Abgeordnetenhaus von Berlin

Drucksache 12 / 5480

12. Wahlperiode

Bericht

des Berliner Datenschutzbeauftragten

zum 31. Dezember 1994

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 16. März 1994 vorgelegten Jahresbericht 1993 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 1994 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.

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

Gliederung

1. Rechtliche Rahmenbedingungen

1.1 Deutschland und Europa

Verfassungsreform ohne Grundrecht auf Datenschutz

Das am 15. November 1994 in Kraft getretene *Gesetz zur Änderung des Grundgesetzes*[1] läßt das Grundrecht auf Datenschutz unberücksichtigt. Damit wurde eine Chance vertan, dem seit dem „Volkszählungsurteil" des Bundesverfassungsgerichts von 1983 eingetretenen Verfassungswandel auch durch eine Änderung des Verfassungstextes Rechnung zu tragen und der massenhaften Verarbeitung und systematischen Verknüpfung personenbezogener Daten eine ausdrückliche Grenze im Grundgesetz zu ziehen.

Im Zuge der Verfassungsreform wurde der Katalog der konkurrierenden Gesetzgebung um „die Untersuchung und die künstliche Veränderung von Erbinformationen" ergänzt (Art. 74 Abs. 1 Nr. 26 GG). Damit ist eine verfassungsrechtliche Voraussetzung für die dringend erforderliche bundesgesetzliche Regelung der Analyse des menschlichen Genoms geschaffen worden, die nun nicht mehr länger aufgeschoben werden sollte.

Bundesgesetzgebung

Zahlreiche im Berichtszeitraum verabschiedete Bundesgesetze enthalten entweder bereichsspezifische Datenschutzregelungen oder Vorschriften, die Auswirkungen für den Datenschutz auch in Berlin haben.

So wurde mit dem *Gesetz zur sozialen Absicherung des Risikos der Pflegebedürftigkeit (Pflegeversicherungsgesetz)* das Sozialgesetzbuch um ein XI. Buch ergänzt, das am 1. Januar 1995 in Kraft getreten ist[2]. Das Gesetz über die Pflegeversicherung ist ein erneutes Beispiel dafür, daß die erhöhte staatliche Fürsorge – in diesem Fall für Pflegebedürftige – auch zu einem stark erhöhten Informationsbedarf der Sozialleistungsträger, insbesondere der neu gebildeten Pflegekassen, führt. Jeder versicherungspflichtige Bürger ist im Pflegefall gehalten, zusätzlich weitreichende Angaben über seinen persönlichen Lebensbereich zu machen, wenn er nicht Gefahr laufen will, daß ihm Leistungen im Fall seiner Pflegebedürftigkeit verwehrt werden. Seine informationelle Selbstbestimmung wird gewissermaßen fürsorglich beschränkt. Ob die von den Pflegekassen an die Pflegebedürftigen sowie die Medizinischen Dienste ausgegebenen umfangreichen Fragebogen sich im Rahmen des gesetzlich Zulässigen halten, wird noch zu prüfen sein. Positiv zu vermerken ist allerdings, daß das Pflegeversicherungsgesetz ein eigenes Kapitel zum Datenschutz enthält, in dem der Schutz der Versichertendaten für diese neu eingeführte Art der Sozialversicherung ergänzend zum X. Buch des Sozialgesetzbuchs geregelt wird.

Die allgemeinen Regeln des Sozialdatenschutzes im X. Buch des Sozialgesetzbuchs wurden durch das *Gesetz zur Änderung von Vorschriften des Sozialgesetzbuchs über den Schutz der Sozialdaten sowie zur Änderung anderer Vorschriften (2. Gesetz zur Änderung des Sozialgesetzbuchs – 2. SGBÄndG)*[3] grundlegend novelliert und in erster Linie den Vorschriften des 1990 geänderten Bundesdatenschutzgesetzes angepaßt. Allerdings wurde noch in der Schlußphase der langwierigen Beratungen dieses Gesetzes im Bundesrat versucht, das Sozialgeheimnis gegenüber dem bisherigen Rechtszustand stark einzuschränken. So erfuhren wir von dritter Seite, daß das Land Berlin im Bundesrat beantragt hatte, durch Anrufung des Vermittlungsausschusses alle Sozialleistungsträger zu ermächtigen, der Polizei und den Gerichten auch den *Aufenthaltsort eines Sozialleistungsempfängers* mitzuteilen. Dieser Vorstoß der Senatsverwaltung für Inneres hätte eine Abkehr von der bisherigen Verwaltungspraxis in Berlin bedeutet, wie sie im gemeinsamen Rundschreiben über die Offenbarung von Sozialdaten im Rahmen der Amtshilfe nach § 68 SGB X der Senatsverwaltungen für Gesundheit, Soziales und Familie, Schule, Jugend und Sport sowie Arbeit und Betriebe[4] niedergelegt ist. Wir sind diesem Antrag ebenso entgegengetreten wie die Senatsverwaltung für Soziales. Auch der Bundesrat hat den Antrag Berlins, den Vermittlungsausschuß aus diesem Grund anzurufen, abgelehnt. Das ist zu begrüßen, denn die Sozialleistungsbehörden dürfen nicht „auf dem kleinen Dienstweg" zum verlängerten Arm der Polizei werden. Das Sozialgesetzbuch sieht auch in seiner neuen Fassung ein praktikables Verfahren vor, nach dem der Richter Ausnahmen vom Sozialgeheimnis für Zwecke der Strafverfolgung anordnen kann, zumal die Voraussetzungen für die Offenbarung der Daten gelockert wurden.

Im Vermittlungsausschuß ist auf Druck der Länder die bisherige Verpflichtung zur Bestellung von besonderen Datenschutzbeauftragten bei den Sozialbehörden gestrichen worden. Allerdings bleiben die Bestimmungen des Berliner Datenschutzgesetzes, die die Bestellung von behördlichen Datenschutzbeauftragten in den Bezirken vorsehen, unberührt[5]. Auch die Bestellung von *besonderen Beauftragten für den Sozialdatenschutz* in den bezirklichen Sozialämtern hat sich bewährt und sollte beibehalten werden.

Mit dem 2. SGB-Änderungsgesetz ist zugleich eine begrenzte Verpflichtung zur Übermittlung von *Wohngelddaten* an die Behörden, die die Fehlbelegungsabgabe einziehen, in das Wohngeldgesetz aufgenommen worden[6]. Dies war erforderlich, weil die Erhebung der Fehlbelegungsabgabe keine Aufgabe nach dem Sozialgesetzbuch ist, so daß dieses bisher eine Datenübermittlung durch die Wohngeldstellen nicht zuließ.

Mit dem *Ersten Gesetz zur Änderung des Melderechtsrahmengesetzes,* das am 20. März 1994 in Kraft trat[7], wurde die Befugnis der Meldebehörden geschaffen, auch vor Wahlen zum Deutschen Bundestag oder zum Europäischen Parlament den Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen Meldedaten von wahlberechtigten Bürgern bezogen auf bestimmte Altersgruppen zu übermitteln. Den Bürgern steht auch in diesen Fällen ein Widerspruchsrecht zu, wie es das Berliner Meldegesetz bereits seit längerem für die Vorbereitung zu den Wahlen zum Abgeordnetenhaus und zu den Bezirksverordnetenversammlungen vorsieht. Im einzelnen bleibt die Regelung im novellierten Melderechtsrahmengesetz allerdings erheblich hinter dem Berliner Landesrecht zurück. In anderen Punkten wird eine Anpassung an das geänderte Melderechtsrahmengesetz erforderlich sein.

Durch eine *Änderung des Stasi-Unterlagen-Gesetzes*[8] erhielt der Bundesbeauftragte für die Stasiunterlagen die Befugnis zur Verwendung bestimmter Informationen aus dem Zentralen Einwohnerregister der ehemaligen DDR, u. a. des Personenkennzeichens. Zugleich wurde der Bundesbeauftragte verpflichtet, diese Daten auf Ersuchen sowohl den Gerichten als auch den Strafverfolgungsbehörden zur Erfüllung ihrer Aufgaben zu übermitteln. Die Kritik der Datenschutzbeauftragten an dieser Regelung blieb unberücksichtigt[9]. Allerdings ist das Gesetz bis Ende 1996 befristet.

Erstmals ist auf Bundesebene durch das am 29. April 1994 in Kraft getretene *Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes* (Sicherheitsüberprüfungsgesetz)[10] die seit langem überfällige gesetzliche Grundlage für Sicherheitsüberprüfungen in der Bundesverwaltung geschaffen worden, während sie für die Berliner Landesverwaltung noch immer aussteht.

Mit erheblicher Verzögerung trat am 16. Juli 1994 das *Gesetz zur Umsetzung der Richtlinie 90/313/EWG des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt*[11] in Kraft. Wesentlicher Bestandteil dieses Gesetzes ist das *Umweltinformationsgesetz (UIG),* dessen Anwendungsbereich größer ist, als es der Titel des Gesetzes nahelegt. Sowohl der Kreis der verpflichteten Behörden als auch der Begriff der „Informationen über die Umwelt" ist so definiert, daß keineswegs nur Umweltbehörden im engeren Sinne ihr Informationsverhalten gegenüber den Bürgern werden ändern müssen, sondern z. B. auch Planungs- und Baubehörden.

1 BGBl. 1994 I, 3146
2 BGBl. 1994 I, 1014
3 BGBl. 1994 I, 1229
4 Anlage 3 zum Jahresbericht 1985, Materialien 10, S. 29
5 vgl. § 19 Abs. 5 BlnDSG
6 § 37 b WoGG
7 BGBl. 1994 I, 529
8 BGBl. 1994 I, 334
9 vgl. Jahresbericht 1993, 4.5.3
10 BGBl. 1994 I, 867; siehe dazu unten 4.6.5
11 BGBl. 1994 I, 1490; dazu unten 4.12

Im Abstand von jeweils vier Wochen sind im letzten Quartal 1994 drei Gesetze im Bereich des Polizei- und Ordnungsrechtes und des Strafprozeßrechtes in Kraft getreten, nämlich das Ausländerzentralregistergesetz, das Bundesgrenzschutzneuregelungsgesetz und das Verbrechensbekämpfungsgesetz.

Mit dem am 1. Oktober 1994 in Kraft getretenen *Gesetz über das Ausländerzentralregister (AZRG)*[12] wurde eine bundesweit zentrale Verarbeitung von Ausländerdaten sanktioniert. In diesem Zusammenhang ist daran zu erinnern, daß ein bundesweites Melderegister für Inländer stets als verfassungswidrig angesehen worden ist, weshalb auch nach dem Einigungsvertrag das Zentrale Einwohnerregister der ehemaligen DDR aufgelöst wurde. Diese besondere Behandlung von Ausländern wird dadurch umso problematischer, als mit dem AZR über den Vollzug des Ausländergesetzes hinaus weitere Zwecke verfolgt werden wie z. B. Verfassungsschutz, Fahndung und vorbeugende Straftatenbekämpfung.

Das *Bundesgrenzschutzneuregelungsgesetz (BGSNeuRegG)* trat am 1. November 1994 in Kraft; es sieht neue weitreichende Befugnisse zum Abgleich zwischen Verfassungsschutz und Bundesgrenzschutz vor[13].

Am 1. Dezember 1994 trat das Gesetz zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze *(Verbrechensbekämpfungsgesetz)*[14] in Kraft, das zum einen Regelungen für ein länderübergreifendes staatsanwaltschaftliches Verfahrensregister und zum anderen neue Befugnisse des Bundesnachrichtendienstes zur Weitergabe von Erkenntnissen aus der Fernmeldeaufklärung an Verfassungsschutzämter, Staatsanwaltschaften und Polizeien enthielt.

Zu Beginn des Jahres 1995 traten außerdem Änderungen der Zivilprozeßordnung in Kraft, die durch das *Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis*[15] und durch das *Gesetz zur Änderung der Vorschriften über die Prozeßkostenhilfe (Prozeßkostenhilfeänderungsgesetz)*[16] ausgelöst worden waren. Bereits am 9. September 1994 war das *Gesetz zur Neuordnung des Berufsrechts der Rechtsanwälte und der Patentanwälte*[17] in Kraft getreten, das erstmals eine gesetzliche Regelung der anwaltlichen Schweigepflicht und der Aufbewahrungsdauer von Handakten enthält.

Mit dem *Gesetz zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz – PTNeuOG)*[18] trat am 1. Januar 1995 auch die zweite Stufe der Postreform in Kraft, in deren Rahmen auch die datenschutzrechtliche Stellung des Telefonkunden gesetzlich neu geregelt wurde.

Schließlich tritt im Laufe des Jahres das *Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften*[19] in Kraft, mit dem die Gewerbeordnung erstmals um ausführliche Regelungen zum Umgang mit personenbezogenen Daten von Gewerbetreibenden ergänzt wird.

Zusammenfassend ist festzustellen, daß auf Bundesebene der bereichsspezifische Datenschutz auch im Berichtszeitraum weiter ausgebaut worden ist, was in der Sache nicht immer zu einer Verbesserung der Rechtsstellung des Bürgers geführt hat. Datenschutzrechtliche Regelungen finden sich inzwischen ganz überwiegend in fachspezifischen Gesetzen und nicht in den allgemeinen Datenschutzgesetzen. Damit folgt der Bundesgesetzgeber zunehmend dem Berliner Beispiel und setzt die Forderung des Bundesverfassungsgerichts nach bereichsspezifischen gesetzlichen Regelungen zur Verwendung personenbezogener Daten um.

Rechtsprechung

Aus der Rechtsprechung des *Bundesverfassungsgerichts* im Berichtszeitraum sind drei Entscheidungen hervorzuheben, die das informationelle Selbstbestimmungsrecht betreffen.

In seinem Beschluß vom 26. April 1994[20] hob das Bundesverfassungsgericht die Verurteilung einer Bürgerin wegen Beleidigung auf, die sich in einem *Brief an ihren inhaftierten Bruder* abfällig über das Personal der Justizvollzugsanstalt geäußert hatte, um ihren Bruder, der Selbstmordabsichten geäußert hatte, seelisch aufzurichten. Die Strafgerichte hatten darin eine strafbare Beleidigung gesehen, weil der Brief der *Kontrolle nach dem Strafvollzugsgesetz* unterlag und die Absenderin dies gewußt habe. Das Bundesverfassungsgericht stellte demgegenüber klar, daß Äußerungen gegenüber Familienangehörigen und Vertrauenspersonen den Schutz der Privatsphäre auch dann genießen, wenn Dritte (hier: Vollzugsbeamte) im Rahmen einer rechtmäßigen Überwachung des Briefverkehrs Kenntnis von diesen Äußerungen erhalten. Der Grundrechtsschutz wirke sich gerade darin aus, daß der vertrauliche Charakter der Mitteilung trotz der staatlichen Überwachung gewahrt bleibe. In einem zweiten Beschluß vom selben Tage[21] hat das Bundesverfassungsgericht festgestellt, daß der bisherige gesetzliche Ausschluß der Ehelichkeitsanfechtung durch das betroffene Kind nach Vollendung des 20. Lebensjahres unabhängig davon, wann das Kind von den Umständen erfährt, die für seine Nichtehelichkeit sprechen, mit dem allgemeinen Persönlichkeitsrecht, insbesondere dem *Recht auf Kenntnis der eigenen Abstammung*, nicht vereinbar und damit verfassungswidrig ist. Das Recht auf Kenntnis der eigenen Abstammung verleiht nach diesem Beschluß allerdings keinen Anspruch auf Verschaffung von Kenntnissen über die eigene Abstammung, sondern schützt nur vor der Vorenthaltung erlangbarer Informationen[22]. Dem Bundesgesetzgeber wurde eine Frist bis zum Ablauf der jetzt begonnenen Legislaturperiode eingeräumt, um einen verfassungsmäßigen Zustand herzustellen. Dies könne entweder dadurch geschehen, daß die Anfechtungsfrist in der Weise ausgestaltet wird, daß sie erst dann zu laufen beginnt, wenn die betroffene Person von den Umständen erfährt, die auf ihre Nichtehelichkeit hindeuten; eine andere Möglichkeit besteht für den Gesetzgeber darin, das Anfechtungsrecht des volljährigen Kindes weiter einzuschränken und zugleich diesem die Möglichkeit zu geben, seine Abstammung ohne Auswirkungen auf das Verwandtschaftsverhältnis zu klären.

Schließlich hat das Bundesverfassungsgericht[23] über eine Frage entschieden, die mehrere Bürger auch bereits an uns herangetragen hatten. Ein Vermieter hatte die Mieter auf Zustimmung zu einer Mieterhöhung verklagt und sich im Prozeß auf das Gutachten eines Sachverständigen gestützt, der Angaben zur ortsüblichen Vergleichsmiete anhand von Vergleichswohnungen gemacht hatte. Dieser Sachverständige war allerdings nicht bereit, im Prozeß *Namen und Anschriften von Mietern und Vermietern der untersuchten Vergleichswohnungen* anzugeben, da er diesen Personen zugesagt habe, ihre Daten nicht weiterzugeben. Während die Zivilgerichte das Sachverständigengutachten gleichwohl für verwertbar hielten, hat das Bundesverfassungsgericht betont, ein solches Vorgehen sei mit dem allgemeinen Persönlichkeitsrecht der Mieter und ihrem Anspruch auf ein rechtsstaatliches Verfahren unvereinbar. Diese müßten die Möglichkeit erhalten, die vom Sachverständigen erhobenen und seiner Bewertung zugrunde gelegten Tatsachen zu überprüfen. Die Verpflichtung des Gerichts, die tatsächlichen Grundlagen eines Gutachtens hinreichend zu überprüfen und daran auch die Prozeßbeteiligten mitwirken zu lassen, vertrage zwar Einschränkungen, soweit Rechte anderer beeinträchtigt würden. Das sei insbesondere der Fall, wenn es sich um Daten aus der engsten Privat- oder Intimsphäre unbeteiligter Dritter handele, deren Preisgabe niemanden zuzumuten sei. Allein der Umstand, daß Dritte eine Bekanntgabe von Tatsachen aus ihrer Privatsphäre nicht wünschen und der Sachverständige sich daran gebunden fühle, sei freilich kein ausreichender Grund dafür, dem Mieter die entsprechenden Tatsachen vorzuenthalten und das Urteil auf ein Gutachten zu stützen, das auf diesen Tatsachen beruhe. Zugleich hat das Bundesverfassungsgericht jedoch hervorgehoben, daß der Prozeßgegner Einzelheiten (noch dazu personenbezogene) über die Grundlagen eines Gutachtens dann nicht verlangen könne, wenn der Sachver-

12 BGBl. 1994 I, 2265; vgl. dazu unten 4.6.3
13 BGBl. 1994 I, 2978; vgl. dazu unten 4.6.1
14 BGBl. 1994 I, 3186; vgl. dazu unten 4.8
15 BGBl. 1994 I, 1566; dazu siehe unten 4.8
16 BGBl. 1994 I, 2954; dazu siehe ebenfalls unten 4.8
17 BGBl. 1994 I, 2278
18 BGBl. 1994 I, 2325; dazu siehe unten 5.2
19 BGBl. 1994 I, S. 3475; siehe dazu unten 4.14

20 1 BvR 1968/88, BVerfGE 90, 255
21 BVerfGE 90, 263
22 BVerfGE 90, 271
23 Beschluß vom 11. Oktober 1994 – 1 BvR 1398/93 –, NJW 1995, 40

ständige sein Gutachten auf statistisch erfaßtes oder allgemein zugängliches Tatsachenmaterial aufbaut oder sich auf Erfahrungswissen und wissenschaftlich begründete Einsichten stützt.

Der *Bundesgerichtshof* hat in einer vor allem in den neuen Bundesländern zum Teil kritisch aufgenommenen Entscheidung einer Bürgerbewegung in Halle untersagt, in einer öffentlich ausgelegten *Liste mit den Klarnamen*, Decknamen, Personenkennziffern sowie Einsatzorten und -richtungen *von mehreren tausend angeblichen inoffiziellen Mitarbeitern des Ministeriums für Staatssicherheit* ohne nähere Angaben über Art und Umfang der jeweiligen IM-Tätigkeit auch den Namen einer Person zu veröffentlichen, die als IM weder eine exponierte Stellung innehatte noch heute im öffentlichen Leben eine herausgehobene Position bekleidet[24]. Der Bundesgerichtshof betonte, die in der Namensnennung liegende *Prangerwirkung* müsse der Betroffene nicht hinnehmen.

In der Presse wurde der Inhalt dieser Entscheidung insoweit teilweise unzutreffend wiedergegeben, als mitgeteilt wurde, der Bundesgerichtshof habe jedem inoffiziellen Mitarbeiter des Ministeriums für Staatssicherheit das Recht zugestanden, die Veröffentlichung seines Namens zivilrechtlich zu unterbinden. Wie sich aus den Urteilsgründen ergibt, war dagegen für das Gericht die massenweise undifferenzierte Veröffentlichung von Daten angeblicher inoffizieller Mitarbeiter ausschlaggebend. Selbst für den Fall, daß der Kläger tatsächlich inoffizieller Mitarbeiter der Staatssicherheit gewesen sei, liege in dieser Form der Veröffentlichung ein rechtswidriger Eingriff in sein informationelles Selbstbestimmungsrecht. Bemerkenswert an dieser Entscheidung ist die generelle Feststellung des Gerichts, daß das Recht auf informationelle Selbstbestimmung nicht nur vor einer überzogenen Ausforschung von personenbezogenen Daten durch den Staat schützt, sondern dem Schutzbedürfnis des Einzelnen auch auf der Ebene bürgerlich-rechtlicher Verhältnisse einen entsprechend hohen Rang gegenüber Eingriffen zuweist, die ihn gegen seinen Willen für die Öffentlichkeit „verfügbar" machen. In diesem Punkt stimmt die Rechtsprechung des Bundesgerichtshofs mit der des Bundesverfassungsgerichts und des Bundesarbeitsgerichts überein.

Demgegenüber räumt der Bundesgerichtshof dem Fernmeldegeheimnis offenbar einen wesentlich geringeren Stellenwert ein als das Bundesverfassungsgericht. Dieses hatte in seinem Fangschaltungsbeschluß[25] festgestellt, daß zwar jeder Fernsprechteilnehmer ohne Grundrechtsverstoß Dritte von seinen Telefongesprächen nach deren Beendigung unterrichten könne, jedoch nicht mit Wirkung für den anderen Gesprächsteilnehmer gegenüber der Telekom oder anderen staatlichen Stellen auf die Wahrung des Fernmeldegeheimnisses verzichten könne. Vielmehr sei jede staatliche Einschaltung, die nicht im Einverständnis mit beiden Kommunikationspartnern erfolge, ein Grundrechtseingriff. Demgegenüber hat der Bundesgerichtshof in einer neueren Entscheidung die Einrichtung einer *„Hörfalle"*, also das Mithören eines Telefongesprächs durch einen Polizeibeamten im Rahmen eines Ermittlungsverfahrens über einen Zweithörer (Hörmuschel) dann für rechtmäßig gehalten, wenn der Benutzer des Anschlusses, an dem dieser Zweithörer angebracht ist, ihm das gestattet hat; dies gelte auch dann, wenn der Polizist das Gespräch ohne Wissen des anderen Teilnehmers mithöre[26]. Im konkreten Fall hatte die Polizei eine Zeugin gebeten, einen Tatverdächtigen anzurufen und das Mithören über einen Zweithörer durch einen Polizeibeamten zu gestatten. Eine richterliche oder staatsanwaltliche Anordnung wurde nicht eingeholt. Der Angerufene räumte bei diesem Gespräch gegenüber der Zeugin seine Beteiligung an einer Straftat ein und wurde anschließend aufgrund der Aussage des mithörenden Polizeibeamten verurteilt. Der Bundesgerichtshof vertrat die Auffassung, durch das Vorgehen der Polizei sei nicht in das Fernmeldegeheimnis des Angerufenen eingegriffen worden, da die Anruferin dem Polizeibeamten ebenso wie jeder Privatperson das Mithören gestatten durfte. Auch eine Verletzung des Persönlichkeitsrechts sei nicht gegeben, da angesichts der Entwicklung im Fernsprechbereich jeder, der sich eines Fernsprechers bedient, damit rechnen müsse, daß privaten Telefonanschlüssen Mithörgeräte angeschlossen sind und benutzt werden; darauf, daß dies unterbleibt, dürfe er grundsätzlich auch dann nicht vertrauen, wenn er von seinem Gesprächspartner keinen Hinweis auf den Anschluß eines solchen Geräts erhält. Dies gilt auch für die Benutzung der inzwischen weit verbreiteten Lautsprecher, die in dem Telefonapparat integriert sind und die Stimme des Gesprächspartners für alle im Raum anwesenden Personen hörbar machen. Diese Entscheidung des Bundesgerichtshofs droht, die engen Voraussetzungen der Strafprozeßordnung für das Abhören von Telefongesprächen und den Einsatz von V-Personen obsolet zu machen. Auch zwingt sie den einzelnen Fernsprechteilnehmer - selbst wenn nicht gegen ihn wegen des Verdachts einer Straftat ermittelt wird - dazu, gravierende Einschränkungen der Vertraulichkeit seiner Telefonate schon deshalb hinzunehmen, weil die Technik heute problemlos das Mithören von Telefongesprächen mit Hilfe von Zusatzlautsprechern und anderen Mithöreinrichtungen gestattet.

