die *Anforderung der Strafakten* halten wir für unzulässig. Da den Antragsteller bei einem ihn begünstigenden Verwaltungsakt eine Mitwirkungspflicht bei der Ermittlung des Sachverhaltes trifft, muß er seine Zustimmung zur Verwendung von Beweismitteln erteilen, die unter das informationelle Selbsbestimmungsrecht fallen. Eine solche Zustimmung lag hier jedoch nicht vor. Da die Akten zudem erst nach Ablauf der Tilgungsfrist im BZR von den Gerichten übersandt worden sind, bestand für die Akten zum Zeitpunkt der Übermittlung bereits ein *Verwertungsverbot.*

Eine Befugnis für die Übermittlung des unbeschränkten Bundeszentralregisterauszuges und der Strafakten an die Rechtsanwaltskammer lag schon deshalb nicht vor, weil bereits die Erhebung der Daten unzulässig war. Wir haben der Senatsverwaltung empfohlen, in Zukunft auf die Einholung unbeschränkter Bundeszentralregisterauszüge zu verzichten und im übrigen das Einverständnis des Antragstellers zur Anforderung personenbezogener Daten des Antragstellers sowie zur Übermittlung der Daten an die Rechtsanwaltskammer einzuholen.

5.8 Kulturelle Angelegenheiten

Opfernamen auf Denkmälern

Im vergangenen Jahr wurde mehrfach die Frage öffentlich diskutiert, wie in Form eines Mahn- oder Denkmals der Judenvernichtung in der Zeit des Nationalsozialismus gedacht werden kann. Im Bezirk Steglitz wurde eine *Spiegelwand* aufgestellt, auf der die Namen von 2 000 ermordeten jüdischen Menschen eingraviert sind. Dagegen sind die Pläne für ein *Denkmal für die ermordeten Juden Europas* zwischen Brandenburger Tor und Potsdamer Platz bisher nicht verwirklicht worden. Der von der Jury ausgewählte Entwurf sieht vor, auf einer begehbaren Platte, die fast 100 × 100 Meter groß sein und 11 Meter aus dem Boden ragen soll, die Namen von 4,2 Millionen Opfern des Holocaust, soweit sie bekannt sind, anzubringen.

Nach der Vorstellung der Urheber dieses Entwurfs für ein Mahnmal, der sich die Jury angeschlossen hat, sollten den in den Konzentrationslagern mit Nummern versehenen Opfern ihre Namen und damit ihre Würde zurückgegeben werden. Dagegen sei ein Gedenken an anonymen Denkmälern, seien es abstrakte Darstellungen oder figürliche Symbole, „verhältnismäßig oberflächlich“. Der Betrachter könne sich der individuellen Betroffenheit leichter entziehen.[146]

Der ausgewählte Entwurf für das *Holocaust-Mahnmal* ist von verschiedenen Seiten heftig kritisiert worden. Dabei haben auch Gesichtspunkte des Datenschutzes eine Rolle gespielt. Die Historiker Arno Lustiger und Julius Schoeps haben angekündigt, daß sie gerichtlich gegen eine Nennung der Namen ihrer ermordeten Angehörigen auf dem Mahnmal vorgehen und sich dabei auf den Datenschutz stützen würden.[147] Auch der Bundesbeauftragte für den Datenschutz ist von Angehörigen der Ermordeten angerufen worden, die befürchteten, daß durch das Bekanntmachen von Namen auf einem jedem zugänglichen Denkmal Hinweise auf jüdische oder vermeintlich jüdische Familien gegeben werden könnten.

Der Vorsitzende des Zentralrats der Juden in Deutschland, Ignatz Bubis, hat seinerseits darauf hingewiesen, daß die bloße Nennung der Nachnamen der Ermordeten nicht ausreicht, um ihnen ihre Individualität zurückzugeben, da bestimmte jüdische Nachnamen sehr häufig sind. Es müßten – wenn man diesem Vorschlag folgen wolle – Vornamen, Geburts- und Todesdatum dazukommen. Dementsprechend seien in Frankfurt die Namen von über 11 000 Frankfurter Juden in die dortige Friedhofsmauer mit Geburts-, Todes- oder Deportationsdaten eingefügt worden. Bei sechs Milionen Opfern sei dies nicht möglich. Bubis wörtlich: „Da entsteht der Eindruck eines Registers.“[148]

Es ist nicht Sache des Datenschutzbeauftragten, sich zur Angemessenheit der Form eines Mahnmals für diesen Zweck zu äußern. Da aber die Angehörigen der Ermordeten selbst diese Frage aufgeworfen haben, sollte im weiteren Verlauf der noch nicht beendeten Diskussion über das nationale Mahnmal am Potsdamer Platz der Gesichtspunkt des Datenschutzes stärker miteinbezogen werden. Auch 50 Jahre nach dem Ende der Nazi-Diktatur muß das Persönlichkeitsrecht der Opfer des Holocaust sehr sorgfältig bedacht werden. Die Überlegung der Befürworter des Entwurfs für die begehbare Grabplatte mit den Namen, damit könne eine persönliche Betroffenheit des Betrachters ausgelöst werden, erscheint zwar plausibel. Mit dem Argument, die namentliche Nennung der Ermordeten würde diesen ihre Würde zurückgegeben, können deren persönlichkeitsrechtliche Belange

146 so der damalige Bausenator Nagel, Landespressedienst vom 3. Juli 1995
147 vgl. Tageszeitung vom 14. und 17. Juli 1995
148 Frankfurter Allgemeine Zeitung vom 29. Juni 1995

aber nicht einfach überspielt werden. Vielmehr müssen die Angehörigen zumindest ein Mitspracherecht erhalten, wenn der ausgewählte Entwurf überhaupt in dieser Form realisiert werden sollte. Die monumentale Nennung aller bekannten Opfernamen unter Hinwegsetzung über die Gefühle und Interessen der Angehörigen würde die Opfer vielmehr zum Instrument einer Politik des öffentlichen Gedenkens machen und sie damit erneut entwürdigen. Dieser Eindruck würde sich noch dadurch verstärken, daß die geplante Grabplatte begehbar sein soll und die Namen der Opfer nicht nur betrachtet, sondern auch „betreten" werden sollen.

Datenschutz in Staatskirchenverträgen

Die herausgehobene verfassungsrechtliche Stellung der Religionsgesellschaften, insbesondere der Evangelischen Kirche in Berlin-Brandenburg, der Katholischen Kirche (Erzbistum Berlin) und der Jüdischen Gemeinde zu Berlin, macht es erforderlich, die rechtlichen Beziehungen zwischen dem Land Berlin und den Kirchen staatsvertraglich zu regeln. Dabei sind auch datenschutzrechtliche Fragen von Bedeutung.

Während der Staatsvertrag über die Beziehungen des Landes Berlin zur Jüdischen Gemeinde zu Berlin ohne unsere Beteiligung ausgehandelt worden und im Februar 1994 in Kraft getreten war[149], beteiligte uns die Senatsverwaltung für Kulturelle Angelegenheiten frühzeitig an den Verhandlungen, die seit Ende 1994 mit der Evangelischen Kirche in Berlin-Brandenburg und dem Erzbistum Berlin geführt werden.

Auch wenn die Verhandlungen mit beiden Kirchen noch nicht zum Abschluß gekommen sind, kann festgehalten werden, daß zumindest in dem Staatsvertrag mit der Evangelischen Kirche in Berlin-Brandenburg voraussichtlich eine Regelung des *Beichtgeheimnisses und der Seelsorge aufgenommen* werden wird, wonach Geistliche in Verfahren, die dem Landesrecht unterliegen, zur Verweigerung des Zeugnisses über das berechtigt sind, was ihnen in ihrer Eigenschaft als Seelsorger anvertraut oder bekannt geworden ist. Ursprünglich wollte sich das Land Berlin lediglich dazu verpflichten, dafür einzutreten, daß die gesetzlichen Bestimmungen zu diesem Bereich aufrechterhalten bleiben.

Im Bereich des *Meldewesens* konnte in einem Zusatz zum Schlußprotokoll zum Entwurf des Staatsvertrages mit der Evangelischen Kirche klargestellt werden, daß entsprechend der Regelung im Meldegesetz das Land aufgrund der von der Kirche vorzulegenden kirchengesetzlichen Regelungen sowie deren Umsetzung feststellt, ob im Bereich der Kirche ausreichende Datenschutzmaßnahmen bestehen.

Es bleibt zu hoffen, daß entsprechende Regelungen auch in den angestrebten Staatsvertrag mit der Katholischen Kirche aufgenommen werden.

5.9 Schule, Berufsbildung und Sport

Integration von behinderten Kindern

Seit knapp zwanzig Jahren gibt es die Möglichkeit, behinderte und nichtbehinderte Kinder gemeinsam zu unterrichten. Den anfänglichen Schulversuchen folgte 1989 die Ergänzung des Schulgesetzes um eine Regelung zur Integration von Schülern mit sonderpädagogischem Förderbedarf (§ 10 a Schulgesetz). Nach dieser Rechtsvorschrift sind bis zum Schuljahr 1996/97 die Voraussetzungen für das uneingeschränkte Wahlrecht der Erziehungsberechtigten von Schülern mit festgestelltem sonderpädagogischem Förderbedarf zu schaffen. Die Eltern können zwischen einer allgemeinen Schule und einer Sonderschule wählen. Jährlich werden ungefähr fünfhundert behinderte Schüler in allgemeine Schulen aufgenommen.

Die Regelung zu den Schülern mit sonderpädagogischem Förderbedarf im Berliner Schulgesetz ermächtigt das für Schulwesen zuständige Mitglied des Senats, eine Rechtsverordnung für die konkrete Umsetzung zu schaffen. Eine solche Rechtsverordnung ist erforderlich, wie im vergangenen Jahr die Probleme einer zunehmenden Zahl von Schülern, die den Grundschulbereich verlassen und in den Sekundarbereich I übergehen, zeigten. Die Schuldatenverordnung gibt den Förderausschüssen eine Befugnis zur Verarbeitung personenbezogener Daten einschließlich des Verfahrens der Kind-Umfeld-Diagnostik, sowie zur Verarbeitung medizinischer und psychologischer Daten. Rechtlich noch nicht festgeschrieben hingegen sind die Aufgaben und die Zusammensetzung des Förderausschusses selbst.

Des weiteren wurde deutlich, daß die Tätigkeit der Förderausschüsse sowie die sonderpädagogische Förderarbeit eine Reihe von Datenerhebungen erforderlich machen, für die gegenwärtig keine Rechtsgrundlage besteht. So werden zwischen der Schule und der Schulaufsicht Daten übermittelt, denen man sicherlich eine Relevanz bezüglich der Förderarbeit nicht absprechen kann, die jedoch weit über den zulässigen Rahmen der Schuldatenverordnung hinausgehen. So wird beispielsweise erfragt, seit wann die Familie in Deutschland lebt, welche Besonderheiten das schulische Lernen beeinträchtigen oder welches die bevorzugte Sprache der Familie ist. Ein bloßer Hinweis auf die Vertraulichkeit dieser Angaben auf den Erhebungsbogen legitimiert jedoch nicht deren Erhebung. Gegenwärtig erfolgt die Feststellung des sonderpädagogischen Förderbedarfs auf Grundlage eines Rundschreibens, das Übergangsregelungen für das Schuljahr 1993/94 traf und erst mit Inkrafttreten der Rechtsverordnung nach § 10 a Schulgesetz aufgehoben werden soll.

Schulverwaltungsprogramme

Aufgrund einer Ausschreibung der Senatsverwaltung für Schule, Berufsbildung und Sport prüfte eine Arbeitsgruppe von Lehrern bei der Landesbildstelle die Praktikabilität und Anwendbarkeit von Datenverarbeitungsprogrammen für Zwecke der Schulverwaltung. Diese Arbeitsgruppe empfahl drei Programmpakete. Daraufhin prüften wir aus datenschutzrechtlicher Sicht die Anwendbarkeit dieser Programme. Für die Programmteile *„Stundenplan- und Vertretungsplanerstellung"* haben wir das Informationsverarbeitungsgesetz als hinreichende Rechtsgrundlage angesehen. Allerdings teilten wir sowohl der Senatsschulverwaltung als auch den Personalräten mit, daß für die Nutzung einzelner Felder sowie für die Bestimmung des Sicherheitsstandards der Abschluß einer Dienstvereinbarung erforderlich ist. So ist bei den Vertretungsplanprogrammen eine Abgrenzung von Zwecken der Personaldatenverarbeitung, für deren Verarbeitung die Schule selbst keine Befugnis hat, notwendig.

In unsere Stellungnahmen flossen auch eine Reihe von Gedanken der Teilnehmer am *„Runden Tisch Datenschutz in der Schule"* ein, der sich unter dem Dach der Technologieberatungsstelle beim Deutschen Gewerkschaftsbund zusammengefunden hat.

Elternadressen

Die Schuldatenverordnung regelt abschließend den Umgang mit Elternadressen und Telefonnummern innerhalb der Schule. Namen, Anschrift und Telefonnummern der *Elternvertreter* können an die Eltern der Klasse und an den Vorsitzenden der Gesamtelternvertretung weitergegeben werden. Auch die Angaben des Vorsitzenden dürfen den Elternvertretern mitgeteilt werden. Für alle darüber hinausgehenden Übermittlungen ist die Einwilligung der Betroffenen erforderlich. An vielen Schulen tauschen die Eltern anläßlich von Elternabenden freiwillig die Adressen aus.

Nicht geregelt ist hingegen der Umgang mit Adreßdaten gewählter Vertreter in Bezirks- bzw. Landesgremien. Eine besondere Regelung ist auch nicht erforderlich. Diese Gremien dürfen bei der Wahrnehmung ihrer Aufgaben auch ohne Einwilligung des Betroffenen (gewählten Vertreters) Angaben verarbeiten, soweit dies für die allgemeine Verwaltungstätigkeit des Gremiums erforderlich ist und schutzwürdige Belange des Betroffenen nicht entgegenstehen. Eine Übermittlung von Adreß- und Telefonangaben gewählter Elternvertreter von der Schule an die Bezirks- bzw. Landesgremien ist zulässig, wenn nicht auf die Vertraulichkeit dieser Angaben hingewiesen wurde. Die Nutzung durch die Gremien muß sich jedoch auf die Wahrnehmung der übertragenen Aufgaben beschränken.

149 GVBl. 1994, S. 67

Eine Übermittlung von Anschriften der *Mitglieder und Vorsitzenden von Bezirks- oder Landesausschüssen* an Dritte ist dagegen anders zu bewerten. Hier steht nicht die Arbeitsfähigkeit der Gremien selbst im Mittelpunkt, sondern die „Erreichbarkeit" bzw. „Ansprechbarkeit" der Mitglieder der Gremien durch andere Personen. Möchte also ein Dritter zu einer Veranstaltung Elternvertreter einladen, so wäre es nur zulässig, den Namen sowie die Anschriften der von ihnen gesuchten bzw. vertretenen Schulen zu übermitteln. Eine Herausgabe von Telefonnummern und Privatadressen ist nicht erforderlich und damit auch nicht zulässig.

5.10 Soziales

Noch immer: Datenerbe des Krieges

Die Deutsche Dienststelle für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen Deutschen Wehrmacht *(Wehrmacht-Auskunftsstelle – WASt –)* ist, vermutlich auch einigungsbedingt, seit Jahren in besonderem Maße mit datenschutzrechtlichen Fragestellungen konfrontiert. So stellt sich die Frage, inwieweit die Deutsche Dienststelle befugt ist, amerikanischen Behörden Auskunft zu erteilen.

Mit dem Gesetz über die Datenverarbeitung bei der Deutschen Dienststelle[150] ist eine Auskunfts- und Datenübermittlungsregelung geschaffen worden, die die Aufgabenstellungen der WASt definiert. Jedoch gibt es weder hier noch in der aufgrund dieses Gesetzes ergangenen Verordnung vom 29. März 1994[151] eine ausdrückliche Befugnis zur Datenübermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes. Zwar verweist das Gesetz über die Verarbeitung personenbezogener Daten bei der WASt auf Vorschriften des zweiten Kapitels des Sozialgesetzbuchs X. Regelungen sind hier jedoch nicht einschlägig. Die Übermittlung personenbezogener Daten aus der Deutschen Dienststelle an *Einwanderungsbehörden* der USA ist von der Einwilligung der Betroffenen abhängig zu machen. Denn nach § 67 b Abs. 1 SGB X ist die Verarbeitung von Sozialdaten außer „nach den nachfolgenden Vorschriften" auch zulässig, soweit der Betroffene eingewilligt hat. Der § 77 SGB X ist nicht als entgegenstehende Regelung für Sonderfälle im nationalen Recht anzusehen, weil diese Vorschrift gerade den Datenexport ins Ausland generell regelt. Die *Einwilligung i*st allerdings eine Obliegenheit des Betroffenen. Ihre Verweigerung kann dazu führen, daß die US-Einwanderungsbehörden den Antrag eines Betroffenen auf Einwanderung/Einbürgerung ablehnen. Darauf sollte der Betroffene hingewiesen werden. Außerdem sollte ihm – ähnlich wie bei der Erteilung eines polizeilichen Führungszeugnisses aus dem Bundeszentralregister – die Möglichkeit gegeben werden, selbst Kenntnis von den bei der Deutschen Dienststelle über ihn vorhandenen Unterlagen zu nehmen, bevor er seine Zustimmung zur Übermittlung an Dienststellen in den Vereinigten Staaten gibt.

> *Um eine Dissertation in einem wichtigen Punkt abschließen zu können, wurde zum Thema: „Täter-Opfer-Dichotomie am Beispiel des Konzentrationslagers Bergen-Belsen" im Rahmen des „Antisemitismus-Forschungsprogramms" bei uns nachgefragt, inwieweit eine Einsicht in Unterlagen des Krankenbuchlagers und der Deutschen Dienststelle möglich sei. Es waren dabei bereits erhebliche Vorarbeiten geleistet, doch wurden weitere Daten über das SS-Überwachungspersonal des KZ Bergen-Belsen benötigt und vermutet, daß diese Angaben aus dem Krankenbuchlager Berlin in Verbindung mit der WASt ermittelt werden könnten. Sowohl vom Krankenbuchlager als auch von der Deutschen Dienststelle waren einzelne Auskünfte zunächst abgelehnt worden.*

Wir haben die Anfrage zum Anlaß genommen, Grundsatzfragen der wissenschaftlichen Forschung anhand der Unterlagen des *Krankenbuchlagers* und der Deutschen Dienststelle zu klären. Sowohl im Krankenbuchlager als auch in der Deutschen Dienststelle befinden sich *Personaldaten* und medizinische Daten, also Daten, die der *ärztlichen Schweigepflicht* unterliegen, und grundsätzlich nicht für wissenschaftliche Forschung vorgehalten werden. Vielmehr haben beide Einrichtungen die Aufgabe, die Klärung sozialrechtlicher Ansprüche zu unterstützen. Tatsächlich sind dort Datenbestände, die für die eigentliche Aufgabenerfüllung der beiden Einrichtungen nicht mehr benötigt werden, weil die Vorfälle weit zurückliegen und die Betroffenen schon vor Zeiträumen verstorben sind, die bei archivrechtlicher Betrachtungsweise einer Nutzung dieser Daten nicht mehr entgegenstehen würden. So geht das Krankenbuchlager bis weit in die Zeit vor dem ersten Weltkrieg zurück. Bei einem großen Teil der Datenbestände handelt es sich somit um Unterlagen, die eigentlich, weil sie für eine aktuelle Aufgabenerfüllung mit sozialer Zielrichtung nicht mehr benötigt werden, dem Landesarchiv angeboten werden müßten und dort auch der wissenschaftlichen Forschung zugänglich wären. Das Landesarchivgesetz, welches unmittelbar nur für die Landesarchivalien gilt, regelt die Nutzbarkeit von personenbezogenem Archivgut und hat in Weiterentwicklung des *„Mephisto-Urteils"* des Bundesverfassungsgerichts maßgebliche Aussagen zum Fortwirken des informationellen Selbstbestimmungsrechts nach dem Tode des Betroffenen gemacht. Schon in diesem Urteil hat das Bundesverfassungsgericht darauf hingewiesen, daß das allgemeine Persönlichkeitsrecht nach dem Tode des Betroffenen nur noch einem abnehmenden Schutz unterliegt und die rechtliche Schutzwirkung dann erlischt, wenn ein angemessener Zeitraum seit dem Tode verstrichen ist.[152] Das Archivgesetz hat diesen Zeitraum bei Unterlagen über Verstorbene, die vor mehr als dreißig Jahren entstanden sind, generell auf zehn Jahre nach dem Tod oder neunzig Jahre nach der Geburt, wenn der Todeszeitpunkt nicht feststeht, festgelegt.

Die Forschung darf allerdings nicht dadurch schlechter gestellt werden, daß bestimmte Datenbestände allein aufgrund organisationstechnischer Umstände noch nicht dem Landesarchiv übergeben worden sind. Denn die Besonderheit der bei der Deutschen Dienststelle und beim Krankenbuchlager vorgehaltenen Datenbestände liegt darin, daß hier auch auf längere Sicht noch nicht damit zu rechnen ist, daß der Gesamtbestand an das Landesarchiv übertragen wird. Vielmehr soll der Gesamtbestand als Einheit erhalten werden. Aufgrund der gleichartigen Interessenlage haben wir daher empfohlen, daß die beiden Dienststellen die Nutzungsregelung des § 8 Landesarchivgesetz hier zumindest entsprechend heranziehen, um auch insoweit der Forschung eine Nutzung der Daten zu ermöglichen. Voraussetzung wäre jedoch, daß durch die Dienstellen jeweils festgestellt ist, daß ein *Schutzbedürfnis* wegen des Todes des Betroffenen oder eines entsprechend abgelaufenen Zeitraumes nach dem Archivgesetz nicht mehr besteht. Auch die Schutzvorschriften nach dem Sozialgesetzbuch würden nicht mehr entgegenstehen. Dieses Ergebnis stimmt mit § 4 BlnDSG überein, wonach personenbezogene Daten Verstorbener der Schutzwirkung des Datenschutzgesetzes nicht mehr unterliegen, wenn schutzwürdige Belange der Betroffenen nicht mehr beeinträchtigt werden können. Auch nach § 35 Abs. 5 SGB I gelten die *Sozialdaten Verstorbener* nur noch in eingeschränktem Umfang als schutzbedürftig. Sie dürfen verarbeitet und genutzt werden, „wenn schutzwürdige Interessen des Verstorbenen oder seiner Angehörigen dadurch nicht beeinträchtigt werden können". Da das Sozialgesetzbuch keine festen Fristen für die Zeit nach dem Tode vorgegeben hat, könnte auch eine kürzere Frist als die zehnjährige nach dem Landesarchivgesetz in Betracht kommen. Denn auch nach dem Landesarchivgesetz, welches die zehnjährige Frist nur als Regelfall vorschreibt, können mitunter kürzere Fristen angesetzt werden, wenn das *öffentliche Interesse*, insbesondere an der *zeitgeschichtlichen Forschung*, überwiegt. Dies ist bei Untersuchungen zum Tätermilieu des Wachpersonals in nationalsozialistischen Vernichtungslagern der Fall.

Der durch den fünfzigsten Jahrestag der Befreiung des Konzentrationslagers Auschwitz aufgerüttelten Öffentlichkeit wäre es schwer zu vermitteln, daß ausgerechnet für diese Täter ein Schutzbedürfnis bejaht werden sollte. Wir meinen vielmehr, daß gerade hier kürzere Fristen hingenommen werden können, wenn das öffentliche Interesse an der Forschung und Aufklärung überwiegt. Die Deutsche Dienststelle, das Krankenbuchlager und das Landesarchiv haben sich diesen datenschutzrechtlichen Standpunkt zu eigen gemacht.

150 GVBl. 1993, 40, 49
151 GVBl. 1994, 107
152 BVerfGE 30, 173, 196

Ein Petent stammte aus einer Ehe, die frühzeitig geschieden wurde. Da das Verhältnis zum Vater immer schlecht war, hat er nie etwas über dessen Leben erfahren. Um die letzte Möglichkeit wahrzunehmen, zumindest einen Teil seines Lebens etwas näher zu beleuchten, hatte er an die Deutsche Dienststelle in der Hoffnung geschrieben, durch Einblick in die Personalakte des Vaters aus seiner Zeit bei der deutschen Wehrmacht mehr über ihn zu erfahren. Von dort bekam er die Auskunft, daß ihm aus Datenschutzgründen erst zehn Jahre nach dem Tod des Vaters Auskunft erteilt werden könne. Der Tod des Vaters lag jedoch erst fünf Jahre zurück.

Gemäß § 6 der Verordnung über die Verarbeitung personenbezogener Daten bei der Deutschen Dienststelle dürfen personenbezogene Daten an Stellen außerhalb des öffentlichen Bereiches unter anderem dann übermittelt werden, wenn *nächste Angehörige des Betroffenen* eingewilligt haben oder eine Einwilligung aus tatsächlichen oder rechtlichen Gründen nicht oder nur unter einem unverhältnismäßig hohen Aufwand erreicht werden kann und aufgrund konkreter Anhaltspunkte zu vermuten ist, daß der Betroffene oder dessen nächster Angehöriger einwilligen würden. In entsprechender Anwendung von § 8 des Landesarchivgesetzes, der eine *verkürzte Nutzungsfrist* vorsieht, wenn nächste Angehörige der Nutzung zugestimmt haben, vertraten wir auch hier den Standpunkt, daß, wenn der Angehörige sogar Dritten die Einsicht verschaffen kann (mit seiner Einwilligung), er natürlich auch selbst das Recht haben muß, in die betroffenen Unterlagen Einblick zu nehmen. Datenschutzrechtliche Bedenken bestanden somit gegen das Vorhaben des Petenten nicht.

Sozialgeheimnis auch für Ausländer

Auch nach Inkraftsetzung der vorläufigen Anwendungshinweise zu den §§ 75, 76 und 77 Ausländergesetz (AuslG)[153] wirft das Verhältnis von *Ausländergesetz und Sozialgesetzbuch* Fragen auf. Nach § 77 AuslG unterbleibt eine Übermittlung personenbezogener Daten, soweit besondere gesetzliche Verwendungsregelungen entgegenstehen. Das Sozialgeheimnis ist eine solche besondere Verwendungsregelung, die eine Datenübermittlung somit nur dann erlaubt, wenn sie im Sozialgesetzbuch selbst geregelt ist. In § 71 SGB X ist eine solche informationsrechtliche Regelung zu sehen, die mit § 76 Ausländergesetz abgestimmt ist: § 71 SGB X und § 76 AuslG unterscheiden zwischen Auskünften, die „auf Ersuchen" der Ausländerbehörde zu erteilen sind und Unterrichtungspflichten, die ohne Ersuchen der Ausländerbehörde und der Leistungsbehörde einzuhalten sind. Die Auskunftspflicht „auf Ersuchen" ist in § 71 Abs. 1 SGB X differenziert geregelt. Die Unterrichtungspflicht nach § 71 Abs. 2 SGB X, die der Unterrichtungspflicht im § 76 Abs. 2 Ausländergesetz entspricht, enthält demgegenüber jedoch nur eine *Pauschalregelung*, deren Anwendungsbereich gerade wegen ihrer allgemeinen Formulierung problematisch erscheint. Die Anwendungshinweise zu § 76 Ausländergesetz (AuslG) enthalten eine restriktive Auskunftsregelung.

Danach ist insbesondere der Verhältnismäßigkeitsgrundsatz zu beachten. Sind die mit der Übermittlung verbundenen Nachteile für den Betroffenen so schwerwiegend, daß die öffentlichen Interessen an der Datenübermittlung überwiegen, hat die Informationsweitergabe zu unterbleiben (vorl. Anwendungsweise Nr. 76.0.7). Für Ausländer, die einem besonderen Ausweisungsschutz unterliegen, besteht keine Übermittlungspflicht (Nr. 76.2.3.0.5). Da die in § 48 Abs. 1 und 3 AuslG genannten Ausländergruppen nur aus schwerwiegenden Gründen der öffentlichen Sicherheit und Ordnung und die in § 48 Abs. 2 AuslG angegebenen Minderjährigen oder Heranwachsenden nur wegen der Begehung bestimmter Straftaten ausgewiesen werden dürfen, ist der Sozialhilfebezug und Jugendhilfebezug kein Ausweisungsgrund, der gemäß § 76 Abs. 2 Nr. 3 AuslG zu übermitteln wäre. Die Unterrichtung der Ausländerbehörde muß in diesen Fällen mangels Rechtsgrundlage unterbleiben.[154]

Nach der grundsätzlichen Einigung der Bundesrepublik Deutschland und Vietnams über die Rückführung der nach dem Ende der DDR in Deutschland verbliebenen Vietnamesen forderte die Polizei ein Sozialamt auf, Auskunft über den nächsten Kontaktbesuch eines Vietnamesen beim Sozialamt zu erteilen, weil dieser an seinem gemeldeten Wohnsitz nicht für die bevorstehende Abschiebung aufgegriffen werden konnte.

Aufgrund des Ersuchens war das Sozialamt nur berechtigt, darüber Auskunft zu erteilen, daß der Aufenthalt des Betroffenen illegal war (§ 76 Abs. 1 Ziffer 2 AuslG). Für diese Tatsachen bestand jedoch kein Mitteilungsbedarf, weil sie der Ausländerbehörde bereits bekannt war. Gegen eine Auslegung des § 76 Abs. 2 AuslG dahingehend, daß über den *momentanen Aufenthalt beim Sozialamt* Auskunft zu erteilen sei, spricht der eindeutig formulierte Gesetzeswortlaut. Um die erwünschten Informationen vom Sozialamt zu erhalten, müßte die Polizei von sich aus bei der Beantragung des Ausweisungshaftbefehls die notwendige richterliche Anordnung nach § 73 SGB X zur Erteilung angemessener Auskünfte für die Durchsetzung des Ausweisungs- oder Abschiebeverfahrens mitbeantragen. Dabei käme auch die Offenbarung des nächsten Kontaktbesuches beim Sozialamt mit in Betracht, wenn sie von der richterlichen Anordnung abgedeckt ist. Dieses Ergebnis stimmt mit der Rechtslage bei deutschen Sozialhilfeempfängern überein. Auch in diesem Fall steht § 68 SGB X der Mitteilung des augenblicklichen Aufenthaltsorts entgegen, wenn nicht ein Richter die Offenbarung ausdrücklich genehmigt.

Fragen des Sozialgeheimnisses

Für das Widerspruchsverfahren enthält § 114 Bundessozialhilfegesetz (BSHG) die Regelung, daß ein Beirat „einzuschalten" ist. Gemäß § 114 Abs. 2 sind in diesem Beirat sozial erfahrene Personen vertreten, die vor dem Erlaß eines Bescheides über einen Widerspruch „beratend zu beteiligen" sind. Fraglich ist, in welchem Umfang den Beiräten ein Akteneinsichtsrecht zusteht.

Der Beirat hat ein Mitsprache-, jedoch kein Entscheidungsrecht. Die Entscheidung über den Widerspruch liegt allein bei dem Leiter der Verwaltung. Jedoch stellt die Nichtbeteiligung sozial erfahrener Personen im Widerspruchsverfahren einen erheblichen Verfahrensmangel dar. Weder das Berliner Ausführungsgesetz zum BSHG noch das BSHG selbst haben die Datenübermittlung im Rahmen dieses Verfahrens geregelt. Es ist somit auf die allgemeinen Vorschriften des Sozialgesetzbuches, insbesondere auf § 69 SGB X zurückzugreifen. Die *Mitwirkung des Beirates* bringt es naturgemäß mit sich, daß seine Mitglieder personenbezogene Daten zur Kenntnis nehmen. Ihnen gerade diese Daten vorzuenthalten, würde der Aufgabenstellung dieses „sozial erfahrenen" Personenkreises widersprechen. Wir sehen in § 114 BSHG eine hinreichende Grundlage für die Beteiligung des Sozialbeirates, wobei natürlich auch hier der datenschutzrechtliche Grundsatz der Verhältnismäßigkeit gilt. Die dem Beirat zur Kenntnis gegebenen Daten müssen geeignet und auf den erforderlichen Umfang beschränkt sein. Dies verlangt aber auch eine *Belehrung* der Mitglieder des Sozialbeirates über das Sozialgeheimnis nach § 35 SGB I sowie eine entsprechende Verpflichtung.

In einem Bezirksamt wurden Empfänger von Sozialhilfe zu gemeinnützigen Arbeiten im Sozialamt herangezogen und beim Anlegen von Sozialhilfeakten und Karteikarten sowie beim Fertigen von Bedarfsberechnungen und Bewilligungsverfügungen eingesetzt. Die Hilfeempfänger hatten Zugang zu Leistungsdaten und Leistungsverhältnissen anderer Sozialhilfeempfänger und somit die Möglichkeit, über sehr persönliche Verhältnisse Kenntnis zu erhalten (z. B. familiäre Verhältnisse, gesundheitliche Verhältnisse, Arbeits- und Einkommensverhältnisse usw.).

Dies war ein unannehmbares Verfahren, das wir unverzüglich einstellen ließen.

In Bezirksämtern bestand Unsicherheit darüber, ob es zulässig ist, Kopien von Reisepässen und Personalausweisen in den Leistungsakten aufzubewahren.

Wir haben dagegen grundsätzlich keine Bedenken, weil es zum Grundbestand des Leistungsverhältnisses gehört, die *Identität des Leistungsempfängers* eindeutig festzustellen. Die Identität ist in zuverlässiger Form nur durch die Vorlage des Personalausweises oder Reisepasses zu überprüfen. Die Erhebung der Nummer des Personalausweises oder die Aufbewahrung einer Kopie des Ausweises in der Leistungsakte halten wir deshalb für unbedenklich.

153 Jahresbericht 1994, 4.6.3

154 §§ 35 Abs. 1 SGB I, 67 SGB X, 77 Abs. 1 AuslG; vorl. Anwendungshinweise Nr. 76.2.3.0.5.3).

Die Verwendung dieser Daten bleibt zweckgebunden und unterliegt dem Sozialgeheimnis nach § 35 SGB I. Dies bedeutet jedoch nicht, daß eine Pflicht besteht, eine vollständige Kopie des Personalausweises zu den Akten zu nehmen; denn es ist durchaus nicht immer vom Verhältnismäßigkeitsgrundsatz gedeckt, wenn eine Ablichtung des Personalausweises zu den Akten genommen wird. Zum Beispiel dann nicht, wenn die Identität des Hilfeempfängers ohnehin schon aufgrund des Erstantrages feststeht, wenn eine persönliche Bekanntheit vorliegt und lediglich ein Verlängerungsantrag auf eine Leistung gestellt worden ist. Auch müssen nicht erforderliche Daten (z. B. besondere Merkmale) geschwärzt werden.

5.11 Stadtentwicklung und Umweltschutz

Regelungsdefizite beseitigt

Unmittelbar vor Ende der Legislaturperiode verabschiedete das Abgeordnetenhaus eine Reihe von Rechtsvorschriften im Umweltbereich, die auch die von uns schon seit längerem angemahnten datenschutzrechtlichen Regelungen enthalten. Eines der schwierigsten und langwierigsten Gesetzgebungsvorhaben war sicherlich das Berliner Bodenschutzgesetz.[155] Bereits vor rund zehn Jahren bzw. im Ostteil unmittelbar nach der Vereinigung begannen die Umweltbehörden *Altlastenverdachtsflächenkataster* sowie *Altlastenkataster* zu erstellen. Durch den Grundstücksbezug dieser Angaben und den daraus vielfach folgenden Personenbezug ergab sich die Notwendigkeit, auch datenschutzrechtliche Regelungen zu treffen.