Die Sozialämter gehen immer mehr dazu über, den Hilfeempfängern die Sozialhilfe bargeldlos auszuzahlen, also auf ein Girokonto bei der Bank zu überweisen. Sieht man einmal von den Schwierigkeiten ab, in die der Hilfeempfänger durch die noch immer vorherrschende Praxis der Banken gerät, kein Girokonto ausschließlich auf Guthabenbasis zu eröffnen und stattdessen auf der Einholung einer Schufa-Auskunft zu bestehen, gewinnt ein anderes Problem an Bedeutung, das uns in der Vergangenheit bereits beschäftigt hat: Darf das Sozialamt (gleiches gilt für das Arbeitsamt oder die Krankenkasse) auf dem Überweisungsträger gegenüber dem Kreditinstitut den Zahlungsgrund „Sozialleistung" angeben? Das *Bundesverwaltungsgericht* hat diese Frage jetzt verneint[27]. Die Angabe des Zahlungsgrundes in dieser Form sei eine nicht erforderliche und deshalb unzulässige Offenbarung eines Sozialdatums. Auch wenn der Hilfeempfänger ohne diese Angabe möglicherweise Gefahr laufe, daß der überwiesene Betrag von einem Gläubiger gepfändet werde, müsse es ihm überlassen bleiben, sich zwischen Pfändungsschutz und Sozialdatenschutz zu entscheiden. Er könne - wenn er eine Kontenpfändung von vornherein ausschließen wolle - in die Angabe des Zahlungsgrundes „Sozialleistung" einwilligen. Solange er dies nicht tue, dürfe als Zahlungsgrund kein Hinweis auf eine Sozialleistung gegeben werden. Selbst dann wäre das Kreditinstitut, das aus dem nicht ausdrücklich als Sozialleistung bezeichnetem Betrag Zahlungen an einen Gläubiger des Hilfeempfängers leistet, diesem gegenüber nochmals zur Zahlung verpflichtet.

Immer wieder wird uns von Bürgern und Behörden die Frage gestellt, in welchem Umfang sich Personen auf den Datenschutz berufen können, die der Verwaltung Hinweise auf das (vermeintlich) strafbare oder ordnungswidrige Verhalten anderer Personen geben. Mit dieser Frage hat sich im Berichtszeitraum auch der *Bundesfinanzhof* beschäftigt[28]. Seine Entscheidung hat nicht nur Bedeutung für das Steuerrecht, sondern auch für andere Bereiche. Der Bundesfinanzhof stellt zunächst klar, daß auch der Name des *Informanten/Denunzianten* dem Steuergeheimnis unterliegt. Zudem hätten auch Informanten einen Anspruch auf den Schutz ihres allgemeinen Persönlichkeitsrechts. Allerdings seien die Finanzbehörden verpflichtet, in einem Strafverfahren wegen falscher Verdächtigung oder Beleidigung den Namen des Informanten gegenüber den Strafverfolgungsbehörden zu offenbaren, wenn durch dessen Handlung das allgemeine Persönlichkeitsrecht des von der Anzeige Betroffenen verletzt werde. Wer zu Unrecht strafrechtlichen Ermittlungstätigkeiten ausgesetzt werde, könne ein berechtigtes Interesse daran haben, den Namen des Informationsgebers zu erfahren. Hat der Informant falsche Angaben gemacht, so muß er mit einem Strafverfahren wegen falscher Verdächtigung, Beleidigung oder übler Nachrede rechnen. Außerhalb des Steuerrechts können sich Auskunftsansprüche des Betroffenen, über den der Informant Angaben gemacht hat, aus dem Datenschutzrecht oder dem Verfahrensrecht ergeben.

Das *Bundesarbeitsgericht* hat sich zu einer Frage geäußert, die auch im Bereich der Berliner Verwaltung entstehen kann: Unter welchen Voraussetzungen kann ein Betriebs- oder Personalrat der beabsichtigten Versetzung eines Beschäftigten auf einen Arbeitsplatz als *betrieblicher oder behördlicher Datenschutzbeauftragter* die

24 BGH, Urteil vom 12. Juli 1994 - VI ZA 1/94 -
25 BVerfGE 85, 386, 399; vgl. Jahresbericht 1992, 1.1
26 BGH, Urteil vom 8. Oktober 1993 - 2 StR 400/93 -, NJW 1994, 596
27 Urteil vom 23. Juni 1994; NJW 1995, 410
28 Urteil vom 8. Februar 1994 - VII R 88/92 -

Zustimmung verweigern? Das Bundesarbeitsgericht hatte diese Frage auf der Grundlage des Betriebsverfassungsgesetzes für die Privatwirtschaft zu klären, seine Festlegungen haben jedoch auch für den öffentlichen Bereich Gültigkeit. Danach kann der Betriebsrat seine Zustimmung mit der Begründung verweigern, der Beschäftigte besitze nicht die nach dem Bundesdatenschutzgesetz vorausgesetzte Fachkunde und Zuverlässigkeit[29]. Bedenken gegen die Zuverlässigkeit können sich daraus ergeben, daß der Arbeitnehmer neben seiner Aufgabe als Datenschutzbeauftragter Tätigkeiten ausübt, die mit seiner Kontrollfunktion unvereinbar sind, weil sie den Arbeitnehmer in einen Interessenkonflikt geraten lassen. Zur Vermeidung solcher Interessenkonflikte haben wir in der Vergangenheit Empfehlungen ausgesprochen[30].

Mit der *Zulässigkeit von verdeckten Aidstests* bei der Einstellung von Bediensteten der Europäischen Kommission hat sich der *Europäische Gerichtshof* auseinandergesetzt[31]. Dabei hat der Gerichtshof seine Auffassung unterstrichen, daß das in Art. 8 der Europäischen Menschenrechtskonvention verankerte Recht auf Achtung des Privatlebens, das sich aus den gemeinsamen Verfassungstraditionen der Mitgliedstaaten herleitet, ein von der Gemeinschaftsrechtsordnung geschütztes Grundrecht darstellt. Dieses umfaßt insbesondere das Recht einer Person, ihren Gesundheitszustand geheim zu halten. Im konkreten Fall hatte ein Bewerber um eine befristete Anstellung bei der Kommission es ausdrücklich abgelehnt, sich einem HIV-Test zu unterziehen. Daraufhin waren ohne sein Wissen Blutuntersuchungen vorgenommen worden, deren Ergebnisse indirekt den Verdacht einer Aids-Erkrankung nahelegten. Dieses Vorgehen hat der Europäische Gerichtshof als unzulässig bezeichnet. Allerdings seien die Gemeinschaftsorgane nicht zur Einstellung des Betroffenen verpflichtet, wenn dieser nach einer entsprechenden Aufklärung seine Zustimmung zu einer vom Arzt für erforderlich gehaltenen Untersuchung verweigere. Die Entscheidung betraf formal zwar lediglich die Einstellungspraxis der Europäischen Kommission, sie hat aber auch Auswirkungen auf die Praxis der Dienstbehörden in den Mitgliedstaaten, soweit diese in vergleichbarer Weise verfahren.

Das Europäische Datenschutzrecht kommt langsam voran

Die Bemühungen zur Formulierung eines einheitlichen europäischen Mindeststandards im Datenschutzrecht sind insofern ein gutes Stück vorangekommen, als der Rat der Europäischen Union am 22. Dezember 1994 eine politische Einigung im Hinblick auf die Festlegung eines Gemeinsamen Standpunktes zum *Entwurf der Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*[32] erzielt hat.

Der Richtlinienentwurf enthält in einer Reihe von Punkten auch Verbesserungen gegenüber dem geltenden deutschen Datenschutzrecht. So wird die Datenerhebung auch im privaten Bereich den Datenschutzregelungen unterworfen, was bisher nach dem Bundesdatenschutzgesetz nicht der Fall ist. Besonders sensible Daten, etwa über rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit sowie Gesundheit oder Sexualleben genießen einen besonderen, über das deutsche Datenschutzrecht hinausgehenden Schutz vor Nutzung oder Weitergabe. Die Rechte der Betroffenen werden erweitert; sie sind regelmäßig über Speicherung oder Weitergabe ihrer Daten zu unterrichten. In bestimmten Fällen erhalten sie ein Widerspruchsrecht gegen die Verarbeitung ihrer Daten. Für die Datenverarbeitung werden neuartige Qualitätsanforderungen formuliert, die das bisher nur im englischen Datenschutzrecht vorhandene Prinzip der „fairen Datenverarbeitung" deutlicher als bisher zum Ausdruck bringen. Schließlich muß die Unabhängigkeit der Aufsichtsbehörde für den privaten Bereich sichergestellt werden.

Sobald die Datenschutzrichtlinie endgültig beschlossen worden ist, wird auch der Berliner Gesetzgeber zu prüfen haben, inwieweit das Berliner Datenschutzgesetz den europäischen Vorgaben angepaßt werden muß.

Von der Erweiterung der Europäischen Union um die drei Länder Österreich, Finnland und Schweden sind Impulse für die Weiterentwicklung eines europäischen Informationsrechts zu erwarten. Bemerkenswert ist vor allem, daß die schwedische Regierung ihre Beitrittserklärung mit einem Vorbehalt versehen hat, wonach sie die weitgehenden Informationszugangsrechte für die Bürger Schwedens auch nach dem Beitritt zur Union nicht einschränken werde. Umgekehrt ist zu hoffen, daß durch die Erweiterung der Union auch die Bemühungen um eine größere Transparenz der Entscheidungen in den europäischen Gremien[33] unterstützt werden und daß darüber hinaus auch in Deutschland frühere Vorschläge für eine allgemeine Informationsfreiheitsgesetzgebung wieder aufgegriffen werden.

1.2 Datenschutz in Berlin

Informationsfreiheit und Datenschutz in der Diskussion über die Reform der Berliner Verfassung

Bereits frühzeitig hatten wir der Enquete-Kommission „Verfassungs- und Parlamentsreform" des Berliner Abgeordnetenhauses detaillierte Vorschläge zur Präzisierung des Grundrechts auf Datenschutz, zur Aufnahme eines allgemeinen Akteneinsichtsrechts und zur Verankerung des Berliner Datenschutzbeauftragten in der Verfassung von Berlin gemacht, die von der Kommission nur zum Teil aufgegriffen worden sind.

Kurz vor der Vereinigung Berlins im Jahre 1990 hat das Abgeordnetenhaus die Grundrechtsqualität des Datenschutzes durch die Aufnahme einer sehr knappen Grundrechtsgarantie im neuen Artikel 21 b der Verfassung von Berlin anerkannt, der zudem noch einem allgemeinen Gesetzesvorbehalt unterliegt. Zuvor hatte bereits die Stadtverordnetenversammlung im ehemaligen Ostteil Berlins eine detaillierte Garantie des Rechtes auf informationelle Selbstbestimmung in die von ihr im Juli 1990 verabschiedete Verfassung aufgenommen, die Grundlage für die Überarbeitung der geltenden Verfassung werden sollte. Auch die Verfassung des Landes Brandenburg knüpft mit ihrem Grundrecht auf Datenschutz an die von der Berliner Stadtverordnetenversammlung beschlossene Formulierung an und enthält zusätzliche Klarstellungen. Unserem entsprechenden Vorschlag hat sich die Mehrheit der Enquete-Kommission nicht angeschlossen[34].

Im Berichtszeitraum erhielten wir insbesondere Gelegenheit, der Kommission unseren Vorschlag für ein allgemeines Akteneinsichtsrecht anhand einer rechtsvergleichenden Analyse im einzelnen zu erläutern. Eine (einfache) Mehrheit in der Kommission fand allerdings lediglich der hinter unseren Empfehlungen zurückbleibende Vorschlag für ein beschränktes Zugangsrecht zu Daten der Verwaltung über die Umwelt und die natürlichen Lebensgrundlagen, verbunden mit der allgemeinen Verpflichtung, das Verwaltungshandeln nach Maßgabe gesetzlicher Regelung durch Auskunfts- und Einsichtsrechte transparent zu machen[35]. Eine Annahme dieses Vorschlages wäre immerhin ein - wenn auch kleiner - Schritt in die richtige Richtung.

Das Bundesverfassungsgericht hat mehrfach die Bedeutung einer unabhängigen Kontrollinstanz zur Wahrung des informationellen Selbstbestimmungsrechtes und im Interesse eines vorgezogenen Rechtsschutzes des Bürgers betont. Dementsprechend sehen auch alle neueren Landesverfassungen die Verankerung der Institution des Datenschutzbeauftragten vor. Insoweit ist es zu begrüßen, daß die Enquete-Kommission einstimmig die Aufnahme eines Artikels in die Verfassung von Berlin befürwortet hat, wonach das Abgeordnetenhaus „zur Wahrung des Grundrechts auf Datenschutz und als Hilfsorgan" einen Datenschutzbeauftragten wählt[36]. Unserem weitergehenden Vorschlag, Aufgaben und Befugnisse des Datenschutzbeauftragten in der Verfassung etwas genauer festzulegen, ist die Kommission allerdings nicht gefolgt.

29 BAG, Beschluß vom 22. März 1994 - 1 ABR 51/93 -
30 Jahresbericht 1991, 2.5.1 und Anlage 4
31 EuGH, Urteil vom 5. Oktober 1994 - Rs. C-404/92 P -, NJW 1994, 3005
32 vgl. Jahresbericht 1993, 1.1

33 vgl. dazu die Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Poppe, BT-Drs. 12/8569
34 Schlußbericht der Enquete-Kommission „Verfassungs- und Parlamentsreform", Art. 12/4376, 29
35 Drs 12/4376, 28 (Art. 21 a Abs. 2 - neu, Art. 50 Abs. 3 - neu)
36 Drs 12/4376, 14 (Art. 32 b Abs. 1 - neu); wortgleich insofern auch der Antrag des Abg. Herbst und anderer Abgeordneter, Drs. 12/4874

Mit der Wahl des Datenschutzbeauftragten „als Hilfsorgan" des Abgeordnetenhauses soll er in die Nähe des Parlamentes gerückt werden und dessen Aufgabe unterstützen, damit die erste Gewalt gestärkt und die Verantwortung der Abgeordneten erhöht werden, „ihre Aufgaben ernst zu nehmen"[37].

Diese Zielsetzung ist zu begrüßen, da das Parlament gerade in Zeiten des zunehmenden Vordringens der Informations- und Kommunikationstechnik immer weniger in der Lage sein wird, eine effektive Kontrolle der Regierung sowie seine Einflußnahme auf die gesellschaftliche Entwicklung mit den herkömmlichen parlamentarischen Mitteln zu gewährleisten[38].

Die vorgeschlagenen Formulierungen erfüllen diese Zielsetzung gleichwohl nicht in hinreichender Weise.

Die Wahrnehmung der Aufgaben des Datenschutzbeauftragten setzt regelmäßig nicht nur intensiven Kontakt mit allen Bereichen der öffentlichen Verwaltung, sondern auch die Möglichkeit voraus, jederzeit diejenigen Unterlagen und Daten der öffentlichen Stellen einzusehen, die er für die Wahrnehmung seiner umfassend definierten Aufgaben für erforderlich hält. Seinen Aufgaben zur Wahrung des Grundrechts auf informationelle Selbstbestimmung kann er nur entsprechen, wenn er - insbesondere angesichts der ihm eingeräumten äußerst geringen Ressourcen - unabhängig über befaßte Themen und Art und Weise des Vorgehens bestimmen kann. Beide Aspekte lassen sich nicht mit den Rechten vereinbaren, die nach der staatsrechtlichen Lehrmeinung dem Parlament selbst zukommen. So bleibt die im Schlußbericht der Enquete-Kommission und im Entwurf für ein 28. Gesetz zur Änderung der Berliner Verfassung vorgesehene Erweiterung der Rechte des einzelnen Abgeordneten (Art. 29 Absätze 2 und 3) hinter den Zugangs- und Einsichtsrechten des Datenschutzbeauftragten zurück, die diesem nach geltendem Gesetzesrecht und aufgrund der Rechtsprechung des Bundesverfassungsgerichts zustehen müssen.

Die derzeitige Konstruktion des Berliner Datenschutzbeauftragten als Oberste Landesbehörde, die auf dem Weg der Dienstaufsicht der Präsidentin bzw. des Präsidenten des Abgeordnetenhauses einerseits, jederzeitiger Berichtspflichten und Rederechte andererseits in die erste Gewalt eingebunden ist, ist eine bewährte, auch in der allgemeinen Datenschutzdiskussion anerkannte Lösung. Sie verbindet einen von parlamentsrechtlichen Vorbehalten losgelösten Befugnisraum einerseits mit der Möglichkeit des Parlaments andererseits, jederzeit zu eigenen Kontrollzwecken auf das Instrumentarium des Datenschutzbeauftragten zuzugreifen bzw. von diesem jederzeit Hinweise auf das Erfordernis eigener Aktivitäten zu erhalten.

Schließlich entspräche es in besonderem Maße der Rechtsprechung des Bundesverfassungsgerichts, wenn die dort für unabdingbar erklärte Unabhängigkeit des Datenschutzbeauftragten in der geschriebenen Verfassung zum Ausdruck käme.

Die weißen Flecken auf der Landkarte des Datenschutzes werden kleiner

Der Landesgesetzgeber hat auch in Berlin im vergangenen Jahr in einer Reihe von fachspezifischen Gesetzen weitere Datenschutzregelungen getroffen. Dies entspricht der Vorgabe im Berliner Datenschutzgesetz, das seinerseits besondere Befugnisse zur Verarbeitung personenbezogener Daten voraussetzt, sie aber nicht ersetzen soll. In dem Maße, wie der Datenschutz bereichsspezifisch geregelt wird, treten die Vorschriften des allgemeinen Berliner Datenschutzgesetzes in den Hintergrund. Sie behalten aber die Funktion, einen datenschutzrechtlichen Mindeststandard zu beschreiben, der von den speziellen gesetzlichen Vorschriften nicht unterschritten werden darf.

Das neue *Berliner Schiedsamtsgesetz*[39] enthält seit dem 1. Juli 1994 eine - wenngleich recht allgemein gehaltene - Befugnis der Gerichte und Behörden zur Übermittlung von personenbezogenen Informationen im Zusammenhang mit der Wahl, Bestätigung, Ablehnung oder Amtsenthebung einer Schiedsperson.

Mit dem am 16. Juli 1994 in Kraft getretenen *Gesetz zur Änderung des Gesetzes zur Ausführung des Bundessozialhilfegesetzes*[40] wurde die landesrechtliche Voraussetzung dafür geschaffen, daß auch im Land Berlin im Rahmen des BASIS-Verfahrens der im geänderten Bundessozialhilfegesetz vorgesehene Datenabgleich zwischen den Sozialämtern durchgeführt werden kann, sobald die Rechtsverordnung nach § 117 BSHG erlassen ist. Dieses ist allerdings noch nicht geschehen.

Das *Berliner Architekten- und Baukammergesetz*[41] vom Juli 1994 enthält erstmals detaillierte Befugnisse zur Verarbeitung personenbezogener Daten, die seit Anfang 1993 auch im Berliner Kammergesetz (betreffend die Ärzte, Zahnärzte, Tierärzte und Apotheker) enthalten sind.

Bereits im April 1993 war durch das *22. Gesetz zur Änderung des Landesbeamtenrechts*[42] eine Regelung in das Landesbeamtengesetz eingefügt worden, nach der die Dienstbehörde nur bei konkreten Zweifeln am festgestellten Ergebnis einer amtsärztlichen Untersuchung des Beamten berechtigt ist, von dem untersuchenden Arzt die maßgebenden Untersuchungsbefunde anzufordern, soweit deren Kenntnis für die Dienstbehörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit für die von ihr zu treffende Entscheidung (insb. vorzeitige Pensionierung) erforderlich ist. In allen anderen Fällen darf der Amtsarzt der Dienstbehörde nur mitteilen, ob der Beamte ganz oder teilweise dienstunfähig ist. Wir hatten in der Vergangenheit mehrfach bemängelt, daß von diesem Grundsatz auch ohne ausdrückliche gesetzliche Regelung abgewichen wurde.

Im Bereich des öffentlichen Dienstrechts stehen in Berlin allerdings bundesrechtlich vorgeschriebene datenschutzrechtliche Spezialregelungen nach wie vor aus: So fehlt neben einem Sicherheitsüberprüfungsgesetz auch die seit Anfang 1993 durch das 9. Dienstrechtsänderungsgesetz des Bundes vorgeschriebene datenschutzgerechte Regelung des Personalaktenrechts. Die Senatsverwaltung für Inneres hat die Verzögerungen im Unterausschuß „Datenschutz" damit begründet, daß weitere Änderungen des Landesbeamtengesetzes aufgrund des Beamtenrechtsrahmengesetzes mit der Novelle zum Personalaktenrecht verbunden werden sollten[43]. Mittlerweile ist das 23. Gesetz zur Änderung des Landesbeamtenrechts in Kraft getreten[44], das nur eine einzige Vorschrift enthält, die die Erstattung von Reise- und Umzugskosten auf die 2. Klasse bei Bahnfahrten begrenzen soll. Das Beispiel verdeutlicht, daß schnelle Änderungen des Beamtenrechts durchaus möglich sind, wenn der politische Wille dafür gegeben ist. Dies scheint bei der notwendigen Anpassung des Landesbeamtenrechts an die Vorgaben des Bundesrechts im Bereich des Datenschutzes nicht der Fall zu sein.

Auch das seit längerem beratene Gesetz über die Rechtsstellung der bezirklichen Gleichstellungs-/Frauenbeauftragten, das auch deren Befugnisse zur Verarbeitung personenbezogener Daten regeln soll, steht noch immer aus.

Dagegen sind inzwischen alle Rechtsverordnungen, die zur Ergänzung des *Gesetzes über die Schaffung bereichsspezifischer Regelungen für die Verarbeitung personenbezogener Daten (Artikelgesetz)*[45] notwendig waren, erlassen worden. Sie betreffen folgende Bereiche:

- die Deutsche Dienststelle für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen Deutschen Wehrmacht (WASt)[46],
- die Berliner Stadtreinigungsbetriebe (BSR), die Berliner Verkehrsbetriebe (BVG) und die Berliner Wasserbetriebe (BWB)[47],
- den öffentlichen Gesundheitsdienst[48],

37 So der Abg. Longolius in der Sitzung des Abgeordnetenhauses am 9. Juni 1994
38 vgl. dazu unten 3.3
39 GVBl. 1994, 109
40 GVBl. 1994, 238; vgl. 3.1
41 GVBl. 1994, 253
42 GVBl. 1993, 187
43 vgl. Jahresbericht 1992, 4.2.7
44 GVBl. 1994, 511
45 vgl. Jahresberichte 1992, 1.2 und 1993, 1.2
46 WASt-Verordnung vom 29. März 1994, GVBl. 1994, 107
47 Verordnung vom 30. Juni 1994, GVBl. 1994, 229
48 VO über die Verarbeitung personenbezogener Daten in Einrichtungen des öffentlichen Gesundheitsdienstes vom 30. Juni 1994, GVBl. 1994, 239; vgl. dazu das neu gefaßte Gesundheitsdienst-Gesetz vom 4. August 1994, GVBl. 1994, 329

– die Schulen[49],

– das Emissionskataster nach dem Bundesimmissionsschutzgesetz[50] und

– die Bewährungshilfe für Jugendliche und Heranwachsende[51].

Auch das Gesetz über die Datenverarbeitung für Zwecke der räumlichen Stadtentwicklung, Stadt- und Regionalplanung und bodenwirtschaftliche Aufgaben *(Stadtplanungsdatenverarbeitungsgesetz)*[52] trat am 12. November 1994 in Kraft und ersetzte die bereits Ende 1993 außer Kraft getretenen Bestimmungen im Ausführungsgesetz zum Baugesetzbuch.

Lediglich die im *Kita-Kostenbeteiligungsgesetz* vorgesehene Rechtsverordnung über Art und Umfang der Verarbeitung personenbezogener Daten ist noch immer nicht erlassen worden, obwohl die vom Gesetzgeber hierfür vorgesehene Frist bereits am 31. Dezember 1993 verstrichen ist. Der Erlaß einer solchen Rechtsverordnung ist – abgesehen davon, daß der Gesetzgeber sie vorgeschrieben hat – notwendig, weil die Eltern zur Ermittlung eines ermäßigten Kostenbeitrags für die Kindertagesstätten umfangreiche Angaben über ihre Einkommensverhältnisse zu machen haben, die von den Jugendämtern zur Ermittlung der Höhe der Kostenbeteiligung verarbeitet werden müssen. Die nach der Landeshaushaltsordnung erlassene Verordnung über die Verarbeitung personenbezogener Daten des Haushaltswesens enthält dafür keine Rechtsgrundlage.

Die bereichsspezifischen Regelungen des Artikelgesetzes zur Verarbeitung von Bürgerdaten bilden zusammen mit den inzwischen erlassenen Rechtsverordnungen und dem ergänzend heranzuziehenden Berliner Datenschutzgesetz für große Teile der Berliner Verwaltung jetzt eine klare Grundlage für die Verarbeitung personenbezogener Daten. Der Vorrang, den das Berliner Datenschutzgesetz den bereichsspezifischen Regelungen entsprechend der Rechtsprechung des Bundesverfassungsgerichts eingeräumt hat, ist damit im Berliner Landesrecht weitgehend umgesetzt worden.

Zwar wurde im Berichtszeitraum ein Antrag der Fraktionen der CDU und der SPD im Abgeordnetenhaus eingebracht, der auf eine Änderung des Berliner Datenschutzgesetzes abzielte, die die geleistete Arbeit des Gesetzgebers zur Schaffung normenklarer Rechtsgrundlagen für die Datenverarbeitung weitgehend überflüssig gemacht hätte[53]. Dieser Antrag wurde im Berichtszeitraum allerdings nicht mehr in den Parlamentsausschüssen beraten.

Zusammenarbeit mit dem Land Brandenburg

Berlin und Brandenburg sind – unabhängig davon, ob es letztlich zu einer Vereinigung kommt oder nicht – zunehmend aufeinander angewiesen. Das zeigt die steigende Zahl von Staatsverträgen, die zwischen beiden Ländern ausgehandelt und abgeschlossen werden. So ist am 1. Januar 1994 der *Staatsvertrag über die Errichtung der Zentralen Adoptionsstelle Berlin-Brandenburg (ZABB)*[54] in Kraft getreten. Vom Parlament beschlossen worden ist auch das *Gesetz zum Staatsvertrag über die Errichtung einer „Stiftung Preußische Schlösser und Gärten Berlin-Brandenburg"*[55], dessen Inkrafttreten allerdings noch aussteht. Beide Staatsverträge enthalten keine besonderen Regelungen über die länderübergreifende Datenverarbeitung. Sie fallen deshalb erheblich hinter den Standard des Berlin-Brandenburgischen Rundfunkstaatsvertrages[56] zurück, der sowohl Regelungen zum materiellen Datenschutzrecht als auch zur Datenschutzkontrolle enthält. Es wäre zu wünschen, daß bei zukünftigen Staatsverträgen, die bis zu einer möglichen Vereinigung abgeschlossen werden, die beiden Länder sich am Modell des Rundfunkstaatsvertrages orientieren würden.

49 VO über die Verarbeitung personenbezogener Daten nach § 5 a des Schulgesetzes für Berlin (SchuldatenVO) vom 13. Oktober 1994, GVBl. 1994, 435

50 VO über die Verarbeitung personenbezogener Daten im Zusammenhang mit nicht genehmigungsbedürftigen Anlagen vom 18. Oktober 1994, GVBl. 1994, 464

51 VO über die automatisierte Verarbeitung personenbezogener Daten durch die Bewährungshelfer/-innen für Jugendliche und Heranwachsende in Berlin vom 8. Oktober 1993, GVBl. 1993, 468

52 GVBl. 1994, 444; vgl. dazu unter 4.12

53 Drs 12/4028

54 GVBl. 1994, 202, 514

55 GVBl. 1994, 515

56 vgl. Jahresbericht 1992, 1.2

2. Technische Rahmenbedingungen

2.1 Entwicklung der Informationstechnik und deren Auswirkung auf die Berliner Verwaltung

Neben den alljährlich zu beobachtenden Trends wie

– die weitere Verbesserung des Preis-/Leistungsverhältnisses für Informations- und Kommunikationstechnik,

– die weitergehende Miniaturisierung der Hardware,

– die insbesondere in Hinblick auf die Benutzeroberflächengestaltung immer komplexer werdende Standardsoftware,

– die zunehmende Vernetzung,

– die weitergehende Integration von Sprach- und Datenkommunikation,

– die Einbeziehung von stehenden und bewegten Bildern (Multimedia),

– der Rückgang proprietärer Systeme zugunsten des Anwachsens mehr oder weniger offener Systeme (Downsizing),

– das Vordringen chipkarten-orientierter Anwendungen,

– die zunehmende Auslagerung von IuK-Dienstleistungen an Dritte (Outsourcing)

sind einige Tendenzen, die sich ebenfalls seit längerem entwickelten, in das Augenmerk der für Informations- und Kommunikationstechnik Verantwortlichen geraten. Dies nicht zuletzt deshalb, weil die Fachpresse, aber auch die allgemeine Berichterstattung der Medien ihnen besondere Aufmerksamkeit verliehen:

– die weltweite Datenkommunikation über das Internet,

– die Client-Server-Architekturen der lokalen Netze,

– die Nutzung optischer Speichermedien,

– von den Laptops über die Notebooks zu den Palmtops.

Die Welt am Netz: Das Internet

Das Internet ist ein weltumspannender Verbund von Computern unterschiedlichster Art. Es entstand in den 70er Jahren aus dem Arpanet (Advanced Research Project Agency) des US-Verteidigungsministeriums. Das Netz hat eine sprunghafte Entwicklung erfahren: Waren 1984 1000 Computer angeschlossen, so waren 1989 bereits 100 000 und drei Jahre später bereits 1 Million Systeme (hosts) im INTERNET angeschlossen. Derzeit nehmen 35 Millionen Benutzer an der Internet-Kommunikation teil, bei gleichmäßiger Weiterentwicklung wird davon ausgegangen, daß 1995 etwa 200 Millionen Personen mit dem Internet arbeiten werden.

Die im Internet *angebotenen Dienste* haben ebenfalls eine erhebliche qualitative Entwicklung genommen. Zunächst wurde das Netz vorwiegend für elektronische Post (electronic mail), Datenübertragung (file transfer) und die Benutzung entfernter Systeme (remote login) verwendet. Mittlerweile werden zusätzlich komplexere Mehrwertdienste angeboten:

– Mit dem Dokument-Informationssystem „Gopher" werden weltweit Dokumente zu bestimmten Fachthemen zum Abruf bereit gehalten. Gesetzestexte, Kommentare, Fachbeiträge zu allen Wissensgebieten können über Internet verbreitet und gelesen werden.

– Das „World Wide Web – WWW" bietet unter einer sehr komfortablen Benutzeroberfläche aktuelle Informationen zu allen möglichen Themen (z. B. über das Internet selbst, Wetterkarten aus Kalifornien, Kinoprogramm aus Berlin) an. Diese Informationen werden auf speziellen WWW-Servern katalogisiert und bereitgehalten.

Mit dem Internet kommt man also dem Traum vom schnellen, weltweit agierenden, fachübergreifenden und billigen Informationsnetz für „jedermann" ein erhebliches Stück weiter. Für Beträge in der Größenordnung der monatlichen Telefonrechnung eines durchschnittlichen Haushaltes kann jeder Benutzer des Internet werden, der einen leistungsfähigen Personalcomputer und ein passendes Modem sein eigen nennt.

Auch diverse *öffentliche Stellen des Landes Berlin* insbesondere im Hochschulbereich nehmen am Internet teil. Über das im Aufbau begriffene Metropolitan Area Network (MAN) Berlins[57] wollen auch die anderen öffentlichen Stellen Anschluß an die globale Informationsquelle Internet erlangen. Dies bedeutet, daß entsprechende Übergänge (gateways) vom neuen Berliner Verwaltungsnetz in das Internet geschaffen werden müssen.

Ein zur beliebigen Nutzung durch jeden bereitgehaltenes offenes Datennetz wie das Internet erzeugt jedoch erhebliche *Sicherheitsrisiken* für die angeschlossenen Systeme und Netze sowie die Daten, die verarbeitet bzw. transportiert werden. Nutzungsbeschränkungen stehen der Philosophie des Internets prinzipiell entgegen. So bleibt es Aufgabe der Betreiber angeschlossener Systeme und Netze, ihre eigenen Systeme und Daten vor dem unbefugten Zugriff (z. B. über remote login) aus dem Internet zu schützen. Solche „Firewalls" müssen dafür sorgen, daß einerseits die erwünschte Kommunikation und Informationsgewinnung über das Internet auch den Nutzern der eigenen Systeme möglichst uneingeschränkt zur Verfügung stehen, andererseits jedoch Angriffe auf diese Systeme aus dem Internet verläßlich abgewehrt werden.

Die Nutzung des Internet ist derzeit noch im wesentlichen auf den Forschungssektor beschränkt, der von der freien Kommunikation und dem ungehinderten Informationszugang abhängig ist. Die zunehmende Kommerzialisierung des Internet dürfte jedoch dazu führen, daß z. B. auch Produkte über das Internet angeboten, gekauft und bezahlt werden können. Daraus werden sich nicht nur Probleme der technischen Sicherheit und der Verläßlichkeit der Kommunikation ergeben. Auch rechtliche Probleme vielfältiger Art werden sich aus den verschiedenen Nutzungsmöglichkeiten ergeben, die dadurch zusätzlich kompliziert werden, daß zwischenstaatliche Grenzen, selbst Grenzen von Staatengemeinschaften wie der EU und zwischen Blöcken unterschiedlicher Weltanschauung und kultureller und religiöser Hintergründe im Internet nicht existieren.

Client-Server-Systeme

Die bereits im Jahresbericht 1993[58] beschriebene Tendenz zur lokalen Zentralisierung der automatisierten Datenverarbeitung findet in dem Konzept der Client-Server-Systeme eine konsequente Realisierungsform. Lokale Netze bestehen dabei aus einem oder mehreren aus Sicht des Anwenders zentralen Servern, die in die Netztopologie so eingebunden sind, daß sie von den Arbeitsplatzsystemen (Clients) direkt zur Erbringung ihrer Leistung aufgefordert werden können.

Beispiele für solche Client-Server-Systeme sind PC-Netze unter NOVELL, heterogene Netze mit UNIX-Servern und MS-DOS-Personalcomputern, homogene Netze mit UNIX-Servern und UNIX-Workstations oder X-Terminals. Aber auch andere Konfigurationen sind denkbar, insbesondere solche mit mehreren Servern für unterschiedliche Spezialaufgaben (Datenbank-Server, Kommunikations-Server, usw.).

Auf die Sicherheitsprobleme von Client-Server-Systemen sind wir in früheren Jahresberichten bei der Behandlung der Herausforderungen des Downsizing des öfteren eingegangen[59]. Nach wie vor erreichen die meisten in lokalen Netzen eingesetzten Systeme nur ein schwaches IT-Sicherheitsniveau, so ist die Entprofessionalisierung der Systemverwaltung, verbunden mit ihrer mangelhaften Kontrollierbarkeit, eine Schwachstelle, die den Einsatz solcher Systeme für sicherheitsbedürftige Anwendungen bedenklich macht. Zugleich verstärkt sich die Abhängigkeit von organisationsfremder Sachkompetenz und Leistungsbereitschaft.

Es kommt daher umso mehr darauf an, die mit den speziellen Anwendungen, den eingesetzten Systemkonfigurationen und den besonderen Bedingungen der räumlichen, personellen und technischen Systemumgebung verbundenen Risiken sorgfältig und realistisch auf konkrete Bedrohungen bezogen (und nicht mit dem primären Ziel, Argumente für den Verzicht auf kostenträchtige Sicherheitsmaßnahmen zu finden) zu untersuchen. Daraus ist dann zu beurteilen, ob mit den vorgesehenen und gar bestehenden Systemen die notwendige Sicherheit erreichbar ist, wenn ja, welche personellen, organisatorischen und technischen Maßnahmen dafür zu ergreifen sind, und wenn nein, wie durch sinnvolle organisatorische Eingriffe in die Anwendungsumgebung die Sicherheit verbessert werden kann.

So ist der Umgang mit *beweglichen Datenträgern,* insbesondere mit Disketten, in starkem Maße zu reduzieren, da sonst vorsätzliche oder fahrlässige Angriffe auf die Systemsicherheit kaum ausgeschlossen werden können. Daten können auf Disketten kopiert werden, nicht freigegebene Programme oder solche mit bekannten oder unbekannten Schadenswirkungen (Viren) können mit Disketten eingespielt werden. Daher sollte bei Arbeitsplatzsystemen (Clients) grundsätzlich auf die Ausstattung mit Laufwerken für bewegliche Datenträger verzichtet werden.

Außerdem sollten sensible Daten bei der Überspielung auf Festplatten, auf Datenträger für den Datenträgeraustausch und bei der Übertragung auf Datenleitungen *kryptographisch verschlüsselt* werden, damit Angriffe auf diese Datenträger und Übertragungswege sinnlos bleiben und nicht zur Beeinträchtigung der informationellen Selbstbestimmung führen.

Diese Forderungen stehen beispielhaft für viele, die in Sicherheitskonzepten für Client-Server-Systeme einzugehen haben. Muster- oder Standardkonzepte führen dabei meistens nicht viel weiter, da diese spezielle Risikolagen der jeweiligen Anwendungen unberücksichtigt lassen müssen.

Zur Unterstützung der Berliner Verwaltung bei der Erstellung solcher Sicherheitskonzepte nach aktuellem Stand der Technik bereiten wir eine neue Broschüre zur Datensicherheit bei Personalcomputern, ob unvernetzt, als Clients in homogenen oder heterogenen lokalen Netzen oder zu Laptops, Notebooks oder Palmtops miniaturisiert, vor.

Optische Speichermedien

Der immer stärker wachsende Aktenberg in der Verwaltung, veranlaßte die „Designer" verschiedener neuer Verfahren, sich bei der Verfahrensentwicklung den Problemen der elektronischen Archivierung zu stellen. Die Forderungen an elektronische Archive sind im wesentlichen die folgenden:

- Die Speicherung *sehr großer Datenmengen* muß möglich sein.
- Ein *ständiger Zugriff* für berechtigte Personen muß möglich sein.
- Die gespeicherten Daten müssen *authentisch* sein, d. h. sie dürfen nicht verändert werden können.
- Das Lesen der Daten muß über einen *langen Zeitraum* hinweg gewährleistet sein.
- Die Vorlagen müssen *originalgetreu reproduziert* werden können.

Für die Realisierung elektronischer Archive reichen bisherige magnetische Speichermedien nicht mehr aus. Alternativen bilden hier optische Speichermedien, die mittels Laserstrahl beschrieben werden und über stark erhöhte Speicherkapazitäten verfügen.

Zu den optischen Speichermedien zählen auch die wahrscheinlich mittlerweile jedem wohl bekannten *CD-ROM* (Compact Disc – Read Only Memory), die dem Musikliebhaber wesentlich mehr Musik, auf wesentlich kleinerem Platz, in wesentlich besserer Qualität bieten oder dem Computer-Freund das Hantieren mit einer großen Anzahl von Disketten bei der Installation einer neuen Software ersparen. Bisher war die Erzeugung von CDs nur Spezialisten überlassen, da keine, für den Normalbürger erschwinglichen Schreibgeräte verfügbar waren. Dieses hatte zur Folge, daß die Speicherung von Informationen auf einer CD nur

57 siehe Abschnitt 2.2
58 Jahresbericht 1993, 2.1
59 Jahresbericht 1992, 2.1; Jahresbericht 1993, 2.1

bei einer entsprechend hohen Stückzahl rentabel war. Mittlerweile sind Laufwerke erhältlich, die es analog z. B. zu einem Disketten-Laufwerk ermöglichen, CDs bei einer Speicherkapazität von 600 bis 650 MByte einmal zu beschreiben.

Das eigentliche Medium zur elektronischen Archivierung ist die sogenannte *WORM* (Write Once Read Many). Die WORM ist ebenfalls ein optisches Speichermedium, das genau einmal beschrieben und beliebig oft gelesen werden kann. Die Speicherkapazität beträgt zur Zeit für eine 12 Zoll WORM (mit einem Durchmesser von 30 cm) ca. 6 GByte (dieses entspricht ca. 3 Millionen Seiten Schreibmaschinentext oder ca. 100 000 als Faksimile gespeicherten Dokumenten). Es ist jedoch zu erwarten, daß die Kapazität in absehbarer Zeit auf ca. 15 GByte ansteigen wird. Häufig verwendet wird auch noch eine kleinere WORM mit 5¼ Zoll Durchmesser und einer Speicherkapazität von ca. 1½ GByte. Die WORM-Technologie steht auch für CDs zur Verfügung.

Als ein wiederbeschreibbares optisches Speichermedium ist die *magneto-optische Platte* (MOD – magneto optical disk) anzusehen. Sie entspricht im wesentlichen einer WORM, ist jedoch durch den Einsatz von Firmware (firmenspezifische Soft- oder Hardware-Programme im Laufwerk zur Sicherstellung der Basis-Funktionen) wiederbeschreibbar. Für eine gesicherte und anerkannte Langzeitarchivierung erscheint diese jedoch nicht einsetzbar und ist eher als Konkurrenz der herkömmlichen magnetischen Platten zu sehen.

Das wichtigste datenschutzrechtliche Problem bei Einsatz der WORM-Technologie besteht in der Sicherstellung der *gesetzlichen Löschungspflichten.* § 4 Abs. 2 Ziffer 6 BlnDSG definiert das Löschen als „das Beseitigen gespeicherter Daten". Unter „Beseitigen" ist dabei das physikalische Löschen zu verstehen.

Dieses ist jedoch, wie oben dargestellt, bei der WORM-Technologie nicht möglich. Ein Löschen von Daten kann nur auf dem logischen Wege erfolgen, indem ein Sperrvermerk in der Plattenverwaltungsdatei, in der Zeiger auf die eigentlichen Daten definiert sind, eingetragen wird, bzw. die entsprechenden Verweise aus der Plattenverwaltungsdatei gelöscht werden. Die Daten bleiben jedoch physikalisch unverändert auf der Platte stehen und könnten, z. B. durch Einspielen einer zu einem früheren Zeitpunkt gesicherten Plattenverwaltungsdatei, wieder identifizierbar gemacht werden.

Das dargestellte Problem könnte man dadurch lösen, indem in bestimmten Zeitabständen eine neue WORM erzeugt wird, die dann nur noch die Daten der ursprünglichen WORM enthält, die nicht als gelöscht gekennzeichnet sind. Die ursprüngliche WORM kann dann physikalisch vernichtet werden. Dieses Verfahren erscheint für Verwaltungszwecke mit unterschiedlichen Aufbewahrungs- bzw. Löschungfristen als nicht tragbar, da damit ein erheblicher Kostenaufwand verbunden ist. Der Preis für eine 12 Zoll WORM beträgt zur Zeit ca. 3000 DM, der für eine 5¼ Zoll WORM 300 DM.

Als sinnvolle Alternative erscheint die oben erwähnte CD-WORM mit einem Preis von ca. 30 DM. Hier kann, insbesondere bei einer Speicherung von Informationen auf einer CD-WORM, die ungefähr gleichen Löschungspflichten unterliegen, ein Umkopieren der Daten mit anschließender Vernichtung der ursprünglichen CD-WORM, als akzeptabel erachtet werden.

Deshalb empfehlen wir, den Einsatz von optischen Speichermedien dem Einsatzzweck anzupassen und den Einsatz von WORMs auf Verfahren zu beschränken, deren Daten keiner oder einer sehr langen Löschungsfrist unterliegen. Für andere Verfahren empfehlen wir den Einsatz von CD-WORMs.

Eine solche Empfehlung haben wir auch gegenüber dem Polizeipräsidenten in Berlin ausgesprochen, der derzeit das ADV-Verfahren *BOWI* (Verkehrsordnungswidrigkeiten) neu konzipiert. Das Konzept sieht vor, alle Vorgänge optisch zu erfassen. Da es sich um ein Verfahren handelt, bei denen Vorgänge gespeichert werden, mit denen Bürger, die gegen Verkehrsregeln verstoßen haben, verfolgt werden, ist auf eine zeitnahe Umsetzung vorhandener Löschungsfristen zu achten.

Miniaturisierung der Hardware

Bereits im Jahresbericht 1990[60] haben wir uns ausführlich mit den technischen und organisatorischen Datenschutzproblemen befaßt, die beim Einsatz von *Laptops* entstehen. Seither wurden immer kleinere, aber immer leistungsfähigere tragbare Rechner auf den Markt gebracht. Sog. Palmtops sind Rechner, die etwa die Größe von Brieftaschen besitzen, jedoch hinreichend Kapazitäten an Prozessorleistung und Speicherplatz aufweisen, um mit den gängigen PC-Betriebssystemen und Benutzeroberflächen arbeiten zu können.

Tragbare Computer sind vor allem dort sinnvoll, wo Mitarbeiter im Außendienst an wechselnden Plätzen Computer nutzen wollen, insbesondere Texte verarbeiten, sonstige Bürofunktionen nutzen oder Daten erfassen. So gibt es vor allem im Bereich der Polizei aktuelle Projekte zum Einsatz von Notebooks in Funkstreifenwagen und zur Erfassung von Ordnungswidrigkeiten im Straßenverkehr durch Kontaktbereichsbeamte und Angestellte im Verkehrsüberwachungsdienst.

Das besondere Risiko beim Einsatz von tragbaren Rechner liegt darin, daß sie verlegt oder aus Fahrzeugen oder Wohnungen entwendet oder geraubt werden können. Damit geraten auch gespeicherte personenbezogene Daten in die Hand Unbefugter. Aus diesem Grunde ist z. B. die *kryptographische Verschlüsselung* dieser Daten in Speichern tragbarer Rechner eine Mindestanforderung bei der Verwendung solcher Systeme im Außendienst.

2.2 Weiterentwicklung der informations- und kommunikationstechnischen Infrastruktur der Berliner Verwaltung

Bereits in den Vorjahren wurden in der Berliner Verwaltung diverse Projekte angestoßen, die der Weiterentwicklung der Infrastruktur für die automatisierte Datenverarbeitung und für die Daten- und Sprachkommunikation dienen sollten. Diese Projekte haben auch aus datenschutzrechtlicher Sicht und unter Aspekten der informationstechnischen Sicherheit immense Bedeutung, denn sie schaffen Rahmenbedingungen, denen sich die zukünftigen Anwendungsverfahren und -projekte unterzuordnen haben. Um zu verhindern, daß hinsichtlich Datenschutz und Datensicherheit falsche Weichenstellungen geschehen, haben wir uns intensiv an den Beratungen zu den Infrastrukturprojekten beteiligt. Wir konnten dabei auf erfreuliche Kooperationsbereitschaft der beteiligten Verwaltungen bauen.

Infrastrukturprojekte GIBES und BROSIA

Mit dem im letzten Jahr durchgeführten Infrastrukturprojekt GIBES – Grundlagen der Ausstattung mit IT-Infrastruktur für die Bezirke und Senatsverwaltungen –[61] wurde der Anfang gemacht, ein Rahmenkonzept für den Aufbau einer IT-Infrastruktur für die Berliner Verwaltung zu erarbeiten. Innerhalb von GIBES wurden im wesentlichen technische Aspekte berücksichtigt. Ergebnis des Projektes war die Festlegung „vorläufiger Technikgrundsätze und technischer Mindest- und Rahmenbedingungen für den Einsatz von IT-Systemen in der Berliner Verwaltung", die als Rundschreiben der Senatsverwaltung für Inneres der gesamten Berliner Verwaltung bekannt gemacht wurden. Mit diesen Technikgrundsätzen soll vor allem erreicht werden, daß bei Ausschreibungen zur Beschaffung von Informations- und Kommunikationstechnik möglichst einheitliche Anforderungen zu Normen und Standards gestellt werden. Als wesentlich wurde weiterhin erkannt, daß die *Erarbeitung eines Sicherheitskonzeptes* für die gesamte Berliner Verwaltung notwendig ist.

Der Hauptausschuß des Abgeordnetenhauses von Berlin hat im März 1994 die Ergebnisse von GIBES positiv bewertet und festgestellt, daß vergleichbare Aussagen auch für die bisher noch nicht ausreichend behandelten Bereiche Sicherheit, Organisation und Anwendungsentwicklung dringend erforderlich sind.

Diese sollen durch das Projekt BROSiA – Berliner Rahmenkonzept für Organisation, Sicherheit und Anwendungsentwicklung beim IT-Einsatz – erarbeitet werden. Wesentliches Ziel von BROSiA ist die Schaffung eines Gesamtwerkes grundlegender IT-Vorschriften zur Organisation der Datenverarbeitung in der Berliner Verwaltung und der Durchführung von IuK-Projekten.