Nach dem *Bodenschutzgesetz* dürfen die Daten in einem automatisierten Bodenbelastungskataster und einer Bodenschadstoffdatenbank gespeichert werden. Sie sind beim Betroffenen mit seiner Kenntnis zu erheben. Der Betroffene ist zur Auskunft verpflichtet. Auch dürfen Daten, die bei Behörden im Rahmen ihrer rechtmäßigen Tätigkeit in anderen Dateien gespeichert sind, für die *Speicherung in die Bodendatenbanken* übermittelt werden. Das Bodenschutzgesetz enthält einen *Datenkatalog,* der die zulässigen Angaben des Bodenbelastungskatasters, der Bodenschadstoffdatenbank und der Bodenzustandsdatenbank aufführt.

Da die Bodendatenbanken einen wichtigen Informationspool für verschiedene Verwaltungen darstellen, wurde eine Datenübermittlung im Rahmen eines *automatisierten Abrufverfahrens* an die Senatsverwaltungen für Bau- und Wohnungswesen und für Finanzen sowie an die Umweltämter der Bezirke zugelassen. Die Details sind in einer Rechtsverordnung festzulegen, die noch aussteht.

Auch aus datenschutzrechtlicher Sicht lobenswert ist, daß im Berliner Bodenschutzgesetz *Informationsfreiheitsrechte* der Bürger und Datenschutzansprüche zueinander ins Verhältnis gesetzt und ein Abwägungsverfahren festgelegt wurde. Danach ist jedem auf Antrag Einsicht in die Bodendatenbanken hinsichtlich der Daten zur Bodenbeschaffenheit und zu Bodenbelastungen zu gewähren, sofern eine solche Einsichtnahme nicht die schutzwürdigen Belange der Allgemeinheit oder des Betroffenen erheblich beeinträchtigt. Einsicht ist auch dann zu gewähren, wenn das Informationsbedürfnis des Antragstellers die Belange der Allgemeinheit oder das Recht des Betroffenen auf informationelle Selbstbestimmung erheblich übersteigt. Im Unterschied zum *Umweltinformationsgesetz* des Bundes wurde hier für einen speziellen Sachverhalt den Informationsfreiheitsrechten der Bürger ein erheblich höheres Gewicht zugewiesen als schutzwürdigen Belangen Betroffener (Grundstückseigentümer). Die Einzelheiten dieser Abwägung bedürfen jedoch ebenfalls der Klärung durch eine Rechtsverordnung.

Bereits vor dem Inkrafttreten des Bodenschutzgesetzes erreichten uns Anfragen, unter welchen Vorgaben *Veröffentlichungen von Altlastenkatastern* auf der Grundlage des Umweltinformationsgesetzes des Bundes möglich sind. Dies enthält eine Grundlage zur Übermittlung ohne Anhörung der Betroffenen, wenn die Haus- bzw. Grundstücksnummern nicht mitübermittelt werden. Grundstücksscharfe Daten wie beispielsweise in Karten mit unterschiedlichen Schraffuren könnten ebenfalls übermittelt werden, wenn nur eine grobe Zuordnung zu gegenwärtigen oder ehemaligen Nutzungsformen möglich ist, die auf einen Altlastenverdacht schließen lassen. Nach der durch das Berliner Bodenschutzgesetz geänderten Rechtslage wäre hier eine weitgehend unbegrenzte Veröffentlichung möglich.

Auch die im Jahresbericht 1994 angemahnte überfällige achte Änderung des *Berliner Wassergesetzes*[156] konnte noch in der alten Legislaturperiode verabschiedet werden. Damit wurden parallel zum Berliner Bodenschutzgesetz die Befugnisse der Berliner Wasserbehörde zum Erheben und sonstigen Verarbeiten personenbezogener Daten normenklar geregelt. Die Daten wurden den konkreten Aufgaben, die auch aus anderen Rechtsvorschriften erwachsen, zugeordnet. Mit dem Berliner Bodenschutzgesetz und dem Berliner Wassergesetz ist für die Verarbeitung grundstücks- und damit auch häufig personenbezogener Daten ein im Vergleich zu anderen Bundesländern guter Stand erreicht worden.

Das ebenfalls kurz vor Ende der Legislaturperiode verabschiedete *Friedhofsgesetz*[157] enthält erstmals nicht nur für landeseigene, sondern auch für nicht landeseigene Friedhöfe eine Datenschutzregelung, die den Friedhofsverwaltungen das Führen von Namensregistern der Nutzungsberechtigten, der Verstorbenen und der auf dem Friedhof gewerblich Tätigen erlaubt. Für die landeseigenen Friedhöfe gilt darüber hinaus die Rechtsverordnung über die Verarbeitung personenbezogener Daten weiter.

Anfang des Jahres 1995 brachte der Senat die Entwürfe eines *Landesfischereigesetzes*[158], eines *Landesfischereischeingesetzes*[159] und eines *Landesjagdgesetzes*[160] im Abgeordnetenhaus ein. Leider mußten wir feststellen, daß diese drei Gesetzesentwürfe zwar eine Reihe von Regelungen beinhalten, zu deren Durchführung die Erhebung und Verarbeitung personenbezogener Daten erforderlich ist, aber keine normenklaren Datenverarbeitungsbefugnisse vorgesehen waren. So sollen Fischereischeine als Ausweise mit Namen und Lichtbild gefertigt werden. Die Ausstellung eines Fischereischeins setzt eine Anglerprüfung voraus, die im Auftrag der zuständigen Senatsverwaltung durch anerkannte fischereiliche Landesverbände durchzuführen ist. Diese Regelungen wären ohne die Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten ins Leere gelaufen. Daher empfahlen wir dem Ausschuß für Umweltschutz des Abgeordnetenhauses, diese drei Gesetze um jeweils eine Verordnungsermächtigung für die zu verarbeitenden personenbezogenen Daten, insbesondere die Art und den Umfang der Daten und die einzelnen Verwendungszwecke, zu ergänzen. Der Berliner Gesetzgeber berücksichtigte im weiteren Verfahren unsere Hinweise.

Zu den vielfältigen Aktivitäten für die beabsichtigte Fusion der Länder Berlin und Brandenburg gehörte auch der *Staatsvertrag zur Landesplanung* (Landesplanungsvertrag). So wird nach diesem Vertrag zum 1. Januar 1996 eine gemeinsame Landesplanungsabteilung in Potsdam eingerichtet. Ausgehend vom Dienstort dieser Behörde wurde auf unsere Empfehlung hin festgelegt, daß für datenschutzrechtliche Belange das Recht des Landes Brandenburg gilt, soweit nicht Bundesrecht anzuwenden ist. Wenn jedoch Daten im Land Berlin zum Zwecke der Planung erhoben werden und für diese Erhebungen in Berlin bereichsspezifische Rechtsvorschriften gelten, sind diese anzuwenden. Der Brandenburgische Datenschutzbeauftragte wird im Einvernehmen mit dem Berliner Datenschutzbeauftragten die Kontrollbefugnis über die gemeinsame Landesplanungsabteilung ausüben.

5.12 Verkehr

Straßenverkehrsgesetz

Das Bundesministerium für Verkehr hat einen Entwurf einer Änderung des Straßenverkehrsgesetzes und anderer Gesetze vorgelegt, der noch 1996 vom Bundestag verabschiedet werden soll. Der Gesetzentwurf wird allerdings den Vorgaben des Bundesverfassungsgerichtes, nach denen die Datenverarbeitungsbefugnisse normenklar und für den Bürger erkennbar geregelt werden müssen, an vielen Stellen nicht gerecht.

155 GVBl. 1995, 646

156 GVBl. 1995, 695
157 GVBl. 1995, 707
158 GVBl. 1995, 358
159 GVBl. 1995, 269
160 GVBl. 1995, 282

Der Entwurf enthält zahlreiche Bestimmungen über die verschiedensten Register, während die *Aktenführung der örtlichen Fahrerlaubnisbehörden* weiterhin ungeregelt bleibt, obwohl gerade hier für klare Regelungen ein dringendes Bedürfnis besteht. Die Verarbeitung personenbezogener Daten in Akten macht in der Praxis immer noch einen nicht unerheblichen Teil der Datenverarbeitung aus. Neben fehlenden datenschutzrechtlichen Regelungen, beispielsweise für ein Verwertungsverbot von im Verkehrszentralregister (VZR) getilgten Daten enthält der Gesetzentwurf sogar Verschlechterungen bereits bestehender Vorschriften. So sollen Regelungen, die bisher einen abschließenden normenklaren Katalog enthalten haben, durch Regelungen ersetzt werden, die einen geringeren Bestimmtheitsgrad haben.

Der Entwurf ist darüber hinaus an vielen Stellen unsystematisch und enthält zahlreiche unbestimmte Datenverarbeitungsregelungen. Es bleibt zu hoffen, daß die Länder sich im Bundesrat für eine Überarbeitung der datenschutzrechtlichen Vorschriften einsetzen werden. Bedauerlich ist deshalb, daß die Senatsverwaltung für Verkehr und Betriebe ihre Stellungnahme zu dem Gesetzentwurf so frühzeitig abgegeben hat, daß unsere Empfehlungen keine Berücksichtigung mehr finden konnten. Die Senatsverwaltung hat in ihrer Stellungnahme datenschutzrechtliche Gesichtspunkte leider auch nicht angesprochen, sondern vielmehr die Schaffung neuer Eingriffsbefugnisse im Fahrerlaubnisbereich angeregt, die von uns nicht für erforderlich gehalten werden.

Führerschein und Datenschutz: ein altes Dilemma

Aus der Verkehrsverwaltung ist in den vergangenen Jahren wenig berichtet worden. Das darf aber nicht zu dem Fehlschluß führen, daß in diesem Bereich keine Datenschutzfragen auftreten. Insbesondere bei der Führerscheinstelle ergeben sich immer wieder Rechtsfragen zur Zulässigkeit verschiedener Verarbeitungsschritte. So hat uns seit Anfang an das Problem beschäftigt, ob weit zurückliegende Daten noch verwertet werden dürfen.

Das Bundesverwaltungsgericht hat sich nunmehr in einem Beschluß zu der Frage der Löschung von Daten in der Führerscheinkartei geäußert.[161] Es hält eine weitere Speicherung für unzulässig, wenn nichts dafür spricht, daß die Eintragung in Zukunft noch praktische Bedeutung hat und deshalb ausgeschlossen werden kann, daß die vorhandenen Daten die Arbeit der zuständigen Behörde noch fördern können. Ob eine Löschung der Daten zu erfolgen hat, ist auf der Grundlage des Verhältnismäßigkeitsprinzipes nach den konkreten Umständen des jeweiligen Einzelfalles zu entscheiden. Im vorliegenden Fall wurde festgestellt, daß der in der Führerscheinkartei eingetragene *Entzug der Fahrerlaubnis* so weit zurückliegt und der Kläger inzwischen so lange unbeanstandet im Besitz einer Fahrerlaubnis ist, daß ein früheres Verhalten aus dem Jahr 1965 kaum noch als Grundlage für eine Prognose für künftiges Verhalten geeignet erscheint und daß sich nicht absehen läßt, ob die Behörde überhaupt noch einmal darauf angewiesen sein könnte, Nachforschungen über ein früheres Verhalten anzustellen. Das Landeseinwohneramt wird aus dieser Entscheidung Konsequenzen zu ziehen haben.

Ermittlungen bei der Eignungsprüfung

Nach § 2 Abs. 1 Straßenverkehrsgesetz (StVG) ist die Fahrerlaubnis zu erteilen, wenn nicht Tatsachen vorliegen, die die Annahme rechtfertigen, daß der Antragsteller zum Führen von Kraftfahrzeugen ungeeignet ist. Zur Erforschung dieser Tatsachen normiert § 9 Straßenverkehrszulassungsordnung (StVZO) einen allgemeinen *Ermittlungsauftrag*. Die Führerscheinstelle erhält die Befugnis zu ermitteln, ob Bedenken gegen die Eignung des Antragstellers zum Führen von Kraftfahrzeugen vorliegen.

Welche konkreten Ermittlungen zur Erfüllung des Auftrags unternommen werden dürfen, ist in speziellen Befugnisnormen geregelt. So schreiben §§ 9 a und b StVZO den Nachweis des *Sehvermögens* vor, § 8 Abs. 3 StVZO berechtigt die Verwaltungsbehörde, ein *Führungszeugnis* über den Antragsteller zu verlangen, während § 13 c StVZO i. V. m. § 30 Abs. 1 Nr. 2 StVG die Befugnis enthält, beim Kraftfahrt-Bundesamt *(Verkehrszentralregister)* anzufragen, ob Nachteiliges über den Antragsteller bekannt ist. Auch darf die Behörde, wenn ihr Tatsachen bekannt werden, die Bedenken gegen die Eignung des Bewerbers begründen, die Beibringung eines *medizinisch-psychologischen Gutachtens* fordern (§ 12 Abs. 1 StVZO).

Darüber hinausgehende Befugnisse zu Ermittlungen bzw. Datenerhebungen (z. B. Anfragen bei der Polizei oder bei der Staatsanwaltschaft oder Heranziehung von Erkenntnissen aus Ermittlungs- bzw. Strafakten) sind in der StVZO nicht geregelt. Allerdings hat laut § 9 StVZO die Verwaltungsbehörde auch zu ermitteln, ob Bedenken gegen die Eignung des Antragstellers vorliegen, weil eine Neigung zum *Trunk*, zum *Rauschgift* oder zu *Ausschreitungen* besteht. Ob eine solche Neigung vorhanden ist, kann das LEA jedoch nicht aufgrund der in der StVZO konkret genannten Ermittlungs-(Datenerhebungs-)befugnisse feststellen. Der Verordnungsgeber hat also offenbar weitergehende Ermittlungsbefugnisse im Einzelfall für zulässig erachtet, ohne jedoch eine entsprechende Ermittlungsbefugnis zu normieren.

Soweit es um die Anforderung von Auskünften bzw. Akten durch das LEA bei dem Polizeipräsidenten in Berlin bzw. der Staatsanwaltschaft und den Gerichten geht, wäre aber eine solche konkrete, d. h. den Eingriffstatbestand und die -ermächtigung regelnde Befugnisnorm wegen der Schwere des Eingriffs erforderlich. Einvernehmlich mit der Senatsverwaltung für Verkehr und Betriebe halten wir es für notwendig, die Straßenverkehrszulassungsordnung um spezielle Datenerhebungsvorschriften zu ergänzen.

Bis dahin kann nur auf die allgemeinen Vorschriften des § 18 ASOG zurückgegriffen werden. Dabei ist jedoch zu beachten, daß gemäß § 18 Abs. 1 Satz 1, Abs. 2 ASOG die Datenerhebungen bzw. -ermittlungen grundsätzlich offen und nicht „hinter dem Rücken“ des Betroffenen durchzuführen sind. Auch sind Datenerhebungen nur insoweit zulässig, als sie zur Aufgabenerfüllung i. S. d. § 9 StVZO erforderlich sind. Hieraus ergibt sich, daß die regelmäßige Datenerhebung durch die Führerscheinstelle nicht zulässig ist.

Weitere Ermittlungen, die über die in der StVZO genannten hinausgehen, sind nur dann erforderlich, wenn *im Einzelfall* Anlaß zu der Annahme besteht, es könnten Eignungsmängel vorhanden sein, die sich aus den sonstigen Unterlagen nicht ergeben oder die aufgrund dieser Unterlagen nicht oder nicht ausreichend beurteilt werden können. In diesem Rahmen ist es jedenfalls nicht erforderlich, daß die Führerscheinstelle die *komplette Ermittlungs-/Strafakte anfordert* und einsieht, zumal diese Akten auch Daten Dritter (z. B. des Opfers, des Anzeigeerstatters, von Zeugen und Mitverurteilten) enthalten.

Dem während der Ermittlungen durch das LEA zu beachtenden Grundsatz der Verhältnismäßigkeit der Mittel würde es entsprechen, die Ersuchen zunächst auf Auskünfte bzw. auf das Anfordern von kopierten Aktenauszügen zu beschränken. Dabei hat die übermittelnde Stelle darauf zu achten, daß die Daten Dritter auf den Kopien nicht zu erkennen sind.

Soweit sich Auskunfts- und Aktenübersendungsersuchen des Landeseinwohneramtes auf bestimmte Sachverhalte oder Informationen beschränkten, wurde ihnen von der Staatsanwaltschaft und den Strafgerichten auch nur insoweit entsprochen.

Bei uneingeschränkten Auskunftsersuchen wurden – jedenfalls soweit es die Staatsanwaltschaft betrifft – regelmäßig die kompletten Akten übersandt. Das geschah deshalb, weil die Staatsanwaltschaft sich nicht in der Lage sieht, die Überprüfung der Erforderlichkeit im Einzelfall schon aufgrund mangelnder Kenntnis von dem konkreten Anlaß der Anfrage durchzuführen. Eine auch von der Senatsverwaltung für Justiz begrüßte Beschränkung der Auskünfte aus Strafakten auf den für die Aufgabenerfüllung der Fahrerlaubnisbehörde erforderlichen Umfang setzt daher grundsätzlich *ein beschränktes und präzisiertes Auskunftsersuchen* des Landeseinwohneramtes voraus.

161 Beschluß vom 18. März 1994 – 11 B 76/93, in: NJW, S. 2499

Aber auch pauschale Anfragen des Landeseinwohneramtes berechtigen nicht zur Übermittlung der kompletten Akte. Nach § 21 Abs. 5 AGGVG dürfen Verwaltungsbehörden Einsicht sowie Auskünfte aus Akten und Dateien der Staatsanwaltschaft nur erhalten, soweit dies zur Erfüllung der ihnen gesetzlich zugewiesenen Aufgaben erforderlich ist. Die Staatsanwaltschaft hat diese Übermittlungsvoraussetzungen zu prüfen, d. h., vor der Weitergabe der Daten ist im Einzelfall festzustellen, ob und ggf. welche Informationen für die Aufgabenerfüllung des Landeseinwohneramtes in bezug auf den Betroffenen erforderlich sind. Nur die Staatsanwaltschaft kann diese Prüfung vornehmen, da nur ihr der Inhalt der Akten bekannt ist. Dies kann in Einzelfällen auch bedeuten, daß vor der Auskunftserteilung – insbesondere bei nicht auf eine bestimmte Fragestellung eingeschränkten Anfragen – beim Landeseinwohneramt nachgefragt werden muß.

Eine im Einzelfall erforderliche Anfrage bei der Polizei ist nur hinsichtlich der laufenden Ermittlungsverfahren zulässig. Die Übersendung kompletter ISVB-Auszüge – also mit bereits abgeschlossenen Ermittlungsverfahren und Hinweisen auf andere Vorgänge – ist nicht erforderlich. Sollte eine Rückmeldung durch die Staatsanwaltschaft nicht erfolgt sein, hat die Polizei zuvor zu klären, welche im ISVB gespeicherten Ermittlungsverfahren abgeschlossen sind.

Die Führerscheinstelle darf nicht bei öffentlichen Stellen aller Art anfragen, um Eignungsmängel nach § 9 StVZO aufzudecken. Vielmehr sind bei der erforderlichen restriktiven Auslegung dieser konkretisierungsbedürftigen Vorschrift über die in der StVZO genannten Ermittlungsmaßnahmen hinaus nur solche Anfragen zulässig, die sich an das Strafgericht bzw. an die den strafrechtlich relevanten Sachverhalt ermittelnden Stellen richten, also an den Polizeipräsidenten in Berlin und die Staatsanwaltschaft. Das entspricht auch dem Regelungsgehalt des § 4 StVG, der im Entziehungsverfahren die Befugnis der Verwaltungsbehörde zu Anfragen bei den Ermittlungsbehörden und dem Strafgericht voraussetzt, um widersprüchliche Entscheidungen unterschiedlicher staatlicher Stellen zu vermeiden.

> *Beim Antrag auf Neuerteilung der Fahrerlaubnis hatte ein Bürger, der unter Bewährungsaufsicht steht, auch auf mehrfaches Nachfragen dem Landeseinwohneramt nicht die Gründe des Entzuges seiner Fahrerlaubnis durch die Volkspolizei genannt. Wegen der Vielzahl der Vorstrafen, die dem Führungszeugnis zu entnehmen waren, ist sein Bewährungshelfer gebeten worden, über den Verlauf der Bewährung zu berichten, um ggf. günstige Aussagen zur Verhaltensänderung und Rückfallwahrscheinlichkeit in die Eignungsbeurteilung einbeziehen zu können. Trotz einer günstigen und die Fahrerlaubnis befürwortenden Beurteilung des Bewährungshelfers hat das Landeseinwohneramt den Antrag auf Neuerteilung abgelehnt und anheimgestellt, den Antrag nach Ablauf der Bewährungszeit zu wiederholen.*

Bis vor wenigen Jahren hat das Landeseinwohneramt regelmäßig bei den Bewährungshelfern eine Stellungnahme eingeholt. Nachdem die Richtlinien, die dies vorsahen, außer Kraft getreten sind, wurde diese Praxis weitgehend eingestellt. Wegen der Besonderheit des Falles sah sich das Landeseinwohneramt ausnahmsweise veranlaßt, an den Bewährungshelfer heranzutreten.

Die Anfrage war nicht mehr von § 9 StVZO gedeckt. Wegen der Zielsetzung des Bewährungshelfers sind seine Berichte vorrangig unter dem Gesichtspunkt der Resozialisierung abgefaßt und enthalten, wie das LEA selbst einräumt, nie Aussagen zur Rückfallwahrscheinlichkeit, die allein für die Fahreignungsbeurteilung nach dem Verkehrsrecht bedeutsam sind. Diese Datenerhebung ist somit nicht erforderlich, was auch der übersandte Bericht eindrucksvoll belegt hat. Er enthielt eine Fülle höchstpersönlicher Informationen aus dem Leben des Petenten, die für die Fahrerlaubnisbehörde unerheblich sind. Künftig werden deshalb keine Berichte von Bewährungshelfern mehr eingeholt werden.

Polizei informiert Führerscheinstelle

Die Polizei teilt der Führerscheinstelle sofort telefonisch und später – regelmäßig nach ca. zwei Wochen – auch schriftlich mit, wessen Führerschein sie *beschlagnahmt* oder *sichergestellt* hat, um zu verhindern, daß dem Betroffenen ein *Ersatzführerschein* ausgestellt wird, wenn dieser einen solchen beantragt.

Mitgeteilt werden alle formlosen *Sicherstellungen*, bei denen der Betroffene den Führerschein freiwillig herausgibt, sowie Beschlagnahmen, die im Zusammenhang mit Führerscheinmaßnahmen wegen Alkohol oder auch Drogen stehen. Außerdem werden von der Polizei Meldungen in den Fällen gemacht, in denen der Betroffene keinen Führerschein bei sich hatte, der hätte beschlagnahmt oder sichergestellt werden können.

Aufgrund des Anrufes der Polizei wird formularmäßig eine Vorabmeldung ausgefüllt und zur Führerscheinakte genommen und eine Eintragung auf der Führerscheinkarteikarte vorgenommen.

Die Rückmeldung über die Aufhebung einer Beschlagnahme oder Beendigung der Sicherstellung erfolgt durch das Gericht oder ggf. durch die Staatsanwaltschaft. Eine Löschung der gespeicherten Daten erfolgt nur in den Fällen, in denen die Beschlagnahme aufgehoben, d. h. der Führerschein auch zurückgegeben wird.

Nach § 44 Abs. 2 Nr. 3 ASOG ist eine Übermittlung durch die Polizei zulässig, soweit es zur Abwehr erheblicher Nachteile für das Gemeinwohl erforderlich ist. Dies ist bei Beschlagnahmen von Führerscheinen im Zusammenhang mit *Trunkenheitsfahrten* oder anderen die Allgemeinheit gefährdenden Verkehrsverstößen der Fall angesichts der hohen Zahl von Versuchen, trotz Beschlagnahme einen Ersatzführerschein zu beantragen. Die Beantragung eines Ersatzführerscheines ist insbesondere deshalb möglich, weil nicht jede Beschlagnahme durch die Polizei später noch einmal gerichtlich überprüft wird und die Führerscheinstelle in vielen Fällen überhaupt keine Mitteilung von der Beschlagnahme erhalten würde, wenn die Polizei diese nicht meldete. In den Fällen, in denen ein gerichtlicher Beschluß nach § 111 a StPO ergeht, wird dieser oftmals erst Wochen später mitgeteilt, so daß eine große Zeitspanne besteht, innerhalb der ein Ersatzführerschein beantragt werden kann. Die Gefahr besteht auch deshalb, weil ein Ersatzführerschein durch die Online-Abfrage beim Kraftfahrtbundesamt noch am Tag der Beantragung ausgestellt werden kann.

Dies gilt auch für Übermittlungen an die Führerscheinstelle bei freiwilligen Herausgaben von Führerscheinen. Die Gefahr, daß ein Ersatzführerschein beantragt wird, besteht nicht nur dann, wenn der Führerschein beschlagnahmt worden ist, sondern auch, wenn er freiwillig herausgegeben wurde, vielleicht um die Beschlagnahme zu verhindern. Die Gefährdung des Gemeinwohls durch Verstöße ist in der Regel gleich groß bei Beschlagnahme oder Sicherstellung. Deshalb muß die Übermittlungsbefugnis auch für Sicherstellungen, d. h. freiwillige Herausgaben des Führerscheins gelten.

Eine Speicherung dieser Informationen darf nach § 42 Abs. 1 ASOG nur so lange erfolgen, wie es zur Aufgabenerfüllung erforderlich ist. Sie sind unverzüglich nach Mitteilung durch die Staatsanwaltschaft oder das Gericht über die Aufhebung/Nichtaufrechterhaltung der Beschlagnahme/Sicherstellung zu löschen.

Die *Löschung in der Führerscheinakte* erfolgt dadurch, daß der Vermerk über die Mitteilung der Polizei aus der Akte genommen wird. Die Form der Löschung auf den Karteikarten ist unzureichend. Die Eintragungen werden mit einem schwarzen, breitschreibenden Faserstift durchgestrichen, oder Bleistifteintragungen werden ausradiert. In beiden Fällen bleibt die Schrift lesbar.

In den sehr seltenen Fällen der Rückgabe ist eine neue – bereinigte – Karteikarte anzulegen und die alte, mit den Eintragungen versehene zu vernichten.

> *Gegen einen Bürger ist Strafanzeige wegen Verstoßes gegen das Betäubungsmittelgesetz erstattet worden, weil der Verdacht des Haschisch-Konsums, Marihuana-Anbaus, -Konsums, -Handels und der Herstellung von Amphetaminen bestand. Die Polizei hat hierüber die Führerscheinstelle informiert.*
>
> *Weil bei dem Inhaber einer Fahrerlaubnis der Konsum von Betäubungsmitteln eignungsausschließend ist, zumindest aber zu erheblichen Bedenken Anlaß gibt, hat das Landeseinwohneramt nach Abschluß des anhängigen Strafverfahrens das rechtskräftige Urteil angefordert und nach der Auswertung die Beibringung des Gutachtens eines Facharztes für Neurologie angeordnet.*

Die Datenübermittlung durch die Polizei hält die Führerscheinstelle im Rahmen des § 44 ASOG für zulässig und verweist auf eine entsprechende Geschäftsanweisung der Polizei. Darüber hinaus vertritt sie die Auffassung, daß es bei der Verwertung der Informationen über Haschischkonsum auf die Rechtmäßigkeit der Übermittlung nicht mehr ankomme, wenn sie nur schlüssig sind bzw. Gefahren aufzeigen, die die Führerscheinstelle abwehren muß.

Das LEA hat die Fahrerlaubnis zu entziehen, wenn sich jemand als ungeeignet zum Führen von Kraftfahrzeugen erweist.[162] Ungeeignet ist, wer unter erheblicher Wirkung geistiger Getränke oder anderer berauschender Mittel am Verkehr teilgenommen oder sonst gegen verkehrsrechtliche Vorschriften oder Strafgesetze erheblich verstoßen hat. Liegen die zum Fahrerlaubnisentzug zwingenden Voraussetzungen nicht vor, sondern bestehen lediglich Zweifel an der Eignung, kann die Führerscheinstelle zur Vorbereitung der Entscheidung über die Entziehung oder Einschränkung der Fahrerlaubnis oder der Anordnung von Auflagen die Beibringung von Gutachten anordnen.[163]

Das Bundesverfassungsgericht hat hierzu entschieden[164], daß die sehr eingehende *medizinisch-psychologische Untersuchung* einen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht darstellt, der nur dann gerechtfertigt ist, wenn die Anforderung eines Gutachtens sich auf solche Mängel bezieht, die bei vernünftiger, lebensnaher Einschätzung die Besorgnis begründen, daß der Betroffene sich als Führer eines Kraftfahrzeuges nicht verkehrsgerecht und umsichtig verhalten wird. Nicht bereits jeder Umstand, der auf die entfernt liegende Möglichkeit eines Eignungsmangels hindeutet, ist ein hinreichender Grund für die Anforderung eines derartigen Gutachtens. Der Entscheidung über die Anforderung müssen tatsächliche Feststellungen zugrundegelegt werden, die einen Eignungsmangel als naheliegend erscheinen lassen. Bei dem einmaligen Genuß von Cannabis ist dies nicht der Fall.

Trifft die Polizei Feststellungen über Fahrten oder gar die Verursachung eines Verkehrsunfalles *unter erheblichem Drogeneinfluß*, kann sie Informationen an das LEA – Referat Fahrerlaubnisse, Personenbeförderung – übermitteln, damit dieses Maßnahmen gemäß § 15 b StVZO einleiten kann. Die Übermittlung ist für die Aufgabenerfüllung der Führerscheinstelle erforderlich und nach § 44 Abs. 1 ASOG zulässig.

Trifft die Polizei Feststellungen, wonach der Betroffene lediglich im *Besitz von Cannabis* ist oder nur von *einem einmaligen* Gebrauch der Droge auszugehen ist, sind diese Daten – nach den vom Bundesverfassungsgericht aufgestellten Grundsätzen – für die Aufgabenerfüllung der Führerscheinstelle nicht erforderlich, da allein dieser Umstand keine Zweifel an der Eignung zum Führen eines Kraftfahrzeuges i. S. d. § 15 b StVZO begründet. Eine Datenübermittlung durch die Polizei an das LEA kann nicht auf § 44 Abs. 1 ASOG gestützt werden.

Auch bei *regelmäßigem Haschisch-Konsum* ist nicht zwangsläufig von Zweifeln an der Eignung, ein Kraftfahrzeug führen zu können, auszugehen. Das Bundesverfassungsgericht brachte hierzu in seiner Entscheidung zum Ausdruck, daß die Ausführungen des Gutachtens „Krankheit und Kraftverkehr“ zu diesem Punkt überprüfungsbedürftig sind. Diese wissenschaftliche Frage muß schnellstmöglich geklärt werden. Sollten die bisherigen Erkenntnisse nicht aufrechterhalten werden, müßte auch in diesen Fällen eine Übermittlung von Daten unterbleiben.

Sofern in einem Strafverfahren Tatsachen bekanntwerden, die die Annahme rechtfertigen, daß ein Inhaber einer Fahrerlaubnis zum Führen von Kraftfahrzeugen ungeeignet ist, so sind diese von dem Gericht oder der Staatsanwaltschaft mitzuteilen.[165] Eine Vorabmeldung der Polizei im Rahmen des § 44 ASOG vor Abgabe des Vorganges an die Staatsanwaltschaft ist nicht erforderlich, zumal – wie der vorliegende Fall belegt – ohnehin die Entscheidung des Gerichtes abgewartet wird, bevor Maßnahmen i. S. d. § 15 b StVZO getroffen werden. Zudem liegen regelmäßig erst im Laufe des Strafverfahrens gesicherte Erkenntnisse vor, die eine Entscheidung darüber zulassen, ob die Prüfung fahrerlaubnisrechtlicher Maßnahmen erforderlich ist. Die Geschäftsanweisung des Polizeipräsidenten ist zu ändern.

Medizinisch-psychologische Untersuchungsstelle

Eine medizinisch-psychologische Untersuchungsstelle hat uns um Stellungnahme gebeten, welche Informationen sie der Führerscheinstelle bei der *Rückgabe der Akten* geben darf. Weil die Gutachten dem Betroffenen direkt übergeben werden, vertreten zwei Verkehrsministerien anderer Länder die Auffassung, daß aufgrund der Mitwirkungspflicht des Betroffenen die Verwaltungsbehörde einen Anspruch darauf hat zu erfahren, ob und aus welchen Gründen die Untersuchung stattgefunden hat oder nicht. Dies sei für das weitere Verwaltungsverfahren und für die von der Verwaltung zu treffenden Entscheidungen maßgeblich.

Die Verwaltungsbehörde kann nach §§ 12 Abs. 1, 15 b Abs. 2, 15 c StVZO die Beibringung von Gutachten fordern, wenn Tatsachen bekanntwerden, die Bedenken gegen die Eignung des Betroffenen begründen. Zur Erstellung des Gutachtens werden mit *Zustimmung des Betroffenen* die für die Begutachtung erforderlichen Verwaltungsvorgänge dem Gutachter übersandt. Nach Beendigung der Untersuchung oder wenn keine Untersuchung erfolgt ist, werden die Vorgänge von der Untersuchungsstelle an die Verwaltungsbehörde zurückgesandt.

Die Weigerung des Betroffenen, ein Gutachten erstellen zu lassen, bzw. die Verweigerung der Zustimmung zur Übersendung der für die Begutachtung erforderlichen Verwaltungsvorgänge oder nicht fristgerecht eingereichte Gutachten können dazu führen, daß die Verwaltungsbehörde die Nichteignung als erwiesen ansieht.

§ 12 Abs. 1 StVZO regelt abschließend, daß die Verwaltungsbehörde von dem Betroffenen die Beibringung eines Gutachtens fordern kann. Weitergehende Erhebungsbefugnisse, die die Verwaltungsbehörde ermächtigen würde, Anfragen beim Gutachter – auch über die Tatsache der Begutachtung – zu stellen, bestehen nicht. Wenn die Verwaltungsbehörde bei ihrer Entscheidung den Grund der Nicht- oder nicht rechtzeitigen Vorlage des Gutachtens wissen will, muß sie dies bei dem Betroffenen selbst erfragen. Der Betroffene könnte sogar mehrere Gutachten in Auftrag geben und das für ihn günstigste auswählen. Es steht ihm frei, das Gutachten an die Verwaltungsbehörde weiterzuleiten oder nicht.

Zudem unterliegt der Gutachter der *Schweigepflicht* nach § 203 StGB. Er ist nur seinem Auftraggeber gegenüber auskunftsberechtigt. Die Schweigepflicht bezieht sich nicht nur auf den Inhalt des Gutachtens, sondern auch auf die Tatsache, daß eine Begutachtung erfolgt ist. Die Mitteilung der Untersuchungsstelle, ob eine Untersuchung stattgefunden hat, darf nur nach ausdrücklicher Einwilligung des Betroffenen erfolgen. Das Landeseinwohneramt erfragt bei der von ihr benannten Untersuchungsstelle nicht mehr, ob eine Untersuchung stattgefunden hat.

Auskunftsrechte unbekannt?

Die Führerscheinstelle hat einem Bürger, der eine schriftliche Bestätigung für den Besitz seiner Fahrerlaubnis von Herbst 1967 bis Juni 1990 haben wollte, mitgeteilt, daß zwar dort sämtliche Unterlagen vorlägen, die begehrte Bescheinigung stehe ihm allerdings nicht zu und deshalb bekomme er sie auch nicht.

Uns gegenüber hat das Landeseinwohneramt zunächst erklärt, daß diese Bestätigungen häufig dazu verwendet werden, bei den Versicherungen günstigere Konditionen hinsichtlich der *Haftpflichtversicherung* durch den Nachweis von Fahrpraxis zu erzielen, was man nicht unterstützen wolle. Später wurde erklärt, daß die ursprüngliche Fahrerlaubnis und damit das Recht und ehemalige Besitzstände erloschen seien. Inzwischen habe der Betroffene einen neuen Führerschein erhalten, und die Führerscheinstelle würde aufgrund eines neuen Antrages Auskunft aus der nach § 10 Abs. 2 Satz 2 StVZO über die *ausgehändigten* Führerscheine zu führenden Kartei über die gegenwärtige Fahrerlaubnis geben.