60 Jahresbericht 1990, 2.4
61 Jahresbericht 1993, 2.1

Insbesondere soll dabei ein IT-Sicherheitsrahmenkonzept für die Berliner Verwaltung definiert werden. Dieses Konzept soll eine IT-Sicherheitsstrategie behördenübergreifend festlegen, erübrigt jedoch nicht die Erstellung von behörden- oder verfahrensspezifischen IT-Sicherheits- bzw. Datenschutzkonzepten. Diese soll durch die Erarbeitung eines Vorgehensmodells zum Erstellen von Risikoanalysen und Sicherheitskonzepten unterstützt werden.

Infrastrukturprojekte MAN und SAZ/LAZ

Seit einigen Jahren wird in Berlin die Strategie verfolgt, die bisher stark zentralistischen Strukturen bei informationstechnischen Anwendungen zu verringern und stattdessen durch dezentrale, offene, sich an internationalen Standards orientierenden Systeme zu ersetzen. In den letzten zwei Jahren wurden mehrere dezentrale Großprojekte initiiert (BASIS, AHW, FIS, ALK und IPV), die eine moderne Kommunikationsinfrastruktur notwendig machen. Dazu wurden unter anderem das Infrastrukturvorhaben eines bezirksübergreifenden Hochgeschwindigkeitsnetzes auf der Grundlage eines *Metropolitan Area Networks (MAN)* und der Aufbau einer zentralen Administrationsunterstützung für dezentrale UNIX-Systeme (Service- und Administrationszentrum - SAZ) und lokaler Administrationszentren (LAZ) begonnen.

Die Einführung eines Berlin-weiten Metropolitan Area Networks (MAN) stellt einen Schritt in eine neue Dimension der Nutzung moderner Kommunikationstechnologie in der Berliner Verwaltung dar. Eine derartige Vernetzung ermöglicht einerseits die Einführung effizienterer Arbeitsmethoden, beinhaltet andererseits jedoch auch erhebliche Gefahren. Der Erarbeitung eines Datenschutz- und Datensicherheitskonzeptes auf Basis einer umfassenden Risikoanalyse kommt daher eine besondere Bedeutung zu.

Erfreulicherweise wurde diese Forderung von den Projektmitarbeitern des MAN-Projektes stark unterstützt und eine Studie an eine externe Firma in Auftrag gegeben, die unter Verwendung des IT-Sicherheitshandbuchs des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine Risikoanalyse und ein darauf aufbauendes Datenschutz- und Datensicherheitskonzept erarbeitet hat. Das uns vorliegende Konzept ist generell als positiv zu bewerten. Die Risikoanalyse stellt die wesentlichen Gefahren und Ansatzpunkte für Angriffe auf die Sicherheit des MAN dar. Die daraus abgeleiteten Maßnahmen beruhen überwiegend auf dem aktuellen Stand der Technik, stellen aber nur eine Kompromißlösung zwischen optimalem Schutz und wirtschaftlichem Aufwand für die Sicherheit dar.

Durch das MAN wird die Möglichkeit gegeben, die bisher isolierten Kommunikationsinseln innerhalb der Berliner Verwaltung zu einem berlinweiten Netz zu verbinden. Die Existenz von physikalischen Verbindungen zwischen bisher unverbundenen Teilnetzen und die Netzphilosophie eines offenen Netzes, wonach theoretisch jeder mit jedem kommunizieren kann, sind aus datenschutzrechtlicher Sicht besonders kritisch zu betrachten. Bisher war eine gewisse *Zugangs- und Benutzerkontrolle* schon durch die Isoliertheit der Systeme bzw. der räumlichen Begrenzung auf einzelne Gebäude oder Etagen gegeben. Durch den Anschluß der lokalen Netze an das MAN wird die Gefahr eines unberechtigten Zugriffs von außen erheblich verstärkt. Daher ist eine Abschottung der Rechner und Verfahren, die das MAN nicht benötigen, unbedingt zu gewährleisten. Auch in der Zukunft darf der Zugriff von Unberechtigten auf Rechner und Verfahren nicht möglich sein. Für die Verfahren, die die Dienste des MAN benutzen, ist bei der Übertragung von personenbezogenen Daten normalerweise eine Verschlüsselung dieser Daten notwendig. Zur Minimierung des Risikos eines unberechtigten Zugriffs ist es weiterhin erforderlich, daß keinerlei Authentifizierungs-Informationen, wie z. B. Paßwörter, unverschlüsselt über das MAN übertragen werden.

Für die Zukunft ist absehbar, daß das MAN nicht nur ein Berlin-weites Netz bleibt, sondern auch Schnittstellen zu öffentlichen Netzen (wie z. B. dem Internet oder dem ISDN) haben wird. Die Öffnung nach außen bedarf der Einführung verstärkter Sicherheitsmechanismen. Für diesen Fall erwarten wir eine Risikoanalyse, auf die ein speziell für die Gegebenheiten der Berliner Verwaltung passendes Abschottungskonzept („Firewall-Konzept") aufgebaut werden muß.

Bei dem im unmittelbaren Zusammenhang mit dem MAN und der Initiierung der Großprojekte stehenden Projekt zur Installation eines *Service- und Administrationszentrums - SAZ* - wurde den Datenschutz- und Datensicherheitsaspekten bisher noch nicht die notwendige Aufmerksamkeit geschenkt. So wird auf diese Aspekte im uns vorliegenden Feinkonzept nur sehr vereinzelt eingegangen.

Das SAZ des LIT soll eine zentrale Systembetreuung für alle Berliner Verwaltungsstellen aufbauen. Dabei sollen die dezentral installierten Rechnersysteme und -netze der einzelnen Standorte durch zentrale Administrations-, Support- und Managementfunktionen unterstützt werden.

Die Einführung einer zentralen Administration ist aus datenschutzrechtlichen Gesichtspunkten durchaus positiv zu bewerten, bietet es doch die Möglichkeit, ausschließlich Fachleute, die über das notwendige Spezialwissen verfügen und gleichzeitig die riskanten Interessenkollisionen entgegenwirkende Anwendungsferne haben[62], für die Administration der Systeme einzusetzen. Gerade in den letzten Jahren mußten wir feststellen, daß bei der Einführung dezentraler Systeme die absolut notwendige fachliche Kompetenz der Systemverwalter nur unzureichend ausgeprägt ist und somit erhebliche Sicherheitsprobleme entstehen.

Eine *zentrale Administration* birgt jedoch auch erhebliche Gefahren, die bis zur Gefährdung der informationellen Gewaltenteilung reichen. Zur Administration ist ein Zugriff auf die zu verwaltenden Systeme natürlich notwendig. Dieses bedeutet aber auch, daß der Abschottung gegen unberechtigte Zugriffe auf diese Systeme aus dem Netz heraus besondere Bedeutung zukommt. Daher haben wir gefordert, nach dem Vorbild des MAN-Projektes für das SAZ-Projekt eine Risikoanalyse durchzuführen, auf deren Grundlage ein Datenschutz- und Datensicherheitskonzept erarbeitet werden kann, das auch bei den Konzepten der Systeme und Verfahren, die von der zentralen Administration erfaßt werden, Berücksichtigung finden kann.

ISDN-Vernetzungskonzept der Berliner Verwaltung

Das Abgeordnetenhaus fordert seit Jahren vom Senat, alle personellen, organisatorischen und technischen Maßnahmen zu ergreifen, die für den Aufbau einer zukunftsorientierten und leistungsfähigen Infrastruktur für die Kommunikations- und Informationstechnik der Berliner Verwaltung erforderlich sind.

Zur Umsetzung dieser Forderung im Bereich der Sprachkommunikation hat das LIT eine Studie an eine externe Firma in Auftrag gegeben, in der ein ISDN-Vernetzungskonzept für die Berliner Verwaltung erarbeitet werden sollte. Die Erstellung und Umsetzung eines zukunftsweisenden Konzeptes für die Telekommunikationsinfrastruktur der Berliner Verwaltung ist gerade aus datenschutzrechtlicher Sicht von besonderer Bedeutung, da einerseits auch hier das *Grundrecht auf unbeobachtbare Kommunikation* gewährleistet sein muß und andererseits die bereits in früheren Jahresberichten[63] dargestellten Gefahren beim Einsatz von ISDN beachtet werden müssen. Leider mußten wir feststellen, daß die mit der Konzeption und dem Betrieb eines ISDN-Netzes verbundenen Datenschutz- und Datensicherheitsprobleme in der Studie nur unzureichend dargestellt sind. Für eine Infrastrukturentscheidung mit einer Tragweite, wie sie das ISDN-Vernetzungskonzept darstellt, halten wir die Erstellung eines Datenschutz- und Datensicherheitskonzeptes auf Basis einer umfassenden Risikoanalyse für unbedingt erforderlich.

So wird z. B. die besondere Problematik der *Rufnummernanzeige* bei telefonischen Beratungsstellen der Berliner Verwaltung im Konzept nicht erörtert. Nach den Regelungen der geltenden Telekommunikations-Datenschutzverordnung (TDSV) muß die Telekom auf Antrag für Personen, Behörden und Organisationen, die selbst oder deren Mitarbeiter besonderen Verschwiegenheitsverpflichtungen unterliegen und die Beratungsaufgaben in sozia-

62 dazu auch Jahresbericht 1989, Anlage 3
63 Jahresbericht 1990, 2.3; Jahresbericht 1991, 2.3

len oder kirchlichen Bereichen ganz oder überwiegend über Telefon abwickeln, sicherstellen, daß die Übermittlung der Rufnummer des anrufenden Anschlusses ausgeschlossen ist. Die Berliner Verwaltung verfügt über eine Vielzahl derartiger Beratungsstellen.

Grundsätzlich muß es dem Bürger auch in Zukunft möglich sein, sich ohne zwangsweise Übermittlung seiner Rufnummer an die Verwaltung zu wenden.

Eine Speicherung von *Verbindungsdaten* ist nach derzeitiger Rechtslage für aus dem Verwaltungsnetz herausgehende Rufe nicht zulässig. Die Rahmendienstvereinbarung über den Einsatz und den Betrieb von digitalen Telefonnebenstellenanlagen vom 15. August 1991 schließt die dauerhafte Speicherung von Verbindungsdaten ausdrücklich aus. Danach sind die Daten nach Beendigung der Verbindung zu löschen. Dies betrifft insbesondere auch die Rufnummer des angerufenen Teilnehmers.

Darüber hinaus ist die Speicherung von Daten über Telefongespräche für einzelne Stellen in der Verwaltung (z. B. die örtlich zuständigen Personalräte, Frauenbeauftragte etc.) generell unzulässig.

Bei der Beschaffung von ISDN-Nebenstellenanlagen ist daher darauf zu achten, daß die Anlage die Möglichkeit bietet, die Speicherung der Daten Angerufener je Endgerät ganz zu unterbinden oder wahlweise eine Speicherung der um die letzten drei Ziffern verkürzten Zielnummer vorzusehen. Die Funktion muß so realisiert sein, daß vollständige Zielnummern in diesen Fällen gar nicht erst gespeichert werden. Einige Hersteller bieten lediglich die Möglichkeit, die Anzeige beziehungsweise den Ausdruck gespeicherter Zielnummern durch die Auswertungssoftware zu verhindern. Dies reicht nicht aus.

Für die Speicherung von Verbindungsdaten für im Verwaltungsnetz ankommende Verbindungen besteht ebenfalls keine Rechtsgrundlage.

2.3 IT-Sicherheitsuntersuchung im Landesamt für Informationstechnik

Aus dem Landesamt für Elektronische Datenverarbeitung (LED) entstand nach der Wiedervereinigung Berlins durch die Zusammenführung mit dem in Ost-Berlin beheimateten Magistratsrechenzentrum das Landesamt für Informationstechnik (LIT). Mit diesem Namenswechsel war auch eine Gewichtsverschiebung hinsichtlich der zu bewältigenden Aufgaben für diese nun für ganz Berlin zuständige Dienstleistungsbehörde verbunden.

Hatte man bereits vor dem einschneidenden gesellschaftlichen Umbruch damit begonnen, die Zuständigkeit für Entwicklung und Pflege von DV-Verfahren der Senats- und Bezirksverwaltungen auf die eigentlichen Anwender zu übertragen, war nun auch dem durch die rasante Entwicklung der Informations- und Kommunikationstechnik bedingten Trend zur dezentralen Datenverarbeitung Rechnung zu tragen. So mußten neben dem klassischen Dienstleistungsangebot, das auf der zentralen Nutzung von Großrechnern für die Massendatenverarbeitung beruht, neue Leistungsinhalte definiert und der Berliner Verwaltung angeboten werden.

Die Struktur des LIT wurde derart verändert, daß mittlerweile die *Service- und Beratungsfunktion* für IuK-Techniken und -Verfahren insbesondere für die dezentrale Datenverarbeitung eine wesentliche Säule des Dienstleistungsangebots dieser Behörde darstellt. Diese Funktion umfaßt die Unterstützung und Beratung hinsichtlich des Einsatzes verschiedenster DV-Komponenten und erstreckt sich von der Hardware über die Software bis hin zur landesweiten Kopplung von Rechnern und Rechnernetzen unterschiedlichster Größe und Konfiguration.

Damit einher geht die Umgestaltung der Großrechenzentren, die auch weiterhin eine wichtige Funktion für die Datenverarbeitung in Berlin haben werden. Eine externe Untersuchung der Sabotage- und Feuerrisiken hatte den Bedarf eines höheren Sicherheitsniveaus deutlich gemacht. Das *neue Sicherheits-Rechenzentrum* soll im „dunklen" Betrieb betrieben werden, d. h. ohne unmittelbare persönliche Anwesenheit von LIT-Mitarbeitern. Die Steuerung der beiden im LIT eingesetzten Großrechnersysteme wird dann von einem zentralen Leitstand aus erfolgen, der an einem vom Rechenzentrum entfernten Ort zu finden sein wird. Dazu sind umfangreiche Sicherungs- und Überwachungseinrichtungen hinsichtlich denkbarer Bedrohungsszenarien konzipiert worden.

Die Planungen zur Umgestaltung des LIT-Dienstgebäudes sehen einen offenen Bereich (Schulung, Beratung, etc.) und einen abgeschotteten Bereich (Rechenzentrumsbetrieb, Systemverwaltung, Ein-/Ausgabe-Stelle, etc.) vor. Es ist zu hoffen, daß dieser Planungsvorschlag trotz der angespannten Haushaltslage realisiert werden kann.

Um beiderseits Erfahrungen zu gewinnen, die bei der Neugestaltung des Rechenbetriebes zu beachtenden Risiken zu erkennen und Schwachstellen festzustellen und in Zukunft zu umgehen, haben wir in Zusammenarbeit mit dem Landesamt für Informationstechnik eine Untersuchung der technischen und organisatorischen Maßnahmen zur Gewährleistung einer datenschutzgerechten Datenverarbeitung im LIT durchgeführt.

Die Sicherheits-Untersuchung hat gezeigt, daß dem Datenschutz im LIT große Aufmerksamkeit gewidmet wird und die Mitarbeiter in hohem Maße für die Belange des Datenschutzes sensibilisiert und offen für mögliche bzw. notwendige Verbesserungen sind. Neben den guten technisch-organisatorischen Maßnahmen beim Großrechnereinsatz waren bei anderen Funktionsbereichen Empfehlungen zur Durchsetzung umfassender Datenschutzkonzepte zu geben:

- Die *Zugangskontrolle* im LIT bedarf im Zusammenhang mit der Umgestaltung des Rechenzentrumsbetriebes einer kritischen Prüfung. Für den Fall, daß das LIT an dem bisher eingesetzten Zugangskontrollsystem festhalten möchte, haben wir eine Überarbeitung des Systems insbesondere hinsichtlich der Identifikations- und Authentifikationsmöglichkeiten für die Administration des Zugangskontrollsystems, einer geeigneten Alarmierung bei Manipulationsversuchen sowie der Bedienungs- und Systemunterlagen empfohlen. Zudem sollte die zum Einsatz des Systems abgeschlossene Dienstvereinbarung neben den Rechten des zuständigen Personalrats auch die Rolle des behördlichen Datenschutzbeauftragten berücksichtigen.

- In der *Verbindungsstelle für ADV-Verfahren Tarif- und Besoldung* wurden Risiken für die Ordnungsmäßigkeit bei der Datenträgerverwaltung erkannt. Wir haben empfohlen, Maßnahmen zu ergreifen, um die Umsetzung der dafür vorhandenen Dienstanweisung zu sichern. Ferner wurde festgestellt, daß die Transportkontrolle beim Datenträgeraustausch aus den östlichen Bezirken verbessert werden muß.

- Im *Aufgabengebiet „Datensammlung/-transfer für die Zahlungsverfahren"* werden sensible personenbezogene Daten auf zwei miteinander nicht vernetzten Personalcomputern bearbeitet. Während der eine Computer relativ gut gesichert wurde, wies der andere gravierende Sicherheitsmängel auf. Wir haben empfohlen, entweder die technisch-organisatorischen Maßnahmen beim zweiten Rechner dem Niveau des ersten Rechners anzugleichen oder den zweiten Rechner außer Betrieb zu setzen und die dort anfallenden Aufgaben auf dem ersten mitzuerledigen.

- Die hausinterne *Bürokommunikation* wies Unzulänglichkeiten auf. Wir haben empfohlen, für den Einsatz des Bürokommunikationssystems eine Rahmenrichtlinie zu schaffen, ein durchgängiges Datenschutz- und Sicherheitskonzept zu erarbeiten, das auch die Kontrolle der ordnungsgemäßen Anwendung des Bürokommunikationssystems einbezieht, die Abschottung zu anderen Verfahren im Netzverbund zu verbessern und die Benutzerprofile dem tatsächlichen Bedarf anzupassen.

- Wir haben empfohlen, im Zusammenhang mit der Neugestaltung der internen Verkabelung des Hausnetzes den dafür zuständigen Mitarbeitern ein geeignetes Werkzeug zur *Dokumentation der Netzstruktur* an die Hand zu geben, um die derzeitigen Defizite der Netzdokumentation zu beseitigen.

- Auch für die *Datenfernübertragung* mangelt es an revisionsfähigen Unterlagen zur Dokumentation des Verfahrens, seiner Verwaltung und der damit verbundenen Sicherheitsmaßnahmen. Eine Ablösung der bereits wesentlich früher[64] als risikobehaftet eingeschätzen SK-12-Knoten ist noch nicht abschließend erfolgt.
- In einem Rechenzentrum stellten wir fest, daß für die Aufgabenerledigung durch die Mitarbeiter der Arbeitsvorbereitung viel zu viele *Paßwörter* notwendig waren, die kaum noch zu handhaben waren, ohne sie in irgendeiner Form aufzuzeichnen. Da solche Aufzeichnungen naturgemäß ein erhebliches Risiko hinsichtlich eines möglichen Mißbrauchs darstellen, sollte - auch im Interesse der betroffenen Mitarbeiter - nach Möglichkeiten gesucht werden, wie dieser mißliche Zustand verbessert werden kann. Wir haben außerdem empfohlen, den Mitarbeitern der Arbeitsvorbereitung im Sinne einer ordnungsgemäßen Funktionentrennung im Rechenzentrum die Möglichkeit zu entziehen, sich in den Status eines Operators zu versetzen.
- Für eine ordnungsgemäße und revisionssichere Arbeit der BS-2000-Systemverwaltung erscheint es aus unserer Sicht notwendig, den Einsatz der Sicherheitskomponente SECOS so zu gestalten, daß die Nutzung der *Systemverwalter-Kennung* (TSOS) wegen ihrer funktionalen Mächtigkeit auf ein Minimum eingeschränkt werden kann und letztlich die Ausnahme bei einem aufgabenbezogenen und damit personenbeziehbaren Systemmanagement darstellt. Um die Benutzerverwaltung auf eine gesicherte Grundlage zu stellen, ist eine Arbeitsanweisung zu erarbeiten, die insbesondere auch die Belange des Einsatzes von LIT-Mitarbeitern regelt.

3. Übergreifende Themen

3.1 Die Informationsrechte des Parlaments

Zwischen „Informationsgleichgewicht" und Eingriffen in den „Kernbereich" der Exekutive

Seit jeher werfen die *Informationsbeziehungen zwischen Parlament und Regierung* (insbesondere zwischen Abgeordnetenhaus und Senat, in ähnlicher Form auch zwischen Bezirksverordnetenversammlungen und Bezirksämtern) datenschutzrechtliche Fragen auf. Dabei sollte einerseits ein „Informationsgleichgewicht" zwischen Parlament und Regierung angestrebt oder besser: der immer bestehende *Informationsvorsprung der Regierung* nicht durch eine Informationsverweigerung gegenüber dem Parlament vergrößert werden. Die Mitglieder des Senats haben dem Abgeordnetenhaus und seinen Ausschüssen auf deren Wunsch Rede und Antwort zu stehen (Art. 34 Abs. 1 Verfassung von Berlin).

Andererseits weist die Verfassung Exekutive und Legislative unterschiedliche Aufgaben zu: Während die Verwaltung Einzelfallentscheidungen zu treffen hat, soll das Parlament die Verwaltung lediglich kontrollieren (nicht an ihrer Stelle handeln) und Gesetze - generell-abstrakte Regelungen - beschließen. Diese Aufgabenverteilung ist gerade Inhalt des verfassungsrechtlichen *Grundsatzes der Gewaltenteilung* und ihre Veränderung würde deshalb auf verfassungsrechtliche Grenzen stoßen.

Wo diese Grenzen im einzelnen liegen, wird seit längerem kontrovers diskutiert. Die Kontroverse ist auch nicht beendet worden durch die Feststellung des Bundesverfassungsgerichtes, daß keine der beiden Gewalten (Parlament oder Regierung) jeweils in den *Kernaufgabenbereich* der anderen Gewalt eingreifen darf[65]. Natürlich darf das Parlament nicht selbst verwalten, also Einzelfallregelungen treffen. Infolgedessen ist der Informationsfluß zwischen Verwaltung und Parlament von vornherein auf das beschränkt, was das Parlament zur Erfüllung seiner Kontroll- und Gesetzgebungsaufgabe benötigt.

64 Jahresbericht 1986, 4.1
65 BVerfGE 68, 1, 87

Eine weitere Grenze ergibt sich aus dem *Gebot der informationellen Gewaltenteilung,* den das Bundesverfassungsgericht erstmals im Volkszählungsurteil[66] bezogen auf die Trennung zwischen Statistik und Verwaltungsvollzug formuliert hat. Auch die Weitergabe von Einzelangaben an das Parlament gelten grundsätzlich als unzulässig und nach den Statistikgesetzen des Bundes und Berlins nur in engen Grenzen erlaubt, wenn Daten in Tabellenform etwa zur Beantwortung Kleiner Anfragen nur einen einzigen Fall ausweisen. Selbst dann dürfen diese Angaben nicht zur Regelung von Einzelfällen verwendet werden.

Die Grenzen der Aufgabengebiete von Legislative und Exekutive sind auch im Schlußbericht der *Enquete-Kommission „Verfassungs- und Parlamentsreform"*[67] erörtert worden. Die Enquete-Kommission hat mit $^2/_3$-Mehrheit vorgeschlagen, das Recht des Abgeordneten neu in die Verfassung aufzunehmen, sich durch Einsicht in Akten und sonstige amtliche Unterlagen der Verwaltung über einen Vorgang zu informieren. Dazu ist ein Beschluß von einem Fünftel der Mitglieder des zuständigen Parlamentsausschusses notwendig. Die Einsichtnahme in Akten darf danach nur abgelehnt werden, wenn überwiegende öffentliche Interessen an der Geheimhaltung dies zwingend erfordern oder schutzwürdige Interessen Einzelner, *insbesondere des Datenschutzes,* entgegenstehen (Art. 29 Abs. 3[68]). Der Senat hat diesen Vorschlag in seiner Stellungnahme vom 20. Dezember 1994[69] als verfassungswidrigen Eingriff in den Kernbereich der Exekutivtätigkeit kritisiert, der auch dem verfassungsändernden Gesetzgeber verwehrt sei.

Ob ein wie auch immer formuliertes Akteneinsichtsrecht von Abgeordneten in die Verfassung von Berlin aufgenommen wird, muß zunächst das Abgeordnetenhaus mit der dafür erforderlichen Mehrheit entscheiden. Der Auftrag des Datenschutzgesetzes in diesem Bereich kann nur so verstanden werden, daß der tatsächlich vorhandene und - in bestimmten Grenzen - von der Verfassung auch gewollte Informationsvorsprung der Exekutive vor der Legislative durch die automatisierte Datenverarbeitung nicht vergrößert werden darf. Man könnte diesen Auftrag auch so verstehen, daß der Berliner Datenschutzbeauftragte Empfehlungen dafür geben kann, wie der Informationsvorsprung der Verwaltung gerade durch den Einsatz der automatisierten Datenverarbeitung im Rahmen des verfassungsrechtlich Zulässigen verkürzt werden kann. Denn die automatisierte Datenverarbeitung bietet sicherlich auch Chancen zur Verbesserung der Kontrollmöglichkeiten des Parlamentes.

Die bei der Neufassung des Berliner Datenschutzgesetzes 1990 eingefügte neue Regelung[70], daß *Gesetzesvorlagen* Angaben über die Daten, die für den Vollzug des Gesetzes mit Datenverarbeitungsanlagen erforderlich sind, und über die Form der vorgesehenen Datenverarbeitung enthalten müssen, kann sowohl dem Schutz des informationellen Selbstbestimmungsrechtes einzelner Bürger als auch dem Schutz der verfassungsmäßigen Ordnung vor einer Gewaltenverschiebung dienen. Leider wird diese zwingende Regelung bei der Erstellung von Gesetzesvorlagen nach unseren Beobachtungen in den seltensten Fällen beachtet. Man könnte sogar daran denken, diese Vorschrift in der Weise zu ergänzen, daß Vorlagen für solche Gesetze, die mit Hilfe der automatisierten Datenverarbeitung vollzogen werden sollen, zusätzlich Angaben darüber enthalten müssen, welche Auswirkungen dies auf die Informationssituation des Parlamentes im Vergleich zur Verwaltung voraussichtlich haben wird oder ob sich sogar Möglichkeiten zur Verkürzung des Informationsvorsprungs der Exekutive gegenüber der Legislative ergeben können.

Aufgrund unserer engen Zusammenarbeit mit dem *Petitionsausschuß* des Abgeordnetenhauses, aber auch aufgrund von Anfragen aus der Verwaltung haben wir uns wiederholt mit der Frage beschäftigt, unter welchen Voraussetzungen dem Petitionsausschuß Verwaltungsvorgänge zur Bearbeitung von Eingaben übermittelt werden dürfen. Man könnte sich auf den Standpunkt

66 BVerfGE 65, 1, 69
67 Drs 12/4376
68 wortgleich übernommen im Antrag des Abg. Herbst und weiterer Abgeordneter über ein 28. Gesetz zur Änderung der Verfassung von Berlin, Drs. 12/4874
69 Senatsvorlage Nr. 5263/94
70 § 20 Abs. 3 BlnDSG

stellen, daß der Petent mit seiner Eingabe an den Petitionsausschuß stillschweigend auch sein Einverständnis mit der Übermittlung der Verwaltungsvorgänge erklärt, über deren Bearbeitung er sich beschwert. Das hilft jedoch in der Mehrzahl der Fälle nicht weiter, weil sehr häufig in den Akten der Verwaltung auch Daten Dritter (neben denen der Behördenmitarbeiter) enthalten sind, über die der Petent nicht verfügen kann. Die Arbeit des Petitionsausschusses wird allerdings erheblich erschwert, wenn man – wie nach geltendem Recht notwendig – darauf besteht, daß alle von der Eingabe betroffenen Personen ihre Einwilligung zur Übermittlung an den Petitionsausschuß erteilen. Ähnliche Fragen ergeben sich, wenn ein Dritter sich im Interesse eines geschäftsunfähigen Bürgers, der nicht wirksam einwilligen kann, an den Petitionsausschuß wendet. Diese Probleme können nur durch eine klare gesetzliche Übermittlungsbefugnis gelöst werden, die das *Gesetz über die Behandlung von Petitionen an das Abgeordnetenhaus von Berlin (Petitionsgesetz)* von 1969 bisher nicht enthält. Wünschenswert wäre auch eine Ergänzung des Petitionsgesetzes mit dem Ziel, die Übermittlung personenbezogener Daten an andere Fachausschüsse auszuschließen, die um eine Stellungnahme zu der Eingabe gebeten werden.

Auch bei der Frage, in welchem Umfang die Verwaltung *Untersuchungsausschüssen* personenbezogene Auskünfte geben muß oder darf, besteht erhebliche Unsicherheit. Zwar haben nach der Verfassung von Berlin (Art. 33 Abs. 2 Satz 1) Gerichte und Behörden einem Untersuchungsausschuß Rechts- und Amtshilfe zu leisten; sie haben auf Verlangen Akten vorzulegen und ihren Dienstkräften Aussagegenehmigungen zu erteilen, soweit nicht Gründe der Staatssicherheit entgegenstehen. Das Gesetz über die Untersuchungsausschüsse des Abgeordnetenhauses von Berlin wiederholt diese allgemein gehaltene Formulierung lediglich. Auch in diesem Bereich ist der Gesetzgeber aufgerufen, normenklare Erhebungs- und Übermittlungsbefugnisse in das Untersuchungsausschußgesetz aufzunehmen. Die Enquete-Kommission „Verfassungs- und Parlamentsreform" hat darüber hinaus einstimmig empfohlen, in der Verfassung von Berlin Gerichte und Behörden zur Aktenvorlage und Erteilung von Aussagegenehmigungen gegenüber Untersuchungsausschüssen zu verpflichten, soweit nicht gegenüber dem Ausschuß schlüssig begründet wird, daß dem Bekanntwerden des Inhalts gesetzliche Vorschriften oder Staatsgeheimnisse oder *schutzwürdige Interessen Einzelner, insbesondere des Datenschutzes,* entgegenstehen oder wenn die Funktionsfähigkeit und die Eigenverantwortung des Senats beeinträchtigt werden[71]. Bis zu dieser wünschenswerten Klärung können sich Parlament und Regierung nur an der Rechtsprechung des Bundesverfassungsgerichtes orientieren[72], die allerdings nur grundsätzliche Aussagen darüber enthält, unter welchen Voraussetzungen die Regierung einem Untersuchungsausschuß die Vorlage von Akten verweigern darf. Zum Verhältnis zwischen dem Beweiserhebungsrecht eines Untersuchungsausssschusses und dem Grundrecht des Bürgers auf Datenschutz hat das Bundesverfassungsgericht hervorgehoben, daß die Bedeutung, die das Kontrollrecht des Parlamentes sowohl für die parlamentarische Demokratie als auch für das Ansehen des Staates hat, in aller Regel dann keine Verkürzung des Aktenherausgabeanspruches zugunsten des Schutzes des allgemeinen Persönlichkeitsrechtes gestattet, wenn Parlament und Regierung Vorkehrungen für den Geheimschutz getroffen haben, die das ungestörte Zusammenwirken beider Verfassungsorgane auf diesem Gebiet gewährleisten, und wenn der Grundsatz der Verhältnismäßigkeit gewahrt ist. Eine Ausnahme hiervon hat das Gericht allerdings für solche Informationen vorgesehen, deren Weitergabe wegen des streng persönlichen Charakters für die Betroffenen unzumutbar ist[73]. Der Berliner Datenschutzbeauftragte hat in der Vergangenheit wiederholt einzelne Untersuchungsausschüsse bei der Ausgestaltung der erforderlichen Geheimschutzvorkehrungen beraten.

Das Berliner Datenschutzgesetz enthält eine eigene, bisher wenig beachtete Vorschrift[74], die eine *Pflicht der Behörden* und sonstigen öffentlichen Stellen *zur Auskunftserteilung gegenüber dem Abgeordnetenhaus,* dessen verfassungsmäßigen Organen und den Fraktionen des Abgeordnetenhauses vorsieht. Dieselbe Verpflichtung gilt für die Bezirksämter gegenüber den Bezirksverordnetenversammlungen, ihren verfassungsmäßigen Organen und ihren Fraktionen. Voraussetzung für die Auskunftspflicht ist, daß das Parlament oder eines seiner Organe im Rahmen seiner Aufgaben und Zuständigkeiten entsprechende Auskünfte über Daten verlangt. Während in anderen Bundesländern die Auskunftserteilung über personenbezogene Daten teilweise völlig ausgeschlossen ist, dürfen in Berlin personenbezogene Daten dem Abgeordnetenhaus und den Bezirksverordnetenversammlungen sowie ihren Organen und den Fraktionen unter bestimmten, im Bundesdatenschutzgesetz genannten engen Voraussetzungen übermittelt werden. Ob ein genereller Ausschluß der Übermittlung von personenbezogenen Daten oder auch nur eine Beschränkung, wie sie im Berliner Datenschutzgesetz vorgesehen ist, mit dem verfassungsrechtlichen Auskunfts- und Kontrollrecht[75] vereinbar ist, kann mit guten Gründen bezweifelt werden. Die erwähnte Vorschrift des Berliner Datenschutzgesetzes ist bisher – allerdings aus einem anderen Grund – kaum angewandt worden: Sie regelt nämlich nicht den praktisch häufigsten Fall der Übermittlung von Daten durch die Verwaltung an das Parlament, die Beantwortung von Kleinen Anfragen einzelner Abgeordneter.

Immer wieder – und im Berichtszeitraum verstärkt – wenden sich Senatsverwaltungen an uns mit der Frage, in welchem Umfang personenbezogene Auskünfte auf *Kleine Anfragen* einzelner Abgeordneter gegeben werden dürfen. Auch hier herrscht erhebliche Rechtsunsicherheit. Die Berliner Verfassung enthält keine Verpflichtung zur Beantwortung Kleiner Anfragen. Da das Parlament als Ganzes und in seinen Ausschüssen jedoch ein Auskunfts- und Kontrollrecht nach Art. 34 der Verfassung von Berlin hat, ist der Senat deshalb zumindest politisch gehalten, auch Kleine Anfragen einzelner Abgeordneter zu beantworten. Dabei steht es allerdings nicht in seinem Ermessen, ob und in welchem Umfang er in der Antwort personenbezogene Daten übermitteln darf. Vielmehr bedarf er hierzu einer speziellen gesetzlichen Übermittlungsbefugnis.

Diese Befugnis ergibt sich nicht aus dem Berliner Datenschutzgesetz, das die Auskunftserteilung an einzelne Abgeordnete nicht regelt. Im übrigen beschränken sich die meisten Kleinen Anfragen nicht auf den Katalog personenbezogener Daten, die nach dem Berliner Datenschutzgesetz dem Abgeordnetenhaus, den Bezirksverordnetenversammlungen und ihren jeweiligen Organen rechtmäßig übermittelt werden dürfen.

Dies läßt sich illustrieren am Beispiel der im Berichtszeitraum gestellten Kleinen Anfrage[76], mit der der Senat um Auskunft gebeten wurde, in welchem Umfang und in welcher Rangfolge die berechtigten Personen ihre personengebundenen Dienstwagen zu rein privaten Zwecken nutzen (*„Wer benutzt seinen personengebundenen Dienstwagen am meisten zu privaten Zwecken?"*). Ergänzend wurde der Senat danach gefragt, ob er erwäge, die Anzahl der personengebundenen Dienstwagen aufgrund der „dramatischen Finanzsituation des Landes Berlin" einzuschränken.

Zu dieser konkreten Anfrage bat uns die Senatsverwaltung für Inneres um eine Stellungnahme, ob die Kleine Anfrage exakt beantwortet werden könne, ohne gegen das Datenschutzgesetz zu verstoßen.

Wir haben darauf hingewiesen, daß wir schon im Februar 1987 gegenüber dem Präsidenten des Abgeordnetenhauses für die Schaffung einer speziellen gesetzlichen Befugnis zur Übermittlung personenbezogener Daten zur Beantwortung parlamentarischer Anfragen eingetreten sind[77], ohne daß bisher eine solche Übermittlungsbefugnis geschaffen worden wäre. Allerdings würde es der verfassungsrechtlichen Bedeutung des parlamentarischen Kontrollrechtes nicht gerecht, wenn man bis zur Schaffung einer gesetzlichen Befugnis jede Beantwortung Kleiner Anfragen, die die Verarbeitung personenbezogener Daten voraussetzt, ablehnte. Vielmehr ist bis zur Schaffung einer gesetzlichen Befugnis im Einzelfall unter Abwägung zwischen dem parlamentarischen Kontrollrecht und dem informationellen Selbstbestimmungsrecht der Betroffenen zu ermitteln, in welchem Umfang personenbezogene Daten verarbeitet werden dürfen.

71 Drs 12/4376, 13 (Art. 33 Abs. 2)
72 BVerfGE 67, 100
73 BVerfGE 67, 100, 144
74 § 20 BlnDSG

75 vgl. Art. 34 der Verfassung von Berlin
76 Nr. 5711 des Abgeordneten Dr. Köppl, Drs. 12/4873
77 vgl. bereits Jahresbericht 1986, 6

Ziel der erwähnten Kleinen Anfrage war es in erster Linie, den Senat zu befragen, ob er angesichts der schwierigen Finanzsituation des Landes eine Einschränkung der Anzahl der personengebundenen Dienstwagen erwägt. Vor diesem Hintergrund war es erforderlich, aber auch ausreichend, dem Fragesteller in anonymisierter Form Auskunft über die mit personengebundenen Dienstwagen privat zurückgelegten Kilometer zu erteilen. Eine entsprechende Aufstellung, die keine Rückschlüsse auf die einzelnen berechtigten Personen zuläßt, hätte von der Senatsverwaltung für Inneres über die Senatskanzlei dem Abgeordnetenhaus zugeleitet werden können, ohne daß dadurch datenschutzrechtliche Belange der Betroffenen berührt worden wären. Die zuvor notwendige Übermittlung personenbezogener Angaben durch die jeweiligen Gehalts- und Lohnstellen, die einen Überblick über die mit den personengebundenen Dienstwagen verbundenen geldwerten Vorteile haben, wäre eine zulässige Verarbeitung von Personaldaten im Rahmen der Zweckbestimmung des jeweiligen Dienstverhältnisses gewesen. Soweit das Land Berlin seinen Amtsträgern personengebundene Dienstfahrzeuge zur Verfügung stellt, sind diese in ihren schutzwürdigen Belangen nicht beeinträchtigt, wenn die Exekutive einem Abgeordneten in anonymisierter Form Auskunft über die private Nutzung dieser Dienstfahrzeuge erteilt. Dagegen wären die schutzwürdigen Belange der Betroffenen gravierend verletzt, wenn der Senat dem anfragenden Abgeordneten die gewünschte Rangliste in personenbezogener Form zur Verfügung gestellt hätte.

Erstaunlicherweise wurde die erwähnte Kleine Anfrage allerdings wesentlich weniger genau beantwortet, als dies - jedenfalls aus Gründen des Datenschutzes - möglich gewesen wäre[78]. In allgemeiner Form wurde lediglich das Verfahren der Abrechnung bei privater Nutzung personengebundener Dienstfahrzeuge beschrieben und dem Abgeordneten im übrigen mitgeteilt, daß „weitergehende, d. h. personenbezogene Einzeldaten ... aus datenschutzrechtlichen Gründen nicht mitgeteilt werden" können.

Auch in anderen Fällen haben wir im Berichtszeitraum den Eindruck gewonnen, daß die Verwaltung bei der Beantwortung Kleiner Anfragen zuweilen den Datenschutz als Vorwand benutzt, obwohl dieser einer genaueren Beantwortung nicht im Wege gestanden hätte. So hat der Senat die Frage, wie viele Arbeitsplätze bei welchen Firmen in den letzten drei Jahren in einem Berliner Bezirk abgebaut worden seien[79], mit dem Hinweis beantwortet, daß aussagekräftige, umfassende Erhebungen zur Beantwortung dieser Fragen dem Senat „insbesondere aufgrund datenschutzrechtlicher Vorschriften, u. a. seit dem sog. „Volkszählungsurteil", nicht zur Verfügung stünden. Daß dem Senat entsprechendes Zahlenmaterial nicht zur Verfügung steht, mag eine Vielzahl von Gründen haben (Einschränkung statistischer Erhebungen, mangelhafte Auskunftsbereitschaft der Unternehmen etc.), datenschutzrechtliche Vorschriften gehören jedenfalls aber nicht dazu. Abgesehen davon, daß Unternehmen, die als juristische Personen organisiert sind, sich nicht auf den Datenschutz berufen können, haben das Bundesverfassungsgericht und die anschließende Statistikgesetzgebung Wege aufgezeigt, wie das erforderliche Zahlenmaterial datenschutzgerecht erhoben werden kann. Daß diese Wege nicht gegangen worden sind, kann nicht dem Datenschutz angelastet werden. Eine so begründete Auskunftsverweigerung gegenüber einem Abgeordneten bringt den Datenschutz in Mißkredit.

In der Antwort auf eine weitere Kleine Anfrage[80] nach den Umständen der Abschiebehaft eines Aussiedlers aus der ehemaligen Sowjetunion, dessen deutsche Staatsangehörigkeit zunächst übersehen wurde, lehnte der Senator für Inneres neben einer allgemeinen Antwort detailliertere Auskünfte „aus datenschutzrechtlichen Gründen *und* zum Schutz des Betroffenen" ab. Ob dies zu Recht geschah, können wir nicht im einzelnen beurteilen. Die Begründung ist aber jedenfalls insofern irreführend, als das Grundrecht auf Datenschutz gerade dem Schutz des Betroffenen dienen soll.

78 Drs 12/4873, 11
79 Kleine Anfrage Nr. 5871 des Abg. Behrendt, LPD vom 24. Oktober 1994, S. 17
80 Nr. 6152 des Abg. Koşan, LPD vom 22. Dezember 1994, S. 1

Die beschriebenen Bereiche bedürfen schon deshalb dringend einer bereichsspezifischen Regelung, weil es hier um die Übermittlung personenbezogener Daten aus der Verwaltung an das Parlament geht.

Bisher war ausschließlich von den herkömmlichen, konventionellen Informationsflüssen zwischen Regierung und Parlament die Rede. Mit zunehmender *Automatisierung* wird aber eine neue Fragestellung in den Vordergrund treten, die noch nicht im Einzelnen untersucht worden ist.

Mit der Novellierung des Berliner Datenschutzgesetzes im Dezember 1990 wurde dem Gesetz eine doppelte Aufgabe zugewiesen: Zum einen soll es das Recht des Einzelnen schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, soweit keine Einschränkungen in diesem Gesetz oder in anderen Rechtsvorschriften zugelassen sind. Zum anderen soll es die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen auch zu dem Zweck regeln, die auf dem *Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Ordnung vor einer Gefährdung infolge der automatisierten Datenverarbeitung* zu bewahren (§ 1 Abs. 1 Nr. 2 BlnDSG). Bereits nach dem Datenschutzgesetz von 1978 hatte der Berliner Datenschutzbeauftragte die Auswirkungen der automatischen Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen dahingehend zu beobachten, ob sie zu einer Beschränkung der Kontrollmöglichkeiten durch die Volksvertretung führen. Diese Vorschrift ist auch im novellierten Datenschutzgesetz enthalten. Der Datenschutzbeauftragte kann Maßnahmen zum Schutz gegen derartige Auswirkungen anregen. Diesem Zweck dient gerade auch die neu in das Gesetz aufgenommene Verpflichtung aller öffentlichen Stellen Berlins, den Datenschutzbeauftragten über die Einführung neuer Automationsvorhaben in ihrem Bereich zu informieren (§ 24 Abs. 3 BlnDSG).

Der Berliner Datenschutzbeauftragte hat bisher seine Hauptaufgabe darin gesehen, das informationelle Selbstbestimmungsrecht der Berlinerinnen und Berliner vor Beeinträchtigungen zu schützen. Daneben stand die gesetzliche Aufgabe, Gefährdungen für das Informationsgleichgewicht zwischen Parlament und Regierung zu beobachten, eher im Hintergrund. Daraus kann jedoch nicht der Schluß gezogen werden, daß derartige Gefährdungen nicht bestehen. In Zukunft wird sich der Berliner Datenschutzbeauftragte vielmehr verstärkt damit auseinanderzusetzen haben, welcher Art diese Gefährdungen sind und wie ihnen wirksam zu begegnen ist.

3.2 Gläserner Bürger: Online-Zugriffe

Nicht alles, was technisch machbar ist, kann bedenkenlos eingesetzt werden. Das gilt auch - und gerade - für die Informationstechnik. Die hiermit verbundenen Möglichkeiten können tief in das Persönlichkeitsrecht der Betroffenen eingreifen und ganz erheblich gesellschaftliche Verhältnisse durch Veränderung des Informationsgefüges beeinflussen.

In seinem Volkszählungsurteil hat das Bundesverfassungsgericht hierzu ausgeführt, daß das informationelle Selbstbestimmungsrecht - d. h. die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden - unter den Bedingungen der automatisierten Datenverarbeitung in besonderem Maße des Schutzes bedürfen. Hervorgehoben wurde die schnelle Abrufbarkeit personenbezogener Daten und die Möglichkeit der Zusammenfügung von Persönlichkeitsbildern, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann[81].

Auf diesem Hintergrund birgt die bereits dargestellte Vernetzung von Informationssystemen verschiedener datenverarbeitender Stellen besondere Gefahren. Sie ermöglicht, daß eine Stelle auf die Datenbestände einer anderen zugreift, ohne daß sie im Einzelfall bei der für die Datei verantwortlichen Stelle um eine Übermittlung von Daten ersuchen und dieser gegenüber ihre

81 BVerfGE 65, 1, 42

Anfrage begründen muß. Diese technische Möglichkeit erlaubt es, daß personenbezogene Daten - auch große Datenmengen - innerhalb kürzester Zeit bei der abrufenden Stelle vorhanden sind.

Die Datenschutz- und datenschutzrechtlichen Spezialgesetze regeln die Problematik unter der Bezeichnung „automatisierte Abrufverfahren" (§§ 10 BDSG, 15 BlnDSG); eingebürgert hat sich die Kurzbezeichnung „Online-Verfahren", wobei der Zugriff innerhalb der datenverarbeitenden Stellen damit nicht gemeint ist.

Die mit diesem Verfahren verbundenen Risiken für das informationelle Selbstbestimmungsrecht sind nicht zu unterschätzen, weil dadurch andere Stellen Verfügungsgewalt über Daten erhalten, die nur der datenverarbeitenden Stelle als „Herr der Daten" zusteht.

Eine vorherige Kontrolle der Berechtigung des Abrufes ist nicht möglich, was eine extensive Nutzung des Online-Anschlusses begünstigt. De facto greift die andere Stelle auf den fremden Datenbestand (zumindest lesend) zu, als ob es sich um eigene Daten handelt.

Die Datenschutzgesetze haben die Möglichkeit der Einrichtung von Online-Verbindungen deshalb beschränkt und lassen sie nur in besonders begründeten Ausnahmefällen zu.

Nach § 10 BDSG ist die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgabe oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die beteiligten Stellen haben zu gewährleisten, daß die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Der Bundesbeauftragte für den Datenschutz ist über die Einrichtung von Abrufverfahren zu unterrichten, an denen Stellen des Bundes beteiligt sind, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

§ 15 BlnDSG setzt für die Einrichtung einer Online-Verbindung eine besondere gesetzliche Erlaubnis voraus. Datenempfänger, Datenart, Zweck des Abrufes, Datensicherungs- und -kontrollmaßnahmen sind darüber hinaus vom Senat durch Rechtsverordnung festzulegen, und der Berliner Datenschutzbeauftragte ist vorher zu hören.

Das vom Gesetzgeber wegen seiner Eingriffsintensität zunächst eher als Ausnahme angesehene Verfahren, das einer Rechtfertigung bedarf, entwickelt sich in der Gesetzgebung jedoch zunehmend zum Regelfall, ohne daß besondere Anforderungen gestellt werden, mit der Folge, daß ein für den Betroffenen nahezu undurchschaubarer Datendschungel entsteht. Ob dieses Ergebnis noch mit dem vom Bundesverfassungsgericht geforderten Gebot der Transparenz der Datenverarbeitung vereinbar wäre, ist zu bezweifeln.

Vor jeder Einrichtung eines derartigen Verfahrens muß deshalb besonders kritisch geprüft werden, ob es überhaupt nötig ist und ob es im Hinblick auf eine besondere Eilbedürftigkeit und eine große Anzahl von Übermittlungen mit den Grundsätzen der Verhältnismäßigkeit und Zweckmäßigkeit vereinbar ist.

Online-Zugriffe auf Landessysteme nach Landesgesetzen

Aus dem Berliner *Melderegister (EWW)* dürfen folgende Stellen bestimmte Daten abrufen:

- die jeweils zuständigen Stellen der Bezirksämter zur Ausstellung der Lohnsteuerkarten und für andere durch Rechtsvorschrift zugewiesene Aufgaben,
- die Feuerwehr zur Einziehung von Benutzungsgebühren,
- die Polizei,
- die Personalausweisbehörde bei deutschen Einwohnern und ihren Kindern unter 16 Jahren,
- die Paßbehörde bei deutschen Einwohnern,
- die Zulassungsstelle für Kraftfahrzeuge.