162 § 15 b Abs. 1 StVZO
163 § 15 b Abs. 2 StVZO
164 1 BvR 689/92
165 § 29 Abs. 2 AGGVG, Nr. 46 Abs. 2 MiStra

Hier geht es allerdings nicht um eine Karteikartenabschrift über die aktuelle Fahrerlaubnis, sondern vielmehr um die Bestätigung der Tatsache, daß der Betroffene in einem zurückliegenden Zeitraum bereits Inhaber einer Fahrerlaubnis war. Nach § 50 ASOG haben die Ordnungsbehörden dem Betroffenen gebührenfrei Auskunft über die zu seiner Person gespeicherten Daten zu erteilen.

In der zu erteilenden Auskunft sind dem Betroffenen die gespeicherten Daten – und nicht beispielsweise die Tatsache, daß eine Karteikarte in der Akte enthalten ist – mitzuteilen. In diesem Zusammenhang spielt es keine Rolle, zu welchem Zweck der Betroffene die Auskunft begehrt oder in welchem Zusammenhang er sie später verwenden will.

Das alles hat die Führerscheinstelle wohl nicht überzeugt, so daß erst die Senatsverwaltung für Verkehr und Betriebe das Landeseinwohneramt bitten mußte, künftig die gewünschten Auskünfte zu erteilen.

Ein Bürger, der einen Antrag auf Neuerteilung der Fahrerlaubnis gestellt hatte, wollte bei der Führerscheinstelle Akteneinsicht nehmen. Das ist zunächst – unter Hinweis auf das laufende Verwaltungsverfahren – abgelehnt worden.

Nachdem das Verfahren abgeschlossen war, hatte er erneut einen Antrag auf Akteneinsicht gestellt. Diesmal ist ihm die Einsichtnahme mit dem Hinweis darauf verweigert worden, es handele sich hier um ein abgeschlossenes Verfahren, weshalb eine Akteneinsicht nicht mehr möglich sei.

Im laufenden Verfahren hatte der beauftragte Rechtsanwalt keine Vertretungsvollmacht vorgelegt. Die Verweigerung der Akteneinsicht war daher insoweit korrekt.

Im übrigen vertrat das LEA die Auffassung, der Grundsatz des § 29 VwVfG, wonach Akteneinsicht nur in *laufenden Verfahren* zu gewähren ist, müsse auch in spezialgesetzlichen Vorschriften Anwendung finden, soweit dort nicht ausdrücklich etwas anderes geregelt ist. Zwar stelle § 50 ASOG eine spezialgesetzliche Regelung gegenüber § 29 VwVfG dar, jedoch ergebe sich aus Abs. 6 kein grundsätzlicher Anspruch auf Akteneinsicht, sondern lediglich die Ermächtigung der Behörde zur Akteneinsichtsgewährung. Aus § 50 Abs. 6 ASOG könne kein weitergehendes Recht als aus § 29 VwVfG hergeleitet werden. Im Ergebnis komme eine Akteneinsicht nach Abschluß des Verfahrens nicht in Betracht. Auf Antrag des Betroffenen werde lediglich Auskunft über die in den vorhandenen Unterlagen gespeicherten Daten erteilt.

Das Verfahren, grundsätzlich keine Akteneinsicht nach *Abschluß des Verwaltungsverfahrens* zu gewähren, haben wir beanstandet.[166]

Gemäß § 29 Abs. 1 VwVfG hat die Behörde den Beteiligten Akteneinsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist.

Unabhängig von diesem verfahrensrechtlichen Akteneinsichtsrecht besteht der *datenschutzrechtliche Anspruch des Betroffenen auf Auskunft und Akteneinsicht* nach § 50 ASOG. Dieser Anspruch ergibt sich unmittelbar aus dem Recht auf informationelle Selbstbestimmung. Das Bundesverfassungsgericht hat das Auskunftsrecht als wesentliche datenschutzrechtliche Schutzvorkehrung ausdrücklich hervorgehoben.[167] Der Gesetzgeber ist dieser Forderung durch § 50 ASOG nachgekommen. Eine Einschränkung der Anwendbarkeit des § 50 ASOG für Ordnungsbehörden besteht nach dem eindeutigen Wortlaut und Sinn und Zweck dieser Regelung nicht.

Die zuständige Ordnungsbehörde hat nach § 50 Abs. 6 ASOG nach *pflichtgemäßem Ermessen* zu entscheiden, ob anstelle einer Auskunftserteilung über die zu seiner Person gespeicherten Daten Akteneinsicht zu gewähren ist. Für die pflichtgemäße Ermessensausübung sind für jeden Einzelfall die Belange der betroffenen Person und die öffentlichen Interessen gegeneinander abzuwägen. Entsprechend der Bedeutung des informationellen Selbstbestimmungsrechtes und des daraus folgenden Akteneinsichtsrechtes ist dabei im Zweifel zugunsten der Akteneinsicht zu entscheiden. Nach der Begründung des Referentenentwurfes zum ASOG wurde die Ermessensregelung in § 50 Abs. 6 ASOG nur deshalb vorgesehen, um der Besonderheit, daß die Erfüllung ordnungsbehördlicher und/oder polizeilicher Aufgaben durch ein vorzeitiges Bekanntwerden behördlicher Maßnahmen unterlaufen werden könnte, Rechnung zu tragen.

Das bedeutet, daß in den Fällen, in denen keine derartigen Befürchtungen bestehen, regelmäßig Akteneinsicht zu gewähren ist. Dies liegt insbesondere bei abgeschlossenen Verwaltungsverfahren nahe.

Das Landeseinwohneramt hat nicht erklärt, aus welchen Gründen die Interessen des Betroffenen bei den Abwägungen im Rahmen des pflichtgemäßen Ermessens hinter den öffentlichen Interessen zurückstehen müßten.

Auch hier mußte erst die Senatsverwaltung für Verkehr und Betriebe das Landeseinwohneramt bitten, dem Petenten Akteneinsicht zu gewähren. Ungeachtet der Rechtsfrage hält sie insbesondere den Aufwand hinsichtlich der auch bei der Verweigerung der Akteneinsicht bestehenden Verpflichtung, Auskünfte zu erteilen – was bei Führerscheinakten praktisch die Zusammenfassung des gesamten Akteninhaltes bedeutet –, für unvertretbar.

Führerscheinstelle vergißt nichts

Auch nach 14 Jahren wird eine strafrechtliche Verurteilung, die sowohl im Bundeszentralregister als auch im Verkehrszentralregister gelöscht ist, in einem Verfahren auf Neuerteilung eines Führerscheines verwertet. Dies mußte ein Bürger, der aus beruflichen Gründen auf seinen Führerschein angewiesen war, feststellen, als ihm eine bereits getilgte Verurteilung entgegengehalten wurde.

§ 51 *Bundeszentralregistergesetz* (BZRG) regelt, daß dem Bürger Verurteilungen, die im Register getilgt worden sind, im Rechtsverkehr nicht mehr vorgehalten und zu seinem Nachteil verwertet werden dürfen. Dieses *Verwertungsverbot* wird jedoch in einigen Fällen, die in § 52 BZRG geregelt sind, durchbrochen. Unter anderem darf eine frühere Verurteilung noch in einem Verfahren herangezogen werden, das die Erteilung oder Entziehung einer Fahrerlaubnis zum Gegenstand hat, wenn die Verurteilung wegen dieser Tat in das Verkehrszentralregister einzutragen war. Ein solcher Fall hatte hier vorgelegen.

Eine unbefristete Verwertungsmöglichkeit getilgter Verurteilungen ist unverhältnismäßig, da sie dem Bewährungsgedanken des BZR nicht Rechnung trägt und die Information mit wachsendem Zeitablauf seit der Verurteilung ungeeignet für Entscheidungen der Fahrerlaubnisbehörde wird. Offensichtlich hatte dies auch der Gesetzgeber schon einmal so gesehen, denn das Bundesverkehrsministerium hatte in einem Gesetzentwurf vom 10. September 1993 bereits eine Änderung des § 52 Abs. 2 BZRG vorgesehen. Danach sollte die Regelung lauten: „Abweichend von § 51 Abs. 1 darf eine frühere Tat ferner in einem Verfahren berücksichtigt werden, solange die Verurteilung wegen dieser Tat nach den Vorschriften der §§ 28 bis 30 b des Straßenverkehrsgesetzes für das Verkehrszentralregister verwertet werden darf.“ Ein gleichlautender Vorschlag fand sich auch schon in einem Entwurf eines Verkehrszentralregistergesetzes von 1980.

Auf unsere und die Bitte anderer Landesbeauftragter hin hat der Bundesbeauftragte für den Datenschutz das Bundesjustizministerium gebeten, das Bundeszentralregister entsprechend zu novellieren. Da der Verhältnismäßigkeitsgrundsatz unmittelbar gilt, sind schon jetzt auf Landesebene, z. B. durch Verwaltungsvorschriften Löschungsfristen bei der Fahrerlaubnisbehörde für strafrechtliche Entscheidungen zu schaffen.

Auch hier: Automatisierung

Die seit Jahren laufenden Planungen zur Einführung eines ADV-Systemes für Führerscheine sind inzwischen so weit, daß uns der Hauptuntersuchungsbericht und das Pflichtenheft vorgelegt wurden.

166 Jahresbericht 1993, 3.1
167 BVerfGE 65, 1, 46

Das geplante *Führerscheinregister* soll nicht nur die Funktion der *Führerscheindatei* erfüllen, sondern dient auch der *Vorgangsverwaltung*. Nach § 10 Abs. 2 Satz 2 StVZO ist das Führerscheinregister auf die Daten über den Nachweis über die ausgegebenen Führerscheine zu beschränken. Es dürfen danach nur Name, Anschrift, Geburtsdatum, Listennummer und Aushändigungsdatum gespeichert werden. Die weitergehenden Vorgangsdaten sind hiervon getrennt – und mit differenzierten Zugriffsbeschränkungen – zu speichern. Das gilt insbesondere für Daten, die aufgrund unterschiedlicher gesetzlicher Aufgaben (z. B. nach dem Personenbeförderungsgesetz oder StVG und StVZO) gespeichert werden.[168] Die angegebene Rechtsgrundlage[169] ist für die Speicherung der weitergehenden Fahrerlaubnisdaten unzureichend. Zwar liegt der *Entwurf einer Fahrerlaubnisverordnung* vor, es ist aber noch nicht absehbar, in welcher Form diese in Kraft treten wird. Weil also hierfür noch keine spezialgesetzlichen Datenverarbeitungsbefugnisse existieren, ist § 42 Abs. 1 ASOG anwendbar. Keine Einwände bestehen danach gegen die Speicherung der Daten der Erst- und Neuerteilung, Erweiterung, Umschreibung, Fahrerlaubnis zur Fahrgastbeförderung und die Konzessionsdaten außerhalb des Führerscheinregisters. Für eine Fülle von darüber hinausgehenden Daten waren den vorgelegten Unterlagen keine Speicherungsbefugnisse zu entnehmen. Teilweise hat das Landeseinwohneramt eingeräumt, daß es selbst keine Rechtsgrundlage für die Speicherung erkennen kann.

Auch zu den beabsichtigten *Übermittlungen an andere Stellen* sind zum Teil nicht nachvollziehbare (z. B. an das Kraftfahrtbundesamt) oder falsche (an die Polizei) Vorschriften genannt. Es ist eine genaue Spezifikation erforderlich, welche Vorschrift die Übermittlung welchen Datums erlaubt. Für die Übermittlung der Konzessionsdaten an das Landesamt für das Meß- und Eichwesen und die Finanzämter konnten keine Rechtsgrundlagen genannt werden. Die Ausführungen zu den beabsichtigten Schnittstellen zu anderen Verfahren sind ebenfalls unzureichend. Auch verschiedene technisch-organisatorische Fragen sind noch klärungsbedürftig. Sofern das Verfahren in absehbarer Zeit realisiert werden soll, ist das Landeseinwohneramt gefordert, umgehend die offenen Fragen zu beantworten.

5.13 Wirtschaft und Technologie

Neufassung der Gewerbeanzeigenverwaltungsvorschrift

Am 1. Dezember 1995 ist die Neufassung der Gewerbeanzeigenverwaltungsvorschrift vorläufig in Kraft getreten, die den Vollzug der §§ 14, 15 und 55 c Gewerbeordnung (GewO) regelt. Danach soll das Gewerbeamt aus jeder Gewerbeanzeige Daten an das Wohnungsamt übermitteln. Die Daten sollen dem Wohnungsamt zur Prüfung dienen, ob Zweckentfremdung von Wohnraum nach dem *Zweckentfremdungsbeseitigungsgesetz* vorliegt. Diese regelmäßige Datenübermittlung ist unzulässig, da es hierfür an einer gesetzlichen Grundlage fehlt. § 2 a Abs. 2 Satz 2 Zweckentfremdungsbeseitigungsgesetz (ZwBesG) stellt klar, daß das Gewerbeamt nur zur Klärung eines konkreten Sachverhaltes dem Wohnungsamt Daten aus der Gewerbeanzeige übermitteln darf.

Bei der Anmeldung von bestimmten Gewerben sollen von Amts wegen ein *Führungszeugnis* für Behörden und eine Auskunft aus dem Gewerbezentralregister eingeholt werden. Es handelt sich um sog. Vertrauensgewerbe wie z. B. Eheanbahnungsinstitute, Gebrauchtwarenhändler, Auskunfteien und Detekteien. Allerdings simmt die Aufzählung der Gewerbe in der Verwaltungsvorschrift nicht voll mit § 38 GewO überein, der die Vertrauensgewerbe abschließend aufführt. Die Einholung eines Führungszeugnisses ist nicht von § 11 GewO gedeckt, da § 38 GewO gerade keine Genehmigungspflicht und damit Zuverlässigkeitsprüfung vor Aufnahme des Gewerbes vorsieht. Hätte der Gesetzgeber eine grundsätzliche Überprüfung der Zuverlässigkeit für erforderlich gehalten, hätte er für die in § 38 GewO genannten Gewerbe eine Erlaubnispflicht regeln müssen. Dies ist jedoch nicht der Fall.

Die Senatsverwaltung für Wirtschaft und Technologie hält an ihrer Auffassung fest, daß § 11 Abs. 1 Satz 1 GewO auch den Fall, daß die Gewerbebehörde nach Anzeige des Gewerbes von sich aus in jedem Einzelfall eine Zuverlässigkeitsprüfung durchführt, abdecke. Es handele sich um ein bei Vertrauensgewerben notwendiges Verfahren. Diese Auffassung steht im Widerspruch zu der Gesetzeslage und auch zu der Praxis z. B. in Hessen. Hier werden Führungszeugnisse nur bei Vorliegen von Anhaltspunkten eingeholt. Zumindest ist in der Verwaltungsvorschrift klarzustellen, daß das Führungszeugnis nicht hinter dem Rücken der Betroffenen eingeholt wird, sondern grundsätzlich sie selbst diese Unterlage beibringen können.

Positiv anzumerken ist, daß die Senatsverwaltung für Wirtschaft und Technologie auf unseren Vorschlag hin in der Verwaltungsvorschrift den Hinweis aufgenommen hat, daß bei Gruppenauskünften von der auskunftbegehrenden Stelle das berechtigte Interesse an der Auskunft jeweils im Einzelfall darzulegen ist. Dieser Hinweis ist wichtig, da das Gesetz selbst keine Regelung über Gruppenauskünfte enthält und sich die Zulässigkeit allein der Gesetzesbegründung entnehmen läßt.

Übermittlung unbeschränkter Bundeszentralregisterauszüge an den Arbeitgeber

Das Gewerbeamt kann zur Überprüfung der Zuverlässigkeit von Mitarbeitern von *Bewachungsunternehmen* unbeschränkte Bundeszentralregisterauszüge einholen. Ergibt sich aus dem unbeschränkten Bundeszentralregisterauszug die Unzuverlässigkeit eines Mitarbeiters, kann das Gewerbeamt die Beendigung des Arbeitsverhältnisses nur durch einen belastenden Verwaltungsakt gegenüber dem Arbeitgeber erreichen. Dem Arbeitgeber muß eine Auflage zu seiner Gewerbeerlaubnis erteilt werden, die ihm die weitere Beschäftigung des Mitarbeiters untersagt. Da ein Verwaltungsakt zu begründen ist, wäre dem Arbeitgeber mitzuteilen, daß die Auflage auf den eingeholten unbeschränkten Bundeszentralregisterauszug gestützt wird. Dies würde eine Datenübermittlung an einen Privaten darstellen. Bei den Gewerbeämtern wird entsprechend verfahren.

So verständlich das Bedürfnis nach Kontrolle der Wachunternehmen und ihres Personals ist: Für die Übermittlung von Daten aus dem Bundeszentralregister oder der Tatsache, daß dort Eintragungen vorliegen, an den Arbeitgeber fehlt es an einer Rechtsgrundlage. Die Pflicht zur Begründung eines Verwaltungsaktes kann die erforderliche Übermittlungsbefugnis nicht ersetzen. § 11 Abs. 4 GewO stellt fest, daß die erhobenen Daten nur für die ausdrücklich genannten Zwecke gespeichert und genutzt werden können. Eine Datenübermittlung ist nur in den in § 11 Abs. 5 GewO geregelten Fällen – und damit nur an öffentliche Stellen – zulässig. Hier würden jedoch Daten an einen privaten Unternehmer übermittelt. Immerhin würde der Arbeitgeber hierdurch erfahren, daß Eintragungen im Bundeszentralregister existieren, also z. B. Verurteilungen wegen Straftaten vorliegen. Der Inhalt des Bundeszentralregisters unterliegt nach dem BZRG Übermittlungsbeschränkungen. Private Stellen sind hier nicht als auskunftsberechtigt genannt.

Dies wird von der Senatsverwaltung für Wirtschaft und Technologie anders gesehen. Sie hat sich der Auffassung des Bundesministeriums der Justiz angeschlossen, daß die Datenübermittlung an den Arbeitgeber als „Nutzen der Daten“ i. S. d. § 4 Abs. 4 GewO anzusehen sei. Sowohl nach den Landesdatenschutzgesetzen als auch nach dem BDSG ist jedoch der Begriff der „Nutzung“ nicht mit dem Begriff der „Übermittlung“ gleichzusetzen. Die Übermittlung der Daten an Private war daher gegenüber der Senatsverwaltung für Wirtschaft und Technologie zu beanstanden.

Auch bei europäischen Subventionen gilt: Geld gegen Daten

Zahlreiche Subventionen und öffentliche Finanzhilfen an die gewerbliche Wirtschaft im Rahmen der regionalen Wirtschaftsförderung werden ganz oder teilweise von der Europäischen Kommission z. B. aus dem Europäischen Fonds für regionale Entwicklung (EFRE) zur Verfügung gestellt. Beantragt werden

168 § 4 Abs. 3 Nr. 1 BlnDSG und § 44 Abs. 1 Satz 2 ASOG
169 § 10 Abs. 2 StVZO

können diese Mittel bei der Senatsverwaltung für Wirtschaft und Technologie, die die Anträge bearbeitet, beurteilt und anschließend an das Bundeswirtschaftsministerium weiterleitet. Schließlich werden die Förderanträge vom Bundeswirtschaftsministerium der Europäischen Kommission zur Entscheidung vorgelegt. Denselben Weg wie die Anträge nehmen nach Bewilligung der europäischen Gelder auch periodische Prüfberichte und Abschlußbewertungen aus den Ländern über das Bundesministerium für Wirtschaft an die Europäische Kommission. Da ein Teil der Maßnahmen des Europäischen Fonds für regionale Entwicklung sowohl aus Mitteln der Europäischen Kommission als auch des Landes finanziert werden, wird ihre Verwendung sowohl vom Rechnungshof von Berlin als auch vom Europäischen Rechnungshof überprüft.

Die Senatsverwaltung für Wirtschaft und Technologie hat uns um eine datenschutzrechtliche Beurteilung der in diesem komplizierten Verfahren entstehenden Datenflüsse gebeten. Sie war zunächst der Auffassung, daß die Datenübermittlungen von der Senatsverwaltung für Wirtschaft und Technologie an dritte Stellen nur auf der Grundlage einer Einwilligung des jeweiligen Antragstellers zulässig sei.

Tatsächlich beruht die Bewilligung von *Mitteln aus dem Europäischen Fonds für regionale Entwicklung* auf mehreren Verordnungen des Rates der Europäischen Gemeinschaften, die als sekundäres Gemeinschaftsrecht zugleich Rechtsvorschriften im Sinne des Berliner Datenschutzgesetzes sind. Sie regeln mit hinreichender Genauigkeit, welche unternehmens- und personenbezogenen Angaben der Antragsteller offenbaren muß, wenn er europäische Subventionen im Rahmen der Strukturförderung erhalten will.

Die Senatsverwaltung für Wirtschaft und Technologie ist sowohl zur Erhebung als auch zur über Übermittlung dieser Daten an das *Bundeswirtschaftsministerium* befugt. Das Bundeswirtschaftsministerium wiederum faßt die von den einzelnen Bundesländern gelieferten Einzelangaben zusammen und übermittelt sie an die *Europäische Kommission;* dies ist sowohl vor der Bewilligung der Gelder als auch danach im Zuge der Erfolgskontrolle im erforderlichen Umfang zulässig, weil auch europäisches Gemeinschaftsrecht, auf das das Berliner Datenschutzgesetz verweist, dies ausdrücklich zuläßt. Im übrigen erfolgt die Übermittlung zu demselben Zweck, zu dem die Daten ursprünglich beim Antragsteller erhoben worden sind. Auch die Kontrolle durch den *Europäischen Rechnungshof* entspricht der Rechtsstruktur der Europäischen Gemeinschaften und führt nicht zu einer dem Berliner Datenschutzgesetz widersprechenden Zweckänderung der Daten. Der *Rechnungshof* von Berlin seinerseits hat eine Kontrollbefugnis aufgrund der Landeshaushaltsordnung, soweit die Maßnahmen der Strukturförderung auch aus Landesmitteln finanziert werden.

Insgesamt folgt daraus, daß die Datenverarbeitung bei der Bewilligung dieser Subventionen nicht von der Einwilliung des Antragstellers abhängt, sondern auf europäisches Gemeinschaftsrecht gestützt werden kann. Wir haben der Senatsverwaltung für Wirtschaft und Technologie allerdings konkrete Empfehlungen gegeben, wie der Antragsteller über diese einigermaßen verwirrenden Datenflüsse, die sein Antrag auslöst, informiert werden sollte.

5.14 Wissenschaft und Forschung

Im Vordergrund unserer Tätigkeit in diesem Geschäftsbereich steht die Beratung wissenschaftlicher Forschungsprojekte, die eine Vielzahl datenschutzrechtlicher Fragestellungen aufwerfen können. Neben den nach wie vor sehr vielfältigen Forschungsvorhaben an Berliner Schulen waren im vergangenen Jahr die medizinische und zeitgeschichtliche Forschung Schwerpunkte. Es wurden insgesamt rund einhundert Projekte datenschutzrechtlich begleitet. In einzelnen Fällen wurden vor Ort Prüfungen vorgenommen. Hierbei traten auch bei der Durchführung der Projekte Mängel zu Tage.

Bedeutung der Einwilligung

Auf der Grundlage eines Melderegisterauszuges war eine große Zahl von Bürgern angeschrieben und um bestimmte Antworten gebeten worden. Bürgern, die auf das erste Schreiben nicht geantwortet hatten, wurde ein zweites Anschreiben zugesandt. Dieses Anschreiben war jedoch so verändert worden, daß für den einzelnen die Freiwilligkeit der Erhebung nicht mehr erkennbar war.

Dies entspricht nicht den Anforderungen an die Einwilligung zur *Mitwirkung an Forschungsprojekten*. Auch bei wiederholten Erhebungen gilt das Prinzip der informierten Einwilligung, das heißt die Betroffenen müssen nicht nur erneut auf die Freiwilligkeit der Erhebung, sondern auch auf die Umstände des Projektes hingewiesen werden.

Im Zusammenhang mit der Verwaltungsreform wurden verschiedene Forschungsvorhaben durch wissenschaftliche Einrichtungen im Bereich des öffentlichen Dienstes des Landes Berlins durchgeführt. In solchen Projekten mischen sich wissenschaftliche Interessen der Forscher und Interessen der Verwaltung, um ein möglichst präzises und für Zwecke der Verwaltungsreform brauchbares Ergebnis zu erzielen.

Gerade Befragungen im Rahmen von Arbeits- bzw. Dienstverhältnissen der Betroffenen erfordern eine umfassende Aufklärung. Ein pauschaler Hinweis allgemein auf den Zweck „Verwaltungsreform“ genügt nicht. Auch muß klar sein, daß ein Mitarbeiter die Teilnahme an einer solchen Untersuchung verweigern kann, ohne daß dies Folgen für ihn hat.

In einem Bezirksamt wurde statt eines Hinweises an die Betroffenen, daß diese durchaus einzelne Fragen auch auslassen können und damit nicht zu beantworten brauchen, den Betroffenen suggeriert, daß nur vollständig ausgefüllte Fragebögen zu sinnvollen Ergebnissen führen. Zwar wurde die Befragung ohne Erhebung der Namen der Betroffenen durchgeführt, jedoch sollten je Person fünfzig verschiedene Merkmale erhoben werden. Dies hätte eine Deanonymisieriung auch bei nur geringem Zusatzwissen ermöglicht.

Wir empfahlen, die unmittelbar auf die Person verweisenden Angaben stark zusammenzufassen, und die Mitarbeiter nochmals über Charakter, Zweck und Freiwilligkeit der Erhebung zu informieren. Unsere Empfehlungen wurden aufgegriffen.

Suche nach neuen Wegen

Für einige Aufgaben ist es notwendig, personenbezogene Daten in Registern vorzuhalten. Die *Speicherung in Registern* stellt jedoch einen der erheblichsten Eingriffe in das informationelle Selbstbestimmungsrecht dar. Register wecken vielfältige Begehrlichkeiten nach Zugang zu den dort gespeicherten Daten. Auch wenn diese Daten mit Einwilligung der Betroffenen gespeichert werden, sind zum einen strenge und klare Regelungen hinsichtlich der Nutzung dieser Angaben erforderlich, zum anderen sollte durch die Organisation die Möglichkeit für Mißbrauch oder vom Betroffenen bei seiner Einwilligung nicht überschaubaren Gebrauch der Daten erschwert werden.

So wird bei der *Ärztekammer Berlin* gegenwärtig ein Projekt zur Speicherung der Angaben von *Dialysepatienten unter dem Namen QuaSiNiere* aufgebaut. Mit Einwilligung der Patienten sollen die Daten der Dialysebehandlungen hintereinander gespeichert werden. Dieses Register, das zunächst nicht Forschungszwecken dient, ist der *Qualitätssicherung* bei diesen sehr aufwendigen Behandlungen gewidmet. Auf eine Anregung des beteiligten Projektteams und des Berliner Datenschutzbeauftragten hin, wurde empfohlen, die Daten der Patienten nicht unmittelbar personenbezogenen im Register zu speichern, sondern den Personenbezug durch die Einrichtung einer Datentreuhänderstelle zu relativieren. Die Behandlungseinrichtungen liefern nach vorliegender Einwilligung der Patienten die Daten personenbezogen an den Datentreuhänder. Der Datentreuhänder trennt den Personenbezug und gibt die mit einer speziellen Codenummer versehenen Daten an das Register weiter. Im Register selbst werden dann die Daten der verschiedenen Behandlungen aneinander gefügt und

die Auswertungen vorgenommen. Mit diesem Modell kann gesichert werden, daß beim Zugriff auf das Register die Herstellung des Personenbezuges faktisch unmöglich ist. Haben hingegen die Patienten den Wunsch, ihre Behandlungsdaten über einen längeren Zeitraum und bei verschiedenen Einrichtungen einzusehen, so kann dies über den Treuhänder geschehen, der dann den Datensatz einer bestimmten Codierung abfordert und dem Betroffenen übermittelt. Auch wenn dieses Modell zunächst kompliziert erscheint, erlauben eine Reihe der heute bestehenden technischen Möglichkeiten, dieses Verfahren zu nutzen.

Besondere Prüfungsberatung

In das Berliner Hochschulgesetz[169a] wurde 1993 ein Passus eingefügt, der die Exmatrikulation auf dem Verwaltungswege vorsieht, wenn die nach der Satzung der Universität bei der Rückmeldung geforderten Nachweise über die Teilnahme an einem Beratungsgespräch oder über Studien- und Prüfungsleistungen nicht vorgelegt werden.[170] Bei der Rückmeldung zum Wintersemester 1995/96 wurden diese Vorschriften erstmals auch an der Humboldt-Universität berücksichtigt. Die Erhebungen fanden ab März 1995 statt. Der behördliche Datenschutzbeauftragte war weder an der Erstellung der Erhebungsbögen noch an dem Verfahren im Vorfeld beteiligt worden. Es fehlte an der entsprechenden Änderung der Satzung für Studienangelegenheiten. Diese wurde erst Ende Juni 1995 von der zuständigen Senatsverwaltung bestätigt. Somit fehlte es an einer wesentlichen rechtlichen Voraussetzung für die Erhebung. Ferner war sie nicht darauf abgestellt worden, daß nur diejenigen, die die Regelstudienzeit für das Grundstudium um zwei Semester überschritten hatten, von der besonderen Prüfungsberatung betroffen sein können. Vielmehr sind alle Studierenden im 6. Fachsemester angeschrieben worden, was für erhebliche Verwirrung sorgte. Der behördliche Datenschutzbeauftragte hatte daraufhin nach Rücksprache mit uns das Verfahren kritisiert. Die bereits erhobenen Datensätze wurden gesperrt, Exmatrikulationen aufgrund der Nichtteilnahme an der besonderen Prüfungsberatung fanden nicht statt. Bei der Rückmeldung zum Sommersemester 1996 wurde eine Vielzahl der Anregungen des behördlichen Datenschutzbeauftragten berücksichtigt, so daß die Erhebung durchgeführt werden konnte.

Datenabfrage bei Hochschulen

In der Vergangenheit erhielten wir mehrfach Anfragen von Immatrikulationsbüros verschiedener Berliner Hochschulen zu Auskunftsersuchen anderer öffentlicher Stellen. Die Ersuchen bezogen sich hauptsächlich auf Angabe der Studienteilnahme/-dauer, Matrikelnummer sowie Zeitpunkt des Examens. Begründet wurde die Anfrage mit der Notwendigkeit der Berechnung von Ortszuschlag, Kindergeld, Zahlung von Waisenrente oder für die Einleitung und Durchführung arbeitsrechtlicher Maßnahmen gegen öffentlich Bedienstete.

Wir haben den Hochschulen jeweils mitgeteilt, daß personenbezogene Daten sowohl nach dem Bundesdatenschutzgesetz als auch nach dem Berliner Datenschutzgesetz beim Betroffenen selbst und nicht hinter seinem Rücken zu erheben sind. Die Erhebung ihrerseits ist jedoch nur dann zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Gesetz der datenverarbeitenden Stelle zugewiesenen Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist.

An dieser Voraussetzung scheitert eine Erhebungsbefugnis, wenn der ersuchenden Behörde bei der Erfüllung ihrer Aufgaben eine der folgende Alternativen zur Verfügung steht:

- Befragung des Betroffenen selbst
- Fristsetzung mit Rückzahlungsandrohung bereits gezahlter Leistungen bei Verweigerung der Auskunft
- Rückzahlungsforderung
- Fristsetzung mit Androhung der Zahlungseinstellung künftiger Leistungen.

169a GVBl. 1995, 727 (Neufassung)
170 Jahresbericht 1994, 4.15

6. Aus der Privatwirtschaft

6.1 Neue gesetzliche Regelung zur Aufsichtsbehörde

Im deutschen Datenschutzrecht wird bisher grundsätzlich zwischen Datenschutz im öffentlichen Bereich und Datenschutz im privaten Bereich unterschieden. Während der Datenschutz im öffentlichen Bereich für Bundesbehörden im Bundesdatenschutzgesetz und für die Landesbehörden in den 16 Landesdatenschutzgesetzen geregelt ist, stellt das Bundesdatenschutzgesetz die alleinige Grundlage für den Datenschutz im privaten Bereich dar.

Dem entspricht auch eine Trennung der Datenschutzbehörden: Während für die Kontrolle der Verwaltung Bundes- und Landesdatenschutzbeauftragte eingerichtet sind, bestimmen nach § 38 Abs. 6 BDSG die Länder „Aufsichtsbehörden". Die Länder sind diesem Auftrag in der Vergangenheit in verschiedener Weise nachgekommen. Während die Länder Hamburg und Bremen die Aufgaben der Aufsichtsbehörde von vorneherein den Landesbeauftragten übertrugen, erklärten die meisten anderen Länder die Innenministerien oder die Bezirksregierungen als Mittelbehörden zur Aufsichtsbehörde.[170a] In Berlin wurde in § 33 BlnDSG die Senatsverwaltung für Inneres bestimmt.

Die Aufspaltung der Aufgaben ist von uns in den vergangenen Jahren mehrfach kritisiert worden.[171] Sie stellte eine unnötige Zersplitterung von Aufgaben zu Lasten der Bürger dar und ist, wie die Beschwerdepraxis zeigt, von niemandem nachvollziehbar gewesen. Im Zusammenhang mit der Verwaltungsreform, bei der die Entlastung der Ministerialbürokratie von Vollzugsaufgaben eines der wesentlichen Elemente ist, hat die Berliner Innenverwaltung von sich aus eine Zusammenführung der Aufgaben angeregt.

Nunmehr hat der Berliner Landesgesetzgeber durch Änderungsgesetz zum Berliner Datenschutzgesetz vom 3. Juli 1995[172] entschieden, daß die Berliner Aufsichtsbehörde nicht mehr wie bisher die Senatsverwaltung für Inneres sein soll, sondern ab 1. August 1995 der Berliner Datenschutzbeauftragte. Der allgemein verbreiteten Meinung, eine Kontrollbehörde im Bereich der Privatwirtschaft bedürfe jedenfalls hinsichtlich der konkreten Eingriffsbefugnisse einer gewissen Aufsicht durch eine parlamentarisch verantwortliche Instanz, wurde dadurch Rechnung getragen, daß der Berliner Datenschutzbeauftragte in seiner Funktion als Aufsichtsbehörde der Rechtsaufsicht des Senats unterstellt wurde. Wir vertreten nach wie vor die Auffassung, daß die Ausgestaltung des Berliner Datenschutzbeauftragten als Wahlamt sowie die verschiedenen Berichtspflichten (vgl. § 29 BlnDSG) hinreichende Ansatzpunkte für eine parlamentarische Kontrolle gewähren.

Im Hinblick auf die Stellung des Datenschutzbeauftragten als Verfassungsorgan[173] sowie die Ausgestaltung als Oberste Landesbehörde (§ 22 Abs. 2 BlnDSG) stellt die Berliner Lösung ein Optimum im Hinblick auf die verfassungsrechtlich gebotene Unabhängigkeit des Datenschutzbeauftragten dar. Sie wird, auch auf dem Hintergrund der Europäischen Datenschutzrichtlinie, die eine einheitliche Kontrollinstanz nahelegt, auch in anderen Ländern zunehmend favorisiert.