Nach § 26 Abs. 3 Meldegesetz ist die Einrichtung solcher Verfahren nur zulässig, soweit die zum Abruf bereitgehaltenen Daten ihrer Art nach für den Empfänger erforderlich sind und das Bereithalten der Daten zum Abruf durch den Empfänger unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Durch technische und organisatorische Maßnahmen ist sicherzustellen, daß die Zulässigkeit des Abrufs im Einzelfall kontrolliert werden kann. Die abrufberechtigten Stellen, die Zwecke, zu denen sie abrufen dürfen, und die Daten, auf die sie zugreifen dürfen, sind in der Anlage 5 der Verordnung zur Durchführung des Meldegesetzes genannt.

Im Berliner Ausführungsgesetz zum Gerichtsverfassungsgesetz ist die Möglichkeit eines Online-Verfahrens für das *Staatsanwaltschaftliche Informationssystem AStA* vorgesehen. Der Abruf soll anderen Strafverfolgungsbehörden und Strafgerichten ermöglicht werden können.

Auf das *Automatisierte Liegenschaftsbuch (ALB)* haben die Senatsverwaltung für Stadtentwicklung und Umweltschutz, Vermessungsämter, Wohnungsämter, Bau- und Wohnungsaufsichtsämter einiger Bezirke und das Bezirkseinwohneramt Kreuzberg Online-Zugriffsmöglichkeiten. Geplant sind entsprechende Anschlüsse auch der anderen Bezirksämter und weitere umfangreiche Zugriffsmöglichkeiten auf das ALB und die automatische Liegenschaftskarte (ALK) des *Liegenschaftskatasters*. Hier sind neben den Grundstücksdaten die Personalien und - soweit verläßlich bekannt - die Anschriften von Eigentümern, Erbbauberechtigten und Nutzungsberechtigten von Grundstücken im Land Berlin gespeichert. Auf diese Daten sollen nach dem Entwurf einer Verordnung zum Gesetz über das Vermessungswesen in Berlin 31 Stellen die Erlaubnis zum Online-Zugriff erhalten[82]. Dazu zählen verschiedene Stellen bei der Senatsverwaltung für Bau- und Wohnungswesen, der Senatsverwaltung für Finanzen, der Senatsverwaltung für Stadtentwicklung und Umweltschutz, der Senatsverwaltung für Wirtschaft und Technologie und der Bezirksämter, die Grundbuchämter, die Finanzämter, die Oberfinanzdirektion, das Landesamt und die Ämter für die Regelung offener Vermögensfragen, das Landeskriminalamt, das Landeseinwohneramt, die Liegenschaftsgesellschaft der Treuhand-Anstalt, die BSR und die GASAG.

Online-Zugriffe auf Landessysteme nach Bundesrecht

Nach der Neufassung des § 117 BSHG dürfen die Träger der Sozialhilfe die Daten von Personen, die *Sozialhilfeleistungen* erhalten, durch ein automatisiertes Abrufverfahren abgleichen. Nach § 117 Abs. 2 BSHG i.V.m. dem Ausführungsgesetz zum BSHG können die Sozialämter der Bezirke im Rahmen von *BASIS* berlinweit auf die Daten der Sozialhilfeempfänger zugreifen[83]. Der Zugriff ist auf die Personalien und die Sozialversicherungsnummer der Betroffenen beschränkt.

Finanzämter und die OFD haben auf das Verfahren *„Dezentrale Computerleistung in den Finanzämtern" (DCL)* und damit auf die Steuerdaten aller Berliner Steuerpflichtigen Online-Zugriff[84]. Nach § 30 Abs. 6 AO ist der automatisierte Abruf von Daten nur zulässig, soweit er der Durchführung eines Verwaltungsverfahrens oder eines gerichtlichen Verfahrens in Steuersachen, eines Strafverfahrens wegen einer Steuerstraftat oder eines Bußgeldverfahrens wegen einer Steuerordnungswidrigkeit oder der zulässigen Weitergabe von Daten dient. Nach dem Entwurf einer Steuerdaten-Abruf-Verordnung[85], die sich derzeit zur Beratung im Bundesrat befindet, dürfen nicht nur die Mitarbeiter der Finanzämter zum Online-Abruf berechtigt werden, sondern auch besonders ermächtigte Amtsträger der Oberfinanzdirektion und Personen, die mit der Entwicklung oder Betreuung automatisierter Steuerdatenverfahren befaßt sind. Obwohl hierfür die Rechtsgrundlage in § 30 Abs. 6 AO fehlt, sind auch die Mitarbeiter der Rechnungshöfe in dem Verordnungsentwurf als abrufberechtigt vorgesehen.

82 vgl. 4.3
83 Jahresbericht 93, 4.9, vgl. unten 4.
84 Jahresberichte 1990 und 1991, 3.2
85 BR-Drs 787/94

Im *Schuldnerverzeichnis* werden so sensible Daten wie die Abgabe einer „eidesstattlichen Versicherung" im Zwangsvollstreckungsverfahren und Haftanordnungen zur Abgabe der „eidesstattlichen Versicherung" gespeichert. Online-Zugriffe auf die Schuldnerverzeichnisse der Amtsgerichte selbst sind zwar nicht vorgesehen; das am 1. Januar 1995 in Kraft getretene Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis[86] sieht jedoch vor, daß die Bezieher von Abdrucken aus dem Schuldnerverzeichnis - das sind die IHK, berufsständische Kammern, bundesweite und regionale Schuldnerverzeichnisse sowie nicht konkret benannte „Antragsteller, deren berechtigtem Interesse durch Einzelauskunft oder durch den Bezug von Listen ... nicht hinreichend Rechnung getragen werden kann" - Online-Verfahren ihrer mit dem Schuldnerverzeichnis der Gerichte identischen Datenbestände einrichten können. Die Einzelheiten, wie Verknüpfungsmöglichkeiten mit anderen Daten, die Ausgestaltung der Abrufverfahren (Authentifikation, Benutzerkennung, Protokollierung usw.) und Regelungen zum Ausschluß der Abrufberechtigung, sind in der ebenfalls am 1. Januar 1995 in Kraft getretenen Schuldnerverzeichnisverordnung (SchuVO) vom 15. Dezember 1994[87] enthalten. Welche Stellen hier Online-Zugriffe erhalten können, ist allerdings auch der Verordnung nicht zu entnehmen.

Nach der kürzlich novellierten *Grundbuchordnung*[88] dürfen Grundbücher künftig automatisiert geführt werden. Auch Online-Zugriffe auf Grundbücher werden zugelassen. Die Landesjustizverwaltungen dürfen „nur" folgenden Stellen Online-Zugriffe erlauben:

- Gerichten,
- Behörden (welchen, wird nicht ausgeführt),
- Notaren,
- öffentlich bestellten Vermessungsingenieuren,
- an dem Grundstück dinglich Berechtigten,
- einer von dinglich Berechtigten beauftragten Person oder Stelle,
- der Staatsbank Berlin sowie
- anderen Stellen oder Personen zur Bearbeitung von Anträgen aus Auskünften.

Auch für automatisiert geführte *Handelsregister* können Online-Zugriffe zugelassen werden[89]. Danach dürfen nicht näher bezeichnete öffentliche Stellen und auch private Stellen Daten aus dem Handelsregister abrufen.

In der novellierten *Gewerbeordnung* sind Online-Zugriffe auf die Gewerbedatenbanken, in denen die Daten aus Gewerbeanzeigen gespeichert sind, für nicht näher bezeichnete öffentliche Stellen vorgesehen. Nach einer Interessenabwägung zwischen den schutzwürdigen Interessen der Gewerbetreibenden und den öffentlichen Aufgaben unter Berücksichtigung der bekannten Kriterien „Vielzahl und Eilbedürftigkeit der Übermittlungen" kann der Leiter des Gewerbeamtes schriftlich festlegen, welche Stellen Zugriff auf die Gewerbedatenbank erhalten sollen.

Im Bereich der Wohnungsämter ist geplant, möglichst viele Schnittstellen zu anderen DV-Verfahren bereitzustellen. Insbesondere der Informationsaustausch innerhalb der Wohnungsämter und auch zwischen verschiedenen Ämtern der Bezirke soll durch Online-Verfahren vereinfacht werden. Gestützt auf § 79 SGB X soll auf das *Wohngeldverfahren* ein bezirksübergreifender Online-Zugriff erfolgen und den Wohngeldstellen ein Online-Zugriff auf *BASIS* ermöglicht werden sowie den Sozialämtern auf das Wohngeldverfahren.

Als ein weiteres Beispiel für den großzügigen Umgang mit dem Zulassen von Online-Verbindungen ist der Bundesrats-Entwurf eines *Strafverfahrensänderungsgesetzes*[90] zu nennen. Danach können Gerichte, Staatsanwaltschaften und andere Justizbehörden sowie sonstige Strafverfolgungsbehörden alle für ihre Aufgaben gespeicherten Daten dem gegenseitigen Zugriff freigeben. Durch die vorgeschlagene Regelung wird der wechselseitige unbeschränkte Zugriff auf die jeweiligen Informationssysteme ohne nähere Konkretisierung der betroffenen Daten und des Zwecks der Übermittlung eröffnet. Eine solche Regelung würde die Grundlage jedweder Online-Abfragen auch über die Länder- und Gewaltenteilungsgrenzen hinweg darstellen, ohne daß die Regelung an die unterschiedlichen Aufgabenstellungen anknüpft und das Zweckbindungsprinzip berücksichtigt wird.

Online-Zugriffe auf Bundessysteme durch Stellen des Landes Berlin

Die Polizei hat Zugriff auf das beim BKA geführte polizeiliche Informationssystem *INPOL* mit seinen verschiedenen Dateien. Grundlage für dieses im Verbund zwischen Bund und den Ländern betriebene Verfahren waren nicht spezifische Gesetze, sondern Beschlüsse der Innenministerkonferenz, die 1975 zu einer Gesamtkonzeption zusammengefaßt wurden. Die INPOL-Gesamtkonzeption wurde 1990 durch die „Grundsätze für die Zusammenarbeit von Bund und Ländern bei der polizeilichen Datenverarbeitung im Rahmen des Informationssystems der Polizei" (INPOL-Grundsätze) ergänzt und überarbeitet. Seit 1992 wird an einer Neukonzeption gearbeitet[91].

Nach § 6 Bundesverfassungsschutzgesetz sind die Verfassungsschutzbehörden verpflichtet, beim Bundesamt für Verfassungsschutz zur Erfüllung ihrer Unterrichtungspflichten gemeinsame Dateien zu führen, die sie im automatisierten Verfahren nutzen. Das Berliner Landesamt für Verfassungsschutz hat auf die im nachrichtendienstlichen Informationssystem *NADIS* gespeicherten Daten Zugriff.

Die Kfz-Zulassungsstelle beim Landeseinwohneramt und die Polizei haben Zugriff auf das *Zentrale Fahrzeugregister* beim Kraftfahrtbundesamt und die Polizei auch auf das örtliche Fahrzeugregister (§ 36 Straßenverkehrsgesetz - StVG), in denen Halter- und Fahrzeugdaten gespeichert sind. Die Polizei hat Zugriff auf die Halterdaten zum Zweck der Strafverfolgung und der Abwehr von Gefahren für die öffentliche Sicherheit sowie zur Verfolgung von bestimmten Ordnungswidrigkeiten mit Verkehrsbezug.

Nach § 30 a StVG dürfen aus dem *Verkehrszentralregister* an die Fahrerlaubnisbehörde beim Landeseinwohneramt und die Polizei durch Abruf im automatisierten Verfahren bestimmte Daten übermittelt werden. Im Verkehrszentralregister sind Verurteilungen durch Strafgerichte wegen Straftaten im Zusammenhang mit der Teilnahme im Straßenverkehr, Entscheidungen der Strafgerichte und der Verwaltungsbehörden auf Entzug der Fahrerlaubnis, Fahrverbote, Versagungen und Verzichte auf Fahrer- und Fahrlehrererlaubnis, Geldbußen für Verkehrsordnungswidrigkeiten unter bestimmten Voraussetzungen gespeichert.

Die Staatsanwaltschaft und die Steuerfahndung sollen nach dem am 1. Dezember 1994 in Kraft getretenen Verbrechensbekämpfungsgesetz[92] auf ein noch einzurichtendes bundesweites *Staatsanwaltschaftliches Informationssystem (SISY)* Zugriff erhalten.

Nach dem im *Ausländerzentralregistergesetz* vom 2. September 1994[93] aufgeführten Online-Verfahren kann für neun Bundesbehörden und verschiedene Landesbehörden der Online-Zugriff auf Daten des Ausländerzentralregisters zugelassen werden:

- die Ausländerbehörden,
- die Aufnahmeeinrichtungen des Asylverfahrensgesetzes,
- das Bundesamt für die Anerkennung ausländischer Flüchtlinge,
- den Bundesgrenzschutz,
- die Stellen eines Landes oder der Zollverwaltung, soweit sie grenzpolizeiliche Aufgaben wahrnehmen,
- sonstige Polizeivollzugsbehörden des Bundes und der Länder,
- die Staatsanwaltschaften,

86 BGBl. I 1994, 1566
87 BGBl. I, 3822
88 § 126 GBO, Art. 1
Gesetz zur Vereinfachung registerrechtlicher und anderer Verfahren (Registerverfahrenbeschleunigungsgesetz - RegVBG) vom 20. Dezember 1993 (BGBl. I, 2182)
89 § 9 a HGB, eingeführt durch Art. 5 RegVBG
90 Drs 620/94
91 Jahresbericht 1993, 4.5.1
92 BGBl. I, 3186 (§ 475 StPO)
93 BGBl. I, 2265

- das Zollkriminalamt,
- die Bundesanstalt für Arbeit und die Hauptzollämter zur Bekämpfung der illegalen Beschäftigung von Ausländern,
- die Bundesanstalt für Arbeit zur Geltendmachung von Ansprüchen,
- die Verfassungsschutzbehörden des Bundes und der Länder,
- den Militärischen Abschirmdienst (MAD),
- den Bundesnachrichtendienst (BND) sowie
- das Bundesverwaltungsamt bei Verfahren zur Erteilung von Einreise-Visa und Feststellung der Staatsangehörigkeit.

Im Gesetzgebungsverfahren wurde nicht überzeugend dargelegt, daß alle diese Stellen, insbesondere aber die Bundesanstalt für Arbeit, die Zollkriminalinstitute, die Verfassungsschutzbehörden oder der BND, einen derartigen Anschluß für ihre Aufgabenerfüllung benötigen. Eine besondere Eilbedürftigkeit und eine große Anzahl von Übermittlungen, die das Gesetz als Kriterien für die Zulassung des Online-Verfahrens vorsieht, sind hier nicht erkennbar.

Die Geheimdienste sollen – wie in der Begründung des Gesetzes vermerkt – auch deshalb einen Online-Anschluß erhalten, weil dadurch die besondere Vertraulichkeit ihrer Aufgabenerfüllung gewahrt würde. Akzeptiert man dies, wäre die Folge, daß für die Geheimdienste Online-Anschlüsse an alle möglichen Datenbanken einzurichten wären. Da die erforderliche Vertraulichkeit auch durch andere Formen der Datenübermittlung sichergestellt werden kann, ist die vorgesehene Online-Verbindung für die Geheimdienste nicht erforderlich und damit auch nicht zulässig.

Online-Zugriffe auf europäische Systeme durch Landesbehörden

Nach Art. 101 des Schengener Durchführungsübereinkommens[94] sollen der Polizeipräsident und die Ausländerbehörde Online-Zugriff auf das der Fahndung dienende *Schengener Informationssystem (SIS)* erhalten, die Ausländerbehörde jedoch nur in dringenden Fällen, sonst erfolgt der Zugriff über das Bundesverwaltungsamt.

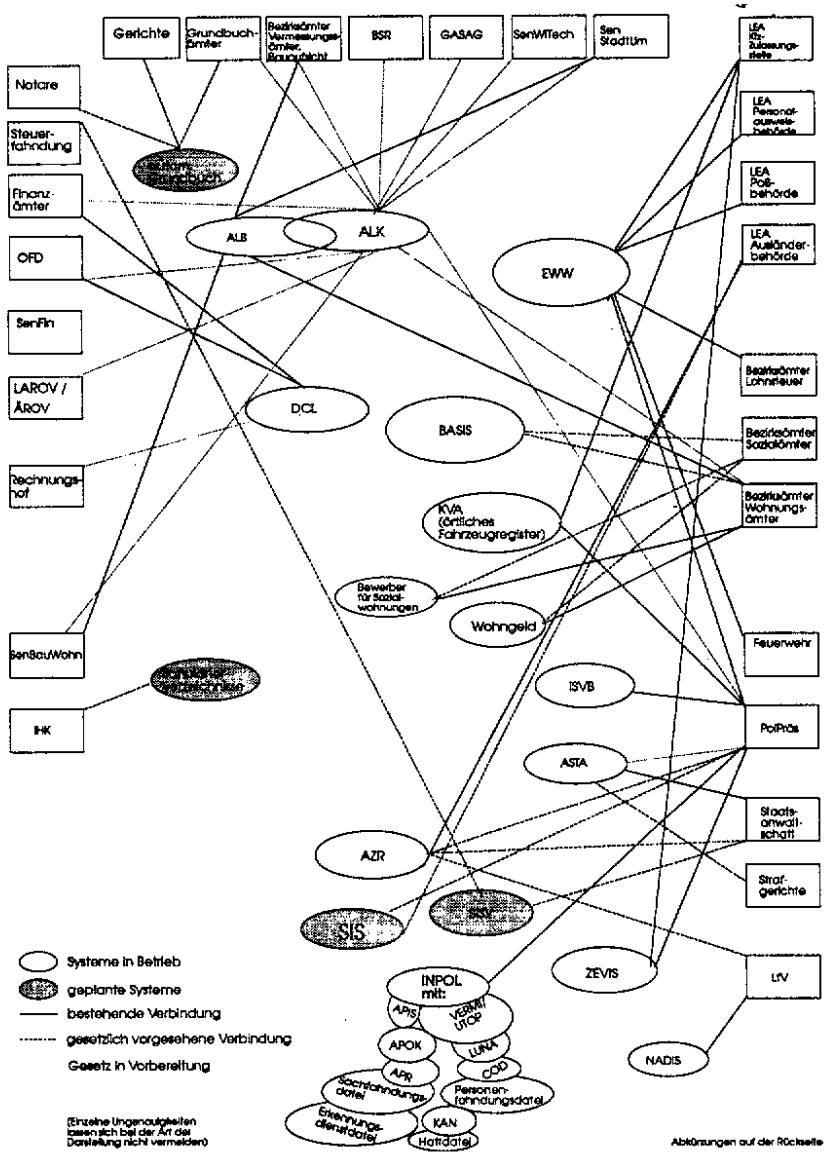
Folgende Bundesbehörden haben zudem Online-Zugriff:

- Bundeskriminalamt,
- Grenzschutzdirektionen und Grenzschutzdienststellen,
- Bahnpolizei/Flughäfen (Bundesgrenzschutz),
- Polizei- und Sicherheitsdienst des Deutschen Bundestages,
- Zollkriminalamt,
- Zollfahndungsdienststellen,
- Auslandsvertretungen (automatisiertes Sichtvermerksverfahren, automatisierter Telex-Zugriff).

Der Online-Zugriff auf *Europol* durch Landesbehörden ist nach dem derzeitigen Stand der Diskussion der Europol-Konvention nicht zu erwarten. Die Bundesländer streben an, Online-Befugnisse durch Polizeibehörden und Staatsanwaltschaften bei der Umsetzung einer Europol-Konvention in nationales Recht vorzusehen.

---

94 vgl. 4.6.1



ALB	Automatisiertes Liegenschaftsbuch bei der Senatsverwaltung für Bau- und Wohnungswesen
ALK	Automatisierte Liegenschaftskarte bei der Senatsverwaltung für Bau- und Wohnungswesen
APIS	Arbeitsdatei PIOS Innere Sicherheit
APOK	Arbeitsdatei PIOS Organisierte Kriminalität
APR	Arbeitsdatei PIOS Rauschgift
ÄROV	Ämter für die Regelung offener Vermögensfragen
ASTA	ADV-Verfahren Amts- und Staatsanwaltschaften
AZR	Ausländerzentralregister
BASIS	Berliner Automatisiertes Sozial- u. Jugendhilfe-Interaktionssystem
BSR	Berliner Stadtreinigungsbetriebe
DCL	Dezentrale Computerleistung in den Finanzämtern
EWW	Einwohnermeldewesen
GASAG	Berliner Gaswerke AG
IHK	Industrie- und Handelskammer
INPOL	Informationssystem der Polizeien der Länder beim undeskriminalamt
KAN	Kriminalaktennachweis
LAROV	Landesamt für die Regelung offener Vermögensfragen
LfV	Landesamt für Verfassungsschutz
LEA	Landeseinwohneramt
LUNA	Leuchtendatei für Unfallnachforschungen
NADIS	Nachrichtendienstliches Informationssystem
OFD	Oberfinanzdirektion
PIOS	Personen, Objekte, Informationen, Sachen
PolPräs	Der Polizeipräsident in Berlin
SenFin	Senatsverwaltung für Finanzen
SenStadtUm	Senatsverwaltung für Stadtentwicklung und Umweltschutz
SenWiTech	Senatsverwaltung für Wirtschaft und Technologie
SIS	Schengener Informationssystem
SISY	Staatsanwaltschaftliches Informationssystem (geplant)
VERMI/UTOT	Datei über Vermißte und unbekannte tote Personen
ZEVIS	Zentrales Verkehrsinformationssystem beim Kraftfahrtbundesamt mit Verkehrszentralregister und Zentralem Fahrzeugregister

3.3 Outsourcing - ein Weg zur schlanken Verwaltung?

Bereits im Jahresbericht 1992[95] hatten wir uns mit der Tendenz zum Downsizing einerseits und der zum Outsourcing andererseits beschäftigt: Was an Datenverarbeitung noch nicht mit dezentralen offenen Systemen - lokale Netze, Personalcomputer, UNIX-Mehrplatzsysteme - nahe am Anwender betrieben werden kann, was also den Einsatz komplexer, besonders leistungsstarker Systeme erfordert, die nur von ausgeprägten Spezialisten bedient werden können, wird ausgelagert in zentrale Rechenzentren. Da die Kapazitäten proprietärer Großsysteme nicht weniger schnell gestiegen sind wie die der Standard-Systeme, können sie wirtschaftlich nur sinnvoll ausgelastet werden, wenn sie ihre Dienstleistungen breit anbieten.

Somit ist es einerseits konsequent, wenn Überlegungen angestellt werden, jene Anwendungen, die wegen ihres Massenumfangs oder wegen ihrer besonderen Anforderungen an Prozessor- oder Speicherleistung noch nicht sinnvoll auf dezentralen Systemen betrieben werden können, bei externen Anbietern verarbeiten zu lassen. Andererseits ist klar, daß die Betreiber von Rechenzentren mit proprietären Systemen zur Auslastung ihrer Systeme offensiv ihre Dienstleistungen anbieten.

Outsourcing ist allgemein die Auslagerung von Unterstützungsleistungen bei der Durchführung eigener Aufgaben auf Organisationen (private Firmen oder öffentlich-rechtliche Institutionen), die sich auf solche Unterstützungsleistungen spezialisiert haben. Es ist ein Mittel zur organisatorischen Verschlankung der Verwaltung (lean administration): Jene Teile des organisatorischen Aufgabenlösungsprozesses, die nicht unmittelbar dem Organisationsziel dienen, sondern sie nur mittelbar als Dienstleistung unterstützen, werden ausgelagert. Interne Strukturen mit Dienstleistungscharakter werden an dafür spezialisierte Organisationen übertragen: Fahr- und Transportdienst, Kantinenbetrieb, Raumreinigung, Datenverarbeitung.

Insbesondere die automatisierte Datenverarbeitung gehört zu jenen Unterstützungsleistungen, die vermehrt auf professionelle Dienstleister übertragen wird. Outsourcing in der Datenverarbeitung ist keineswegs ein neues Phänomen. Service-Rechenzentren, Dienstleister für spezielle Aufgaben wie Datenerfassung, Mikroverfilmung, Aktenvernichtung gibt es schon seit langem, wenn auch nicht unter einem griffigen Stichwort, sondern als *Datenverarbeitung im Auftrag*. Die Möglichkeit, Aufgaben der Datenverarbeitung an spezialisierte Organisationen zu übertragen, ist seit Beginn der Datenschutzgesetzgebung vorgesehen gewesen, ein Grund, angesichts des Anwachsens der Auftragsvergabe nach außen, auf die rechtliche Situation dabei hinzuweisen:

§ 3 BlnDSG ermöglicht Behörden und sonstigen öffentlichen Stellen des Landes Berlin, personenbezogene Daten in ihrem Auftrag durch andere Personen und Stellen verarbeiten zu lassen. Dabei wird grundsätzlich kein Unterschied gemacht, ob diese anderen Personen oder Stellen private sind oder öffentlich-rechtlicher Natur sind. Es werden dabei folgende Rahmenbedingungen gesetzt:

- Die *datenschutzrechtliche Verantwortung* verbleibt beim Auftraggeber (§ 3 Abs. 1 Satz 1). Dies gilt insbesondere für jene Vorschriften, die die Zulässigkeit der Datenverarbeitung und die unmittelbaren Pflichten der Behörden gegenüber dem Betroffenen (Auskunft, Benachrichtigung, Berichtigung, Sperrung und Löschung) betreffen. Diese Vorschriften gelten für den Auftragnehmer nicht (§ 3 Abs. 2 Satz 1).

- Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten (§ 3 Abs. 2 Satz 2). Dies setzt aber voraus, daß der Auftraggeber solche *Weisungen zur Durchführung der Datenverarbeitung* und zur Umsetzung der technischen und organisatorischen Maßnahmen des Datenschutzes dabei unmißverständlich und revisionssicher, d. h. schriftlich im Rahmen des Kooperationsvertrages (heute Outsourcing-Vertrages) gegeben hat.

- *Weisungen*, die eine Datenverarbeitung betreffen, die *gegen Datenschutzvorschriften verstoßen*, oder Daten betreffen, die rechtswidrig erlangt wurden, darf eine öffentliche Stelle des Landes als Auftragnehmer nicht ausführen (§ 3 Abs. 2 Sätze 3 und 5). In diesem Falle ist die Aufsichtsbehörde des Auftraggebers ebenso zu benachrichtigen wie dieser selbst (§ 3 Abs. 2 Satz 4). Ein privater Auftragnehmer hat den Auftraggeber auf die Rechtswidrigkeit hinzuweisen (§ 11 Abs. 2 Satz 2 BDSG). Erfahrungen, wie ein privater Auftragnehmer sich seinen zahlenden Kunden gegenüber in einem solchen Falle verhält, liegen noch nicht vor.

- Der Auftraggeber hat den *Auftragnehmer* unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen *sorgfältig auszuwählen* (§ 3 Abs. 1 Satz 2). Wir gehen davon aus, daß nur das Landesamt für Informationstechnik in diesem Sinne pauschal als geeignet angesehen werden kann. Die Ausführungen in Abschnitt 2.3 bestätigen diese Position.

- Private Organisationen, bei denen das Land Berlin oder eine landesunmittelbare Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts Anteilsmehrheiten besitzen oder über Stimmenmehrheiten verfügen, unterliegen der *Kontrolle des Berliner Datenschutzbeauftragten* (§ 3 Abs. 3 Satz 1), während der Betriebs- und Geschäftszeiten unter Einschränkung des Grundrechts auf Unverletzlichkeit der Wohnung (§ 3 Abs. 3 Satz 2).

Besonders wichtig bei der Auftragsvergabe an private Unternehmen, wie sie derzeit verstärkt durch die Berliner Verwaltung praktiziert wird, sind die besonderen Regelungen von § 3 Abs. 4:

- Bei Auftragnehmern, die nicht dem Berliner Datenschutzgesetz unterliegen, muß der Auftraggeber vertraglich sicherstellen, daß der Auftragnehmer die Vorschriften des Berliner Datenschutzgesetzes befolgt (§ 3 Abs. 4 Satz 1, 1. Halbsatz). Wird der Auftrag in Berlin ausgeführt, hat sich der Auftragnehmer der Kontrolle des Berliner Datenschutzbeauftragten (§ 3 Abs. 4 Satz 1, 2. Halbsatz), anderenfalls der des jeweiligen Landesdatenschutzbeauftragten zu unterwerfen (§ 3 Abs. 4 Satz 2). Datenschutzbeauftragter und die Datenschutzaufsichtsbehörde des privaten Auftragnehmers sind vom Auftraggeber zu unterrichten (§ 3 Abs. 4 Satz 3).

Die Datenverarbeitung im Auftrag ist deutlich von der Übertragung ganzer Aufgaben an Dienstleister zu unterscheiden, zu deren Erfüllung jedoch personenbezogene Daten verarbeitet werden[96]. In diesem Falle ist die Datenverarbeitung nicht Zweck des Auftrages, sondern Mittel zum Zweck, der in der Erfüllung einer umfassenderen Aufgabe liegt. In diesem Falle liegt keine Auftragsdatenverarbeitung vor. Wenn eine öffentliche Stelle einem solchen Dienstleister personenbezogene Daten zur Verfügung stellen will, damit die Aufgabe erfüllt werden kann, liegt eine Datenübermittlung vor, deren Rechtmäßigkeit nach §§ 12 bis 15 BlnDSG zu beurteilen ist.

Wenn es sich bei der übertragenen Aufgabe um eine Aufgabe der öffentlichen Verwaltung i.S.v. § 2 Abs. 1 Satz 2 BlnDSG handelt, so fällt auch ein privater Auftragnehmer in den Anwendungsbereich des Berliner Datenschutzgesetzes. Ist dies nicht der Fall, gelten die Vorschriften desjenigen Datenschutzgesetzes, in dessen Geltungsbereich der Auftragnehmer im Normalfall fällt.

Deutlich wird die häufig mißverstandene Problematik am Beispiel der Projekte zu Bürgerbüros. Diese in zwei Bezirksämtern neu eingerichteten Stellen sollen den Fachämtern bestimmte publikumsbezogene Aufgaben (Bürgerberatung, Ausgabe von Formularen, Entgegennahme von Anträgen, Entscheidung über Anträge in einfachen Fällen) abnehmen und zu diesem Zwecke personenbezogene Daten verarbeiten, die die Fachämter bereitstellen oder die beim Bürger erhoben werden. Hier handelt es sich um eine Datenübermittlung zwischen Bürgerbüro und Fachamt, nicht nur um die Bereitstellung von Daten zur Auftragsdatenverarbeitung[97].

95 Jahresbericht 1992, 2.1

96 vgl. Jahresbericht 1993, 3.2 und Anlage ...

97 zur ausführlicheren Behandlung s. u. 3.2

Bei Kontrollmaßnahmen sind bezüglich der Umsetzung dieser Vorschriften erhebliche Defizite festgestellt worden. Die „historisch gewachsene" Zusammenarbeit der Berliner Behörden mit dem Landesamt für Informationstechnik war in wichtigen Fällen noch nicht in konkrete Weisungen, Vereinbarungen oder Verträge umgesetzt worden. Auf Grund früherer Beanstandungen ist erst jetzt die Zusammenarbeit zwischen dem Landeseinwohneramt und dem Landesamt für Informationstechnik bezüglich des ADV-Verfahrens *Einwohnerwesen (EWW)* nach den Vorgaben des § 3 BlnDSG geregelt worden. Die Auftragsdatenverarbeitung des LIT für das Statistische Landesamt ist dagegen noch ohne konkrete Regelungen[98].

Obwohl Auftragsdatenverarbeitung durch private Unternehmen, speziell für Datenerfassung, Mikroverfilmung und Datenträgervernichtung bereits allgemein üblich ist, liegen uns bisher nur zwei Unterrichtungen gemäß § 3 Abs. 4 Satz 3 BlnDSG vor.

Die Bereitsstellung von personenbezogenen Daten für den Auftragnehmer, damit dieser den Auftrag ausführen kann, stellt keine *Übermittlung der Daten* i.S.v. § 4 Abs. 2 Nr. 4 BlnDSG dar. Da also die Weitergabe von Daten an Dritte nur bei Übermittlungen rechtlichen Beschränkungen unterliegt, gibt es keine grundsätzlichen Einwände gegen die Auftragsdatenverarbeitung durch öffentliche oder private Dritte, also in diesem Falle nicht gegen das Outsourcing.

Anders kann der Fall gelagert sein, wenn die Daten einem Offenbarungsverbot unterliegen, weil bei der Auftragsdurchführung dem Auftragnehmer die Daten in der Regel offenbart werden. Für *Sozialdaten,* deren Offenbarung in §§ 67 - 78 SGB X abschließend geregelt ist, sind in § 80 SGB X die Regeln definiert, unter denen sie im Auftrag durch Dritte verarbeitet werden dürfen. Dabei werden die ansonsten geltenden Regeln erheblich verschärft.

Für Daten, die der *ärztlichen Schweigepflicht* unterliegen, gilt dies nicht. Die Offenbarungsbefugnisse für solche Daten sind abschließend in § 2 Berufsordnung der Ärztekammer Berlin und § 26 Landeskrankenhausgesetz geregelt. Regelungen, die die Offenbarung von personenbezogenen medizinischen Daten zu Zwecken der Auftragsdatenverarbeitung erlauben, gibt es nicht. Daher ist sie verboten, wenn nicht andere Offenbarungsbefugnisse herangezogen werden können. Solche Offenbarungsbefugnisse gibt es nicht an Datenverarbeiter außerhalb des jeweiligen Krankenhauses.

Bereits 1986 hatte die Konferenz der Datenschutzbeauftragten in einer Entschließung festgestellt, daß wegen der ärztlichen Schweigepflicht die Verarbeitung medizinischer Daten eines Krankenhauses bestenfalls in einem anderen Krankenhaus erfolgen darf[99].

Trotz all dieser rechtlichen Hindernisse erfolgt in den Berliner Krankenhäusern der derzeit wichtigste Outsourcing-Prozeß. Mehrere Krankenhäuser beabsichtigen, ihre eigene Datenverarbeitung in Zukunft einzuschränken und dafür die Leistungen eines Rechenzentrums in Anspruch zu nehmen, das von einem Outsourcing-Unternehmen betrieben wird. Darüber hinaus soll die gleiche Firma bei diversen Krankenhäusern die Fernwartung der proprietären Systeme übernehmen.

Wir haben die Firma zum Versuch angeregt, das mit der Auftragsdatenverarbeitung bei Daten, die der ärztlichen Schweigepflicht unterliegen, verbundene Dilemma mit technischen Mitteln zu lösen. Damit wäre ein Beitrag zur Lösung eines Grundsatzproblems geleistet, der auch bei anderen ähnlich gelagerten Fällen Vorbildfunktion haben könnte.

Das von der Firma vorgelegte Konzept beruht auf folgenden technischen Möglichkeiten:

- Den einzelnen Krankenhäusern wird im proprietären Großrechner der Firma eine eigene virtuelle Betriebssystemumgebung zur Datenverarbeitung auf dem Host, der Speicherung auf Festplatten und der Datensicherung und Archivierung auf Magnetbändern bereitgestellt. Damit ist den Krankenhäusern der Zugriff auf Daten anderer Krankenhäuser wirksam verwehrt.
- Der Betrieb des virtuellen Betriebssystems und der Anwendungen sowie der Ausdruck von Daten erfolgt über auch weiterhin von den Krankenhäusern vorzuhaltende Systeme bei den Krankenhäusern selbst.
- Die von der Gesellschaft für Systemforschung und Dienstleistungen im Gesundheitswesen mbH Berlin (GSD) entwickelten Anwendungsverfahren und Programm- und Datenstrukturen stehen der Firma nur als ausführbarer Code, also nicht als Quellprogramme, zur Verfügung, so daß eine Interpretation der Daten für die Firma nicht möglich ist.
- Die übergeordnete Verwaltung des virtuellen Betriebssystems durch einen sog. Hypervisor schließt es ebenfalls aus, daß dieser ohne ein besonderes Paßwort, das nur den Krankenhäusern zur Verfügung steht, Zugang zu interpretationsfähigen Anwendungsdaten erhält. Ein Fall, in dem das Krankenhaus dem Hypervisor dieses Paßwort preisgeben muß, wird ausgeschlossen.
- Zwischen den Krankenhäusern und dem Firmen-Rechenzentrum erfolgt die Datenübertragung verschlüsselt über Standleitungen.
- Die Daten auf den Sicherungsbändern und -kassetten werden anwendungsabhängig und paßwortgeschützt komprimiert. Sie sind durch ein Fremdsystem nicht mehr interpretierbar.

Das Konzept berücksichtigt noch weitere Maßnahmen im Detail, mit denen verhindert wird, daß andere als der Auftraggeber die personenbezogenen Daten zur Kenntnis nehmen können.

Unter diesen Voraussetzungen haben wir es akzeptiert, daß ein Outsourcing bei der Verarbeitung von personenbezogenen Daten erfolgt, die der ärztlichen Schweigepflicht unterliegen.

3.4 Modellbezirksamt

1993 wurde in Weißensee und im Oktober 1994 in Köpenick als erster Schritt zum „Modellbezirksamt" ein *Bürgerbüro* eröffnet. Durch die Bündelung von Aufgaben soll den Bürgern der Weg zu unterschiedlichen Behörden erspart und stattdessen *eine* Anlaufstelle für die verschiedensten Anliegen angeboten werden. Als Nebeneffekt soll dadurch der Publikumsverkehr in den Fachabteilungen, die sich dann verstärkt auf ihre eigentlichen Aufgaben konzentrieren können, reduziert werden.

Mit Anträgen auf einen Wohnberechtigungsschein, in sozialhilfe- und melderechtlichen Angelegenheiten bis hin zur Ausstellung von Ferienpässen sollen die Bürger sich an das Bürgerbüro wenden können. Hier sollen nicht nur die Formulare für die verschiedensten Anträge erhältlich sein, sondern auch eine Beratung und Hilfe beim Ausfüllen von Formularen erfolgen sowie - z. B. bei der Erteilung von Wohnberechtigungsscheinen - gleich über Anträge entschieden werden.

Wir begrüßen dieses Projekt, da auch beim Datenschutz der Gedanke der Bürgernähe im Vordergrund steht. Durch die Zusammenfassung der verschiedenen Aufgaben, bei denen in einer Hand eine Fülle personenbezogener Daten zusammenkommt, sind jedoch bestimmte datenschutzrechtliche Anforderungen einzuhalten. Auch dies ist Voraussetzung für die notwendige Akzeptanz dieser Einrichtungen bei den Bürgern.

Die Senatsverwaltung für Inneres hat uns frühzeitig eingebunden und mit umfangreichen Papieren versorgt. Schon in der Problemanalyse war sich die eingesetzte Projektgruppe darüber im klaren, daß die geplanten Maßnahmen einen großen Klärungsbedarf im Bereich des Datenschutzes hervorrufen werden. Datenschutzfragen sind in der Folge allerdings nur noch im Zusammenhang mit der Einführung der automatisierten Datenverarbeitung berücksichtigt worden.

Bislang ging auch die von der Senatsverwaltung für Inneres eingesetzte Projektgruppe davon aus, daß die Tätigkeit der Bürgerbüros eine *Datenverarbeitung im Auftrag* ist, die Daten ratsuchender oder antragstellender Bürger also im Auftrag und in der datenschutzrechtlichen Verantwortung der Fachämter (z. B. des Sozialamtes oder des Wohnungsamtes) verarbeitet werden. Diese Ansicht ist unzutreffend.

98 siehe Abschnitt 4.6.4
99 Entschließung vom 14. März 1986

Vielmehr erfüllen die Bürgerbüros mit ihren weitgehenden Befugnissen im Beratungsbereich eigene Aufgaben und unterliegen damit bei dem Umgang mit personenbezogenen Daten besonderen Zulässigkeitsvoraussetzungen. Sie verarbeiten die personenbezogenen Daten nach den §§ 25 Verwaltungsverfahrensgesetz (VwVfG), 14 ff. Sozialgesetzbuch (SGB) I im Rahmen eigener Beratungstätigkeit. Soweit nicht bereits geschehen, ist ein Organisationsakt - beispielsweise ein Bezirksamtsbeschluß - erforderlich, um diese zunächst ausschließlich den Fachämtern obliegenden Beratungsaufgaben dem Bürgerbüro zu übertragen[100].

Bei einer Zusammenfassung verschiedenster Aufgaben sind der Gestaltungsfreiheit hinsichtlich der Organisation und der Geschäftsverteilung jedoch durch das Recht auf informationelle Selbstbestimmung Grenzen gesetzt.

Personenbezogene Daten dürfen nur für die gesetzlich bestimmten Zwecke genutzt werden[101]. Zur Sicherung der Zweckbindung ist bei der Verarbeitung personenbezogener Daten auf die jeweilige gesetzlich zugewiesene Aufgabe und die Organisationseinheit, die für sie zuständig ist (sog. *funktionaler Behördenbegriff*[102]) abzustellen. Die Verwendung für einen anderen Zweck - z. B. durch Übermittlung - unterliegt besonderen Zulässigkeitsvoraussetzungen. Ihre Funktion als Schranke gegen eine unkontrollierte Zweck- und Aufgabenentfremdung können die Übermittlungsvorschriften jedoch nur erfüllen, wenn die beteiligten Institutionen immer dann, wenn sie unterschiedliche Aufgaben wahrnehmen, auch als verschiedene Stellen betrachtet werden. Das Bundesverfassungsgericht hat im Volkszählungsurteil aus dem Grundrecht auf Datenschutz auch den Grundsatz der informationellen Gewaltenteilung abgeleitet[103].

Auf den ersten Blick scheint das Bürgerbüro mit seiner Zusammenfassung von Aufgaben verschiedenster Stellen diesem Grundsatz entgegenzustehen. Zwar bestehen aus datenschutzrechtlicher Sicht keine Bedenken, wenn eine strikte funktionale Aufgabentrennung beibehalten wird, z. B. wenn jeweils ein Mitarbeiter nur eine Aufgabe wahrnimmt. Da aber bei der Erfüllung mehrerer Funktionen durch *einen* Mitarbeiter im Bürgerbüro Übermittlungsverbote nicht greifen können, weil er bei der Beratung Informationen aus verschiedenen Bereichen unmittelbar erhält, sind stattdessen *Verwertungsverbote* für die bekanntgewordenen Daten zu beachten. Vor jeder Nutzung personenbezogener Daten zu anderen Zwecken ist von den Mitarbeitern des Bürgerbüros zu prüfen, ob die Einzeldaten zu diesem Zweck genutzt oder an andere Stellen übermittelt werden dürfen. Wenn dies nicht der Fall ist, dürfen die Daten in einem anderen Zusammenhang nur mit der ausdrücklichen Einwilligung des Betroffenen genutzt werden und unterliegen ansonsten einem Verwertungsverbot.

Darüber hinaus gilt es, bei der Zusammenlegung der unterschiedlichen Aufgaben entstehende *Interessenkollisionen* zu vermeiden. Bei der Wahrnehmung von Aufgaben beispielsweise der Ordnungs- und der mit dem Sozialgeheimnis als besonderem Amtsgeheimnis versehenen Leistungsverwaltung muß dafür Sorge getragen werden, daß durch eine personelle - u. U. sogar durch eine räumliche - Trennung derartige Interessenkonflikte nicht entstehen können.

In diesen Fällen läßt sich die Allzuständigkeit eines Bürgerbüromitarbeiters nicht konsequent durchführen. Im Hinblick auf die Zahl der Mitarbeiter und die sich zwangsläufig ergebende Spezialisierung der Beschäftigten läßt sich das Problem nach unserer Auffassung durch Arbeitsgruppen auffangen.

Aus dem datenschutzrechtlichen Erfordernis der klaren *Trennung von Behördenfunktionen* sowie der strikten Zweckbindung der für die jeweilige Aufgabe erhobenen und genutzten personenbezogenen Daten folgt auch, daß der Betroffene das Recht hat zu entscheiden, ob er das zentrale Beratungs- und Bearbeitungsangebot nutzt - mit der Folge, daß im Bürgerbüro Angaben aus den unterschiedlichen Lebensbereichen bekannt werden - oder weiter die verschiedenen Fachämter in Anspruch nehmen will. Auf diese *Wahlmöglichkeit* muß er vor Beginn der Beratung in geeigneter Form hingewiesen werden.

Die einzelnen Arbeitsschritte des Bürgerbüros sind datenschutzrechtlich unterschiedlich zu bewerten:

Bereits beim *Abholen von Formularen* werden Daten offenbart. Allein durch den Kontakt mit dem Bürger - beispielsweise bei der Ausgabe von Vordrucken - entsteht zwar noch kein Personenbezug, aber immerhin Personenbeziehbarkeit. Dies kann insbesondere im Zusammenhang mit der Verarbeitung von Sozialdaten Bedeutung haben. Der Betroffene muß anonym bleiben können. Aus diesem Grund müssen die Formulare auch ausliegen, damit sich der Betroffene - ohne daß er sich oder sein Anliegen zu erkennen geben muß - bedienen kann.

Eine Erhebung personenbezogener Daten findet hier nicht statt, da kein zielgerichtetes Beschaffen von personenbezogenen Daten vorliegt. Bei diesem Arbeitsschritt ist lediglich ein Hinweis auf die Freiwilligkeit der Inanspruchnahme des Bürgerbüros erforderlich.

Will der Betroffene die *Vordrucke* selbst ausfüllen und *verschlossen übergeben*, findet eine Datenerhebung ebenfalls nicht statt. Das Bürgerbüro hat für eine verschlossene Weiterleitung zu sorgen. Hier ist ebenfalls lediglich ein Hinweis auf die Freiwilligkeit der Inanspruchnahme des Bürgerbüros erforderlich.

Wird vom Bürger ein *ausgefülltes Formular offen übergeben*, hat das Bürgerbüro für eine verschlossene Weiterleitung an das jeweilige Fachamt zu sorgen[104]. Für die Transportsicherung - und damit einhergehend die Verpflichtung, die unbefugte Kenntnisnahme Dritter zu verhindern - ist das Bürgerbüro verantwortlich. Da keine Erhebung personenbezogener Daten durch oder für das Bürgerbüro stattfindet, sondern vielmehr für das Fachamt, ist auch insoweit lediglich der Hinweis auf die Freiwilligkeit der Inanspruchnahme des Bürgerbüros erforderlich.

Wenn im Zusammenhang mit einer *Beratung* oder bei Hilfestellungen beim Ausfüllen von Formularen im Bürgerbüro personenbezogene Daten bekannt werden - was der Regelfall sein dürfte -, kann die Verarbeitung mangels gesetzlicher Erhebungsbefugnis für diese Beratungsaufgaben nur auf die *Einwilligung* des Betroffenen gestützt werden. Ihre Wirksamkeit hängt von verschiedenen Voraussetzungen ab (Schriftform, Aufklärung). Es könnte hierfür ein gesondertes Formular entworfen werden, damit die bereits vorhandenen Einheitsvordrucke, die diese Einwilligungsklausel nicht enthalten, verwandt werden können.

Bei der *Weitergabe der Daten an das Fachamt* handelt es sich in diesem Fall um eine Übermittlung. Die Weiterverarbeitung erfolgt nach § 12 Abs. 1 Satz 2 BlnDSG hier zum gleichen Zweck und ist damit zulässig.

Hat das *Bürgerbüro* eine *Entscheidungsbefugnis*, z. B. bei der Erteilung von Wohnberechtigungsscheinen, handelt es sich um eine Funktionsübertragung mit der Folge, daß der Zugriff auf die Daten der originär zuständigen Stelle sowie die Weitergabe der Daten dorthin interne Vorgänge darstellen und keiner ausdrücklichen Rechtsgrundlage bzw. Einwilligung bedürfen (§ 11 Abs. 1 BlnDSG). Weil das Bürgerbüro als Fachamt auftritt, kann auf die Einwilligungen der Antragsteller verzichtet werden, wenn die Fachdienststelle Erhebungs- und Weiterverarbeitungsbefugnisse hat.

Zur Erfüllung ihrer Aufgaben sollen die Bürgerbüros auch *Online-Zugriffe* auf das Melderegister und das WBS-Verfahren erhalten. Nach § 15 BlnDSG darf ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte nur eingerichtet werden, wenn ein Gesetz dies ausdrücklich zuläßt. Die Vorschrift über die Zulässigkeit des einzelnen Abrufes bleibt unberührt. Dies ist hinsichtlich des *EWW-Verfahrens* unproblematisch, da das Meldegesetz eine Befugnis enthält und die Einzelheiten in der DVO-Meldegesetz bzw. der Anlage dazu geregelt sind.

100 s. o. Outsourcing, 2.4.3
101 BVerfGE 65, 1, 46
102 § 4 Abs. 3 Nr. 1 BlnDSG
103 BVerfGE 65, 1

104 vgl. u. a. unseren Jahresbericht 1987, 5.7

Etwas anderes gilt für den Zugriff auf das *WBS-Verfahren.* Sofern dem Bürgerbüro die Entscheidungsbefugnis vom Bezirksamt übertragen worden ist, greift es als datenverarbeitende Stelle „Wohnungsamt" auf das WBS-Verfahren – also auf die eigenen Daten – zu. Insoweit handelt es sich nicht um ein automatisiertes Abrufverfahren durch Dritte mit der Folge, daß kein Gesetz erforderlich ist.