Aufgabe der Aufsichtsbehörde über die private Datenverarbeitung ist es nach § 1 BDSG, den Einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Struktur und Terminologie des Bundesdatenschutzgesetzes sind grundsätzlich die gleichen wie die der Landesdatenschutzgesetze. So müssen auch die Daten im privaten Bereich personenbezogen sein, wenn sie unter das Bundesdatenschutzgesetz fallen sollen. Wie im öffentlichen Bereich knüpft das Bundesdatenschutzgesetz im privaten Bereich an bestimmte Verarbeitungskategorien an. Anders als in den Landesgesetzen stellt allerdings bisher das Erheben keine Phase der Datenverarbeitung dar und wird im privaten

170a Im Saarland und in Schleswig-Holstein, wo zunächst die Landesbeauftragten eingesetzt worden waren, fand nach der Zuordnung der Landesbeauftragten zum Landtag ein Wechsel ins Innenministerium statt; in Niedersachsen wurde umgekehrt die Aufgaben vom Innenministerium auf den Landesbeauftragten übertragen, wobei das Innenministerium weiterhin die – im BDSG nicht vorgesehene – Funktion der „Obersten Aufsichtsbehörde" wahrnimmt.
171 Jahresbericht 1993, 1.2
172 GVBl. S. 404
173 vgl. 1.1

Bereich nur in sehr eng umgrenzten Rahmen geschützt (hier wird die Umsetzung der Europäischen Richtlinie zu erheblichen Änderungen führen müssen).

Wichtigster Unterschied zum Datenschutz im öffentlichen Bereich ist der Umstand, daß das Bundesdatenschutzgesetz im privaten Bereich nur anwendbar ist, soweit diese Stellen Daten in oder aus Dateien verarbeiten oder nutzen. Hier hat sich damit die in der Ursprungsfassung des Bundesdatenschutzgesetzes grundlegende Unterscheidung zwischen Datenverarbeitung in und aus Dateien einerseits und Datenverarbeitung in oder aus Akten oder sonstigen konventionellen Datenträgern erhalten. Es sei dahin gestellt, ob diese Unterscheidung von jeher sinnvoll war und künftig beibehalten werden sollte (die Europäische Richtlinie verwendet den Dateienbegriff ebenfalls, allerdings in einer Form, die erheblich mehr an strukturierten Datensammlungen umfaßt als die deutsche Definition). Im Hinblick auf die Rationalisierung und die Digitalisierung unserer Informationswelt werden ohnhin immer mehr Formen der Datenverarbeitung unter einen der beiden in § 3 Abs. 2 BDSG definierten Dateibegriffe fallen.

Es ist aber derzeit noch nicht auszuschließen, daß manche von den Bürgern aus der Privatwirtschaft an uns herangetragenen Fälle mangels Dateibezug nicht unter das Bundesdatenschutzgesetz fallen. Dann ist zwar keine Entscheidung nach diesem Gesetz möglich, gleichwohl ist dem Datenschutzbeauftragten aber nicht verwehrt, einerseits diesen Bürgern Anregungen auf der Grundlage anderer einschlägiger Gesetze zu geben, andererseits die datenverarbeitenden Unternehmen auf Mängel hinzuweisen und Empfehlungen zu ihrer Abstellung zu unterbreiten.

Nach dem Bundesdatenschutzgesetz hat die Aufsichtsbehörde vor allem folgende Aufgaben:

- Sie hat nach § 38 BDSG Beschwerden von Bürgerinnen und Bürgern über eine Verletzung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz zu überprüfen. Hierzu gab es auf den verschiedensten Gebieten schon genügend Anlaß.
- Zu den gesetzlichen Aufgaben gehört es ferner, Betriebe, die der Gesetzgeber unter dem Gesichtspunkt des Datenschutzes als besonders gefährlich angesehen hat, nach § 32 BDSG zu registrieren und nach § 38 von Amts wegen zu überprüfen. Nach § 32 Abs. 1 BDSG gehören dazu nichtöffentliche Stellen, die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung speichern (z. B. Auskunfteien oder Detekteien), zum Zwecke der anonymisierten Übermittlung speichern (z. B. Markt- und Meinungsforschungsinstitute) oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen (z. B. Rechenzentren).

  Die sich daraus ergebende Prüfpraxis wird sicher davon profitieren, daß unsere Behörde über eine effektive DV-Ausstattung und über viel ADV-Know how verfügt, das wie im öffentlichen Bereich so auch hier im privaten Bereich Anwendung finden kann.

- Aber auch bei Betrieben, die nicht unter den Katalog der sogenannten Fremdverarbeiter fallen, muß die Datenschutzaufsichtsbehörde eingreifen, wenn hinreichende Anhaltspunkte dafür vorliegen, daß in diesen Betrieben eine Datenschutzverletzung stattfindet. Die Praxis wird erweisen, inwieweit damit datenschutzwidrige Praxen verhindert oder beseitigt werden können.

6.2 Der Düsseldorfer Kreis

Ohne daß das Bundesdatenschutzgesetz eine Vorgabe enthielte, haben die Bundesländer den dort vorgesehenen Aufsichtsbehörden, deren Rechte sich aus dem Bundesdatenschutzgesetz ergeben, *„Oberste Aufsichtsbehörden für den Datenschutz“* übergeordnet. Wo die Aufgaben der Aufsichtsbehörden von den Mittelbehörden wahrgenommen werden (z. B. in Bayern, Hessen oder Nordrhein-Westfalen), fungieren sie als ministerielle Fachaufsicht in Verbindung mit der Grundsatzzuständigkeit für den Datenschutz im Lande (z. B. zur Datenschutzgesetzgebung); wo die Ministerien selbst zur Aufsichtsbehörde erklärt wurden, nehmen sie beide Aufgaben gleichzeitig wahr. Die Innenministerien beaufsichtigen insoweit in Niedersachsen den Landesbeauftragten, in Thüringen das Landesverwaltungsamt. In Berlin ist die Aufgabe der „Obersten Aufsichtsbehörde“ (wie in Bremen und Hamburg) auf den Berliner Datenschutzbeauftragten übergegangen – natürlich ohne die verbleibenden ministeriellen Aufgaben.

Die „Obersten Aufsichtsbehörden“ betrachten als ihre Aufgabe in erster Linie die Koordinierung der Auslegung der Bestimmungen des Bundesdatenschutzgesetzes sowie die entsprechenden Verhandlungen mit den Spitzenverbänden der Wirtschaft, z. B. dem Zentralen Kreditausschuß, dem Verband der Handelsauskunfteien oder dem Gesamtverband der deutschen Versicherungswirtschaft. Als Beratungskreis wurde auf Initiative des nordrhein-westfälischen Innenministeriums 1978 der „Düsseldorfer Kreis“ gegründet, dem auch der Bundesdatenschutzbeauftragte angehört. Wie zuvor die Senatsverwaltung für Inneres werden wir uns an den Beratungen engagiert beteiligen, um im Bereich der Privatwirtschaft ein hohes Datenschutzniveau zu erreichen.

Derzeitige Themen sind unter anderem die Herausgabe von Telefonverzeichnissen auf elektronischen Datenträgern[174], die BahnCard[175], die Einführung von Krankenversichertenkarten auch in den privaten Krankenversicherungen[176], die Kriterien für Meldungen an den Verband der Schadenversicherer sowie die Übermittlung und Nutzung firmeninterner Telefonbücher für Werbezwecke.

6.3 Unsere ersten Themen

Unsere Vorgabe bei der Übernahme der Aufgabe der Aufsichtsbehörde war zunächst die Wahrung der Kontinuität: Die Versetzung zweier Mitarbeiter aus der Innenverwaltung, die seit Jahren mit der Materie befaßt waren, erleichterte es, zuvor eingegangene Fragestellungen bruchlos weiterzubearbeiten. Dies schloß nicht aus, daß im einen oder anderen Fall neue Akzente gesetzt wurden.

Quantitativ von erheblichem Gewicht war die Übernahme der Zuständigkeit für die Deutsche Bahn AG und der damit verbundenen Verpflichtung zur Bearbeitung der Vielzahl von Beschwerden, die zur BahnCard eingingen.[177] Aber auch einige andere Probleme kristallisierten sich bald als schwierig heraus.

Wertpapierhandelsgesetz

Das *Wertpapierhandelsgesetz* (WpHG)[178] ist am 1. Januar 1995 in Kraft getreten. Es enthält eine Bestimmung, deren datenschutzrechtliche Bedeutung offensichtlich unterschätzt worden war und die demnach zu erheblicher Unruhe auch bei Bürgern führte, denen der Datenschutz sonst nicht als persönliches Problem vertraut ist.

Nach diesem Gesetz ist ein „Wertpapierdienstleistungsunternehmen“ unter anderem verpflichtet, den Kundenauftrag mit der erforderlichen Sachkenntnis, Sorgfalt und Gewissenhaftigkeit im Interesse seiner Kunden zu erbringen. Hierzu ist er verpflichtet, „von seinen Kunden Angaben über ihre Erfahrungen oder Kenntnisse in Geschäften, die Gegenstand von Wertpapierdienstleistungen sein sollen, über ihre mit den Geschäften verfolgten Ziele und über ihre finanziellen Verhältnisse zu verlangen“ (§ 31 Abs. 2 Ziff. 1).

Die Banken nahmen diese neue Bestimmung zum Anlaß, mit Hilfe von Fragebogen umfangreiche *Datenerhebungen über ihre Kunden* vorzunehmen, wobei der Umfang und die Art und Weise der Erhebung von Bank zu Bank unterschiedlich war.

Unter anderem wurde gefragt:

- Welche weiteren Privatkonten haben Sie?
- Wie hoch ist Ihr Verfügungskredit?

174 vgl. 4.3
175 vgl. 3.1
176 vgl. 3.2
177 vgl. 3.1
178 Gesetz über den Wertpapierhandel vom 26. Juli 1994, BGBl. I, S. 1749

- Welche Kreditkarten haben Sie?
- Sparen Sie regelmäßig?
- Planen Sie den Erwerb einer Immobilie?
- Welche Versicherungen haben Sie?
- Geschätztes Gesamtvermögen, differenziert nach Geld-, Substanz- und Sachwerten
- Einkommen aus selbständiger Tätigkeit, Gehalt, Rente, Miete, Zinsen
- Erbschaften
- Name des Steuerberaters
- Wie sind Ihre bisherigen Anlageerfahrungen?
- Erfolge/Verluste?

Gefragt wurde in vielen Instituten offensichtlich *jeder Geldanleger.* Uns erreichten etwa Beschwerden einer über achtzigjährigen Frau, die lediglich völlig risikolose Papiere besitzt, oder eines Mannes, der sein Vermögen seit Jahrzehnten von der Bank selbst verwalten läßt.

Wenn sich Kunden weigerten, den Fragebogen auszufüllen, haben einzelne Anlageberater es sogar abgelehnt, mit den Kunden Anlagegeschäfte zu tätigen. Fälschlicherweise wurde behauptet, das Bankinstitut sei aufgrund des Wertpapierhandelsgesetzes gesetzlich verpflichtet, die im Fragebogen enthaltenen Daten zu speichern. Vereinzelt mußten Anleger ihrem Bankberater bestätigen, daß eine anlage- und objektgerechte Beratung nicht möglich sei.

Bei der Beurteilung ist davon auszugehen, daß die Banken nur verpflichtet sind, den Auftrag, die hierzu erteilte Anweisung des Kunden, die Ausführung des Auftrags, den Namen des Angestellten, der den Auftrag des Kunden angenommen hat, sowie die Uhrzeit der Erteilung und Ausführung des Auftrags aufzuzeichnen (§ 34 WpHG). Weitergehende *gesetzliche Aufzeichnungspflichten* bestehen nicht, da das Bundesministerium der Finanzen von Verordnungsermächtigung nach § 34 Abs. 2 WpHG bisher nicht Gebrauch gemacht hat. § 31 Abs. 2 WpHG verpflichtet demgegenüber die Banken nur dazu, die Kunden zu befragen, nicht aber die Daten auch zu speichern.

Andererseits muß die Bank aber in der Lage sein, die Erfüllung ihrer *Beratungspflicht* nach § 31 Abs. 2 WpHG in bestimmtem Umfang zu *dokumentieren.* Dies ist nach § 28 Abs. 1 Nr. 1 und 2 BDSG zulässig, jedenfalls soweit dies die Zivilgerichte zur Haftungseinschränkung der Banken verlangen. Die hierdurch entstehenden Unklarheiten können nur durch klare Vorgaben der *Wertpapieraufsicht* beseitigt werden, die so bald wie möglich die erforderlichen Richtlinien erlassen sollte, die vor allem eine Unterscheidung produkt- und kundenbezogener Befragung berücksichtigen müssen.

Im Einzelfall gehen wir davon aus, daß die Befragung nur bei einem *konkreten Anlagewunsch* des Kunden durchgeführt werden sollte. Die Befragung von Kunden, die bereits ein Depot haben, aber weder jetzt noch in Zukunft beabsichtigen, Änderungen vorzunehmen, sind nicht zu befragen. Wünscht der Kunde eine Anlage, die völlig *risikofrei* ist, hat eine Befragung zu unterbleiben.

Wohnungsbaugesellschaften

Wohnungsbewerber müssen bei den Berliner Wohnungsbaugesellschaften in der Regel umfangreiche Fragebögen ausfüllen. Erfragt werden auch von ihnen nicht benötigte Daten, wie z. B.: Nationalität, Paß- oder Personalausweisnummer, derzeitige Tätigkeit, Arbeitgeber der Mitbewohner, die nicht Vertragspartner der Wohnungsbaugesellschaft sind. Einige Mieter der Wohnungsbaugesellschaften mußten sogar umfangreiche Fragebögen ausfüllen, obwohl sie nur wegen eines Sanierungsfalls einen Wohnungswechsel durchführten.

Gegen die Speicherung von personenbezogenen Daten von Wohnungsinteressenten bestehen keine Bedenken, soweit die Daten von den Wohnungsbaugesellschaften benötigt werden, um das Wohnungsgesuch sachgerecht zu bearbeiten. Die Speicherung von nicht benötigten Daten ist demgegenüber rechtswidrig. Danach dürfen die Wohnungsbaugesellschaften die personenbezogenen Daten erheben, die sie benötigen, um sich von einer ausreichenden *Bonität des zukünftigen Mieters* zu überzeugen und eine adäquate Wohnung für ihn zu finden. Leider halten sich viele Wohnungsbaugesellschaften nicht an diese klaren Vorgaben.

Wir werden darauf drängen, daß die Wohnungsbaugesellschaften ihre rechtswidrigen Datenspeicherungen beenden. Wir sind allerdings auch der Meinung, daß wir einzelnen Petenten grundsätzlich nicht empfehlen können, die rechtswidrig abgeforderten Daten nicht preiszugeben. Es ist nämlich nicht auszuschließen, daß ihnen hierdurch Nachteile bei der Wohnungsbewerbung entstehen könnten.

Auskunfteien, Detekteien

Drei Berliner Detekteien stehen in dem Verdacht, illegal personenbezogene Daten erhoben zu haben.[179] *Die Mitarbeiter dieser Auskunfteien sollen bei zahlreichen Institutionen (z. B. Einwohnermeldeämter, Gerichte, Banken, Bundesversicherungsanstalt für Angestellte, Landesverwaltungsamt, Krankenkassen, Arbeitsämter, Polizeidienststellen, Interpol) angerufen und sich als Mitarbeiter von Behörden oder sonstigen Institutionen ausgegeben haben. Unter Angabe einer Legende sollen sie Auskünfte über praktisch alles erhalten haben, was sie erfahren wollten, z. B. aktuelle Anschriften, Geburtsdaten, Kontostände, Krankheiten, Kreditwürdigkeit, Arbeitgeber u. v. m. Die Auftraggeber waren insbesondere Unternehmen, die sich über die Bonität einer bestimmten Person informieren wollten – darunter bundesweit bekannte Großfirmen.*

Auskunfteien dürfen zwar grundsätzlich auch ohne das Wissen der Betroffenen personenbezogene Daten erheben, dies muß aber nach Treu und Glauben und auf rechtmäßige Weise geschehen (§§ 29 Abs. 1 Satz 2, 28 Abs. 1 Satz 2 BDSG). Eine Datenerhebung mit Hilfe von Legenden ist nicht gestattet. Dies gilt insbesondere für Legenden, die den Straftatbestand der Amtsanmaßung und den Mißbrauch von Titeln (§§ 132, 132 a StGB) erfüllen. Nach dem Bundesdatenschutzgesetz selbst macht sich strafbar, wer die Übermittlung geschützter Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht (§ 43 Abs. 2 Ziff. 1).

Die strafrechtlichen Ermittlungen gegen die Mitarbeiter der Auskunfteien sind noch nicht abgeschlossen. Schon jetzt kann aber festgehalten werden, daß viele Behörden und private Institutionen (im gesamten Bundesgebiet) fahrlässig personenbezogene Daten telefonisch weitergegeben haben. Noch stärker als bisher müssen klare innerbehördliche und innerbetriebliche Regeln aufgestellt werden, damit sich ein derartiger Fall nicht wiederholt.

Arbeitnehmer muß Krankheit offenbaren

Arbeitnehmer haben im Fall einer Erkrankung eine Anzeigepflicht gegenüber dem Arbeitgeber. Sie müssen ihrem Arbeitgeber eine Arbeitsverhinderung wegen Krankheit unverzüglich anzeigen. Dies ergibt sich für Arbeiter aus § 3 Lohnfortzahlungsgesetz und für Angestellte aus ihrer Treuepflicht gegenüber dem Arbeitgeber bzw. aus dem Tarifvertrag.

Der Inhalt der Anzeige bezieht sich allerdings nur auf die *Tatsache der Arbeitsverhinderung* und ihre voraussichtliche Dauer. Hingegen kann der Arbeitgeber grundsätzlich keine Auskunft über die *Art der Krankheit oder der Krankheitssymptome* verlangen. Etwas anderes gilt nur, wenn der Arbeitgeber ein berechtigtes Interesse an der Information hat, etwa weil es sich um bestimmte ansteckende Krankheiten handelt oder weil er für die Prüfung der Voraussetzungen der Zahlung von Krankheitsbezügen weitere Auskünfte benötigt. Ein Auskunftsanspruch ist ihm auch dann zu gewähren, wenn er wegen der von ihm zu zahlenden Lohnfortzahlung Regreßansprüche gegen einen Schädiger (z. B. Diskothekenschlägerei) geltend machen kann. Nur in diesen Fällen darf er folglich die Daten über die Krankheit des Arbeitnehmers speichern.

179 Größter Datenklau. In: Focus vom 24. April 1995, S. 18 ff.

Ein Berliner Arbeitgeber versuchte, die oben dargestellten gesetzlichen Restriktionen dadurch zu umgehen, daß er von seinen Mitarbeitern die Einwilligung zu einer qualifizierten Krankmeldung verlangte. Er vertrat die Ansicht, daß die Einwilligung der Mitarbeiter dazu führt, daß die Speicherung der Krankheitsdaten nunmehr rechtmäßig erfolgt. Er berief sich insoweit auf § 4 Abs. 1 BDSG. Danach ist die Verarbeitung personenbezogener Daten zulässig, soweit der Betroffene eingewilligt hat.

Eine wirksame Einwilligung setzt allerdings voraus, daß sie freiwillig vorgenommen wird. Auch im Rahmen eines Arbeitsverhältnisses kann die Freiwilligkeit einer Einwilligung nicht generell ausgeschlossen werden. Vielmehr stellt sie sich auch hier als eine Form der Verwirklichung des Selbstbestimmungsrechtes des Einzelnen dar. Der Arbeitnehmer mag z. B. auch im Arbeitsleben die Speicherung von positiven Daten über sich durchaus wünschen. Andererseits darf aber auch nicht übersehen werden, daß sich der Arbeitnehmer gerade in der augenblicklichen Wirtschaftslage oftmals in der Gefahr befindet, keine eigene Entscheidung treffen zu können, da er sonst seine Aufstiegschancen gefährdet oder gegebenenfalls seinen Arbeitsplatz aufs Spiel setzt. Wegen des *wirtschaftlichen und psychologischen Drucks*, unter dem der Arbeitnehmer steht, kann von einer *freiwilligen Einwilligung* deshalb nur dann ausgegangen werden, wenn die Datenverarbeitung für den Arbeitnehmer offensichtlich so vorteilhaft ist, daß ein Mißbrauch der Einwilligung von vornherein nicht in Betracht kommt.

Eine Einwilligung in die Speicherung der Daten über die Art einer Erkrankung ist somit unwirksam, da sie nicht freiwillig erfolgt. Wir haben deshalb den Arbeitgeber aufgefordert, die oben dargestellte rechtswidrige Datenspeicherung zu beenden.

Kontrolle des Betriebsrates durch den betrieblichen Datenschutzbeauftragten?

Dem betrieblichen Datenschutzbeauftragten ist gemäß § 37 Abs. 1 BDSG die Aufgabe zugewiesen, die Ausführung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz sicherzustellen.

Der Betriebsrat eines Unternehmens vertrat die Ansicht, daß der betriebliche Datenschutzbeauftragte nicht das Recht habe, die Einhaltung des Datenschutzes im Betriebsrat sicherzustellen. Wir haben den Betriebsrat darauf hingewiesen, daß seine Rechtsansicht unrichtig ist.

Bereits der weitgefaßte Wortlaut des § 37 Abs. 1 BDSG legt es nahe, daß das Kontrollrecht des betrieblichen Datenschutzbeauftragten gegenüber jeder speichernden Stelle nach § 3 Abs. 8 BDSG besteht. Als Teil der speichernden Stelle im Unternehmen ist aber auch der Betriebsrat anzusehen, da die von ihm wahrgenommene Datenverarbeitung nicht im Auftrag des Arbeitgebers stattfindet, er also nicht Dritter im Sinne des § 3 Abs. 9 BDSG ist.

Das Bundesdatenschutzgesetz soll eine Beeinträchtigung des Persönlichkeitsrechtes des Einzelnen durch den Umgang mit seinen personenbezogenen Daten verhindern. Um diesen Schutz umfassend sicherstellen zu können, ist es erforderlich, auch den Betriebsrat der Kontrolle des betrieblichen Datenschutzbeauftragten zu unterwerfen, da ansonsten die Gefahr bestände, daß im Betriebsrat eine datenschutzfreie Zone entstehen könnte. Als Alternative für eine Kontrolle des betrieblichen Datenschutzbeauftragten käme nämlich nur die Kontrolle durch die Aufsichtsbehörde in Betracht. Bei der Kontrolle durch die Aufsichtsbehörde ist aber zu bedenken, daß sie nach § 38 Abs. 1 BDSG nur zulässig ist, wenn der Aufsichtsbehörde *hinreichende* Anhaltspunkte für die Verletzung der Vorschriften über den Datenschutz vorliegen. Eine regelmäßige Überwachung ist damit nicht möglich. Außerdem ist eine solche Kontrolle weniger wirksam, da die Aufsichtsbehörde mit den betrieblichen Gegebenheiten nicht vertraut ist und eine Kontrolle sämtlicher Betriebsräte auch die personellen und sächlichen Mittel der Aufsichtsbehörde übersteigt.

Wir erkennen an, daß ein vorrangiges Prinzip des Betriebsverfassungsgesetzes der Grundsatz der *Eigenständigkeit des Betriebsrats* darstellt. Danach muß der Betriebsrat seine Aufgaben vom Arbeitgeber unabhängig und eigenständig wahrnehmen können. Es besteht aber nicht die Gefahr, daß eine Überwachung des Betriebsrats durch den betrieblichen Datenschutzbeauftragten zu einer mittelbaren Kontrolle des Betriebsrats durch den Arbeitgeber führt.

Der betriebliche Datenschutzbeauftragte ist gemäß § 36 Abs. 3 BDSG bei seiner Tätigkeit nicht den Weisungen des Arbeitgebers unterworfen und darf wegen der Erfüllung seiner Aufgabe nicht benachteiligt werden. Auch der Widerruf seiner Bestellung ist nur eingeschränkt möglich. Dies zeigt, daß der betriebliche Datenschutzbeauftragte nach der gesetzlichen Regelung eben nicht vom Arbeitgeber abhängig ist, sondern eine neutrale Stellung einnimmt. Er ist deswegen auch nicht der Vertrauensmann des Arbeitgebers, sondern vertrauensvoller Ansprechpartner aller Betroffenen in deren Datenschutzangelegenheiten. Die Behauptung, der betriebliche Datenschutzbeauftragte sei vom Arbeitgeber abhängig, steht also im Widerspruch zu der eindeutigen gesetzlichen Vorschrift. Auch besteht keine Gefahr, daß der betriebliche Datenschutzbeauftragte Geheimnisse des Betriebsrats an den Arbeitgeber verrät. Zum einen ist der betriebliche Datenschutzbeauftragte gemäß § 5 BDSG auf das Datengeheimnis verpflichtet; zum anderen unterliegt er noch einer besonderen Verschwiegenheitspflicht gemäß § 36 Abs. 4 BDSG. Folglich ist er nach der gesetzlichen Regelung nicht berechtigt, die Informationen, die er durch die Kontrolle des Betriebsrats erlangt hat, an den Arbeitgeber weiterzugeben.

Innenrevision bei Banken und Arbeitnehmerdatenschutz

In einer Berliner Bank geriet ein Mitarbeiter in den dringenden Verdacht, durch Straftaten, denen eine Bereicherungsabsicht zugrunde lag, seinen Arbeitgeber geschädigt zu haben. Zur Überprüfung der Angelegenheit schaltete das Bankhaus seine Innenrevision ein. Bei der Revision wurden u.a. zahlreiche Mitarbeiterkonten kontrolliert.

Auch bei den ohne Zweifel grundsätzlich rechtmäßigen Revisionsmaßnahmen müssen die Banken darauf achten, daß das informationelle Selbstbestimmungsrecht der Mitarbeiter nicht in rechtswidriger Weise berührt wird. Obwohl der Grundsatz gilt, daß die Prüfungshandlungen der Innenrevision sich auf die Betriebsabläufe aller Teilbereiche des Kreditinstitutes erstrecken können, kann es kein *uneingeschränktes Revisionsrecht* geben. Grundsätzlich hat die Revision selbstverständlich das Recht, Kundenkonten zu kontrollieren. Im vorliegenden Fall interessierte sich die Revision jedoch nicht für die Konten als Kundenkonten, sondern ausschließlich als Mitarbeiterkonten. Hierbei hat die Revision den Umstand ausgenutzt, daß die jeweiligen Mitarbeiter – eigentlich eher zufällig – bei ihrem Arbeitgeber ihr Privatkonto führten. Diese Konten darf die Innenrevision nur überprüfen, wenn sie als normale Kundenkonten für die Revision von Bedeutung sind. Die generelle Kontrolle von *Mitarbeiterkonten* ist auch und gerade zur Aufklärung von Straftaten – insbesondere ohne vorherige Einschaltung des Betriebsrates und Mitteilung an die Betroffenen – nicht zu akzeptieren. Lediglich bei *konkreten Verdachtsmomenten* im Einzelfall können Kontrollmaßnahmen gerechtfertigt sein, bevor die Bank als Arbeitgeber die Strafverfolgungsbehörden einschaltet, um das betrügerische Verhalten eines Mitarbeiters zu unterbinden.

Widerspruch gegen Werbung

Ein Bürger nahm an einem Quiz, das von einer Berliner Zeitung organisiert wurde, teil. Als er im Anschluß an die Quizveranstaltung von der Zeitung Werbung erhielt, legte er Widerspruch gegen die weitere Nutzung seiner Anschrift für Werbezwecke ein. Trotz des Widerspruches erhielt er nach etwa drei Monaten wiederum Werbung der betreffenden Zeitung. Daraufhin beschwerte sich der Bürger darüber, daß sein Widerspruch nach der ersten Werbung nicht beachtet war. Außerdem machte er von seinem Recht gemäß § 34 Abs. 1 Nr. 1 BDSG Gebrauch. Danach kann der Betroffene Auskunft verlangen über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft und die Empfänger beziehen. Die Zeitung teilte ihm daraufhin mit, daß sie nicht in der Lage sei, ihm die Herkunft der Daten mitzuteilen, da seine Daten im Anschluß an sein letztes Schreiben gelöscht wurden. Inzwischen hat der Bürger insgesamt vier Werbeschreiben der Zeitung erhalten.

Wir wiesen die Zeitung darauf hin, daß die datenspeichernde Stelle rechtswidrig handelt, wenn sie den *Auskunftsanspruch* des Bürgers dadurch umgeht, daß sie seine Daten nach Erhalt des Auskunftsverlangens löscht. Im konkreten Fall stellte sich heraus, daß sich die Zeitung für ihre Werbeaktionen – mit Ausnahme der ersten Werbung – mehrerer Adressenhändler bedient hatte. Die Bürger, die einer Werbung widersprachen, wurden aus dem Adressenbestand der Zeitung gelöscht. Anschließend besorgte sich die Zeitung für eine neue Werbeaktion neue Adressen über einen Adressenhändler. Falls sich die Adresse eines Bürgers, der der Werbung widersprochen hatte, in dem neuen Adressenbestand befand, erhielt er wiederum ein Werbeschreiben der Zeitung. Da eine zweite Werbung nach erfolgtem Widerspruch rechtswidrig ist, handelte die Zeitung rechtswidrig.

Um eine derartige rechtswidrige Werbeaktion in Zukunft zu vermeiden, wird die Zeitung eine *hausinterne Robinsonliste* einführen. Wenn die Zeitung zukünftig mit Adressenunternehmen zusammenarbeit, wird sie sicherstellen, daß diese Unternehmen nur Personen bewerben, die nicht auf dieser Liste geführt werden. Die Sicherstellung soll insbesondere mit Hilfe von Vertragsstrafen erreicht werden.

Nachsendeantrag und Adressenhandel

Uns gingen mehrere Beschwerden von Bürgern zu, die sich über die Werbung einer Lottogesellschaft beschwerten. Das Besondere an der Werbeaktion der Lottogesellschaft war, daß sie zahlreiche Minderjährige zur Teilnahme am Glücksspiel einlud. Die Bürger wollten insbesondere erfahren, woher die Lottogesellschaft die Daten der minderjährigen Kinder erhalten hatte.

Es gelang uns in den vorliegenden Fällen, den gesamten Datenfluß nachzuvollziehen. Die Bürger hatten vor etwa einem Jahr einen Nachsendeantrag bei der Deutschen Post AG gestellt. Die Umzugsmeldekarte der Post enthielt auch die Namen der Kinder. Die Deutsche Post AG und die Deutsche Postadress GmbH haben einen Vertrag geschlossen, in dem sich die Deutsche Post AG verpflichtet, alle bei ihr über Umzugsmeldekarten gemeldeten Umzüge an die Deutsche Postadress GmbH zu übermitteln, sofern die Betroffenen einer Weitergabe der Umzugsmeldungen nicht widersprochen haben. Die von der Deutschen Post AG übermittelten personenbezogenen Daten (alte und neue Anschrift) werden von der Deutschen Postadress GmbH manuell erfaßt und anschließend in der dort geführten Umzugsadressendatei gespeichert.

Die Deutsche Postadress GmbH ist ein Adressenhändler, der die genannte Umzugsadressendatei an verschiedene Institutionen verkauft. So wird die Datei u. a. von Firmen verwendet, die – wie z. B. Versandhäuser – ihre *Kundendaten aktualisieren* wollen. In den vorliegenden Fällen wurden die Daten für Werbezwecke verkauft. Die *Lottogesellschaft* kaufte von der Deutschen Postadress GmbH Adressen von männlichen Personen für die oben erwähnte Werbeaktion. Für die Vertragspartner war – obwohl dies offensichtlich nicht ausdrücklich geregelt wurde – klar, daß die Lottogesellschaft kein Interesse an männlichen Kindern und Jugendlichen hatte. Da allerdings in der Umzugsadressendatei auch Kinderadressen gespeichert waren, hat die Deutsche Postadress GmbH auch diese an die Lottogesellschaft verkauft. Die Deutsche Postadress GmbH behauptet, bei dem Verkauf der Daten versehentlich nicht daran gedacht zu haben, daß auch Kinder und Jugendlichen in der Umzugsadressendatei enthalten sind.

Der *Adressenhandel* stellt eine geschäftsmäßige Datenverarbeitung für fremde Zwecke dar, für die die Rechtsvorschriften des BDSG gelten (§§ 27 bis 38, insbesondere § 29 BDSG). Die Speicherung personenbezogener Daten durch Adressenhandelsunternehmen ist zulässig, soweit kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden (§ 29 Abs. 1 Satz 1 Nr. 1 BDSG). Das Speichern ist auch zulässig, soweit die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen worden sind (§ 29 Abs. 1 Satz 1 Nr. 2 BDSG). Die Übermittlung von Adreßdaten zur Direktwerbung erfolgt in der Regel nach § 29 Abs. 2 Satz 1 Nr. 1 b) i. V. m. § 28 Abs. 2 Satz 1 Nr. 1 b) BDSG. Nach diesen Vorschriften ist die Übermittlung von listenmäßig oder sonst zusammengefaßten Daten über Angehörige einer Personengruppe zulässig, wenn sie sich auf gewisse Kriterien – wie Namen, Titel, akademische Grade, Anschrift etc. – beschränkt und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Im Regelfall werden schutzwürdige Belange weder durch die Speicherung noch durch die Datenübermittlung beeinträchtigt. Auch das werbende Unternehmen handelt grundsätzlich nicht rechtswidrig, wenn es die durch ein Adreßhandelsunternehmen erlangten personenbezogenen Daten für Werbezwecke nutzt. Der Betroffene hat allerdings das Recht zu verlangen, daß seine Daten gelöscht bzw. nicht mehr weiter für Werbezwecke genutzt (beim werbenden Unternehmen) oder übermittelt (beim Adressenhändler) werden.

In den vorliegenden Fällen kann allerdings ausnahmsweise davon ausgegangen werden, daß die Werbeaktion der Lottogesellschaft rechtswidrig erfolgte. Bei der *Werbung von Jugendlichen für Glücksspiele* ist offensichtlich, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung oder Nutzung zu Werbezwecken hat (vgl. § 28 Abs. 2 Nr. 1 b) BDSG). Da die Lottogesellschaft die Daten vom Adressenhändler in gutem Glauben erworben hat, liegt kein vorsätzlich rechtswidriges Handeln der unter unserer Kontrolle stehenden Lottogesellschaft vor (die Deutsche Postadress GmbH befindet sich nicht in unserem örtlichen Zuständigkeitsbereich). Wir werden der Lottogesellschaft allerdings empfehlen, sich in Zukunft von Adressenhändlern zusichern zu lassen, daß die Adressen nur von volljährigen Personen stammen. Die Zusicherung sollte mit einer Vertragsstrafenvereinbarung bekräftigt werden.

Videoüberwachung im Taxi

Zunehmende datenschutzrechtliche Probleme sind mit dem Einsatz der Videotechnik verbunden, die alle Lebensbereiche durchdringen. Aus Großbritannien wird gemeldet, daß bereits ganze Städte flächendeckend durch Videokameras überwacht werden; die dabei aufgenommenen Videofilme sind schon in einer Weise, die Persönlichkeitsrechte massivst beeinträchtigt, im Fernsehen gezeigt worden. Das Bundesdatenschutzgesetz regelt diesen Bereich nur äußerst unzulänglich und wird insoweit verbessert werden müssen. Gleichwohl müssen bereits jetzt Kriterien für den Videoeinsatz aufgestellt werden.

Um sich vor Überfällen zu schützen, haben einige Taxiunternehmer Videoüberwachungsanlagen in ihre Taxen eingebaut. Die Fahrgäste werden zu Beginn und am Ende der Fahrt für jeweils zehn bis zwanzig Sekunden gefilmt.

Es kann grundsätzlich davon ausgegangen werden, daß die zu schützenden Rechtsgüter des Taxifahrers (Leben, Gesundheit, Eigentum) höher zu bewerten sind als das allgemeine Persönlichkeitsrecht. Trotzdem ist es unverhältnismäßig, wenn der Taxifahrer diese Rechtsgüter durch einen Eingriff in auch hochrangige Rechtsgüter von *unbeteiligten* Dritten (Fahrgäste, die keine Überfälle beabsichtigen) schützt.[180] Eine Videoaufnahme ist somit nur rechtmäßig, wenn eine wirksame Einwilligung vorliegt. Diese kann ausdrücklich oder konkludent erfolgen. Grundsätzlich empfehlen wir, sowohl innen als auch außen einen deutlich sichtbaren Hinweis auf die Videoüberwachung anzubringen, der auch von Ausländern (Sprachunkundigen) verstanden wird.

Das Taxiunternehmen hat sicherzustellen, daß der Videofilm sicher aufbewahrt wird, Dritten nicht zugänglich gemacht wird und je nach Technik und Praktikabilität so bald wie möglich wieder gelöscht wird. In der Regel wird man davon ausgehen können, daß eine Löschung spätestens am Schichtende bzw. am nächsten Tag vor Arbeitsbeginn erfolgen sollte. Für eine weitergehende Speicherung liegt die Einwilligung des Fahrgastes zu dem offensichtlich vorliegenden Zweck (Verhinderung von Überfällen) nicht vor. Aus datenschutzrechtlicher Sicht sind Videosysteme zu empfehlen, bei denen zu einem bestimmten Zeitpunkt (z. B. nach 2 Stunden bzw. nach 10 Fahrgästen) die alten Aufnahmen gelöscht bzw. überspielt werden.

180 vgl. auch Urteil des BGH vom 25. 4. 1995 – VI ZR 272/94 (KG), NJW 1995, S. 1955

7. Durchsetzung des Datenschutzes

7.1 Sicherstellung des Datenschutzes in den Behörden

Behördliche Datenschutzbeauftragte

Die Zahl der behördlichen Datenschutzbeauftragten ist nur noch geringfügig gestiegen. Die meisten Stellen haben inzwischen einen behördlichen Datenschutzbeauftragten bestellt. Übrig bleiben einige wenige öffentliche Institutionen, die der inneren Organisation des Datenschutzes offensichtlich nur eine geringe Priorität einräumen.

In Hinblick auf die Qualifikation der behördlichen Datenschutzbeauftragten sind widersprüchliche Beobachtungen zu machen. Einerseits mehren sich Anfragen von Stellen, denen an einer profunden Ausbildung ihrer behördlichen Datenschutzbeauftragten gelegen war. Hier konnte auf das Kursangebot verschiedener Institutionen verwiesen werden. Andererseits wurde das von der *Verwaltungsakademie* zusammen mit uns gemachte Angebot eines speziellen Kurses für behördliche Datenschutzbeauftragte nicht im erwarteten Maße angenommen, obwohl die Akademie in Rundschreiben an die behördlichen Datenschutzbeauftragten speziell darauf hingewiesen hat. Im Wintersemester 1995/96 mußte der Kurs sogar mangels Interessenten abgesagt werden.

Wie im vergangenen Jahr entstanden Probleme hinsichtlich der *Eignung* einzelner behördlicher Datenschutzbeauftragter.

An einer Universität stand seit langem die Neubesetzung der Position eines behördlichen Datenschutzbeauftragten an. Die Führung des Hauses wollte den *EDV-Leiter* auf diese Stelle setzen, weil sie der Meinung war, daß die Datenschutzproblematik überwiegend mit EDV-technischen Fragen zu tun habe. Gegen diese Absicht erhob der Personalrat Einspruch, weil er Zweifel an der Unabhängigkeit hatte. Die Interessen eines EDV-Leiters könnten mit denen des behördlichen Datenschutzbeauftragten kollidieren, da er seine eigenen Entscheidungen als EDV-Leiter in seiner Rolle als behördlicher Datenschutzbeauftragter kritisch zu hinterfragen oder gar zu kontrollieren hätte.

Diese Auffassung wird durch ein Urteil des Bundesarbeitsgerichts unterstützt, in dem dargelegt wird, daß der behördliche Datenschutzbeauftragte die Rechte Dritter – insbesondere der Arbeitnehmer – gegen mögliche Beeinträchtigungen durch die Datenverarbeitung schützen können muß. Mit seiner Stellung und Funktion wäre es nicht zu vereinbaren, wenn er in erster Linie seine eigene Tätigkeit kontrollieren müßte.[181]

Im übrigen dürfte eine Diskussion über Unverträglichkeiten in der Position des Datenschutzbeauftragten mit seinem sonstigen Aufgabengebiet in einer großen Universität schon deshalb überflüssig sein, weil derart große und komplexe Organisationen eines hauptamtlichen Datenschutzbeauftragten bedürfen.

Ähnlich gelagert war der Fall an einer Fachhochschule. Hier sollte der *Vertreter des Kanzlers* mit den Aufgaben eines behördlichen Datenschutzbeauftragten betraut werden. Auch hier hat der Personalrat gegen die Entscheidung der Hausleitung gestimmt und uns um eine unterstützende Stellungnahme gebeten. Es wurden in erster Linie eine Interessenkollision mit dem Amt und der neuen Aufgabe befürchtet. Auch in diesem Falle haben wir den Verantwortlichen geraten, von einer Bestellung des Kanzlervertreters abzusehen und fachlich geeignete Mitarbeiter vorzuziehen, die auf Grund ihrer Position unabhängig in Datenschutzfragen urteilen können.

Dateienregister

Inzwischen steht für die Meldungen zum Geräteverzeichnis des Dateienregisters eine erweiterte Version des vom Landesamt für Informationstechnik entwickelten *INVENT-Verfahrens* zur Verfügung. Es erleichtert die automatisierten Meldungen erheblich. Allerdings wurde in Anwenderkreisen und in Sitzungen der Organisationsstellen beklagt, daß trotz der Meldungen auf Disketten auf den zusätzlichen papierenen Ausdruck der Meldungen nicht verzichtet werden kann.

Dies zeigt, daß der Sinn des Dateienregisters nicht überall verstanden wird. Beide Verzeichnisse des Dateienregisters, Dateien- und Geräteverzeichnis, sind – soweit keine gesetzlichen Ausnahmeregelungen bestehen – öffentliche Register, in die jeder Bürger ohne besonderen Anlaß Einsicht nehmen darf. Dazu muß die Meldung in schriftlicher und verständlicher Weise vorliegen. Die Vertrautheit im Umgang mit Computern kann bei den Bürgern nicht soweit vorausgesetzt werden, daß es ihm zuzumuten wäre, sich bei der Wahrnahme seiner gesetzlichen Rechte an einen Computer zu setzen, um die Einsicht zu erhalten. Außerdem ist es den meldenden Stellen eher zuzumuten, Ausdrucke der elektronisch vorhandenen Meldungen zu fertigen, als unserer Dienststelle, die nur über beschränkte Druckkapazitäten verfügt.

Einzuräumen ist, daß das ganze Meldeverfahren kompliziert ist und – auch bei Nutzung des INVENT-Verfahrens – manche Behörden offensichtlich überfordert. Vor allem fast alle Bezirksämter haben sich vor diesem Hintergrund bisher geweigert, die gesetzlichen Meldevorgaben zu befolgen. In der Tat wird – spätestens im Zusammenhang mit der Umsetzung der EU-Richtlinie – zu prüfen sein, ob die Meldevorschriften des Berliner Datenschutzgesetzes und der Dateienregisterordnung nicht mit dem Ziel einer Vereinfachung und Entbürokratisierung zu überarbeiten sind, ohne dabei deren Zwecke zu gefährden. Die Transparenz der Datenverarbeitung muß dabei für den Bürger und für uns erhalten bleiben.

In einem Rundschreiben an die betroffenen öffentlichen Stellen haben wir diese von allen Meldungen unterrichtet, die uns aus der Zeit vor der Novellierung des Berliner Datenschutzgesetzes im Jahre 1990 vorlagen, aber danach nicht im Rahmen einer Änderungsmeldung an das neue Dateienregister angepaßt wurden. Wir baten um Überprüfung, ob diese Dateien überhaupt noch in der gemeldeten Form existieren würden, und um einen Abgleich mit den internen Übersichten. Neben der Vollständigkeit ging es darum, Inkonsistenzen des Berliner Dateienregisters zu beseitigen: Neue Meldungen konnten den alten Meldungen nicht zugeordnet werden, weil nicht die gleichen Namen vergeben wurden.

Die Reaktion zeigt, daß viele öffentliche Stellen Probleme haben, diesen Abgleich durchzuführen, weil sie es bisher versäumt haben, personenbezogene Dateien und die dazugehörigen ADV-Systeme ordnungs- und gesetzesgemäß einheitlich, vollständig und nachvollziehbar zu dokumentieren. Nur in solchen Fällen kann eine solche Anfrage den beklagten hohen Aufwand zur Folge haben. Die Stellen, die von vornherein eine klare organisatorische Struktur für ihre interne Dateien- und Geräteübersicht aufgebaut haben, hatten kaum Schwierigkeiten, unserem Informationswunsch zu entsprechen.

Unterstützung des Berliner Datenschutzbeauftragten

Nach § 38 BlnDSG sind alle Behörden verpflichtet, den Datenschutzbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Insbesondere ist ihnen Auskunft zu ihren Fragen zu gewähren. Leider müssen wir feststellen, daß mitunter dieser Verpflichtung nicht nachgegangen wird. Bei einigen Behörden, zu denen z. B. die Führerscheinstelle im Landeseinwohneramt gehört, gibt es fast keinen Vorgang, bei dem die Beantwortung nicht angemahnt werden muß. Diese Verhaltensweise wird dem Anspruch des Bürgers nicht gerecht, möglichst umgehend über die datenschutzrechtliche Bewertung seines Anliegens unterrichtet zu werden.

Da wir uns in erster Linie dem Bürger verpflichtet fühlen, müssen derartige Verwaltungen damit rechnen, daß von uns aufgrund des Sachverhaltsvortrags des Betroffenen eine Beanstandung erfolgt, ohne daß die Antwort abgewartet wird.

7.2 Der Berliner Datenschutzbeauftragte

Nach seiner einstimmigen Wiederwahl (bei einer Enthaltung) am 19. Januar 1995 wurde Dr. Hansjürgen Garstka am 9. Februar 1995 für weitere fünf Jahre erneut zum Berliner Datenschutzbeauftragten ernannt.

181 Urteil vom 22. 3. 1994 – ARB 51/93 –

Die laufende Amtsperiode wird gekennzeichnet sein von schwierigen Entscheidungen verschiedener Art. Sollten die Bevölkerungen Berlins und Brandenburgs am 5. Mai 1996 der *Fusion der beiden Bundesländer* zustimmen, wird sehr bald die künftige Struktur der Dienststelle des Landesbeauftragten eines gemeinsamen Landes festzulegen sein. Dabei muß auch erörtert werden, ob ein Magistratsdatenschutzbeauftragter mit herausgehobener Aufgabenstellung eingerichtet werden soll. Kommt es wider Erwarten zu einem anderen Ausgang, werden ebenfalls koordinierte Vorgehensweisen erforderlich sein, um eine angemessene Kontrolle der gleichwohl entstehenden gemeinsamen Infrastrukturen zu gewährleisten.

Der rapide *Zuwachs des Anteils automatischer Datenverarbeitung* an der Verwaltungstätigkeit einschließlich deren institutioneller und regionaler Vernetzung wird neue Überlegungen darüber erforderlich machen, auf welche Weise künftig eine Datenschutzaufsicht im öffentlichen, aber auch im privaten Bereich sichergestellt werden kann. Sicher ist, daß die Knappheit der Haushalte, die zum Anlaß erheblicher Personaleinsparungen teilweise zugunsten der weiteren Automatisierung genommen wird, nicht zu einer Reduzierung der – vermehrt erforderlichen – Kontrollmöglichkeiten führen darf.

Schließlich wird die *Umsetzung der EU-Richtlinie* ebenfalls Anlaß sein müssen, Organisation und Instrumentarium unserer Dienststelle insbesondere auf ihre Effektivität hin zu überprüfen – nach der Richtlinie stehen „wirksame Einwirkungsbefugnisse“ (sic!) der „Kontrollstelle“ ganz im Vordergrund (Art. 28 Abs. 3 Satz 1, 2. Anstrich BDSG).

Im Berichtsjahr konnte im Bereich Technik und Organisation eine zusätzliche Stelle mit einer Diplomingenieurin besetzt werden; damit verfügen wir über Expertinnen und Experten in den wesentlichen Bereichen der Datenverarbeitung proprietärer Systeme, Netzwerke, UNIX-Systeme sowie PCs – jeweils eine einzige Person für das ganze Land Berlin!

Zur Bewältigung der Aufgaben der Aufsichtsbehörde wurden zum 1. August 1996 zwei Mitarbeiter der Senatsverwaltung für Inneres, die zuvor mit Fragen des Datenschutzes befaßt waren, in unsere Dienststelle versetzt. Eine weitere Stelle wurde für die erforderlichen Geschäftsstellenarbeiten, insbesondere die Führung des für Fremdverarbeiter vorgeschriebenen Dateienregisters, zur Verfügung gestellt. Der Organisationsplan wurde entsprechend um einen Bereich „Private Datenverarbeitung“ ergänzt.

Ein Überblick über unsere *Geschäftsverteilung* zum Ende des Berichtszeitraums befindet sich in den Anlagen.[182]

Aufgabenentwicklung

Die Zahl der Eingaben ist im Berichtszeitraum erheblich angestiegen. Presseveröffentlichungen zur Werbung und dem Adressenhandel führten zu vielen Anfragen zu diesem Thema. Im Zusammenhang mit den Wahlen zum Abgeordnetenhaus und den Bezirksverordnetenversammlungen haben uns ebenfalls zahlreiche Eingaben erreicht. Die meisten Beschwerden richteten sich gegen Einrichtungen der Ordnungsverwaltung (wobei der Bereich Meldewesen – nicht zuletzt wegen der Wahl – wiederum am häufigsten betroffen war), gefolgt vom Sicherheitsbereich (Justiz, Polizei und Landesamt für Verfassungsschutz) und der Leistungsverwaltung. Die bereits im vergangenen Jahr beachtliche Zahl von Eingaben gegen die Verarbeitung von Personaldaten ist erheblich gestiegen.

Die Beratungsersuchen der Verwaltung gingen im Berichtszeitraum verstärkt in Richtung der Klein-Server-Technologien. Bei den Rechtsfragen stehen weiterhin die Bereiche Bildung und Forschung sowie Gesundheit und Soziales vorn, wobei festzustellen ist, daß die Verwaltung insgesamt verstärkt von der Möglichkeit Gebrauch macht, sich im Vorfeld in Datenschutzfragen beraten zu lassen.

Mit Übernahme der Aufgaben der Aufsichtsbehörde werden von uns auch alle Eingaben und Beratungsersuchen aus dem privaten Bereich bearbeitet; im Zeitraum zwischen 1. August und Jahresende sind hierzu über 200 Vorgänge eröffnet worden. Einen Schwerpunkt bildeten hier die Eingaben zur BahnCard, die auch vom Bundesbeauftragten und den Aufsichtsbehörden anderer Länder an uns abgegeben wurden.

Nach Klärung der organisatorischen Vorfragen werden zu Beginn des neuen Jahres auch die systematischen Kontrollen der Fremddatenverarbeiter wieder aufgenommen. Das entsprechende Register, in das jeder Einsicht nehmen kann, ist inzwischen neu aufgebaut worden.

Abgeordnetenhaus

Wegen der großen Terminnot zum Ende der Legislaturperiode hat der Berliner Datenschutzbeauftragte darauf verzichtet, wie in den Vorjahren anläßlich der parlamentarischen Beratung des Jahresberichts 1994 von seinem *Rederecht* im Plenum Gebrauch zu machen. Statt dessen wurde eine kurze Rede zu Protokoll gegeben.[183]

Zu danken war für die gute Zusammenarbeit, die zwischen dem Hause, seinen Organen und Ausschüssen und dem Datenschutzbeauftragten möglich war. Insbesondere ist die Arbeit des *Unterausschusses Datenschutz* des Ausschusses für Inneres, Sicherheit und Ordnung hervorzuheben, der im Berichtsjahr noch vier Sitzungen durchführte und dessen Arbeit von allen Fraktionen für die sachliche und konstruktive Zusammenarbeit gelobt wurde. Besonderer Dank galt dem langjährigen *Vorsitzenden Helmut Hildebrandt*, der sich in besonderer Weise um die Fortentwicklung des Datenschutzes in Berlin verdient gemacht hat und der in der neuen Wahlperiode nicht mehr Mitglied des Abgeordnetenhauses ist.

Erneut suchte eine Reihe anderer Ausschüsse, darunter der Petitionsausschuß, unsere Beratung.

Kooperation

Das Datenschutzgesetz verpflichtet den Datenschutzbeauftragten, mit allen Stellen zusammenzuarbeiten, die wie er die Aufgabe haben, die Einhaltung der Vorschriften über den Datenschutz zu kontrollieren (§ 24 Abs. 4 BlnDSG). Am bedeutsamsten ist die Zusammenarbeit mit dem *Bundesbeauftragten für den Datenschutz* sowie den anderen Landesbeauftragten, deren gemeinsame *Konferenz* im vergangenen Jahr zweimal in Bremen tagte und wiederum eine Reihe von Beschlüssen zu grundlegenden Fragen des Datenschutzes faßte.[184] Erneut war die Zusammenarbeit mit dem *Landesbeauftragten von Brandenburg* intensiv und einvernehmlich.

Neu war die Kooperation mit dem Düsseldorfer Kreis; die regelmäßigen Kooperationssitzungen mit der Senatsverwaltung für Inneres wurden fortgesetzt.

Auf *nationaler, europäischer und internationaler* Ebene wurde die besondere Kooperation auf dem Gebiet des Datenschutzes bei *Telekommunikation und Neuen Medien* fortgesetzt.[185] Mit einer gemeinsamen Sitzung mit der *Privacy Working Group* im Rahmen des *National Information Infrastructure-Projektes der US-Regierung*, zu der diese nach Washington eingeladen hatte, erreichte insbesondere die Arbeit der Internationalen Arbeitsgruppe einen neuen Höhepunkt. Auf Grund der Diskussionen, in der die Mitglieder unseres Arbeitskreises vor allem eine Stärkung der Rechte der Betroffenen sowie bessere Kontrollmöglichkeiten empfahlen, wurden weitere Nachbesserungen der Principles for Providing and Using Personal Information[186] vorgenommen, die mangels einer gesetzlichen Regelung als Richtschnur für den Datenschutz für den privaten Bereich in den USA gelten können.

Wie alle zwei Jahre traf sich die Internationale Arbeitsgruppe erneut aus Anlaß der *Internationalen Funkausstellung* im Rahmen des Internationalen Mediendialogs, diesmal zu einem Symposium „Multimedia und Datenschutz“.[187]

182 Anlage 5

183 vgl. Anlage 1

184 vgl. die Anlagen zu 2.

185 vgl. 4

186 Information Infrastructure Task Force, Privacy Working Group: Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information. Washington Juni 1995. Vgl. auch: U.S. Department of Commerce, National Telecommunications and Information Administration: Privacy and the NII: Safeguarding Telecommunications – Related Personal Information. Washington 1995

187 Die Vorträge sind in der von uns herausgegebenen Broschüre Materialien zum Datenschutz Heft 22 abgedruckt.

Öffentlichkeitsarbeit

Im Vordergrund unserer Öffentlichkeitsarbeit steht das Bemühen, die Bürger mit den datenschutzrechtlichen Vorschriften vertraut zu machen. Hierzu dient die Gesetzessammlung *„Berliner Informationsgesetzbuch“*.[188] Diese Publikation hat große Resonanz gefunden. Von einigen Heften wurden Neuauflagen herausgegeben, insbesondere vom Berliner Datenschutzgesetz in seiner neuen Fassung.

Auch zwei neue Hefte sind inzwischen erschienen:

Teil 1 – Datenschutzgesetze – wurde um Heft 3 – *Besonderes Berliner Datenschutzrecht* – ergänzt. In immer mehr Berliner Gesetzen und Verordnungen sind inzwischen spezielle datenschutzrechtliche Regelungen enthalten, so z. B. in dem Zweckentfremdungsbeseitigungsgesetz, dem Gesundheitsdienstgesetz, dem Friedhofsgesetz, dem Gesetz über die Stadtreinigung und im Hochschulgesetz. Das Heft soll einen Überblick über diese Regelungen geben und führt für 24 Gesetze die hier geltenden Datenschutzbestimmungen auf.

In einem neuen Teil 4 – Kultur, Wissenschafts- und Schulrecht – haben wir *„Datenschutz in der Schule“* als Heft 1 aufgenommen. Hier sind die wichtigsten rechtlichen Regelungen über den Datenschutz in diesem Bereich zusammengefaßt. Die in dem Heft enthaltene Auswahl von Vorschriften soll eine Hilfestellung für interessierte Eltern, Schüler und Lehrer sein. Alle Berliner Schulen haben ein Exemplar erhalten.

Anregungen, welche Vorschriften und Texte noch in das Informationsgesetzbuch aufgenommen werden könnten, nehmen wir gern entgegen.

In unserer Reihe „Materialien zum Datenschutz“ ist die Broschüre *„Datenschutz bei Telekommunikation und Medien 1993/94“* erschienen. Sie enthält Beiträge aus unseren Jahresberichten, Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, gemeinsame Erklärungen der Konferenz der Europäischen Datenschutzbeauftragten und einen Bericht einer Arbeitsgruppe der Internationalen Datenschutzkonferenz zu diesem immer aktueller werdenden Thema.

Auch wir verschließen uns nicht den internationalen Entwicklungen: Nachdem wir bereits zu den Pionieren unter den Anbietern bei Bildschirmtext gehört haben – dort ist bereits seit 1981 ein Angebot des Berliner Datenschutzbeauftragten enthalten (*92 6790≠) –, werden wir mit Erscheinen dieses Jahresberichts auch im Internet präsent sein. Das deutsche Forschungsnetz hat uns zusammen mit der Technischen Universität ermöglicht, eine eigene Domain einzurichten (datenschutz−berlin.de), in der weltweit Informationen über den Datenschutz abgerufen werden können.

188 Jahresbericht 1994, 6.2

7.3 Und zum Schluß wieder: Falsch verstandener Datenschutz

Immer wieder wird der Datenschutz vorgeschoben, um aus Bequemlichkeit oder Unwissenheit die mit einer allgemeinen Auskunftserteilung verbundenen Arbeiten zu vermeiden. In der Öffentlichkeit besteht wenig Verständnis für diese Praxis. Sie diskreditiert auch den Datenschutz, da er unzutreffend als Grund für bürgerunfreundliches Verhalten genannt wird.

> *Ein Tiefbauamt hat einer Tierschutzjugendgruppe, die auf Straßenfesten einen Info-Stand aufbauen wollte, auf die Frage, welche Feste im Herbst und Winter stattfinden, lapidar geantwortet, man sei „aus Datenschutzgründen“ nicht berechtigt, Mitteilungen über Veranstalter an Dritte weiterzugeben.*

Zwar ist es zutreffend, daß das Bezirksamt personenbezogene Daten nur im Rahmen der Übermittlungsbestimmungen oder mit Einwilligung des Betroffenen weitergeben darf. Es wäre hier aber ein leichtes gewesen, bei der Jugendgruppe die Einwilligung für die Weiterleitung des Briefes an den oder die Veranstalter einzuholen, wenn nicht ohnehin die Veranstalter deutlich gemacht hätten, daß sie als Ansprechpartner für Teilnehmer und andere Interessenten zur Verfügung stehen.

> *Die Tagespresse hat berichtet, daß ein Veterinär- und Lebensmittelaufsichtsamt „aus datenschutzrechtlichen Überlegungen“ keine Antwort darauf geben könne, wie viele Katzen im Bezirk leben. Erst auf Nachfrage wurde eingeräumt, daß man keine Zahlen nennen könne, weil darüber keine Aufzeichnungen existieren und freilaufende Katzen im Bezirk kein Problem seien.*

Die Datenschutzgesetze verhindern die Auskunft nicht. In ihren Anwendungsbereich fällt nur die Verarbeitung personenbezogener Daten, nämlich von Einzelangaben über persönliche oder sachliche Verhältnisse von natürlichen Personen. Darunter fallen Katzen zweifelsfrei nicht. Selbst wenn die Katzen Namen hätten, hätte hier selbstverständlich eine Auskunft, die ohnehin nur über die Anzahl gewünscht wurde, erteilt werden können.

Berlin, 20. März 1996

Dr. Hansjürgen Garstka
Berliner Datenschutzbeauftragter

Anlage 1

1. Rede des Berliner Datenschutzbeauftragten zu Protokoll der Sitzung des Abgeordnetenhauses am 7. September 1995

Sehr verehrte Frau Präsidentin,
sehr geehrte Damen und Herren!

Zum letzten Mal in dieser Legislaturperiode steht der Bericht des Datenschutzbeauftragten sowie die Stellungnahme des Senats dazu auf der Tagesordnung der Plenarsitzung des Abgeordnetenhauses. Dies möchte ich zum Anlaß nehmen, einen kurzen Rückblick auf die Entwicklung des Datenschutzes zu geben und einige kurze Bemerkungen zum Stand des Datenschutzes in unserem Lande zu machen.

Als die neue Legislaturperiode begann, war eine Neufassung des Datenschutzgesetzes in Kraft, die nur noch wenig Raum ließ für eine generalklauselartige Bewertung von Eingriffen in die informationelle Selbstbestimmung. Nunmehr war es vielmehr erforderlich, in Einzelregelungen die spezifischen Anforderungen der vielfältigen Gesetzesmaterien an die Verarbeitung personenbezogener Daten zu formulieren.

Der Gesetzgeber hat sich in der vergangenen Legislaturperiode dieser Aufgabe mit großem Ernst und ich meine mit Erfolg gewidmet: In eine Reihe von Gesetzen wurden angemessene Regelungen der Datenverarbeitung und des Datenschutzes eingefügt; das letzte große Vorhaben, die Neufassung der Bestimmungen zur Verarbeitung von Personaldaten und der Führung von Personalakten im öffentlichen Dienst, wird dieses Abgeordnetenhaus noch verabschieden; lediglich die normenklare Regelung der Durchführung von Sicherheitsüberprüfungen steht aus, da ein Konsens über die Notwendigkeit und die Inhalte eines derartigen Gesetzes offenbar nicht erreicht werden konnte. Weite Bereiche der erforderlichen Regelungen wurden in einem Artikelgesetz erfaßt, das seinerseits auf dem Wege der Verordnungsermächtigung Raum ließ für zeit- und problemnahe Bestimmungen, die bis auf wenige Ausnahmen vom Senat inzwischen auch erlassen wurden.

Die strengen Anforderungen, die der Landesgesetzgeber selbst an die Regelungsdichte im Bereich des Datenschutzes gestellt hatte, machten Ausnahmen erforderlich, die zu bedeutsamen Auseinandersetzungen zwischen Senat und Datenschutzbeauftragten, sowie zu entsprechenden Debatten in diesem Hause führten:

Die Verarbeitung personenbezogener Daten zu Zwecken der „allgemeinen Verwaltung“, also zu Zwecken, die jedem Teil der Verwaltung eigen sind und deren Regelung in den jeweiligen, die Aufgabenbereiche der Verwaltung umschreibenden Gesetzen zu einem unvertretbaren und geradezu grotesken Aufwand geführt hätte, wurde gebündelt in dem Gesetz zur Informationsverarbeitung in der Berliner Verwaltung geregelt – ein Gesetz übrigens, das in verschiedener Hinsicht Mängel aufweist und in der neuen Legislaturperiode dringendst novelliert werden muß. Die entsprechenden Vorarbeiten sind von der Senatsverwaltung für Inneres und uns bereits geleistet worden.

Die Verarbeitung personenbezogener Daten zum Vollzug von Bundesrecht auf dem Hintergrund des Berliner Datenschutzgesetzes machte ebenfalls Schwierigkeiten. Da das Bundesdatenschutzgesetz im Gegensatz zum Berliner Gesetz vielfältige Generalklauseln enthält, sieht der Bundesgesetzgeber nur bei besonders eingriffsintensiven Materien die Notwendigkeit bereichsspezifischer Regelungen. Derartige Bestimmungen sind in den letzten Jahren vielfältig verabschiedet worden (z. B. in den Bereichen der Sozial-, der Gewerbe- oder Ausländerbehörden). Es blieben aber weite Bereiche, wo derartige bundesrechtliche Initiativen nicht ergriffen wurden oder nicht voran kamen. Hier hatten wir, um das Regelungskonzept des Berliner Datenschutzgesetzes zu wahren, den Erlaß von Ausführungsgesetzen gefordert, was in einigen Gebieten auch zur Schaffung entsprechender Gesetze führte (etwa bei der Bauverwaltung oder der Regelung offener Vermögensfragen). Für den nach wie vor vorhandenen Rest an Bundesrecht ohne Datenschutzregelungen wurde am Ende der Legislaturperiode das Berliner Datenschutzgesetz dahingehend novelliert, daß hier künftig die Befugnisnormen des Bundesdatenschutzgesetzes ergänzend Anwendung finden.

Viel Kritik hat der Datenschutz deswegen auf sich gezogen, weil die Forderung nach bereichsspezifischer Regelung auch dann galt, wenn wegen der Art der Daten oder deren Verarbeitung schutzwürdige Belange gar nicht beeinträchtigt werden konnten – man denke z. B. an die Verwendung von Adressen in den Verteilern, die die Verwaltung für die Versendung von amtlichen Schriftstücken, aber auch von Informationsmaterialien führt. Auch für die Verarbeitung dieser „Trivialdaten“ konnte am Ende der Legislaturperiode im Einvernehmen zwischen Fraktionen, Verwaltung und Datenschutzbeauftragten eine legislative Lösung gefunden werden.

Im Ergebnis konnte der Grundsatz des Berliner Datenschutzgesetzes, die Verarbeitung personenbezogener Daten in der Verwaltung nur auf der Grundlage spezifischer Vorschriften zuzulassen, gewahrt werden, auch wenn von verschiedenen Seiten vielfältige Kritik geäußert wurde. Einer der häufigsten Einwände war der, daß diese Regelungen die ohnehin vorhandene Normenflut noch vergrößerten. Dem war und ist zu erwidern, daß die Normenflut selbstverständlich da abzubauen ist, wo sie nur Selbstbeschäftigung der Verwaltung ohne Effekte für den Bürger erzeugt – das öffentliche Dienstrecht ist hier ein hervorragendes Beispiel. Wenn es dagegen um Grundrechte der Bürger und deren Beschränkung geht – und die Verarbeitung der Daten des Bürgers gehört hierzu –, bleibt der Gesetzgeber aufgerufen, die Eingriffsmöglichkeiten des Staates klar zu bestimmen.

In der angesprochenen Novellierung des Berliner Datenschutzgesetzes hat dieses Haus einen weiteren Schritt zur Förderung des Datenschutzes in unserem Land getan: Es folgte den langjährigen Empfehlungen des Datenschutzbeauftragten, die Kontrolle des Datenschutzes im öffentlichen und im privaten Bereich in eine Hand zu geben. Seit dem 1. August dieses Jahres ist der Datenschutzbeauftragte auch Aufsichtsbehörde für Privatunternehmen. Eine Aufgabe, die wir mit großem Ernst übernommen haben, und deren Wahrnehmung dazu führen wird, das informationelle Selbstbestimmungsrecht der Bürger unseres Landes auch außerhalb der Verwaltung zu stärken.

Trotz dieser Erfolge auf der Ebene der Gesetzgebung sind auch nach über fünfzehn Jahren Datenschutzpraxis in der Verwaltung noch Defizite aufzuarbeiten. Noch immer stehen bei Entscheidungen über Erhebung, Speicherung, Nutzung und Weitergabe personenbezogener Daten häufig nicht der Bürger, sondern die Eigeninteressen der Verwaltung im Vordergrund. Manche Erwiderung des Senats auf unseren Tätigkeitsbericht bringt trotz allen Wohlwollens, von dem die Berliner Verwaltung im Unterschied zu Erfahrungen anderwärts geprägt ist, dies deutlich zum Ausdruck. Wenn es, um nur ein einziges Beispiel zu nennen, etwa die Innenverwaltung ablehnt, dem Wunsch eines eingebürgerten Deutschen zu entsprechen und das Geburtsland (dem er sich auf Grund der dort herrschenden Verhältnisse entfremdet hat) im Personalausweis nicht ausdrücklich aufzunehmen, so zeigt dies, daß es nach wie vor erheblicher Anstrengungen bedarf, im Einzelfall dem informationellen Selbstbestimmungsrecht des Bürgers auch bei widerstrebenden Interessen der Verwaltung Geltung zu verschaffen.

Sehr geehrte Damen und Herren,

bei der heutigen Gelegenheit möchte ich mich nochmals herzlich für die gute Zusammenarbeit bedanken, die zwischen diesem Hause, seinen Organen und Ausschüssen und dem Datenschutzbeauftragten möglich war. Vieles konnte auf diesem Hintergrund erreicht werden. Danken möchte ich vor allem den Mitgliedern des Unterausschusses Datenschutz des Innenausschusses sowie seinem scheidenden Vorsitzenden Helmut Hildebrand, die in großer Sachlichkeit und Geduld die Probleme des Datenschutzes erörterten und sich im übrigen, sicherlich aus guten Gründen, nicht immer unserer Auffassung anschlossen.

2. Beschlüsse, Entschließungen und Stellungnahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Anlage 2.1

Entschließung der 49. Konferenz am 9./10. März 1995 in Bremen zum

Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz) – Bundesrats-Drucksache 94/95

Zu den Beratungen des Entwurfs für ein Gesetz über das Bundeskriminalamt erklären die Datenschutzbeauftragten des Bundes und der Länder:

Auch aus Sicht des Datenschutzes ist es zu begrüßen, daß die seit langem überfälligen bereichsspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung insbesondere im polizeilichen Informationssystem (INPOL) nunmehr in das Gesetzgebungsverfahren eingebracht werden. Der Gesetzentwurf enthält im Vergleich zu den Vorentwürfen eine Reihe von Vorschriften, die datenschutzrechtlich positiv zu werten sind. Hierzu gehören:

- der Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sog. „Feststellung des Anfangsverdachts";
- das Erfordernis der Einwilligung für die Speicherung von Daten über Zeugen und mögliche Opfer;
- Übermittlungsverbote bei überwiegenden schutzwürdigen Interessen der Betroffenen oder bei entgegenstehenden gesetzlichen Verwendungsregelungen;
- die Beachtung landesgesetzlicher Löschungsfristen.

Andererseits begegnet der Gesetzentwurf jedoch nach wie vor gewichtigen Bedenken, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht, deren Voraussetzungen und Reichweite unklar oder nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt sind. Dies gilt insbesondere für

- die Verwendung des Begriffs der Straftaten von erheblicher Bedeutung ohne Definition, um welche Tatbestände es sich handelt, weil damit nicht mehr voraussehbar ist, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind;
- die Befugnisse der Zentralstelle zu selbständigen Datenerhebungen und Übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Einvernehmen mit den jeweils verantwortlichen Länderpolizeien;
- die unklare Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Befugnisse zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie die fehlende klare Zweckbindungs- und Zweckänderungsregelung;
- die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne eindeutige Begrenzung auf den Schutz gefährdeter Ermittler.

Die Datenschutzbeauftragten fordern den Gesetzgeber auf, die Schwachstellen des Entwurfs auszuräumen. Insbesondere fordern sie klare verfassungskonforme Regelungen zur Auskunftserteilung an Betroffene und der Prüfrechte für INPOL-Daten dahingehend, daß die Datenschutzkontrollrechte bei der datenschutzrechtlichen Verantwortung der Stellen anknüpfen, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen.

Anlage 2.2

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 in Bremen zu

Maßhalten beim vorbeugenden personellen Sabotageschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, bei Sicherheitsüberprüfungen zum personellen Sabotageschutz Augenmaß zu bewahren. Bei diesen Sicherheitsüberprüfungen werden sensible Daten, z. B. über politische Anschauungen oder Alkoholkonsum, vorbeugend erhoben, also ohne daß der Betroffene dazu Anlaß geboten hätte. Polizei und Verfassungsschutz sind routinemäßig beteiligt. Schon wenn der Betroffene im Verlauf der Überprüfung auch nur in den Verdacht der Unzuverlässigkeit gerät, kann dies bereits erheblichen Einfluß zumindest auf das berufliche Fortkommen nehmen.

Gegenwärtig sind solche Überprüfungen spezialgesetzlich für den Atombereich und für Flughäfen vorgesehen. Das Bundesministerium des Innern will jetzt klären, inwieweit Beschäftigte in anderen Einrichtungen überprüft werden sollen.

Unstreitig können solche Überprüfungen unbescholtener Bürger nur zum Schutz von „lebens- und verteidigungswichtigen Einrichtungen" angemessen sein und nur Personen betreffen, die dort an „sicherheitsempfindlichen Stellen" tätig sind. Als „lebenswichtig" sehen die Innenminister und -senatoren aber bereits Stellen an, „die für das Funktionieren des Gemeinwesens unverzichtbar sind". Damit könnten Beschäftigte in weiten Bereichen des öffentlichen Dienstes und der Wirtschaft mit Sicherheitsüberprüfungen überzogen werden.

Die Datenschutzbeauftragten meinen, daß das Persönlichkeitsrecht hier größere Zurückhaltung gebietet. Die Sicherheitsüberprüfungen müssen auf Bereiche beschränkt bleiben, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß.

Soweit in solchen Bereichen Sicherheitsüberprüfungen durchgeführt werden sollen, bedarf es einer ebenso klaren gesetzlichen Grundlage, wie bisher im Atomgesetz und im Luftverkehrsgesetz. Die zu schützenden Arten lebens- und verteidigungswichtiger Einrichtungen müssen durch Rechtsvorschrift abschließend festgelegt sein. Dabei sind für die jeweiligen Bereiche angemessene Regelungen zu treffen, die mit Rücksicht auf die Interessen Betroffener folgende allgemeine Grundsätze beachten:

- möglichst klare Vorgaben zur „Sicherheitsempfindlichkeit" in der Vorschrift und exakte Festlegung dieser Stellen durch die zuständige Behörde nach Anhörung der Personalvertretung der einzelnen Einrichtung,
- Zustimmung des Betroffenen als Verfahrensvoraussetzung,
- abschließender Katalog der regelmäßig durchzuführenden Maßnahmen, dabei Beschränkung auf vorhandene Erkenntnisse, keine Ausforschungsermittlungen,
- strenge Zweckbindung und angemessene organisatorische Vorkehrungen zu deren Gewährleistung, insbesondere Trennung von Personalakte,
- eigene Verfahrensrechte des Betroffenen, insbesondere rechtliches Gehör vor ablehnender Entscheidung und aktenkundige Gegendarstellung,
- angemessener Auskunftsanspruch, einschließlich Akteneinsicht,
- effektive Datenschutzkontrolle, auch zur Datenverarbeitung in Akten bei nicht-öffentlichen Stellen.

Im Regelfall muß zusätzlich gelten:

- Überprüfung durch die zuständige Aufsichtsbehörde selbst, nicht durch Verfassungsschutzbehörden,
- keine Einbeziehung weiterer Personen (wie Ehegatten usw.),
- Ausnahmetatbestände wären – auch zum Verfahren – präzise zu fassen.

Die Praxis der Sicherheitsüberprüfungen zum personellen Sabotageschutz steht in Bund und Ländern vor einer wichtigen Weichenstellung. Sie muß klar und angemessen sein.

Anlage 2.3

Entschließung der 49. Konferenz am 9./10. März 1995 in Bremen zum

Datenschutz bei elektronischen Mitteilungssystemen (e-mail)

Es ist damit zu rechnen, daß in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche bedeutsame Informationen und insbesondere personenbezogene Daten über Netze ausgetauscht werden.

Die zunehmende Nutzung von elektronischen Mitteilungssystemen (Electronic-Mail, Dokumentenaustausch über Datenfernübertragung, Message Handling Systems MHS/X.400) hat zur Folge, daß Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit verschärft werden, weil Unbefugte Zugriffe auf Daten und Programme erhalten können und die Übertragungswege vom Kommunikationspartner nicht sicher zu kontrollieren sind. Deshalb ist beim Einsatz solcher Systeme das Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In diesem Zusammenhang gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information durch eine Vielzahl umfassender aufeinander abgestimmter Sicherheitsmaßnahmen an Bedeutung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, daß den folgenden Sicherheitsaspekten beim Einsatz von elektronischen Mitteilungssystemen Rechnung getragen wird:

1. Authentizität von Benutzern, Nachrichten und Systemmeldungen

   Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit bestehen, anhand bestimmter Kriterien die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen (z. B. Empfangs- und Weiterleitungsbestätigungen, Sendeanforderungen, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

2. Vertraulichkeit von übertragenen Daten

   Für alle Arten von Daten in elektronischen Mitteilungssystemen – Nachrichten sowie Verkehrs- und Verbindungsdaten – muß die Vertraulichkeit gewahrt bleiben. Sie ist durch geeignete Maßnahmen, z. B. kryptografische Verfahren, sicherzustellen.

3. Integrität von Nachrichten und Meldungen

   Es ist zu gewährleisten, daß bei Speicherung und Weiterleitung von Daten keine unbefugte, unerkannte Veränderung erfolgen kann.

4. Fälschungssichere Kommunikationsnachweise

   Die für die Anerkennung einer elektronischen Kommunikation erforderlichen fälschungssicheren Sende-, Empfangs- und Übertragungsnachweise müssen dem Anwender auf Wunsch zur Verfügung stehen.

5. Ausschluß von Kommunikationsprofilen

   Die Erstellung von Kommunikationsprofilen muß verhindert werden. Gespeicherte Protokollierungsdaten dürfen nur zu Zwecken des Datenschutzes und der Datensicherung (§§ 14 Abs. 4, 31 BDSG bzw. landesgesetzliche Regelungen) verwendet werden.

Empfehlungen zum Einsatz von elektronischen Mitteilungssystemen:

Zum sicheren Einsatz von elektronischen Mitteilungssystemen sind als Grundschutzmaßnahmen folgende Empfehlungen zu beachten:

1. Grundsätzlich sind nur solche Produkte einzusetzen, die die Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahre 1988 erfüllen. Vorhandene Systeme – insbesondere solche, die noch auf Empfehlungen von 1984 basieren –, sollen künftig durch geeignete Zusatzprodukte hinsichtlich ihrer Sicherheit verbessert oder durch neuere Softwareversionen ersetzt werden.

2. Bei Übertragung von personenbezogenen Daten ist eine Verschlüsselung vorzusehen. Die Verschlüsselung der Daten muß mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgen. Neben der Auswahl eines effektiven Verschlüsselungsalgorithmus (z. B. DES, IDEA) muß dabei insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein. Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.

3. Zur Absicherung der Integrität der Daten sollte auf Verfahren der „elektronischen Unterschrift“ zurückgegriffen werden.

4. Nach Möglichkeit ist die Funktion des Systemverwalters von der des Netzwerkverwalters – insbesondere der Verwaltung des elektronischen Mitteilungssystems – aus Sicherheitsgründen zu trennen.

5. Es ist grundsätzlich separat administrierbare Hard- oder Software – z. B. in Form eines Kommunikationsservers – für das elektronische Mitteilungssystem vorzusehen.

6. Bei Verwendungen von öffentlichen Übertragungswegen, sind die vorhandenen Sicherheitsmechanismen dieser Netze z. B. geschlossene Benutzergruppen, Rufnummernidentifikation, Teilnehmerzeichengabe und automatische Rückruffunktion zur Abwehr des Zugriffs durch Externe zu nutzen.

7. Zur Beweissicherung einer stattgefundenen Kommunikation sollte die eingesetzte Software folgende Funktionen beinhalten:
   - Zustellungs-/Empfangsnachweise
   - Sende-/Empfangsübergabenachweise

Anlage 2.4

Entschließung der 49. Konferenz am 9./10. März 1995 in Bremen zu

Automatische Erhebung von Straßenbenutzungsgebühren

Gegenwärtig werden Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren in mehreren Versuchsfeldern erprobt. Sie können im Rahmen der weiteren Entwicklung zu zentralen Komponenten umfassender Verkehrstelematiksysteme (z. B. Verkehrsinformation und -leitung) werden.

Mit der Einführung derartiger Verkehrstelematiksysteme besteht die Gefahr, daß personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern, erhoben und verarbeitet werden. Exakte Bewegungsprofile können dadurch erstellt werden. Damit wären technische Voraussetzungen geschaffen, daß Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil das Grundrecht auf freie Entfaltung der Persönlichkeit auch das Recht umfaßt, sich möglichst frei und unbeobachtet zu bewegen. Vor diesem Hintergrund ist es besonders wichtig, elektronische Mautsysteme datenschutzgerecht auszugestalten. Bei den anstehenden Entscheidungen sind andere Verfahren wie z. B. die Vignette einzubeziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, daß der Grundsatz der datenschutzgerechten Ausgestaltung von Systemen zur automatischen Erhebung von Straßenbenutzungsgebühren von allen Beteiligten am Feldversuch auf der BAB A 555 akzeptiert wird. Zur Umsetzung dieses Grundsatzes fordern die Datenschutzbeauftragten:

- Der Grundsatz der „datenfreien Fahrt“ muß auch künftig gewährleistet sein. Über Verkehrsteilnehmer, die ordnungsgemäß bezahlen, dürfen keine Daten erhoben oder verarbeitet werden, die die Herstellung eines Personenbezugs ermöglichen. Es sind ausschließlich solche Zahlungsverfahren anzuwenden, bei denen die Abrechnungsdaten nur dezentral beim Verkehrsteilnehmer gespeichert werden. Die Verkehrsteilnehmer dürfen jedoch nicht gezwungen werden, einen lückenlosen Nachweis über ihre Bewegungen zu führen.
- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Möglichkeit einer flächendeckenden Kontrolle ist von vornherein technisch und rechtlich auszuschließen. Die Gebührenkontrolle ist so zu gestalten, daß die Identität des Verkehrsteilnehmers nur dann aufgedeckt wird, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Gebühren nicht entrichtet worden sind.
- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Verkehrsteilnehmer durchschaubar sein. Der Verkehrsteilnehmer muß jederzeit über sein Guthaben, die Abbuchung und den eventuellen Kontrollvorgang informiert sein.
- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, daß sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

Die hierbei anzuwendenden Verfahren wären gesetzlich abschließend vorzugeben. Dabei ist sicherzustellen, daß anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen. Ferner ist zu gewährleisten, daß Betreiber derartiger Systeme – unabhängig von ihrer Rechtsform – einer Datenschutzkontrolle nach einheitlichen Kriterien unterliegen. Die Bundesregierung wird aufgefordert, bei der anstehenden internationalen Normierung elektronischer Mautsysteme die datenschutzrechtlichen Anforderungen durchzusetzen.

Anlage 2.5

Entschließung der 49. Konferenz am 9./10. März 1995 in Bremen zu

Anforderungen an den Persönlichkeitsschutz im Medienbereich

Die unabhängige und unzensierte Berichterstattung durch Presse, Rundfunk und Film (Art. 5 Abs. 1 Satz 2 GG) dient der freien individuellen und öffentlichen Meinungsbildung. Das Bundesverfassungsgericht hat die freie Meinungsbildung als Voraussetzung sowohl der Persönlichkeitsentfaltung als auch der demokratischen Ordnung bezeichnet. Insofern besteht ein enger Zusammenhang zwischen der Selbstbestimmung des Einzelnen und der Medienfreiheit.

Die rasante Entwicklung der Medientechnik, die Zunahme interaktiver Teledienste und die verstärkte kommerzielle Nutzung von Pressedatenbanken eröffnen einerseits neue Informationsmöglichkeiten für den Bürger, verschärfen aber die Gefährdungen des Rechts auf informationelle Selbstbestimmung. Diesen Gefährdungen muß der Datenschutz auf rechtlicher und technisch-organisatorischer Ebene angemessen begegnen.

– Electronic Publishing und Medienarchive –

Neue Formen der Verbreitung von Informationen über Netze und auf elektronischen Datenträgern führen in bisher unbekanntem Maß zu großen Informationsbeständen, in denen potentiell jedermann gezielt auf personenbezogene Daten zugreifen kann. Zudem öffnen Medienarchive, die bislang ausschließlich für journalistische Zwecke genutzt wurden, riesige Datensammlungen für medienfremde Nutzer. In Persönlichkeitsrechte wird dann besonders tief eingegriffen, wenn auch lange zurückliegende Publikationen praktisch von jedermann recherchiert werden können. Damit droht das in verschiedenen Rechtsbereichen vorgesehene „Recht auf Vergessen“ wirkungslos zu werden, das z. B. durch die Löschungsvorschriften für das Bundeszentralregister gewährleistet werden soll.

Angesichts dieser Entwicklungen muß die Reichweite der datenschutzrechtlichen Sonderstellung der Medien („Medienprivileg“) neu bestimmt werden. Es ist zumindest gesetzlich klarzustellen, daß die geschäftsmäßige Verwendung personenbezogener Daten außerhalb des eigenen Medienbereichs, insbesondere durch kommerzielle Pressedatenbanken, nicht unter das „Medienprivileg“ fällt.

– Interaktive Dienste und Mediennutzungsprofile –

Auch beim Ausbau neuer digitaler Kommunikationsformen (interaktive Dienste wie z. B. Video on Demand) müssen die Persönlichkeitsrechte der Nutzer gewahrt werden. Dabei ist stärker als bisher von vornherein Wert darauf zu legen, daß datenschutzfreundliche Techniken entwickelt werden und zum Einsatz kommen, bei denen personenbezogene Verbindungs- und Nutzungsdaten erst gar nicht entstehen. Von besonderer Bedeutung sind hier anonyme Zahlverfahren, z. B. Prepaid-Karten, auf denen Informationen über die Nutzung ausschließlich dezentral gespeichert werden.

Entsprechend den Bestimmungen im Bildschirmtextstaatsvertrag und in den neueren Mediengesetzen ist sicherzustellen, daß sich die Erhebung und die Aufzeichnung von Verbindungs- und Abrechnungsdaten auf das erforderliche Maß beschränken. Dieser strikte Verarbeitungsrahmen darf auch nicht dadurch ausgeweitet werden, daß die Nutzung eines Dienstes von der Einwilligung in eine zweckfremde Verwendung der Daten abhängig gemacht wird. Die Länder sollten entsprechende einheitliche Regelungen für alle interaktiven Dienste treffen.

Da es sich bei den angesprochenen Diensten um Bestandteile einer entstehenden globalen Informationsinfrastruktur handelt, wird die Bundesregierung aufgefordert, sich auf internationaler Ebene für entsprechende Regelungen einzusetzen.

– Rechte der Betroffenen gegenüber den Medien –

Während die von der Berichterstattung Betroffenen – neben dem für alle Bereiche geltenden Gegendarstellungsrecht – gegenüber den öffentlich-rechtlichen und privaten Rundfunkveranstaltern inzwischen weitere elementare Datenschutzrechte besitzen, gibt es gegenüber der Presse keine vergleichbaren Regelungen.

So kann derjenige, der durch die Berichterstattung der Rundfunkveranstalter in seinem Persönlichkeitsrecht beeinträchtigt wird, in den meisten Fällen nach der Publikation Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Gegenüber der Presse hat er kein entsprechendes Auskunftsrecht. Die meisten Rundfunkveranstalter sind – anders als die Presse – zudem verpflichtet, etwaige Gegendarstellungen zu den gespeicherten Daten zu nehmen, auf die sie sich beziehen (Mitspeicherungspflicht). Ein sachlicher Grund für diese Unterscheidungen ist nicht erkennbar.

Das Presserecht sollte insofern der Rechtslage nach dem Rundfunkrecht (z. B. § 41 Abs. 3 BDSG und Art. 17 Abs. 2 ZDF-Staatsvertrag) angeglichen werden.

Gegenüber Pressedatenbanken, die nicht nur dem eigenen internen Gebrauch dienen, sollte der Betroffene darüber hinaus ein Auskunftsrecht bezüglich des zu seiner Person gespeicherten veröffentlichten Materials haben.

– Öffentlichkeitsarbeit der Behörden –

Personenbezogene Veröffentlichungen von Behörden können das Recht auf informationelle Selbstbestimmung erheblich beeinträchtigen. Das gilt für die Personen, auf die die Aktivitäten der Behörde unmittelbar gerichtet sind, wie auch für andere Verfahrensbeteiligte (wie z. B. Einwender, Opfer von Straftaten, Zeugen) und im besonderen Maße für unbeteiligte Personen aus dem sozialen Umfeld des Betroffenen. Deshalb ist bei der Weitergabe von Daten aus Strafermittlungsverfahren an die Medien besonders zurückhaltend zu verfahren.

Für den Umfang des Anspruchs der Medien auf Weitergabe personenbezogener Daten in Form von Presseerklärungen und Auskünften gibt es keine konkreten gesetzlichen Festlegungen. Die Datenschutzbeauftragten des Bundes und der Länder halten

es daher für geboten, daß der Gesetzgeber Kriterien für die Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und der Freiheit der Berichterstattung durch Rundfunk und Presse deutlicher als bisher festlegt. Dafür kommen die Vorschriften des Landespresserechts, in besonders sensiblen Bereichen aber auch spezialgesetzliche Regelungen wie etwa die Strafprozeßordnung in Betracht.

– Gerichtsfernsehen –

Die Datenschutzbeauftragten des Bundes und der Länder treten den in jüngster Zeit zunehmend erhobenen Forderungen nach einer Aufhebung des Verbots der Hörfunk- und Fernsehberichterstattung aus Gerichtsverhandlungen entgegen. Insbesondere bei Strafprozessen vor laufenden Mikrofonen und Kameras würde es unweigerlich zu einer gravierenden Beeinträchtigung des Persönlichkeitsrechts der Angeklagten, der Opfer, der Zeugen und ihrer Angehörigen kommen. Selbst mit Einwilligung aller Prozeßbeteiligten darf die Hörfunk- und Fernsehberichterstattung nicht zugelassen werden.

Die Gerichtsverhandlung darf nicht zu einem masssenmedial vermittelten „modernen Pranger“ werden.

Anlage 2.6

Entschließung der 49. Konferenz am 9./10. März 1995 in Bremen zum

Sozialgesetzbuch VII

– Verfassungsgemäßer Datenschutz für Unfallversicherte erforderlich –

Durch die Träger der gesetzlichen Unfallversicherung werden oft Daten der Versicherten hinter deren Rücken oder zumindest ohne deren konkrete Kenntnis erhoben und weitergegeben. Der vorliegende Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz – SGB VII sieht dazu keine Änderungen vor.

Aus dem Recht auf informationelle Selbstbestimmung der Versicherten, insbesondere auf Transparenz der einzelnen Verfahrensschritte, ergeben sich mehrere grundlegende Forderungen, die bei einer Überarbeitung des Referentenentwurfes berücksichtigt werden müssen:

1. Auskunftspflicht behandelnder Ärzte gegenüber Unfallversicherungsträgern

   Für behandelnde Ärzte sollte eine gesetzliche Auskunftspflicht gegenüber Unfallversicherungsträgern nur festgelegt werden, soweit dies erforderlich ist für eine sachgerechte und schnelle Heilung (§ 557 Abs. 2 RVO – § 34 Referentenentwurf SGB VII). Die gesetzliche Auskunftspflicht ist daher auf Angaben über die Behandlung und den Zustand des Verletzten zu beschränken. Danach dürfen Vorerkrankungen, die aus Sicht des Arztes mit dem aktuellen Status in keinem Zusammenhang stehen oder keine Bedeutung im Zusammenhang mit dem Arbeitsunfall oder der Berufskrankheit haben, nicht übermittelt werden (Beispiel: Handverletzung und Salmonellenvergiftung).

2. Datenerhebung, -verarbeitung und -nutzung durch Durchgangsärzte und Berufskrankheitenärzte

   Soweit von den Unfallversicherungsträgern bestellte Durchgangsärzte personenbezogene Daten über den Unfallverletzten erheben und Unfallversicherungsträgern und anderen Stellen mitteilen, muß dies auf eine normenklare gesetzliche Grundlage gestellt werden; die bisherige Regelung in dem zwischen den Verbänden der Kassenärzte und der Unfallversicherungsträger geschlossenen „Ärzteabkommen“ reicht für die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen nicht aus. Entsprechendes gilt für die geplante Einführung eines Berufskrankheitenarztes.

3. Mitteilung personenbezogener Patientendaten durch Unfallversicherungsträger an ärztliche Gutachter

   Im Hinblick auf das Recht der Betroffenen, der Bestellung eines bestimmten Gutachters im Einzelfall aus wichtigem Grund – z. B. wegen möglicher Befangenheit – zu widersprechen, haben die Betroffenen ein besonderes berechtigtes Interesse an der Transparenz dieser Datenübermittlungen.

   Gesetzlich festzulegen ist daher, daß dem Betroffenen vor Übermittlung seiner Daten an einen Gutachter der Zweck des Gutachtens und die Person des Gutachters unter Hinweis auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X mitzuteilen sind.

4. Eingriffe der Unfallversicherungsträger und ihrer Verbände in das Recht auf informationelle Selbstbestimmung

   Aufgaben der Unfallversicherungsträger und ihrer Verbände und ihre Befugnisse zur Datenerhebung, -verarbeitung und -nutzung – einschließlich der Aufbewahrungsfristen – sind differenziert in der verfassungsrechtlich gebotenen Klarheit gesetzlich zu regeln. Der vorliegende Referentenentwurf erscheint in diesem Punkt weitgehend unzureichend. So werden undifferenziert Unfallversicherungsträger und ihre Verbände behandelt, die Fachaufgaben dieser Stellen nicht oder nicht hinreichend deutlich genannt und andererseits Selbstverständlichkeiten wie das Führen von Dateien über erforderliche Daten aufgeführt. Außerdem beschränkt sich die Regelung auf die Datenverarbeitung in Dateien und übergeht die gerade im Bereich der Berufsgenossenschaften mit Gutachten und ähnlichen Unterlagen stark ausgeprägte Datenverarbeitung in Akten.

   Die Zuweisung von Aufgaben und Befugnissen an Verbände der gesetzlichen Unfallversicherung muß zudem wie bei allen anderen Verbänden von Leistungsträgern durch die Einrichtung einer staatlichen Aufsicht ergänzt werden. Soweit Vorschriften der Unfallversicherungsträger und ihrer Verbände (z. B. Unfallverhütungsvorschriften) durch Regelungen über die Erhebung, Verarbeitung und Nutzung sensibler medizinischer Daten in das Recht auf informationelle Selbstbestimmung eingreifen, sind diese Eingriffe gesetzlich zu regeln.

5. Anzeige eines Berufsunfalls und einer Berufskrankheit

   Bei Datenschutzkontrollen der bisherigen Anzeigen von Berufsunfällen und -krankheiten hat sich gezeigt, daß der Umfang der an die verschiedenen Stellen übermittelten Daten zum Teil dem Grundsatz der Verhältnismäßigkeit, insbesondere der Erforderlichkeit, nicht Rechnung trägt. Der Inhalt dieser Anzeigen muß an diesen Grundsätzen gemessen neu festgelegt werden.

6. Zentraldateien mehrerer Unfallversicherungsträger oder ihrer Verbände

   Zweck und Inhalt zentral geführter Dateien sind in angemessenem Umfang gesetzlich präzise zu regeln. Dasselbe gilt für die Datenverarbeitung und -nutzung sowie die Festlegung der jeweils speichernden Stelle.

   Die rechtzeitige Beteiligung des jeweils zuständigen Bundes- oder Landesbeauftragten für den Datenschutz vor Einrichtung einer Zentraldatei ist vorzusehen.

7. Anforderung medizinischer Unterlagen bei anderen Sozialleistungsträgern

   Der in § 76 Abs. 2 SGB X vorgesehene Hinweis auf das Widerspruchsrecht gegen die Übermittlung medizinischer Daten geht stets dann ins Leere, wenn bei der speichernden bzw. übermittelnden Stelle kein Verwaltungsverfahren läuft.

   Es ist daher festzulegen, daß ein Unfallversicherungsträger vor der Anforderung von Sozialdaten im Sinne des § 76 SGB X bei anderen Sozialleistungsträgern den Versicherten auf dessen Widerspruchsrecht nach § 76 Abs. 2 SGB X gegenüber der übermittelnden Stelle hinzuweisen hat.

8. Akteneinsichtsrecht der Versicherten

   Hinsichtlich des gesetzlichen Akteneinsichtsrechts nach § 25 SGB X treten in der Praxis seitens der Unfallversicherungsträger Unsicherheiten auf, ob zum Schutz von Betriebs- und Geschäftsgeheimnissen oder Urheberrechten das Einsichtsrecht beschränkt werden muß. Hierzu ist eine gesetzliche Klarstellung geboten, daß diese Rechte dem Akteneinsichtsrecht nicht entgegenstehen.

Anlage 2.7

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zu

Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen

Die gesetzlichen Krankenkassen schließen sich zunehmend zu landesweiten oder überregionalen gesetzlichen Krankenkassen zusammen. Es stellt sich daher verstärkt die Frage, welche bzw. wie viele Geschäftsstellen solcher Krankenkassen umfassend auf alle gespeicherten Daten eines Versicherten zugreifen können.

Die Datenschutzbeauftragten halten nur folgendes für vertretbar:

1. Geschäftsstellen einer Krankenkasse können ohne schriftliches Einverständnis des Versicherten nur auf einen „Stammdatensatz“ zugreifen. Dieser „Stammdatensatz“ darf nur den Namen, das Geburtsdatum, die Anschrift, die Krankenversichertennummer und die betreuende Geschäftsstelle des Versicherten umfassen.
2. Lediglich eine Geschäftsstelle kann umfassend auf den Datensatz eines Versicherten zugreifen, sofern der Versicherte nicht ausdrücklich und eindeutig schriftlich in derartige Zugriffsmöglichkeiten durch weitere Geschäftsstellen eingewilligt hat.
3. Vor der Einwilligung ist der Betroffene umfassend aufzuklären. Die Daten dürfen nur zweckgebunden verwendet werden.

Anlage 2.8

Entschließung der 49. Konferenz am 9./10. März 1995 in Bremen zu

Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z. B. die bislang bekannt gewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder*) erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.

   Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten sind Verkürzungen vorzunehmen.
3. Die derzeit geltende generelle 30jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

   Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte – abweichend von der bisherigen Praxis, nach der es auf die Weglegung der Akte ankommt – regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

   Ergeht keine rechtskraftfähige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.
4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.
5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.
6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.
7. Für die Daten von Nebenbeteiligten (z. B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die voll ständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.
8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

Anlage 2.9

Entschließung der 49. Konferenz am 9./10. März 1995 in Bremen zum

Datenschutz bei Wahlen

Bei der Durchführung von Wahlen haben sich Probleme bei der Verarbeitung personenbezogener Daten ergeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die folgende Entschließung*) gefaßt:

1. Durchführung von Wahlstatistiken

   Diejenigen Wahlberechtigten, in deren Wahlbezirk eine repräsentative Wahlstatistik durchgeführt werden soll, sind bereits mit der Wahlbenachrichtigung hierüber zu informieren. In allgemeiner Form ist auch im Wahllokal ein gut sichtbarer Hinweis auf die Einbeziehung in die Wahlstatistik anzubringen.

   Die Statistik sollte nur in solchen Wahlbezirken durchgeführt werden, in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt. Das Kriterium ist vom Landeswahlleiter vor der Festlegung der Auswahlbezirke zu prüfen. Gegebenenfalls sind ungeeignete Wahlbezirke auszutauschen.

*) Bei Stimmenthaltung von Hamburg

*) Bei Stimmenthaltung von Baden-Württemberg zu Nr. 4

Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse sollte durch den Wahlvorstand erfolgen, während die statistische Auszählung der Stimmzettel durch die jeweils für die Durchführung der Statistik zuständige Stelle vorzunehmen ist.

Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- und personenbezogen zusammengeführt werden, gefährden das Wahlgeheimnis und sind daher unzulässig.

2. Auslegung von Wählerverzeichnissen

Durch die Einsicht in das Wählerverzeichnis besteht nach der jetzigen Rechtslage die Gefahr, daß Daten sowohl von Bürgern, über die in Melderegistern eine Auskunftssperre eingetragen ist, als auch von Bürgern, die in einer speziellen sozialen Situation leben (z. B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Kliniken, Obdachlose), offenbart werden.

Um einerseits die Kontrollmöglichkeit durch die Öffentlichkeit im Vorfeld einer Wahl weiterhin zu gewährleisten, andererseits die datenschutzrechtlichen Belange der genannten Betroffenen zu wahren und dem Mißbrauch einer Adreßrecherche vorzubeugen, fordern die Datenschutzbeauftragten des Bundes und der Länder, daß bei allen Wahlen

- entweder in den öffentlich ausliegenden Wählerverzeichnissen nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgeführt werden
- oder aber bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden, wenn er vorher die Adresse dieser Person aufgegeben hat.

Im übrigen sind Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht zu veröffentlichen.

3. Gewinnung von Wahlhelfern

Bei der Gewinnung von Wahlhelfern sind folgende Grundsätze zu beachten:

Es dürfen nur die zur Bestellung erforderlichen Daten, wie Name, Vorname und Wohnanschrift, erhoben werden. Die Betroffenen sind über den Zweck der Datenerhebung und die weitere Datenverarbeitung umfassend zu unterrichten.

Über die Abwicklung der jeweiligen Wahl hinaus dürfen die Daten der Wahlhelfer in einer Wahlhelferdatei nur gespeichert werden, wenn sie dieser Speicherung nicht widersprochen haben. Die Wahlhelfer sind auf ihr Widerspruchsrecht hinzuweisen.

Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zuläßt. Im Falle der Freiwilligkeit muß es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben. Nach Gründen, die einer Übernahme des Ehrenamtes entgegenstehen, darf erst im förmlichen Verfahren durch die Wahlbehörde gefragt werden.

4. Erteilung von Wahlscheinen

Die in den Wahlordnungen des Bundes und der Länder enthaltene Regelung, nach der die Antragstellung für die Erteilung eines Wahlscheines auf einem Vordruck zu begründen ist und der Grund gegenüber der Gemeinde glaubhaft gemacht werden muß, ist aus datenschutzrechtlicher Sicht unverhältnismäßig. Da sich aus der geforderten Differenzierung der Begründung keine unterschiedlichen Rechtsfolgen ableiten, ist diese entbehrlich. Es genügt in der Antragstellung eine Erklärung des Wahlberechtigten, daß er am Tag der Wahl aus wichtigem Grund das für ihn zuständige Wahllokal nicht aufsuchen kann.

Anlage 2.10

Entschließung der 50. Konferenz am 09./10. November 1995 zu

Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 09./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z. B. Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)
- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z. B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.
- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.
- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

- ob Daten auf einer Chipkarte gespeichert werden,
- welche der Gesundheitsdaten auf die Karte aufgenommen werden,
- welche Daten auf der Karte wieder gelöscht werden,
- ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
- welche Daten im Einzelfall zugänglich gemacht werden.

Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungs-Nr., gespeichert werden, da andernfalls – zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad – die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z. B. durch Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z. B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine Chipkartenvermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte – z. B. mit Hilfe von Schlüsselbegriffen – dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z. B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine „Einwilligung“ in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor „billigen Gesundheitskarten“ ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung, . . ., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten – einschließlich der Sicherungskopien – übertragen oder nicht.

7. Leserecht des Karteninhabers

Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Anlage 2.11

Entschließung der 50. Konferenz am 9./10. November 1995 zur

Weiterentwicklung des Datenschutzes in der Europäischen Union

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 8. September 1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für die Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenommen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehen Instanzen sichergestellt wird.

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10. Februar 1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der u. a. folgende Aussagen enthält: „Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (. . .) wird gewährleistet“.

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28. April 1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild anderer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17. Februar 1993 und 9./10. März 1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie von öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikations-Netze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einen in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

- Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden.
- Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau.
- Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte.
- Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.
- Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entgegengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

Materielle Datenschutzregelungen

Mit der kürzlich verabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

- Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedstaaten einschließlich ihrer Datenschutzkontrolle der Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.
- Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch in unzureichender Form verabschiedet werden.
- Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.
- Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.
- In den Bereichen Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.
- Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes auf hohem Niveau in den Staaten der EU.
- Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z. B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist.

Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26. Mai 1994, 8. September 1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25. August 1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutz-

beauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EU-Organe und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollen die Funktionen des Europäischen Datenschutzbeauftragten und des Bürgerbeauftragten nach den EG-Verträgen nicht vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die Europäische Union institutionell abgesichert wird.

Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EUV derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Verantwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereichen Justiz und Inneres muß daher – unbeschadet der Kontrolle durch die nationalen Datenschutzbehörden – auch eine im Rahmen ihrer jeweiligen Zuständigkeiten lückenlose Kontrolle durch die nationalen Parlamente und Gerichte sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

Anlage 2.12

Entschließung der 50. Konferenz am 9./10. November 1995 zum

Datenschutz bei der Neuordnung der Telekommunikation (Postreform III)

Mit der Postreform III soll die Neugestaltung des Telekommunikationssektors in Deutschland nach den Vorgaben des Liberalisierungskonzepts der Europäischen Union abgeschlossen werden. Entstehen wird ein riesiger Markt mit einer Vielzahl von großen und kleinen, teilweise auch grenzüberschreitend tätigen Netzbetreibern und Diensteanbietern. Die Akteure auf diesem Telekommunikationsmarkt werden zum größeren Teil als Privatunternehmen operieren, es werden aber auch öffentliche Stellen ihre Leistungen anbieten. Der gesetzgeberische Abschluß der Liberalisierung und der Privatisierung des TK-Sektors wird die rechtliche Grundlage bilden für den endgültigen Eintritt in das Zeitalter von weltweiter Vernetzung, Multimedia und interaktiven Diensten und damit für den rapiden Anstieg des Konsums von Angeboten der Telekommunikation, des interaktiven Rundfunks und der Datenverarbeitung.

Die Konsequenzen sind absehbar: Gegenüber der heutigen Situation werden unvergleichlich mehr personenbezogene Daten durch mehr Stellen registriert und ausgewertet werden. Betroffen sind alle, die fernsehen, telefonieren, fernkopieren, Texte und Dokumente über Datenleitung schicken oder Telebanking oder Teleshopping betreiben. Die Risiken für den Einzelnen durch die vermehrten Möglichkeiten der Verhaltens- und Umfeldkontrolle oder der Ausforschung persönlicher Lebensgewohnheiten und Eigenschaften vergrößern sich entsprechend.

Der vom Bundesministerium für Post und Telekommunikation vorgelegte Referentenentwurf für ein Telekommunikationsgesetz (TKG-E, Stand: 6.Oktober 1995) macht es erforderlich, erneut die Realisierung der grundlegenden Rahmenbedingungen für eine datenschutzgerechte Gestaltung der künftigen Telekommunikationslandschaft – soweit die Gesetzgebungskompetenz des Bundes betroffen ist – anzumahnen.

Ein wirksamer Datenschutz muß – wie bereits jetzt gesetzlich fixiert – auch künftig gleichberechtigtes Regulierungsziel neben z. B. der Sicherstellung der flächendeckenden Grundversorgung mit Telekommunikationsdienstleistungen bleiben.

Kundenwünsche nach variablerer und komfortablerer Nutzung der technischen Möglichkeiten werden zunehmen. Gerade deshalb müssen die Prinzipien der Datenvermeidung und der strikten Begrenzung der Datenverarbeitung auf das erforderliche Ausmaß ihren Vorrang bei der Ausgestaltung der kommunikationstechnischen Infrastruktur behalten. Netzbetreiber und Diensteanbieter sollten verpflichtet werden, überall dort, wo dies technisch möglich ist, auch anonyme Zugangs- und Nutzungsformen für ihre Leistungen bereitzustellen. Für eine sichere Datenübertragung sind ohne prohibitive Zusatzkosten wirksame Verschlüsselungsverfahren bereitzustellen.

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis müssen für alle Netzbetreiber und Diensteanbieter ungeachtet ihrer Rechtsform und ihrer Kundenstruktur (z. B. sogenannte Corporate Networks) einheitlich auf einem hohen Niveau gesichert werden. Der bisherige Schutzstandard darf keinesfalls unter den durch die Postreform II erreichten Stand gesenkt werden. Ein hohes Datenschutzniveau ist als Grundversorgung unabdingbar; seine Gewährleistung sollte deshalb Teil der Universaldienstleistung sein. Die in Grundrechte eingreifenden Regelungen sind im Telekommunikationsgesetz selbst und nicht in Verordnungen zu treffen. Die untergesetzlichen, den Datenschutz betreffenden Normen gehören in eine einzige, nicht verstreut in mehrere Verordnungen.

Entscheidend für die Wirksamkeit des Grundrechtsschutzes ist die strikte Einhaltung der Zweckbindung der Verbindungs- und Rechnungsdaten. Das „Feststellen mißbräuchlicher Inanspruchnahme“ oder die „bedarfsgerechte Gestaltung“ von TK-Leistungen dürfen nicht als Anlaß für eine umfassende Auswertung dieser Angaben oder sogar der Nachrichteninhalte herangezogen werden.

Für den Kunden bzw. Teilnehmer ist es von größter Bedeutung, die Verarbeitungsvorgänge im TK-Bereich überschauen zu können. Er muß auch künftig über die Nutzungsrisiken bestimmter Kommunikationstechniken (z. B. Mobilfunk) ebenso wie über seine Widerspruchsmöglichkeiten umfassend aufgeklärt werden. Keinesfalls darf die Einwilligung des Betroffenen mißbraucht werden, um bereichsspezifische Schutznormen oder effiziente Datensicherungsvorkehrungen zu umgehen.

Um auch und gerade für das besonders schutzwürdige Fernmeldegeheimnis einen durchgängig hohen Schutzstandard zu sichern, braucht es eine unabhängige Kontrolle nach bundesweit einheitlichen Kriterien. Die Zuweisung dieser Überwachungsaufgabe an die im TKG-Entwurf vorgesehene Regulierungsbehörde ist wegen deren mangelhafter Unabhängigkeit und der von ihr wahrzunehmenden Regulierungsaufgaben, die mit Interessenkonflikten verbunden sein werden, nicht akzeptabel.

Deshalb sollte aufgrund seiner langjährigen fachlichen Erfahrung bei der Kontrolle der TELEKOM und seiner umfassenden Querschnittskenntnisse im TK-Bereich der Bundesbeauftragte für den Datenschutz eine zentrale Funktion für die Kontrolle im Telekommunikationsbereich erhalten. Die Aufgaben, die die Landesbeauftragten für den Datenschutz und die Aufsichtsbehörden im Rahmen ihrer Zuständigkeiten erfüllen, sind gesetzlich klar zu regeln.

Die Akzeptanz der Informationsgesellschaft der Zukunft hängt wesentlich ab von der Sicherung des Grundrechts auf unbeobachtete Kommunikation. Das Telekommunikationsgesetz wird einen entscheidenden Baustein für die rechtliche Ausgestaltung der künftigen TK-Infrastruktur bilden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher dazu auf, die von ihr vorgeschlagenen Regelungen im weiteren Gesetzgebungsverfahren zu berücksichtigen und sich für ihre Umsetzung auch auf der europäischen Ebene (z. B. in der ISDN-Richtlinie) einzusetzen.

Anlage 2.13

Entschließung der 50. Konferenz am 9./10. November 1995 zu

Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

1. Für die Übermittlung von personenbezogenen Daten durch Justiz und Polizei an die Medien sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

2. Die Übermittlung personenbezogener Daten an die Medien ist nur ausnahmsweise gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

3. Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten/Angeklagten und deren Angehörige sowie die Schwere, die Umstände und die Folgen des Delikts.

   Bei der Übermittlung von personenbezogenen Daten über Beschuldigte/Angeklagte sind auch der Grad des Tatverdachts und der Stand des Verfahrens zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines „überwiegenden Interesses“ der Öffentlichkeit anzulegen.

   Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. Akteneinsicht durch Medienvertreter kommt nicht in Betracht.

4. Grundsätzlich sind in Auskünfte und Erklärungen über das Ermittlungs- und Strafverfahren keine Namen und sonstige personenbezogene Angaben, die Opfer von Straftaten, Zeugen, Beschuldigte und Angeklagte bestimmbar machen, aufzunehmen. Vor allem bei Hinweisen auf den Wohnort, das Alter, den Beruf und die familiären Verhältnisse oder sonstigen sozialen Bindungen (z. B. Partei- oder Vereinsmitgliedschaft) ist zu prüfen, inwieweit dadurch eine Identifizierung des Betroffenen möglich wird.

5. Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

6. Ist die Bekanntgabe der Person des Beschuldigten oder Angeklagten wegen des überwiegenden öffentlichen Interesses gerechtfertigt, muß auch bei der Übermittlung sonstiger personenbezogener Daten abgewogen werden, ob diese Informationen für die Berichterstattung über die Tat selbst oder die Hintergründe, die zu der Tat geführt haben, erforderlich sind, und in welchem Umfang der Betroffene dadurch in seinem Persönlichkeitsrecht beeinträchtigt wird.

7. Die Bekanntgabe von Vorstrafen ist nur ausnahmsweise zulässig. Sie setzt voraus, daß die frühere Verurteilung im Bundeszentralregister noch nicht getilgt und ihre Kenntnis für eine nachvollziehbare Berichterstattung über eine schwerwiegende Straftat – auch unter Berücksichtigung des Persönlichkeitsrechts des Betroffenen und des Resozialisierungsgedankens – erforderlich ist. Besondere Zurückhaltung ist bei Auskünften und Erklärungen über Sachverhalte geboten, die der früheren Verurteilung zugrunde liegen.

8. Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren gegen diesen Personenkreis besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren.

9. Opfer, Zeugen und Familienangehörige haben in der Regel keine Veranlassung gegeben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekannt gemacht werden. Die Übermittlung personenbezogener Daten über diesen Personenkreis an die Medien kommt deshalb grundsätzlich nicht in Betracht.

10. Bildveröffentlichungen greifen wegen der damit verbundenen sozialen Prangerwirkung besonders tief in das Persönlichkeitsrecht des Betroffenen ein. Eine Bildherausgabe kommt daher für Zwecke der Medienberichterstattung nicht in Betracht.

Anlage 2.14

Entschließung der 50. Konferenz am 9./10. November 1995 zu

Planungen für ein Korruptionsbekämpfungsgesetz

Derzeit gibt es Vorschläge, die Bekämpfung der Korruption durch Verschärfungen des Strafrechts und des Strafprozeßrechts mit weiteren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu organisieren. Ein Beispiel dafür ist der Beschluß des Bundesrates vom 3. November 1995 zur Einbringung eines Korruptionsbekämpfungsgesetzes.

Nach dem vom Bundesrat beschlossenen Gesetzentwurf sollen Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden, bei deren Verdacht die Überwachung des Fernmeldeverkehrs und der Einsatz technischer Mittel ohne Wissen des Betroffenen (§§ 100 a, 100 c StPO) angeordnet werden dürfen.

Die Datenschutzbeauftragten weisen demgegenüber darauf hin, daß es vorrangig um Prävention, nicht um Repression geht. Die Datenschutzbeauftragten treten für eine entschlossene und wirksame Bekämpfung der Korruption mit rechtsstaatlichen Mitteln unter strikter Beachtung der Freiheitsrechte ein.

Sie wenden sich zugleich gegen eine Rechtspolitik, welche – noch bevor sie sich darüber im klaren ist, was die bisherigen Verschärfungen und Eingriffe an Vorteilen und an Nachteilen gebracht haben – auf weitere Verschärfungen und Eingriffe setzt.

Gerade gegenüber der Korruption gibt es Möglichkeiten, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger nicht antasten:

- Rotation derjenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, deren Position und Aufgaben erfahrungsgemäß für Bestechungsversuche in Betracht kommen;
- Vier- und Sechsaugenprinzip bei bestimmten Entscheidungen;
- Trennung von Planung, Überwachung und Ausführung, von Ausschreibung und Vergabe;
- Prüfverfahren und Innenrevision;
- Codes of Conduct (formalisierte „Ethikprogramme“) im Bereich der Wirtschaft;
- verbesserte Transparenz von Entscheidungsprozessen in der Verwaltung.

Die in den Gesetzentwürfen vorgesehene weitere Einschränkung von Grundrechten, die mit einer abermaligen Erweiterung der Telefonüberwachung verbunden wäre, ist nur vertretbar, wenn sie nach einer sorgfältigen Güter- und Risikoabwägung zusätzlich zu den o. g. Verfahrens- und Verhaltensmaßregeln als geeignet und unbedingt erforderlich anzusehen wäre.

Die Datenschutzbeauftragten verlangen, daß vor einer zusätzlichen Aufnahme von Straftatbeständen in den Katalog der Abhörvorschrift des § 100 a StPO diese Abwägung durchgeführt wird.

Die Datenschutzbeauftragten fordern weiterhin, daß eine Erweiterung des genannten Straftatenkataloges nur befristet vorgenommen wird, damit sich vor einer Verlängerung die Notwendigkeit stellt, auf der Grundlage einer sorgfältigen Erfolgs- und Effektivitätskontrolle erneut die Erforderlichkeit und Verhältnismäßigkeit einer solchen Erweiterung des Grundrechtseingriffs zu überprüfen.

Die Datenschutzbeauftragten verlangen, daß der Gesetzgeber vor weiteren Eingriffen in Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Schließlich gibt die anstehende erneute Erweiterung des Katalogs von § 100 a StPO Veranlassung, den Umfang der darin genannten Straftaten sobald wie möglich grundlegend zu überprüfen.

Anlage 2.15

Entschließung der 50. Konferenz am 9./10. November 1995 zum

Entwurf einer Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) des Bundesministeriums für Post und Telekommunikation (Stand: 6. Juni 1995)

Das Bundesministerium für Post und Telekommunikation hat den Entwurf einer Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) vorgelegt, der auf der Grundlage des bereits seit Anfang dieses Jahres geltenden Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG) den Schutz personenbezogener Daten der am Fernmeldeverkehr beteiligten Bürger regeln soll. Die Verordnung muß entsprechend der gesetzlichen Vorgabe dem Grundsatz der Verhältnismäßigkeit genügen, insbesondere hat sie die Erhebung, Verarbeitung und Nutzung der Daten auf das Erforderliche zu beschränken und ihre Zweckbindung zu gewährleisten. Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, daß der vorliegende Entwurf diesen aus der Verfassung abgeleiteten gesetzlichen Vorgaben teilweise nicht genügt.

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung vom 8. März 1991 auf die Bedeutung des Grundrechts auf unbeobachtete Kommunikation hingewiesen und gefordert, daß das Telekommunikationsdatenschutzrecht dieses Grundrecht zu sichern hat. Im Zeitalter der elektronischen Information und Kommunikation ist es geboten, die Betreiber zur Bereitstellung anonymer Nutzungsmöglichkeiten zu verpflichten und den Bürger in die Lage zu versetzen, selbst zu entscheiden, ob er seine personenbezogenen Daten preisgeben und sich den damit verbundenen Risiken aussetzen will.

Im einzelnen halten die Datenschutzbeauftragten den vorliegenden Entwurf in folgenden Punkten für verbesserungsbedürftig, auch um eine Absenkung des Datenschutzniveaus gegenüber der gegenwärtigen Rechtslage zu verhindern:

- Die Verarbeitung von Kundendaten muß auch in Zukunft ausdrücklich auf Telekommunikationszwecke und Zwecke der Informationsdienstleistung beschränkt werden; jede Aufweichung des Zweckbindungsgrundsatzes ist abzulehnen.
- Auch im Bereich des Sprachtelefondienstes soll nach dem Entwurf die Speicherung der vollständigen Rufnummer des angerufenen Teilnehmers bis zu 80 Tagen nach Rechnungsversand zur Regel werden. Bislang war dies nur vorgesehen, wenn der Anrufer einen Einzelverbindungsnachweis beantragt hat; dabei sollte es auch in Zukunft bleiben.
- Eine Auswertung der Verbindungsdaten nach Zielrufnummern auch außerhalb des Sprachtelefondienstes ohne Einwilligung des Kunden ist nach § 10 Abs. 2 Nr. 2 PTRegG unzulässig. Hiernach „dürfen Daten des Anrufenden nur mit dessen Einwilligung verwendet und müssen Daten des Angerufenen unverzüglich anonymisiert werden“.
- Die Übermittlung von Verbindungsdaten an Diensteanbieter darf auch für Zwecke des Entgelteinzuges weiterhin nur mit Einwilligung des Kunden zugelassen werden, wenn der Datenempfänger sich vertraglich zur Einhaltung des Fernmeldegeheimnisses verpflichtet hat.
- Ein Einzelverbindungsnachweis sollte auch in Zukunft nur erteilt werden, wenn der Antragsteller das Einverständnis der zum Haushalt gehörenden Mitbenutzer des Anschlusses nachweisen kann.
- Die Anonymität von Anrufern bei Beratungseinrichtungen muß auch dann gewährleistet sein, wenn sie über ein Mobilfunknetz anrufen. Es ist nicht nachzuvollziehen, daß gerade an den dynamischsten und modernsten Teilbereich der Telekommunikation geringere Datenschutzanforderungen gestellt werden sollen als an das traditionelle Festnetz. Ohnehin ist eine Entwicklung absehbar, die Mobilfunk- und Festnetze zusammenwachsen läßt.
- Der Anrufer muß im Sprachtelefondienst die kostenfreie Möglichkeit haben, die Übermittlung seiner Rufnummer an den angerufenen Anschluß dauernd oder fallweise auszuschließen.
- Beim angerufenen Anschluß im Sprachtelefondienst muß auch in Zukunft die Abschaltung der Rufnummernanzeige allgemein und im Einzelfall möglich sein, damit Personen, die sich in räumlicher Nähe zum Angerufenen aufhalten, nicht zwangsläufig Kenntnis vom jeweiligen Anrufer erhalten.
- Die regelmäßige Herausfilterung der Daten solcher Verbindungen, für die tatsächliche Anhaltspunkte den Verdacht eines strafbaren Mißbrauchs von Fernmeldeanlagen oder der mißbräuchlichen Inanspruchnahme von Telekommunikations- oder Informationsdienstleistungen begründen, kommt einer präventiven Rasterfahndung der dem Fernmeldegeheimnis unterliegenden Verbindungsdaten gleich, in die bereits im Vorfeld eines konkreten Verdachts sämtliche Teilnehmer einbezogen werden. Die entsprechende Regelung sollte dieses Verfahren lediglich auf den Einzelfall beschränken.
- Hinsichtlich der Erhebung, Verarbeitung und Nutzung von Nachrichteninhalten sind die strengen Vorgaben von § 10 Abs. 2 Sätze 2 – 5 PTRegG einzuhalten. Insoweit fehlt in dem vorliegenden Entwurf eine Einschränkung auf den Einzelfall und die Verankerung der nach § 10 PTRegG vorgesehenen Informations- und Unterrichtungspflichten.
- Die geplante Umwandlung der bisherigen Telefonauskunft ist datenschutzrechtlich nur vertretbar, wenn der Kunde über die Verwendungsmöglichkeit in der Telefonauskunft und sein Widerspruchsrecht hinreichend informiert wird. So muß er insbesondere wissen, daß nicht nur seine Rufnummern, sondern sämtliche Angaben, die er für die Teilnehmerverzeichnisse freigegeben hat, auch beauskunftet und verwendet werden können, sofern er dem nicht widersprochen hat.
- Die vorgesehenen Regelungen über öffentliche Kundenverzeichnisse und die Telefonauskunft tragen den besonderen Risiken der Verbreitung von Kundendaten in elektronischer Form, etwa auf CD-ROM oder durch Abruf aus Online-Diensten (Adreß-Selektion, bundesweite Recherche, umgekehrte Rufnummernsuche) nicht Rechnung. Der Kunde muß ein differenziertes Widerspruchsrecht erhalten, das ihm ermöglicht, seine Daten zwar in das herkömmliche Telefonbuch aufnehmen oder von der Telefonauskunft mitteilen zu lassen, eine Aufnahme in elektronische Verzeichnisse mit qualitativ weitergehenden Verarbeitungsmöglichkeiten jedoch zu unterbinden.

- Der Verordnungsentwurf läßt abweichend von der gegenwärtigen Praxis bei der Deutschen Telekom AG die Erstellung von Einzelverbindungsnachweisen mit vollständigen Zielrufnummern ohne Einflußmöglichkeit der angerufenen Kunden zu. Die Anonymität des Angerufenen wird aber auch durch die Verkürzung der Zielrufnummer um die letzten drei Ziffern nicht hinreichend gewährleistet. Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung vom 9./10. März 1994 darauf hingewiesen, daß dem Schutz des informationellen Selbstbestimmungsrechts und des Fernmeldegeheimnisses des Angerufenen am besten dadurch entsprochen würde, wenn jeder inländische Anschlußinhaber selbst entscheiden könnte, ob und gegebenenfalls wie seine Rufnummer auf Einzelverbindungsnachweisen erscheinen soll. Obwohl ein entsprechendes Verfahren in den Niederlanden bereits erfolgreich praktiziert wird, hat der Bundesminister für Post und Telekommunikation diesen Vorschlag bisher nicht aufgegriffen.
- Die Vorschriften für Bildschirmtextdienste sollten, auch im Sinne der Rechtssicherheit, möglichst weitgehend mit denen des Bildschirmtext-Staatsvertrages harmonisiert werden. Insbesondere sollte die Speicherung von Abrechnungsdaten so beschränkt werden, daß Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von den einzelnen Kunden in Anspruch genommener Angebote nicht erkennbar sind, es sei denn, der Kunde beantragt mit Einverständnis der Mitbenutzer einen Einzelverbindungsnachweis. Ferner ist vorzusehen, daß Abrechnungsdaten nicht erst sechs Monate nach Bekanntgabe der Entgeltrechnung gelöscht werden, sondern unverzüglich, wenn sie für Abrechnungszwecke nicht mehr erforderlich sind.

3. Gemeinsame Erklärungen und Stellungnahmen der Europäischen Konferenz der Datenschutzbeauftragten

Anlage 3.1

Erklärung der Europäischen Konferenz der Datenschutzbeauftragten vom 15. März 1995 zum

Grünbuch über die Liberalisierung der Telekommunikationsinfrastruktur und der Kabelfernsehnetze
Teil I KOM (94) 440 endg.
Teil II KOM (94) 682 endg.

(Übersetzung)

Die Liberalisierung der Telekommunikationsinfrastruktur und der Kabelfernsehnetze in der Europäischen Union wird weitreichende Auswirkungen für den Datenschutz der Unionsbürger haben. Die Europäischen Datenschutzbeauftragten stimmen daher der klaren Aussage der Kommission in dem Grünbuch zu, daß gemeinsame Regelungen des Datenschutzes für die Entwicklung der Informationsgesellschaft grundlegend sind. Ein effektiver Schutz personenbezogener Daten von Telekommunikations- und Medienbenutzern wird nicht automatisch aus einem Wettbewerb im Bereich der Infrastrukturen und Dienste entstehen. Datenschutz kann nicht allein den Kräften des Marktes überlassen werden.

Daher sind spezifische Regelungen zum Datenschutz in einem liberalisierten und wettbewerbsorientierten Telekommunikationsumfeld notwendig. Die Vorschläge der Kommission für eine ISDN-Richtlinie und für eine Richtlinie über den offenen Netzzugang beim Sprachtelefondienst sollten beschleunigt und ihr Inhalt harmonisiert werden. Sie sollten vom Rat und dem Europäischen Parlament gleichzeitig beraten und verabschiedet werden unter Berücksichtigung der Erklärung der Europäischen Datenschutzbeauftragten vom 23. Dezember 1994 über den geänderten Vorschlag für eine ISDN-Richtlinie.

Die Europäischen Datenschutzbeauftragten begrüßen den Plan der Kommission, die gesellschaftlichen und sozialen Auswirkungen der Verbreitung neuer Technologien und eines wettbewerbsorientierten Umfeldes für die Kommunikationsinfrastruktur zu untersuchen. Die Kommission betont zu Recht die Notwendigkeit, die Entwicklung einer in „Informationsbesitzer“ und „Informationshabenichtse“ zu verhindern. Dies schließt die Notwendigkeit ein, jeden Teilnehmer über die Datenschutzrisiken bei der Benutzung von Telekommunikationsinfrastrukturen oder -diensten zu informieren.

Darüber hinaus muß eine zweigeteilte Informationsgesellschaft auch in einem anderen Sinne verhindert werden: Es sollte keinen Unterschied geben zwischen denen, die sich Datenschutz und Datensicherheit leisten können, und denen, die dies nicht können.

Das Konzept eines Universaldienstes sollte daher einen hohen Datenschutzstandard als Teil eines Minimalangebots von bestimmter Qualität haben. Insbesondere sollte das Angebot eines anonymen Netzzugangs durch Benutzung von Guthabenkarten und anderen Einrichtungen, die keine identifizierbaren elektronischen Spuren im Netz hinterlassen, obligatorisch sein. Die Datenschutzbeauftragten betonen die Wichtigkeit des weiteren Angebots von öffentlichen Telefonen unter der Voraussetzung, daß derartige Einrichtungen auch dort angeboten werden. Die Möglichkeit des anonymen Zugangs zu Netzen und Diensten wird sogar noch wichtiger im Hinblick auf das schnelle Zusammenwachsen von Telekommunikation und Rundfunk. In dem Ausmaß, in dem die Massenkommunikation mehr und mehr individualisiert wird (z. B. bei video on demand), steigt auch die Bedrohung für den Datenschutz. Ohne anonyme Zugangs- und Zahlungsverfahren werden sensible Profile über das Benutzerverhalten automatisch generiert werden. Der Teilnehmer sollte bei der Benutzung von Netzen oder Diensten die technische Möglichkeit haben, dies zu verhindern.

In bezug auf die Rufnummernvergabe weisen die Europäischen Datenschutzbeauftragten auf ihre Erklärung zum Grünbuch über ein gemeinsames Konzept für Mobilkommunikation und personal communications in der Europäischen Union (KOM [94] 145 endg.) hin. Bei der Anhörung zum Grünbuch über die Liberalisierung der Telekommunikationsinfrastruktur am 20./21. Februar 1995 wurde das Konzept des Eigentums an den Telefonnummern – das im Grünbuch selbst nicht erwähnt wird – kurz diskutiert. Die Europäischen Datenschutzbeauftragten bitten um weitere Präzisierung dieses Konzepts. Es könnte den Datenschutz für den Einzelnen verbessern, falls es so verstanden würde, daß es ein Recht beinhaltet, die eigene Telefonnummer geheimzuhalten, der Aufnahme in Teilnehmerverzeichnisse ohne zusätzliche Kosten zu widersprechen und den Verkauf von Telefonnummern und anderen personenbezogenen Daten für Marketing-Zwecke zu verhindern.

Zahlreiche Maßnahmen der Europäischen Union (z. B. die Richtlinie des Rates vom 29. April 1991 zur Angleichung der Rechtsvorschriften der Mitgliedsstaaten über Telekommunikationsendeinrichtungen einschließlich der gegenseitigen Anerkennung ihrer Konformität (91/263/EWG) führen zu einer Harmonisierung durch die Erteilung von Typengenehmigungen, die spezifische technische Einrichtungen zur Gewährleistung des Datenschutzes nicht zulassen. Die Europäischen Datenschutzbeauftragten halten es daher für notwendig, kompensatorische Regelungen zu schaffen, die die Genehmigung technischer Datenschutzeinrichtungen in den Mitgliedsstaaten ermöglichen. Es sollte klargestellt werden, daß die Lizensierungsbedingungen für eine Kommunikationsinfrastruktur einen hohen Standard für Datenschutz und Datensicherheit ebenso sicherstellen müssen, wie dies für einen hohen Standard beim Verbraucherschutz der Fall ist (vgl. S. 122 des Grünbuchs).

Die Europäischen Datenschutzbeauftragten begrüßen die Erklärung der Kommission in ihrer Mitteilung vom 23. November 1994 über den Konsultationsprozeß bezüglich des Grünbuchs über eine gemeinsames Konzept für Mobilkommunikation und Personal Communications (KOM [94] 492), daß ein Bericht über die Notwendigkeit zusätzlicher Maßnahmen zum Datenschutz noch vor dem 1. Januar 1996 erstellt werden wird. Dieser Bericht sollte nicht auf die Mobilkommunikation beschränkt werden, sondern auch die Liberalisierung der Telekommunikationsinfrastruktur und der Kabelfernsehnetze umfassen. Die Datenschutzbeauftragten sind bereit, zu dem Bericht im Rahmen von formellen oder informellen Beratungen beizutragen.

Anlage 3.2

Stellungnahme der Europäischen Konferenz der Datenschutzbeauftragten am 6./7. April 1995 in Lissabon zum Entwurf einer Europäischen Datenschutzrichtlinie

(Übersetzung)

1. Die EU-Datenschutzbeauftragten, die am 6. und 7. April 1995 in Lissabon zusammenkamen, gingen auf die ausführliche Arbeit und Beratungen zum Entwurf der Allgemeinen Datenschutzrichtlinie ein. Sie sind fest davon überzeugt, daß der gemeinsame Standpunkt des Ministerrates den besten Weg nach vorne darstellt; er stellt einen angemessenen Rahmen dar, innerhalb dessen die Mitgliedstaaten ihre innerstaatliche Gesetzgebung weiterentwickeln können.

2. Im September 1990 veröffentliche die Europäische Kommission ein Paket von Vorschlägen zum Datenschutz. Der Hauptbestandteil des Paketes bestand im Entwurf der Allgemeinen Richtlinie, die darauf abzielt, die verschiedenen Datenschutzgesetze in der Union für die Zwecke des Binnenmarktes gemäß Artikel 100 A. des Römischen Vertrages auf hoher Ebene anzugleichen. Das Europäische Parlament prüfte den Entwurf und nahm dazu Stellung. Im Anschluß daran veröffentlichte die Europäische Kommission im Oktober 1992 einen überarbeiteten Richtlinienentwurf. Am 20. Februar 1995 nahm der Ministerrat formell den gemeinsamen Standpunkt zur Richtlinie an, der nun im Rahmen des gemeinsamen Entscheidungsverfahrens an das Europäische Parlament verwiesen wurde.

3. Die Datenschutzbeauftragten erinnerten daran, daß sie die Entwicklung der Richtlinie seit 1990 aktiv verfolgt haben. Auf ihren Sitzungen in Dublin, Boppard und Paris prüften sie den Richtlinienentwurf und schlugen daraufhin Textänderungen vor. Im Anschluß daran nahmen sie zur Frage des geltenden Rechtes Stellung. Die Datenschutzbeauftragten nahmen mit Befriedigung zur Kenntnis, daß der Ministerrat und die Europäische Kommission positiv auf ihre Vorschläge reagierten.

4. Die Datenschutzbeauftragten nehmen die Weiterentwicklung des Textes mit Freude zur Kenntnis. In die Richtlinie ist viel Flexibilität eingeflossen, so daß die Mitgliedstaaten sie auf eine Art und Weise in das innerstaatliche Recht übertragen können, die mit staatlichen, rechtlichen und verfassungsrechtlichen Bedingungen in Einklang steht.

   Der Spielraum und das Ermessen, das die Richtlinie den Mitgliedstaaten einräumt, kann so eingesetzt werden, daß die neuen innerstaatlichen Gesetze den Menschen einen wertvollen Schutz bieten und die Organisationen dazu ermuntern, die besten Praktiken im Umgang mit Informationen zu verwenden, ohne ihnen jedoch unangemessene Kosten aufzubürden. Daher geben die Datenschutzbeauftragten ihrer vollen Unterstützung des gemeinsamen Standpunktes Ausdruck.

5. Die Datenschutzbeauftragten möchten den Wert der Richtlinie betonen. Sie rückt die Mitgliedstaaten in diesem wichtigen Punkt näher aneinander; sie stellt eine Grundlage für die nächste Generation von Datenschutzgesetzen in der Europäischen Union dar. Nach Ansicht der Datenschutzbeauftragten gibt es keine offenstehenden und noch zu klärenden Grundsatzfragen und sie würden daher jegliche Änderung der Richtlinie in höchstem Maße bedauern, wenn diese das Niveau des Schutzes, das den Menschen gewährt wird, gefährden würde.

Anlage 3.3

Stellungnahme der Europäischen Konferenz der Datenschutzbeauftragten am 6./7. April 1995 in Lissabon zur Telekommunikation und zur Informationsgesellschaft

(Übersetzung)

Die Konferenz der Datenschutzbeauftragten der Europäischen Union, die am 6. und 7. April 1995 in Lissabon tagte, begrüßte die Tatsache, daß die Europäische Kommission offiziell den Geänderten Vorschlag für eine ISDN-Richtlinie (COM [94] 128 final – COD 288) vorgestellt hat und daß die französische Präsidentschaft diese auf die Tagesordnung des Rates gesetzt hat.

Gleichzeitig sind die Datenschutzbeauftragten darüber besorgt, daß die Ratsarbeitsgruppe für den Vorschlag verantwortlich ist.

Die Entscheidung der Arbeitsgruppe, die Beratungen des Geänderten Vorschlages so lange zu vertagen, bis die Europäische Datenschutzrichtlinie endgültig angenommen worden ist, zeigt, daß die Kommission und die Arbeitsgruppe sich der Tatsache bewußt sind, daß der Datenschutz das Hauptziel dieses spezifischen Vorschlages ist. Dennoch sind die Datenschutzbeauftragten der Europäischen Union der Ansicht, daß der ISDN-Entwurf im Hinblick auf ihre ausführlichen Stellungnahmen vom 23. Dezember 1994 rasch weiterentwickelt werden sollte. Das ist erforderlich, um die notwendige Harmonisierung und Synchronisierung der Maßnahmen der Europäischen Union in diesem Bereich zu erreichen, die die Datenschutzbeauftragten auf ihrer Konferenz in Madrid 1994 forderten.

In Anbetracht der bevorstehenden Annäherung des Fernmelde- und Rundfunkwesens (Multimedia-Anwendungen) in der entstehenden Europäischen Informationsgesellschaft betonen die Datenschutzbeauftragten, daß sie sich für die Anhebung des Datenschutzniveaus in diesem Bereich einsetzen. Ein hohes Datenschutzniveau und die Wahlfreiheit des Einzelnen sind Vorbedingungen für die öffentliche Akzeptanz, ohne die die Informationsgesellschaft nicht Realität werden wird.

Anlage 3.4

Stellungnahme der Europäischen Konferenz der Datenschutzbeauftragten am 6./7. April 1995 in Lissabon zur weiteren Arbeit dieses Gremiums

Die Mitglieder der Konferenz stimmen darin überein, daß eine Änderung der Organisation der Konferenz erforderlich ist, um eine dauerhafte und sichtbare Präsenz innerhalb Europas zu schaffen.

Dies wird erforderlich sein, da es in der Zukunft in steigendem Maße dringende, schwierige und wichtige Angelegenheiten zu bewältigen geben wird.

Dies wird erforderlich sein, auch wenn gemäß Artikel 29 der EG-Richtlinie erwartungsgemäß eine Arbeitsgruppe eingerichtet wird. Der Schwerpunktbereich dieser Gruppe wäre nicht weit genug gefaßt, um sich mit der Bandbreite der Angelegenheiten zu befassen, mit denen wir konfrontiert werden.

Um dieser Konferenz eine dauerhaftere Grundlage zu schaffen, wird die Unterstützung durch ein Sekretariat erforderlich sein. Zum gegenwärtigen Zeitpunkt ist es nicht gegeben, ein getrenntes Sekretariat einzurichten.

Stattdessen wird vorgeschlagen, daß die Mitglieder turnusgemäß diese Funktion für jeweils ein Jahr ausüben. Das Land, das die Frühjahrskonferenz ausrichtet, übernimmt diese Zuständigkeit bis zum Zeitpunkt der nächsten Frühjahrskonferenz. Es erhält die Unterstützung der Vorsitzenden aller Arbeitsgruppen, die von der Konferenz eingerichtet werden.

Die Konferenz wird eine ständige Adresse haben, von der aus die Post an die zuständigen Mitgliedsländer weitergeleitet wird.

Dies wird von der niederländischen Delegation organisiert werden.

Anlage 3.5

Kopenhagener Resolution der Konferenz der Datenschutzbeauftragten der Europäischen Union vom 8. September 1995

(1) Der Vertrag über die Europäische Union nimmt an zwei Stellen (Art. F Abs. 2 und Art. K.2 Abs. 1) ausdrücklich auf die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten Bezug und garantiert darin die Achtung der in der Konvention festgeschriebenen Grundrechte. Damit ist auch Art. 8 der EMRK – Gebot der Achtung der privaten Sphäre – von der Garantie des Unionsvertrages mitumfaßt.

Die Konferenz nimmt die für 1996 geplante Regierungskonferenz zum Anlaß, im Hinblick auf den europäischen Grundrechtsschutz im allgemeinen und auf das Recht des einzelnen auf Datenschutz im besonderen eine weitergehende Änderung bzw. Ergänzung der Unions- und Gemeinschaftsverträge zu fordern. Sie unterstützt dabei die Bestrebungen zur Schaffung eines verbindlichen europäischen Grundrechtskatalogs und plädiert darüber hinaus für die Aufnahme eines europäischen Grundrechts auf Datenschutz in diesen Katalog, wodurch die Unionsorgane wie die nationalen Stellen gebunden werden und der Datenschutz den Bürgern in einklagbarer Form gewährt wird.

(2) Gemeinschaftsrechtliche Regelungen verpflichten die Mitgliedstaaten in immer größerem Maße zur Erhebung und Verarbeitung personenbezogener Daten, und gleichzeitig führen die europäischen Einrichtungen selbst zunehmend personenbezogene Datenbanken. Diese Einrichtungen sind jedoch nicht an die Grundsätze des Datenschutzes gebunden, insbesondere unterliegen sie keinem Datenschutzgesetz. Da der Datenschutz aber nicht mehr länger aus dem Wirken der Gemeinschafts- und Unionsorgane ausgeklammert bleiben kann, mahnt die Konferenz die Schaffung gemeinschaftsbezogener Datenschutzregelungen an.

Zwar war in dem von der Europäischen Kommission am 13. September 1990 vorgelegten Datenschutzpaket eine „Erklärung der Kommission betreffend die Anwendung der Grundsätze der Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten auf die Organe und Einrichtungen der EG“ enthalten, die auf die Anwendung der Datenschutzrichtlinie auf EG-Institutionen abzielte. Dieses Vorhaben muß weiterverfolgt werden. Die am 24. Juli 1995 verabschiedete Datenschutzrichtlinie richtet sich nur an die nationalen Gesetzgeber als Adressaten.

(3) Um künftig sicherzustellen, daß den vielfältigen und umfangreichen Aktivitäten der Gemeinschaft die rechtzeitige und systematische Prüfung der datenschutzrechtlichen Auswirkungen zuteil wird, fordert die Konferenz für die Gewährleistung des Datenschutzes durch Gemeinschaftsorgane und -einrichtungen die Schaffung rechtsverbindlicher Regelungen. Sie erinnert in diesem Zusammenhang an die Zusatzerklärung der Datenschutzbeauftragten der EG-Länder zur Berliner Resolution der Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989 und ihren Vorschlag, wonach die Grundsätze der Europaratskonvention 108 durch entsprechende Rechtsakte der Europäischen Gemeinschaft für alle Mitgliedstaaten ebenso wie für die Institutionen der EG selbst verbindlich gemacht werden sollten.

(4) Während die Datenschutzregelungen der Mitgliedstaaten unabhängige Kontrollinstanzen zur Sicherung der gesetzlichen Rechte des Betroffenen vorsehen, fehlt es nach wie vor an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Organe oder Einrichtungen der Gemeinschaft in seinen Rechten verletzt zu sein. Die Konferenz verweist auch in diesem Zusammenhang auf die Zusatzerklärung der Datenschutzbeauftragten der EG-Länder zur Berliner Resolution aus dem Jahre 1989 und ihren Vorschlag betreffend die Einrichtung einer unabhängigen Datenschutzkontrollinstanz. Diese sollte nicht nur Eingaben von Betroffenen entgegennehmen, sondern auch die Verarbeitung personenbezogener Daten innerhalb der Gemeinschaftsorgane und -einrichtungen – nicht nur anlaßbezogen – kontrollieren, die Organe und Einrichtungen der Gemeinschaft in allen Datenschutzfragen beraten sowie mit den nationalen Datenschutzorganen zusammenarbeiten.

Es ist daher notwendig und dringend geboten, in den Unions- und Gemeinschaftsverträgen die Schaffung einer unabhängigen Kontrollinstanz für die Verarbeitung personenbezogener Daten durch Gemeinschaftsorgane und -einrichtungen vorzusehen. Die Mitgliedstaaten sollten einen derartigen Vorschlag unterbreiten und einem geeigneten Text im Rahmen der Internationalen Konferenz zur Überprüfung der Verträge in 1996 zustimmen.

Anlage 3.6

Stellungnahme der Europäischen Konferenz der Datenschutzbeauftragten vom 24. November 1995 zum

Bericht der Europäischen Kommission (DG XIII) über den Universaldienst im wettbewerbsorientierten Telekommunikationsbereich

(Übersetzung)

Das Konzept eines universellen Dienstes im wettbewerbsorientierten Telekommunikationsbereich wird für die sich entwikkelnde Europäische Informationsgesellschaft von großer Bedeutung sein. Die bisherige Diskussion über den Umfang einer zukünftigen Universaldienst-Verpflichtung (vgl. Themenkreis 1 des Themenpapiers der Komission vom 19. September 1995) konzentrierte sich bisher auf die Frage, ob diese auf den einfachen Sprachtelefondienst beschränkt oder auf zusätzliche Merkmale wie Rufnummernanzeige beim Angerufenen, Einzelverbindungsnachweise, Voice-Mail oder sogar den Zugang zum Internet erweitert werden sollte.

Unabhängig vom Ergebnis dieser Debatte sind die Europäischen Datenschutzbeauftragten der Ansicht, daß jegliche Universaldienstverpflichtung einen hohen Datenschutzstandard für die jeweiligen Dienste und Merkmale, die universell angeboten werden sollen, enthalten sollte. Um ein Beispiel zu geben: Entsprechend dem Entwurf der ONP-Sprachtelefondienst-Richtlinie (KOM [94] 689) wird die Rufnummernanzeige beim Angerufenen Teil der Universaldienstverpflichtung sein. Dieses Leistungsmerkmal sollte für den Anrufer die Möglichkeit enthalten, die Übermittlung seiner Rufnummer von Fall zu Fall als Teil der Universaldienstverpflichtung auszuschließen. Ein weiteres Beispiel bildet das zukünftige Angebot eines universellen Teilnehmerverzeichnisses in der Europäischen Union.

Das Datenschutzniveau für den einzelnen Benutzer sollte innerhalb des Geltungsbereichs des Universaldienstes nicht niedriger sein als außerhalb dieses Bereichs. Datenschutz muß bezahlbar bleiben in dem Sinne, daß die Benutzung von Datenschutz-Optionen nicht mit höheren Kosten verbunden sein darf.

Der Zugang zu Netzen und insbesondere der „öffentliche Zugang“ (vgl. Themenkreis 3 des Themenpapiers des Komission) sollte wenigstens als Option auf einer anonymen Basis möglich sein. Dies gilt ebenso für Abrechnungsverfahren. Jede zukünftige Universaldienstverpflichtung sollte das Angebot von Guthabenkarten und anderen Mitteln, die keine identifizierbaren elektronischen Spuren im Netz hinterlassen, umfassen. Die Europäischen Datenschutzbeauftragten weisen auf ihre Erklärung vom 15. März 1995 zum Grünbuch über die Liberalisierung der Telekomunikationsinfrastruktur und der Kabelfernsehnetze hin, in der sie die Notwendigkeit der Schaffung von technischen Möglichkeiten zur Vermeidung sensibler Benutzerprofile in der Informationsgesellschaft betont haben.

Anlage 3.7

Zweite Gemeinsame Erklärung der Europäischen Konferenz der Datenschutzbeauftragten vom 22. Dezember 1995 zum geänderten Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen vom 13. Juni 1994 (KOM [94] 128 endg.-COD 288)

A. Grundsätzliche Anmerkungen

Es ist zu begrüßen, daß nach der endgültigen Annahme der allgemeinen Datenschutzrichtlinie durch den Europäischen Rat am 24. Juli 1995 die Diskussion des geänderten Entwurfs für eine ISDN-Richtlinie im Rat wieder in Gang gekommen ist. Angesichts der Tatsache, daß die Liberalisierung der Telekommunikationsmärkte höchste politische Priorität hat und entsprechende Regulierungsmaßnahmen, wie die Sprachtelefondienst-Richtlinie, kurz vor der endgültigen Verabschiedung stehen, ohne die notwendigen spezifischen Datenschutzregelungen für diesen Bereich zu enthalten, erscheint es besonders dringlich, daß der Vorschlag für eine ISDN-Richtlinie verabschiedet und der neuen liberalisierten Umgebung angepaßt wird.

Die Europäischen Datenschutzbeauftragten haben dies in ihrer Erklärung von Lissabon am 6./7. April 1995 betont, wobei sie sich auf ihre detaillierte Gemeinsame Erklärung zum geänderten Entwurf einer ISDN-Richtlinie vom 23. Dezember 1994 (vgl. Jahresbericht 1994, Anlage 3.4) bezogen haben.

Obwohl im zweiten Halbjahr 1995 die Diskussionen in der Ratsarbeitsgruppe „Telekommunikation“ beschleunigt wurden, ist es bedauerlich, daß diese detaillierten Anmerkungen der Europäischen Datenschutzbeauftragten bisher nicht berücksichtigt wurden. Die Datenschutzbeauftragten haben deshalb ihre Erörterung des ISDN-Richtlinienentwurfs im Lichte der Diskussionen in der Ratsarbeitsgruppe fortgesetzt und dabei auch die Empfehlung Nr. R (95) 4 des Europarats zum Schutz personenbezogener Daten im Bereich der Telekommunikationsdienste mit besonderer Berücksichtigung des Telefondienstes (beschlossen vom Ministerausschuß am 7. Februar 1995) berücksichtigt.

Die Datenschutzbeauftragten messen den folgenden allgemeinen Forderungen besondere Bedeutung bei, bevor sie zusätzlich zu den Anmerkungen vom Dezember 1994 weitere detaillierte Empfehlungen geben:

1. Eine neue grundsätzliche Bestimmung sollte in die ISDN-Richtlinie aufgenommen werden, durch die Netzbetreiber, Diensteanbieter und Hersteller dazu aufgefordert werden, Netze, Endgeräte und Software so zu gestalten und zu betreiben, daß die Verarbeitung personenbezogener Daten auf ein Mindestmaß beschränkt wird. Insbesondere sollten anonyme Zugangsmöglichkeiten zu Telekommunikationsnetzen und Diensten sowie anonyme Verfahren der Bezahlung zumindest als eine Option vorgesehen werden (vgl. Ziff. 2.2, Anhang zur Empfehlung Nr. R [95] 4).

2. Ein besonderer Zweckbindungsgrundsatz für den Telekommunikationsbereich ist ein wesentlicher Bestandteil eines gemeinsamen Mindeststandards für den Datenschutz in der Europäischen Union. Dies bezieht sich insbesondere auf die Verarbeitung von Daten für die Gebührenabrechnung ebenso wie auf die Daten, die durch die Nutzung interaktiver Kommunikationssysteme (z. B. Teleshopping mit Menüoptionen) entstehen.

3. Die Begrenzung der Speicherung von Inhaltsdaten nach dem Ende der Übertragung ebenso wie das Prinzip der Vertraulichkeit und des Fernmeldegeheimnisses (Artikel 5 und 7 des ursprünglichen Entwurfs) sollten wieder in die Richtlinie aufgenommen werden. Es ist von besonderer Bedeutung, daß das Europäische Recht die Vertraulichkeit von Inhaltsdaten in einer liberalisierten Umgebung garantiert, da die innerstaatliche Rechtsordnung einiger Mitgliedsstaaten diese Daten nur vor Eingriffen durch öffentliche Stellen – wie die herkömmlichen Telekommunikationsorganisationen – als Monopolisten schützt.

4. Die Europäischen Datenschutzbeauftragten betonen die Bedeutung einer Verpflichtung der Hersteller und Netz- sowie Diensteanbieter, eine Verschlüsselung von Endgerät zu Endgerät anzubieten. Verschlüsselung, die nicht von Endgerät zu Endgerät stattfindet, bietet insbesondere in der Mobilkommunikation nicht immer ausreichende wirkliche Sicherheit.

5. In den Erwägungsgründen 9 und 10 der allgemeinen Datenschutzrichtlinie vom 24. Juli 1995 ist festgelegt, daß die Mitgliedstaaten innerhalb des Spielraums zur Umsetzung dieser Richtlinie für eine Verbesserung des durch ihre gegenwärtige Gesetzgebung vorgesehenen Datenschutzstandards eintreten sollen. Die Harmonisierung der nationalen Gesetzgebung zur Verarbeitung personenbezogener Daten darf nicht zu einer Absenkung des Schutzniveaus führen, sondern muß im Gegenteil die Sicherung hohen Schutzniveaus in der Gemeinschaft anstreben. Obwohl die ISDN-Richtlinie speziellere Vorschriften enthält als die allgemeine Datenschutzrichtlinie, ist es gleichwohl eine Harmonisierungsmaßnahme und derselbe Grundsatz wie in den zitierten Erwägungsgründen sollte bei der Umsetzung der ISDN-Richtlinie beachtet werden. Insbesondere im Bereich der Teilnehmerverzeichnisse (Artikel 11) gibt es in den Mitgliedstaaten eine große Vielfalt von Möglichkeiten, die Eintragung in solchen Verzeichnissen zu unterbinden, wodurch teilweise ein höherer Schutzstandard gewährleistet wird. Dieser sollte durch die IDSN-Richtlinie nicht verringert werden.

6. Angesichts der Tatsache, daß die Liberalisierung der europäischen Telekommunikationsmärkte rasch voranschreitet, unterstreichen die Europäischen Datenschutzbeauftragten die Notwendigkeit, die Möglichkeit einer frühen Umsetzung zumindest bestimmter Vorschriften der ISDN-Richtlinie (z. B. bezüglich der Gebühren- und Verkehrsdaten) noch vor dem Ende der Übergangszeit nach Artikel 32 der allgemeinen Datenschutzrichtlinie zu prüfen.

B. Zusätzliche spezielle Anmerkungen

1. Artikel 1 – Ziel

Die Einbeziehung der juristischen Personen im Text des geänderten Vorschlags (vgl. Artikel 2 Abs. 3) wird von den Datenschutzbeauftragten unterstützt. Das Fernmeldegeheimnis soll nicht nur die Privatsphäre des Einzelnen, sondern auch Betriebsgeheimnisse schützen: Inhaltsdaten, Verbindungsdaten sowie Daten über die (interaktive) Nutzung von Telekommunikationsdiensten.

Darüber hinaus weisen sie auf den Umstand hin, daß spezielle Risiken für den Schutz der Privatsphäre sich aus dem Einsatz von Nebenstellenanlagen geben; diese Anlagen ermöglichen es dem Arbeitgeber, auf die gesamten Verbindungsdaten der Telefongespräche zuzugreifen, an denen seine Beschäftigten beteiligt sind. Diese speziellen Risiken rechtfertifen es zumindest, – solange spezielles Gemeinschaftsrecht zum Schutz der Arbeitnehmerdaten fehlt – im Rahmen der ISDN-Richtlinie die Endgeräteherstellen dazu zu verpflichten, daß sie ihre Kunden über die geltenden Vorschriften zur Verarbeitung personenbezogener Daten aufklären, die durch ihre Endgeräte ausgelöst wird.

2. Artikel 2 – Begriffsbestimmungen

Vor dem Hintergrund der bevorstehenden Liberalisierung des Telekommunikationsmarktes unterstützen die Europäischen Datenschutzbeauftragten eine einheitliche Begriffsbestimmung des Anbieters von Telekommunikationsdienstleistungen, die alle Funktionen im Zusammenhang mit dem Betrieb von Telekommunikationsnetzen umfaßt. Diese neue Begriffsbestimmung sollte die Definitionen in Artikel 2 Abs. 1 und 2 des geänderten Entwurfs ersetzen. In einer Wettbewerbsumgebung wird der Unterschied zwischen Netzbetreibern und Diensteanbietern zunehmend verwischt, und dementsprechend wird es nicht mehr gerechtfertigt sein, diese unterschiedlichen datenschutzrecht-

lichen Verpflichtungen zu unterwerfen. Die Bündelung verschiedener Dienste durch denselben Anbieter verdeutlicht die praktische Notwendigkeit einer einheitlichen und umfassenden Begriffsbestimmung, die alle denkbaren „Rollen“ eines „Telekommunikationsanbieters“ erfaßt (z. B. Anbieter des Zugangs zu Telekommunikationsnetzen; Anbieter von Online-Diensten, die Mehrwert-Dienste zur Verfügung stellen; Anbieter von Rechenkapazität, die zugleich inhaltliche Mehrwert-Dienste anbieten; Endgerätehersteller).

3. Artikel 3 – Betroffene Dienste

Artikel 3 Abs. 2 des geänderten Entwurfs sollte angesichts der in der vorhergehenden Anmerkung vorgeschlagenen einheitlichen Begriffsbestimmung gestrichen werden.

Es ist offenkundig, daß die Anwendung der Bestimmungen der ISDN-Richtlinie auf Dienste, die über analoge Netze angeboten werden, unter bestimmten Umständen technisch unmöglich sein wird. Allerdings können bestimmte Vorschriften, wie etwa Artikel 11 (Teilnehmerverzeichnisse) und Artikel 13 (unerbetene Anrufe) unabhängig von der angewandten Netztechnologie umgesetzt werden. In jedem Fall sollte Artikel 3 Abs. 3 keine ausdrücklichen Beschränkungen enthalten, die in einer gemischt analog-digitalen Netzumgebung zur Umgehung der Richtlinie geradezu auffordern würden. Tatsächlich können sowohl die Verarbeitung von Verbindungs- und Gebührendaten als auch die Rufnummernanzeige auch in gemischt analog-digitalen Netzen erfolgen.

4. Artikel 4 – Sicherheit

Die Datenschutzbeauftragten befürworten die Beibehaltung der Verpflichtung, die Teilnehmer über besondere Risiken für die Netzsicherheit insbesondere bei der Mobilkommunikation zu informieren. Sie unterstreichen die bereits zuvor getroffene Aussage, daß Verschlüsselung, die nicht von Endgerät zu Endgerät stattfindet, nicht immer ausreichende Sicherheit bietet.

5. Artikel 5 – Daten für die Gebührenabrechnung

Das wahlweise Angebot von anonymen (spurlosen) Bezahlungsverfahren sollte in die ISDN-Richtlinie entweder als gesonderter Artikel oder als neuer erster Absatz in Artikel 5 des Entwurfs aufgenommen werden. Im zweiten Fall sollte die Überschrift des Artikels 5 in „Bezahlungsverfahren“ abgeändert werden.

Die Bedeutung anonymer Bezahlungsverfahren wird unterstrichen durch die Tatsache, daß Artikel 18 des Entwurfs der Sprachtelefondienst-Richtlinie, deren zweite Lesung im Europäischen Parlament soeben stattgefunden hat, die Kommission verpflichtet, die Standardisierung einer harmonisierten europäischen vorausbezahlten Telefonkarte sicherzustellen. Auch die Europäische Kommission hat smart cards und elektronische Geldbörsen als eine Methode des Zugangs der Bürger zu Diensten in ihre Liste der Vorhaben von gemeinsamem Interesse nach der vorgeschlagenen Ratsentscheidung über eine Reihe von Richtlinien für transeuropäische Telekommunikationsnetze aufgenommen (KOM [95] 224 endg., Anhang 1).

Die Europäischen Datenschutzbeauftragten haben sich für die Wiederaufnahme eines modifizierten Verbots elektronischer Profile eingesetzt (vgl. Artikel 4 Abs. 2 des ursprünglichen Richtlinienentwurfs; Gemeinsame Erklärung vom Dezember 1994, S. 4). Dies ist insbesondere wichtig hinsichtlich der Nutzung von Daten für die Gebührenabrechnung. Gebührendaten sollten ausschließlich für Abrechnungs- und Zahlungszwecke genutzt werden. Obwohl es legitim sein kann, bestimmte Gebührendaten wie die Zahl der Einheiten zu analysieren, um andere Abrechnungsmöglicheiten und Tarife anbieten zu können, sollten solche Daten nicht dazu genutzt werden, um detaillierte individuelle Verhaltensprofile zu erzeugen.

6. Artikel 8 – Anzeige der Rufnummer des Anrufers

Die Europäischen Datenschutzbeauftragten haben in ihrer Gemeinsamen Erklärung vom Dezember 1994 darauf hingewiesen, daß die Speicherung der Anzeige der Rufnummer des Anrufers durch den Angerufenen ohne Wissen des Anrufers eine treuwidrige Datenverarbeitung darstellt. Dies ergibt sich offenbar auch aus Artikel 10 der allgemeinen Datenschutzrichtlinie.

Sollten hinsichtlich dieser Interpretation Zweifel bestehen, müßte Artikel 8 der ISDN-Richtlinie um eine entsprechende Klarstellung ergänzt werden.

In modernen digitalen Netzen können sowohl die Identifikation des Anrufers oder eines Teilnehmers, der versucht hat, anzurufen, als auch die Identifikation eines angerufenen Teilnehmers nach dem Ende des Gesprächs oder des Anrufversuchs gespeichert werden. Im ersten Fall bieten Betreiber (z. B. in Großbritannien) die Möglichkeit für den angerufenen Teilnehmer an, durch Wahl einer bestimmten Nummernfolge herauszufinden, wer zuletzt versucht hat, ihn anzurufen. Im zweiten Fall ermöglicht die Wahlwiederholungsfunktion die Herstellung der letzten Verbindung, die von diesem Endgerät aus initiiert wurde. Beide Funktionen können von Unbefugten genutzt werden. Die Datenschutzbeauftragten halten es deshalb für notwendig, Artikel 8 des geänderten Vorschlags so umzuformulieren, daß diese Vorschrift abstrakt die verschiedenen Situationen erfaßt (die die vorliegende Entwurfsfassung noch nicht hinreichend erfaßt).

Artikel 8 könnte wie folgt neu gefaßt werden:

„Identifizierung und Speicherung der Rufnummer

1. Alle Funktionen, die zu einer Identifizierung und Speicherung der Rufnummer des Anrufers oder des Angerufenen durch den Angerufenen oder den Anrufer führen können, müssen so realisiert werden, daß sie durch eine Blockierfunktion ergänzt werden, die vom Anrufer oder Angerufenen nach Wahl anschlußbezogen oder gesprächsbezogen genutzt werden kann.“

Die Datenschutzbeauftragten schlagen vor, daß Artikel 8 Absatz 2 ebenso wie Artikel 8 Abs. 3 Satz 1 gestrichen werden. Artikel 8 Abs. 3 Sätze 2 und 3 sollten als neuer Artikel 8 Abs. 2 wie folgt gefaßt werden:

„2. Die Mitgliedstaaten stellen sicher, daß die Kunden den Zugriff unberechtigter Personen auf die Anzeige der eingehenden Rufnummer und der gewählten Rufnummer ausschließen können.

Der angerufene Kunde muß die Möglichkeit haben, die Entgegennahme eingehender Anrufe auf solche zu beschränken, bei denen die Rufnummer angezeigt wird.“

Artikel 8 Abs. 4 und 5 des geänderten Vorschlags bleiben unverändert und werden Abs. 3 und 4 (neu).

7. Artikel 9 – Ausnahmen

Soweit Notrufe in den Geltungsbereich der ISDN-Richtlinie fallen, vertreten die Datenschutzbeauftragten die Auffassung, daß die Ausnahme in Artikel 9 Abs. 2 a (Anerkennung bestimmter Organisationen) von den Mitgliedstaaten in einer funktionalen statt in einer organisatorischen Weise angewandt werden sollte. Diese Ausnahme soll nicht pauschal auf jede Organisation angewandt werden, die auch Notrufe entgegennimmt, sondern nur auf spezielle Notrufstellen (Polizei, Feuerwehr).

8. Artikel 10 – Anrufweiterschaltung

Da Artikel 14 Abs. 2 des ursprünglichen Entwurfs gestrichen worden ist, weist der gegenwärtige Artikel 10 des geänderten Entwurfs ein deutliches Ungleichgewicht hinsichtlich des Schutzes der drei an einer Anrufweiterschaltung beteiligten Teilnehmer auf, das behoben werden sollte. Der gegenwärtige Entwurf enthält keine Antwort auf die Frage, in welcher Weise das Interesse des Anrufers geschützt werden soll, der nicht weiß, daß sein Anruf weitergeschaltet wird.

Darüber hinaus sind die Datenschutzbeauftragten vor dem Hintergrund der Erörterungen in der Ratsarbeitsgruppe der Auffassung, daß die drei wesentlichen Punkte des geänderten Vorschlags beibehalten werden sollten:

- Information des dritten Teilnehmers darüber, daß Anrufe zu ihm weitergeschaltet werden und wer die Weiterschaltung ausgelöst hat;
- Zustimmung des dritten Teilnehmers und
- Möglichkeit des dritten Teilnehmers, die Anrufweiterschaltung jederzeit zu beenden.

9. Artikel 11 – Teilnehmerverzeichnisse

Die Datenschutzbeauftragten haben in ihrer ersten Gemeinsamen Erklärung das Recht des Einzelnen betont, kostenfrei den Eintrag in Teilnehmerverzeichnisse jeder Form (konventionell oder elektronisch) auszuschließen. Dieses Recht gewinnt mit der Liberalisierung des Marktes für Teilnehmerverzeichnisse und der Durchsetzung billiger elektronischer Teilnehmerverzeichnisse (CD-ROM) an Bedeutung. Der Teilnehmer sollte das Recht haben, differenziert nicht nur hinsichtlich des Umfangs der Daten, sondern auch bezüglich des Medientyps, der für die Speicherung der Teilnehmerinformation genutzt wird, die Verarbeitung seiner Daten auszuschließen. Er sollte auch das Recht haben, die Aufnahme in ein veröffentlichtes Verzeichnis auszuschließen, aber gleichwohl mit der Offenbarung seiner personenbezogenen Daten durch einen Auskunftsdienst auf Anfrage einverstanden zu sein.

Darüber hinaus sollte der Teilnehmer die Möglichkeit haben, seinen Widerspruch gegen die Nutzung seiner personenbezogenen Daten für Werbezwecke im Teilnehmerverzeichnis veröffentlichen zu lassen. Zu diesem Zweck schlagen die Datenschutzbeauftragten vor, die folgenden Worte in Artikel 11, Satz 2 am Ende anzufügen:

> „. . . oder im Teilnehmerverzeichnis vermerken zu lassen, daß seine Daten nicht für Werbezwecke genutzt werden dürfen."

Die Datenschutzbeauftragten unterstützen die Beibehaltung des Rechts, kostenfrei einen Eintrag im Teilnehmerverzeichnis auszuschließen, insbesondere vor dem Hintergrund der Tatsache, daß Artikel 16 des Entwurfs für eine Sprachtelefondienst-Richtlinie, die wahrscheinlich bald endgültig beschlossen wird, dieses Recht nicht mehr enthält.

10. Artikel 13 – Unerbetene Anrufe

Die Datenschutzbeauftragten haben erhebliche Unterschiede in den vier Sprachversionen festgestellt, die sie untersucht haben (Englisch, Französisch, Deutsch und Spanisch). Offensichtlich gibt es gegenwärtig keine einheitliche Version dieses Artikels.

Insbesondere ist unklar, ob eine Untersuchung für allgemeine Forschungszwecke oder statistische Zwecke (abgesehen von der Marktforschung) vom geänderten Entwurf erfaßt wird. Nur die spanische Version scheint alle Untersuchungen für Zwecke der Marktforschung oder der allgemeinen Forschung einzuschließen.

Die Datenschutzbeauftragten unterstützen eine Harmonisierung der unterschiedlichen Sprachversionen, die berücksichtigt, daß für den angerufenen Teilnehmer, der einen unerbetenen Anruf erhält, die Beeinträchtigung seiner Privatsphäre unabhängig von dem jeweiligen Zweck eintritt, den der Anrufer verfolgt.

Anlage 4

Abkürzungsverzeichnis

ADV	–	Automatisierte Datenverarbeitung
ÄROV	–	Ämter für offene Vermögensfragen
AGE	–	Automatisierte Autobahngebührenerfassung
AGGVG	–	Gesetz zur Ausführung des Gerichtsverfassungsgesetzes
AHW	–	Automatisiertes Haushaltswesen (Projekt)
ALK	–	Automatisierte Liegenschaftskarte
AO	–	Abgabenordnung
AOÄG	–	Abgabenordnungsänderungsgesetz
AOAnwG	–	Abgabenordnungsanwendungsgesetz
APC	–	Arbeitsplatzcomputer
ASOG	–	Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin (Allgemeines Sicherheits- und Ordnungsgesetz)
AuslG	–	Ausländergesetz
AusReg	–	Ausländerregister
AV-Schüler	–	Ausführungsvorschriften über die Führung schriftlicher Unterlagen über Schüler
BASIS	–	Berliner Automatisiertes Sozialhilfe Interaktions-System (Projekt)
BauGB	–	Baugesetzbuch
BBG	–	Bundesbeamtengesetz
BBesG	–	Bundesbesoldungsgesetz
BDSG	–	Bundesdatenschutzgesetz
BGB	–	Bürgerliches Gesetzbuch
BGBl.	–	Bundesgesetzblatt
BImschG	–	Bundesimmissionsschutzgesetz
BlnDSG	–	Berliner Datenschutzgesetz
BKA	–	Bundeskriminalamt
BND	–	Bundesnachrichtendienst
BOWI	–	ADV-Verfahren Bußgeld und Verkehrsordnungswidrigkeiten
BR-Drs.	–	Bundesrats-Drucksache
BRAO	–	Bundesrechtsanwaltsordnung
BROSiA	–	Berliner Rahmenkozept für Organisation, Sicherheit und Anwendungsentwicklung beim IT-Einsatz
BRRG	–	Beamtenrechtsrahmengesetz
BSHG	–	Bundessozialhilfegesetz
BSI	–	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	–	Bundestags-Drucksache
BVG	–	Berliner Verkehrsbetriebe
BZRG	–	Bundeszentralregistergesetz
CCO . . .	–	Citicorp Card Operations GmbH
CD-ROM	–	Compact Disk-Read Only Memory
CD-WORM	–	Compact Disk-Write Once Read Multiple
CuR	–	Computer und Recht
DateiRegVO	–	Dateienregisterverordnung Berlin
DCL	–	Dezentrale Computer-Leistung (Besteuerungsverfahren)
DCE	–	Distributed Computing Environment
DFS	–	Distributed File System
DV	–	Datenverarbeitung
DVO-MeldeG	–	Durchführungsverordnung zum Meldegesetz
EALG	–	Entschädigungs- und Ausgleichsleistungsgesetz
EU	–	Europäische Union
EWW	–	ADV-Verfahren Einwohnerwesen
f.	–	folgende Seite
ff.	–	folgende Seiten
FIS	–	Fachübergreifendes Informationssystem (Projekt)
FÜV	–	Fernmeldeverkehr-Überwachungs-Verordnung
GewO	–	Gewerbeordnung
GEZ	–	Gebühreneinzugszentrale
GG	–	Grundgesetz
GGO I	–	Gemeinsame Geschäftsordnung für die Berliner Verwaltung – Allgemeiner Teil I
GIBES	–	Grundlagen der Ausstattung mit IT-Infrastruktur für die Bezirks- und Senatsverwaltungen (Infrastrukturprojekt)
GPS	–	Global Positioning System
GSD	–	Gesellschaft für Systemforschung und Dienstleistungen im Gesundheitswesen
GMBl.	–	Gemeinsames Ministerialblatt
GVBl.	–	Gesetz- und Verordnungsblatt
G 10-Gesetz	–	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
HdK	–	Hochschule der Künste
IHK-G	–	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern
INPOL	–	Informationssystem der Polizei
INVENT	–	Inventarisierung IT-Gerätebestands
IPV	–	Integrierte Personalverwaltung (Projekt)
ISDN	–	Integrated Services Digital Network (Dienste integrierendes digitales Netz)
ISVB	–	Informationssystem Verbrechensbekämpfung
IT	–	Informationstechnik
ITSEC	–	Information Technology Security Evaluation Criteria
IuK- . . .	–	Informations- und Kommunikations- . . .
IVG	–	Informationsverarbeitungsgesetz Berlin
i. V. m.	–	in Verbindung mit
JGG	–	Jugendgerichtsgesetz
JVA	–	Justizvollzugsanstalt
KpS-Richtlinien	–	Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen
KStG	–	Kirchensteuergesetz
LADG	–	Landesantidiskriminierungsgesetz

LAN	–	Local Area Network – lokales Netz
LAZ	–	Lokales Administrationszentrum
LBG	–	Landesbeamtengesetz
LEA	–	Landeseinwohneramt
LfVG	–	Gesetz über das Landesamt für Verfassungsschutz
LGG	–	Landesgleichstellungsgesetz
LikaAbrufVO	–	Verordnungen über die Benutzung des Liegenschaftskatasters mit Hilfe automatisierter Abrufverfahren
LikaAbgabeVO	–	Abgabe digitaler Angaben aus dem Liegenschaftskataster
LIT	–	Landesamt für Informationstechnik
LVwA	–	Landesverwaltungsamt
MAN	–	Metropolitan Area Network – stadtweites Netz
MBA	–	Modellbezirksamt (Infrastrukturprojekt)
MiStra	–	Anordnung über Mitteilungen in Strafsachen
MiZi	–	Anordnung über Mitteilungen in Zivilsachen
MfS	–	Ministerium für Staatssicherheit der ehemaligen DDR
MOD	–	Magneto-Optical Disk
MS-DOS	–	Microsoft-Disk Operating System (PC-Betriebssystem)
NII	–	National Information Infrastructure
NJW	–	Neue Juristische Wochenschrift
OrgKG	–	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität
OrgKGErgG	–	Gesetz zur Ergänzung des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität
PC	–	Personalcomputer
PTNeuOG	–	Postneuordnungsgesetz
RDV	–	Recht der Datenverarbeitung
SAZ	–	Service- und Administrationszentrum (Infrastrukturprojekt)
SGB	–	Sozialgesetzbuch
SMD	–	Sozialmedizinischer Dienst
SRZ	–	Sicherheitsrechenzentrum
SÜG-Bund	–	Sicherheitsüberprüfungsgesetz des Bundes
StaLa	–	Statistisches Landesamt
StGB	–	Strafgesetzbuch
StPO	–	Strafprozeßordnung
StudDatVO	–	Studentendatenverordnung
StVG	–	Straßenverkehrsgesetz
StVO	–	Straßenverkehrsordnung
StVollzG	–	Strafvollzugsgesetz
StUG	–	Stasi-Unterlagen-Gesetz
SISY	–	Staatsanwaltschaftliches Informationssystem
TDSV	–	Telekommunikations-Datenschutzverordnung
UDSV	–	Teledienstunternehmen-Datenschutzverordnung
UVollzO	–	Untersuchungshaftvollzugsordnung
VermDVG	–	Vermögensrechtsdatenverarbeitungsgesetz
VermG	–	Vermögensgesetz
VGO	–	Vollzugsgeschäftsordnung
VwVfG	–	Verwaltungsverfahrensgesetz
WAN	–	Wide Area Network (Weitbereichsnetz)
WBS	–	Wohnberechtigungsschein
WORM	–	Write Once Read Multiple (einmal beschreibbare Speicher)
WWW	–	World Wide Web (Mehrwertdienst auf dem Internet)

Anlage 5

Auszug aus dem Geschäftsverteilungsplan des Berliner Datenschutzbeauftragten

Stand: . Januar 996

Berliner Datenschutzbeauftragter

Dr. Hansjürgen Garstka

Sekretariat

Birgit Münch

Bereich Recht und Verwaltung

Bereichsleiter, Vertreter des DSB für den Bereich und für AV; Datenschutzrecht; nationale und internationale Kooperation; Abgeordnetenhaus, Rechnungshof, Senatskanzlei, Bundes- und Europaangelegenheiten

Dr. Alexander Dix

Gesundheit; Jugend und Familie; Kulturelle Angelegenheiten; Soziales; Schutz von Gesundheits- und Sozialdaten

Dr. Ulrich von Petersdorff

Schule, Berufsbildung und Sport; Wissenschaft und Forschung; Umweltschutz; Forschung und Statistik

Dr. Rainer Metschke

Arbeit und Frauen; Betriebe; Personaldaten; Beratung von Personalräten

Birgit Saager

Telekommunikation und Medien

Sven Mörs

Sekretariat

Laima Nicolaus

Allgemeine Verwaltung; Büroorganisation; Haushaltsplanung und -bewirtschaftung

Doris Werth

Allgemeine Verwaltung; Personalsachbearbeitung

Alexandra Trost

Rechnungsstelle

Monika Klößing

Sekretariat

Carola Peplau

Bereich Bürger und Öffentlichkeit

Bereichsleiterin; Vertreterin des DSB für den Bereich; Konzeption und Durchführung der Öffentlichkeitsarbeit; Landesamt für Verfassungsschutz

Claudia Schmid

Redaktion von Veröffentlichungen; Bau- und Wohnungswesen; Polizeipräsident; Stadtentwicklung

Volker Brozio

Finanzen; Justiz; Wirtschaft und Technologie; Verkehr; Rechtspflege

Dagmar Hartge

Bürgerberatung und -betreuung; Inneres; Bezirksämter; Geschäftsordnung

Detlef Schmidt

Sekretariat

Sabine Krissel

Bereich private Datenverarbeitung

Bereichsleiter, Vertreter des DSB für den Bereich; Grundsatzangelegenheiten des Bereichs; Banken, Versicherungen, Kreditauskunfteien; Deutsche Bahn AG

Dr. Dieter Baumeister

Private Datenverarbeitung für eigene Zwecke; private Datenverarbeitung für fremde Zwecke

Daniel Holzapfel

Sektretariat

Monika Klößing

Führung des Registers für Fremdverarbeiter

Nicole Müller

Bereich Technik und Organisation

Bereichsleiter; Vertreter des DSB als Dienststellenleiter und für den Bereich; Grundsatzfragen der ADV-Organisation und -Technik und ihrer Entwicklung

Hanns-Wilhelm Heibey

Großrechner mit proprietären Betriebssystemen

Joachim Laß

Rechner- und Kommunikationsnetze

Ursula Meyer zu Natrup

Koordination der technisch-organisatorischen Beratung und Prüfung; Grundsatzfragen der Dateienregister; Beratung der behördlichen Datenschutzbeauftragten

Jürgen Horn

Systeme unter UNIX und seinen Derivaten

Dagmar Töpfer

Personalcomputer, lokale Netze

Ralf Hauser

Systemverwaltung

Andre Drescher

Sekretariat, Informationsausgabe, Poststelle

Nicole Müller

Schreibdienst

Martina Hingst

Stichwortverzeichnis

Angegeben sind die Fundstellen aller Jahresberichte seit 1979. Die Ziffern ohne Jahreszahl beziehen sich auf den Zusammendruck der Jahresberichte in den von mir herausgegebenen Materialien zum Datenschutz, Band 2, Datenschutz in Berlin 1979 bis 1983. Die Ziffern mit den Jahreszahlen von 1983 bis 1989 beziehen sich auf die jeweiligen Drucksachen des Abgeordnetenhauses, ab 1990 auf die von mir herausgegebene Broschüre des jeweiligen Jahresberichts.