Wird das Bürgerbüro beratend anstelle des Fachamtes tätig – es kommt nicht zur Entscheidung bzw. sie ist – aus welchen Gründen auch immer – überhaupt nicht gewollt –, geschieht dies im Rahmen der gesetzlichen Beratungsaufgabe des § 25 VwVfG. Der Zugriff erfolgt als datenverarbeitende Stelle „Bürgerbüro". Für die Einrichtung eines Online-Verfahrens in diesem Zusammenhang ist eine Rechtsgrundlage erforderlich, die noch zu schaffen ist. Die gesetzliche Grundlage ist zwingend erforderlich, da nach allgemeiner Lebenserfahrung nicht in jedem Fall eine Entscheidung getroffen wird. Es bietet sich an, die Befugnis zur Einrichtung des Abrufverfahrens in das IVG mit der Ermächtigung zum Erlaß einer Rechtsverordnung aufzunehmen.

Bis zur Schaffung einer Rechtsgrundlage ist vor dem jeweiligen Zugriff im Einzelfall die Einwilligung des Betroffenen erforderlich. Der Bürger sollte *vor* der Erteilung der Einwilligung seinen Datensatz bzw. die Daten, die abgerufen werden können, zur Kenntnis erhalten. Er soll wissen, was das Bürgerbüro zu sehen bekommt, um entscheiden zu können, ob er überhaupt seine Einwilligung geben will (informierte Einwilligung). Jeder Zugriff im Online-Verfahren muß nach § 5 Abs. 3 Nr. 6 BlnDSG protokolliert werden.

Die Befugnisse und Verpflichtungen der Mitarbeiter der Bürgerbüros sind in einer Dienstanweisung festzulegen, die die Besonderheiten des Sozialdatenschutzes, die Verpflichtung zur Fortbildung der Mitarbeiter, die Dienstaufsicht und Kontrollmechanismen berücksichtigt sowie regelt, wie dem funktionalen Behördenbegriff in Interessenkonflikten Rechnung getragen werden soll. Darüber hinaus sind den Mitarbeitern klare Handlungsdirektiven – beispielsweise hinsichtlich der Einholung der erforderlichen Einwilligungen für die Verarbeitung der personenbezogenen Daten – zu geben. Hier sollte auch das Recht des Betroffenen festgeschrieben werden, vor einem beabsichtigten Online-Zugriff die zum Abruf bereitstehenden Daten zur Kenntnis nehmen zu können und die weiteren Rechte der Betroffenen (z. B. Auskunft, Sperrung, Löschung usw.) sowie die Pflichten der datenverarbeitenden Stelle erläutert werden.

Eine solche Konzeption der Datenverarbeitung im Bürgerbüro/Modellbezirksamt nimmt den Bürger als „Kunden" des „Unternehmens Stadt" ernst, statt die Daten ohne sein Wissen und ohne ihm eine Einflußmöglichkeit zu verknüpfen und zu anderen Zwecken als denjenigen zu nutzen, für die der Bürger sie der Verwaltung ursprünglich offenbart hat, zu geben, in einem großen Datenpool zusammenzuführen.

3.5 Telefax – eine Pannengeschichte

Ein Mitarbeiter der Senatsverwaltung für Bau- und Wohnungswesen traute seinen Augen nicht: Auf seinem Telefax-Gerät erschienen zwei als vertraulich gekennzeichnete Schreiben der Senatsverwaltung für Inneres, in denen diese sich zur Eignung von bestimmten Mitarbeitern für die weitere Tätigkeit im öffentlichen Dienst äußerte. Aber der Adressat war nicht die Senatsverwaltung für Bau- und Wohnungswesen, sondern das Landesverwaltungsamt.

Wenn es denn eilig wird, greifen Behörden auch bei vertraulichen Sendungen gern auf den Telefax-Dienst zurück, der so schnell und direkt und darüber hinaus auch preisgünstig Mitteilungen transportieren kann. Da aber im Vergleich zum Einsatz von Boten oder sogar der Briefpost der Telefax-Dienst größere Risiken für die Vertraulichkeit der Nachrichten bei der Übermittlung birgt, bleiben die Pannen nicht aus. Im beschriebenen Fall handelt es sich um einen Wählfehler, wie er auch beim Telefonieren immer wieder vorkommt. Nur gibt es anders als beim Telefon keinen Gesprächspartner, der auf die *Falschverbindung* hinweisen kann, bevor Vertrauliches ausgeplaudert wird.

Die Faxgeräte zeigen zwar an, welche Nummer angewählt wurde, bevor die Verbindung zustande kommt. Wenn aber diese Anzeige der Telefax-Bedienkraft entgeht und sie nicht erkennt, daß die Nummer falsch ist, erfolgt die Übertragung ungehindert und vollständig. Dem kann zwar entgegengehalten werden, daß der Anteil der Telefax-Anschlüsse im Fernsprechnetz im Vergleich zu normalen Fernsprechanschlüssen noch so verschwindend klein ist, daß versehentliche Fehlanwahlen keinen Schaden anrichten, weil es unwahrscheinlich ist, daß auf der Empfängerseite auch ein Telefax-Gerät installiert ist, welches die Sendung entgegennehmen kann. Bestimmte Umstände widerlegen in diesem Zusammenhang jedoch die Wahrscheinlichkeitsrechnung immer wieder, so daß die Zahl der uns bekannt werdenden Fehlsendungen nicht unbeachtlich ist.

Im oben beschriebenen Fall wurde der Wahrscheinlichkeit durch den Umstand nachgeholfen, daß im Bereich der Telefonnebenstellenanlage am Fehrbelliner Platz, zu dem mehrere Behörden gehören, diverse Telefax-Anschlüsse mit aufeinanderfolgenden Telefonnummern versehen worden sind. So sind z. B. zwischen den Nebenstellennummern 3100 und 3150 mehr als die Hälfte der Anschlüsse nach dem Telefonverzeichnis der Berliner Verwaltung Telefaxanschlüsse der Senatsverwaltungen für Inneres, Finanzen, Gesundheit und Bau- und Wohnungwesen, des Statistischen Landesamtes, des Landesverwaltungsamtes und des Hauptpersonalrates. In diesem Nummernbereich hat sich der oben beschriebene Fall abgespielt. Die beschriebenen Voraussetzungen sind jedoch auch bei anderen Nebenstellenanlagen des Landes Berlin gegeben. So z. B. auch im Bezirksamt Zehlendorf:

Eine Mitarbeiterin des Büros der Bezirksverordnetenversammlung staunte nicht schlecht, als die vier Worte „Per Telefax – Vertraulich – Verschlossen" eine Faxsendung einleiteten, mit der die Senatsverwaltung für Justiz Informationen zu einer amtsärztlichen Untersuchung eines Beamten übermittelte. Adressat war allerdings der zuständige Amtsarzt.

Auch hier lag offenkundig ein Wählfehler vor, der mit der notwendigen Aufmerksamkeit hätte vermieden werden können. Die Senatsverwaltung sprach erwartungsgemäß vom bedauerlichen Einzelfall, der sich nicht wiederholen würde. Allerdings setzt dies voraus, daß man sich darüber klar wird, daß die Versandform mit Telefax sich nur unter sehr restriktiven Bedingungen und dann nur im besonderen Notfall für Post mit dem Vermerk „Verschlossen – Vertraulich" eignet.

Im Büro eines Unternehmens wunderte man sich über die wiederholten Faxsendungen aus dem Urban-Krankenhaus. Diesmal ging es um den Befundbericht für eine Maßnahme in einer Rehabilitationsklinik, Daten also, die der ärztlichen Schweigepflicht unterfallen und die an diese Klinik gesendet werden sollten.

Das Krankenhaus begründete dies mit der Fehlfunktion eines überalterten Telefax-Gerätes. Bereits zwei Jahre zuvor mußten wir Fehlsendungen aus dem gleichen Krankenhaus an den gleichen falschen Adressaten beanstanden, u.a. einen Unterbringungsantrag nach dem Psychiatriegesetz, der für das Amtsgericht Tempelhof-Kreuzberg bestimmt war. Dies geschah in der Verantwortung der Abteilung Gesundheit des Bezirksamtes Kreuzberg. Damals wurde die Ursache offensichtlich konkreter ermittelt: Statt der Normalanwahl war von der Bedienkraft die Option *„Kurzwahl"* gewählt worden, dann aber doch eine vollständige Nummer eingegeben worden. Die erste Ziffer der angewählten Nummer wurde vom Gerät als Kurzwahlnummer interpretiert – und schon gingen die Faxe an die Haustechnikfirma, mit der das Krankenhaus als Kunde ebenfalls über Telefax kommuniziert. Auch hier wurde der Wahrscheinlichkeit einer Fehlübermittlung erheblich nachgeholfen.

Wir selbst waren erstaunt, als wir unter unserer Anschrift ein Telefax des Landesamtes für Informationstechnik erhielten, in dem wir zur Abgabe eines Angebotes für Computerzubehör aufgefordert wurden. Da das LIT weiß, daß wir damit nicht handeln, konnte es nur ein irrtümlicher Versand sein.

Da das Telefax keine personenbezogenen Daten enthielt, war es natürlich kein Beanstandungsgrund, nicht einmal ein Fall für uns, aber eine Erfahrung, die einen Hinweis für andere Fälle nötig macht, in denen es um sensible Informationen geht. Wie dem Telefax zu entnehmen war, kam es direkt aus dem Bürokommunikationssystem des LIT. In diesem Falle war ganz offensichtlich ein *falscher Verteiler* in das System eingegeben worden, ein Umstand, der ebenfalls die Wahrscheinlichkeit von Fehlsendungen bei Telefax kräftig erhöhen kann.

Wenn man außerdem bedenkt, daß die Vertraulichkeit von Telefaxsendungen ganz entscheidend von den räumlichen und organisatorischen Bedingungen in der Umgebung des empfangenden Gerätes abhängt, muß dringend davor gewarnt werden, *vertrauliche Sendungen* ohne vorherige Kontrolle der Richtigkeit der Anwahl und ohne Sicherstellung, daß nur der korrekte Empfänger die Sendung in Empfang nehmen kann, per Telefax zu versenden. Dieser Hinweis ist umso dringender, als zwei der beschriebenen Fälle und viele ältere Fälle zeigen, daß diese Übermittlungsform auch für höchst sensible Daten benutzt wird: wertende Personalunterlagen, Daten über psychische Erkrankungen (Amtsgerichte verlangen die Übersendung von Anträgen zur Unterbringung nach dem Psychiatriegesetz per Fax !), Daten, die dem Bank- oder Steuergeheimnis unterliegen.

Auch die Polizei ist dazu übergegangen, Ermittlungen mittels Telefax zu führen. Darüber hatte sich ein Petent beschwert, weil die Sendung an ihn über das Telefaxgerät seines Arbeitgebers in falsche Hände geraten war. Zwar war die Übersendungsform mit dem Empfänger vorab telefonisch verabredet worden, so daß die Polizei keine Vorwürfe dafür treffen können, jedoch haben wir den Fall zum Anlaß genommen, die Polizei aufzufordern, ihre Fernkopier-Geschäftsanweisung zur Sicherung der Vertraulichkeit zu ergänzen.

Für die Verwendung von Telefax bei der Übersendung personenbezogener Daten ist gem. § 5 Abs. 3 Nr. 9 BlnDSG zu gewährleisten, daß bei der Übertragung der Sendung diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden kann (Transportkontrolle). Der Transport beginnt mit der Absendung des Fax und endet mit der Entgegennahme durch den vorgesehenen Empfänger. Daher ist insbesonders

- vor der Absendung durch die Kontrolle der angezeigten Nummer zu prüfen, ob die richtige Nummer gewählt wurde. Anderenfalls ist die Übertragung zu unterbinden;
- bei vertraulichen Sendungen durch telefonische Absprache sicherzustellen, daß der vorgesehene Empfänger die Sendung am Gerät entgegennimmt. Ist das Empfangsgerät in einer mit dem Empfang vertraulicher Sendung betrauten Poststelle installiert, so hat der Absender sich davon zu vergewissern, daß die Weiterleitung der Sendung nach den Vorschriften erfolgt, die für geöffnete vertrauliche Briefsendungen gelten;
- darauf zu achten, daß die Sende- und Empfangsprotokolle nach ihrer Prüfung vertraulich abgelegt werden, denn sie unterliegen dem Fernmeldegeheimnis;
- bei besonders vertraulichen Sendungen auf Telefax zu verzichten, wenn nicht eine verschlüsselte Übertragungsweise möglich ist. Telefaxsendungen sind genauso abhörbar wie Telefonate!

Viele dieser Hinweise sind obsolet, wenn Telefax-Geräte benutzt werden, die über *Sicherheitsfunktionen* verfügen und sofern diese Funktionen sinnvoll genutzt werden. Solche Sicherheitsfunktionen sind z. B.:

- Verschluß des Ausgabeschachtes beim empfangenden Gerät
- Paßwortschutz für den Zugriff auf im Empfangsgerät gespeicherte Sendungen
- Verschlüsselung bzw. Scrambling der Telefax-Sendungen
- Aufnahme des Faksimiles der ersten übertragenen Seite in das Sendeprotokoll zum Nachweis, was übersandt wurde.

3.6 Namensverwechslungen

Ein Mann erhielt die Aufforderung eines Jugendamtes, seine Einkünfte und sein Vermögen offenzulegen, damit geprüft werden kann, welcher Unterhalt für sein nichteheliches Kind angemessen sei. Die Ehefrau war entsetzt.

Ein Arbeitnehmer mußte feststellen, daß das Finanzamt versucht hatte, bei seinem Arbeitgeber das Gehalt wegen rückständiger Einkommenssteuer zu pfänden. Ein anderer Arbeitnehmer machte die gleiche Erfahrung mit der Staatsanwaltschaft.

Eine nichtsahnende Frau wurde von einem Rechtsanwalt aufgefordert, die von ihr bei einem Versandhaus bestellten Waren endlich zu bezahlen.

Jemand erhielt einen Gebührenbescheid für Transport und Verwahrung, weil er angeblich von der Polizei hilflos aufgefunden und in Gewahrsam genommen worden sei.

In allen Fällen handelte es sich um Namensverwechslungen. Die Beispiele zeigen, daß derartige Verwechslungen nicht nur Stoff für die Klatschspalten der Boulevardpresse liefern, sondern durchaus zu einer Beeinträchtigung der Privatsphäre führen können: Während beim falschen Adressaten eine Menge Ärger ausgelöst werden kann, werden über den eigentlichen Adressaten häufig hochsensible Daten offenbart - wie man sieht, nicht nur an das Opfer der Verwechslung, sondern auch an Dritte wie Familienangehörige, Arbeitgeber oder Rechtsanwälte.

Die Verpflichtung, bei der Adressierung von Unterlagen mit personenbezogenen Daten sorgfältig umzugehen, stellt daher eine der wesentlichen Aspekte der Transportkontrolle dar, zu der jede datenverarbeitende Stelle verpflichtet ist (§ 5 Abs. 2 BlnDSG).

Hauptursache für Namensverwechslungen sind Nachlässigkeiten bei der Erforschung der Adressen von Personen, deren aktuelle Adresse nicht bekannt ist. Insbesondere Gläubigern stehen hierfür einige Informationsquellen zur Verfügung, deren Nutzung, wie unsere Beispiele zeigen, ihre Tücken haben können.

Soweit es sich um öffentlich-rechtliche Ansprüche in Höhe von mindestens 1000 DM handelt, sind Sozialleistungsträger eine beliebte Auskunftsstelle. § 68 Abs. 1 SGB X läßt die Übermittlung von Name, Vorname, Geburtsdatum, Geburtsort, derzeitiger Anschrift des Betroffenen sowie Namen und Anschriften seiner derzeitigen Arbeitgeber zu, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Sozialleistungsträger können sogar ohne diese Einschränkungen Daten austauschen (§§ 69, 3 SGB X).

So hatte im Falle unseres nichtsahnenden „Vaters" das Jugendamt bei einer Landesversicherungsanstalt nach der aktuellen Adresse gefragt: Korrekt angegeben wurden Name, Vorname und Geburtsort des Vaters sowie Name und Vorname des Kindes. Als Geburtsdatum war fälschlicherweise das Datum der Anfrage eingetragen - die Landesversicherungsanstalt förderte die Daten des falschen Vaters sowie seines Arbeitgebers zutage. Das Beispiel zeigt die Bedeutung des Geburtsdatums als Identifikationsmerkmal. Obwohl sich die Bürger immer wieder über den relativ großzügigen Umgang der Behörden mit dem Geburtsdatum erregen, stellt dieses Merkmal gleichwohl ein wichtiges Mittel zur Vermeidung von Verwechslungen dar. Die offensichtlich fehlerhafte Angabe des Geburtsdatums in unserem Fall hätte auf alle Fälle Anlaß sein müssen, vor der Herausgabe zusätzliche Angaben zu verlangen.

Auch das Finanzamt erhielt die falschen Daten von einem Sozialleistungsträger, hier der Bundesversicherungsanstalt für Angestellte. Hier hätte allerdings das Finanzamt selbst bereits die Verwechslung bemerken müssen. Erfragt worden war die Adresse des Arbeitgebers; allerdings stimmte in der Antwort der BfA die Adresse des angeblich Steuerpflichtigen nicht mit der Adresse des betroffenen Bürgers überein. Gerade bei der Vielzahl der bei der BfA versicherten Personen sind Namens- und Geburtsdatenidentitäten nie ganz auszuschließen, so daß hier bei der Verwertung der Daten besondere Sorgfalt geboten ist.

Die Staatsanwaltschaft wiederum hatte bei der AOK nachgefragt und alle zur Identifikation erforderlichen Daten angegeben. Hier lag die Nachlässigkeit bei der AOK: Man nimmt an, daß bei der Abfrage nicht alle von der Staatsanwaltschaft angegebenen Daten im Suchsystem eingegeben wurden und auch bei der Beantwortung kein Abgleich mit den Angaben der Staatsanwaltschaft vorgenommen wurde. Die AOK hat diesen Fall zum Anlaß genommen, Hinweise zur Sorgfaltspflicht bei der Bearbeitung von Auskunftsersuchen an die Mitarbeiter herauszugeben. Auch soll geklärt werden, wie künftig schriftliche Auskünfte der AOK dokumentiert werden können.

Im Falle der „Versandhauskundin" hatte der Anwalt das Melderegister genutzt, das vom Landeseinwohneramt geführt wird. Hier kann jeder, der ein berechtigtes Interesse glaubhaft macht (also jeder Gläubiger) eine Auskunft u. a. über gegenwärtige und frühere Anschriften erhalten (§ 28 Abs. 2 Meldegesetz).

Eine Auskunft erfolgt allerdings nur dann, wenn die gesuchte Person eindeutig identifiziert wird. Auch hier gelten als klassische Suchmerkmale Name, Vorname und Geburtsdatum. In unserem Fall wurde auch mit Hilfe dieser Merkmale gesucht. Im Melderegister war unter diesen Angaben nur unsere Petentin gespeichert, nicht jedoch die eigentliche Adressatin. Allerdings hatte der anfragende Anwalt zusätzlich als viertes Merkmal die - letzte bekannte - Anschrift angegeben. Diese war im Melderegister nicht verzeichnet.

Das Landeseinwohneramt ist der Auffassung, daß in diesen Fällen gleichwohl eine Auskunft erteilt werden kann, da die den Anfragenden bekannten Anschriften unterschiedlichster Herkunft sein können, z. B. vorübergehender oder besuchsweiser Aufenthalt, Geschäfts- oder Gewerbeadressen oder einfach eine nicht gemeldete Wohnung; hinzu kommen die Fälle, in denen die Anschrift frei erfunden ist. Die Meldebehörde räumt daher dem Geburtsdatum Vorrang vor einer Anschrift ein; eine Auskunft über die gesuchte Person könne auch bei abweichender Adressenangabe erteilt werden. Gerade bei Anfragen von Versandhäusern oder Inkassofirmen könnten Schutzbehauptungen oder bewußt falsche Angaben nicht ausgeschlossen werden.

Diese Auffassung teilen wir nicht. Die Meldebehörde darf nur Auskunft über einzelne, bestimmte Einwohner erteilen. Die Geschäftsanweisung über die Auswirkungen des Meldegesetzes legt ausdrücklich fest, daß Datenübermittlungen nur dann stattfinden dürfen, wenn alle notwendigen Maßnahmen zu einer eindeutigen Identifizierung der gesuchten Person ergriffen wurden. Für den Fall, daß nur eine Person im Melderegister gespeichert ist, darf dann keine Auskunft erteilt werden, wenn eines der vorgegebenen Merkmale erheblich abweicht. Bei einer unzutreffenden Anschrift handelt es sich immer dann um eine erhebliche Abweichung, wenn der Gesuchte nicht früher unter dieser Anschrift gemeldet war. Eine Auskunft hat in diesem Fall zu unterbleiben. Es ist insbesondere nicht Aufgabe der Meldebehörde, zu prüfen, ob im Geschäftsverkehr falsche Angaben gemacht wurden oder nicht.

Ein bei einer Betriebskrankenkasse Versicherter erhielt wiederholt Nachweise zum Erhalt von Krankengeld und Bescheinigungen wegen des Bezuges von Entgeltersatzleistungen einer namensgleichen Person.

Jeweils nach Erhalt der ihn nicht betreffenden Unterlagen hat er die Krankenkasse auf diesen Umstand aufmerksam gemacht. Dabei erhielt er wiederholt die Auskunft, daß der richtige Adressat in der gleichen Straße wohne, später habe man ihm mitgeteilt, der Doppelgänger lebe in einem anderen Bezirk. Dann wiederum wurde eingeräumt, daß „die Daten wohl etwas durcheinandergeraten seien". Prüfung und erforderliche Maßnahmen unterblieben bis zur Beschwerde des Petenten.

Die fehlerhafte Versendung war auf eine nachlässige Bearbeitung einer Adreßänderung des richtigen Adressaten zurückzuführen. Wenn, wie hier, die Versicherungsnummer falsch oder nicht angegeben wird, steht ein Suchprogramm zur Verfügung, das sofort erkennen läßt, ob Daten mehrerer namensgleicher Personen gespeichert sind. Ist dies der Fall, muß die Identität der Betroffenen sorgfältig geprüft werden - was im vorliegenden Fall unterblieb. Da die entsprechenden Verfahrensschritte bei der Änderung der Stammdaten nicht festgelegt waren, wurde wegen Verstoßes gegen die Verpflichtung zur Organisationskontrolle (§ 5 Abs. 3 Nr. 10 BlnDSG) ein Mangel festgestellt.

4. Aus den einzelnen Geschäftsbereichen

4.1 Senatskanzlei

Sicherheitsüberprüfungen weiterhin ohne Rechtsgrundlage

Die Zuständigkeit für die Aufsicht über das Landesamt für Verfassungsschutz ging zum 1. Dezember 1994 auf den Regierenden Bürgermeister über. Damit wurden auch die datenschutzrechtlichen Hypotheken übernommen.

Nachdem das neue Landesverfassungsschutzgesetz (LfVG) im Jahr 1993 in Kraft getreten war, blieb der bedeutendste gesetzgeberische Mangel das Fehlen hinreichender Rechtsvorschriften für die Durchführung von Sicherheitsüberprüfungen. Zwar ist das Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz - SÜG) am 21. April 1994 in Kraft getreten[105], ohne daß die Änderungsvorschläge der Datenschutzbeauftragten aufgegriffen worden wären[106].

Hierzu sind im Sommer 1994 Ausführungsvorschriften sowie Ausführungsvorschriften zu Sicherheitsüberprüfungen in der Wirtschaft ergangen[107]. Auch hier sind die Anregungen der Datenschutzbeauftragten kaum berücksichtigt worden.

Eine Änderung wurde bei den Datenspeicherungen über Personen, die die sicherheitsempfindliche Tätigkeit nicht aufgenommen haben, vorgenommen. Nachdem in diesen Fällen ursprünglich die Sicherheitsüberprüfungsakte und die NADIS-Erfassung noch elf Jahre aufrechterhalten werden sollten, wurde eine frühere Löschung der Daten vorgesehen, allerdings beschränkt auf die Personen, bei denen keine sicherheitserheblichen Erkenntnisse bei der Überprüfung angefallen sind.

Die Regelungen über die Akteneinsicht des Betroffenen hingegen bleiben noch hinter den ohnehin bedenklichen Bestimmungen des SÜG zurück. Auch bei der Anhörung des Betroffenen wurden unsere Empfehlungen[108] nicht berücksichtigt.

Ein Berliner Gesetz zur Durchführung der Sicherheitsüberprüfungen fehlt allerdings noch immer. Der angeblich seit März 1993 von der Senatsverwaltung für Inneres erarbeitete Gesetzentwurf liegt uns noch nicht vor, obwohl der Senat in seiner Antwort auf eine Kleine Anfrage im März 1994 mitgeteilt hat, daß die Arbeit an dem Gesetz „weiter zügig vorangetrieben" würden und noch im Jahr 1994 mit einer Gesetzesvorlage zu rechnen sei[109].

Die Folge ist, daß die Sicherheitsüberprüfungen, die derzeit in dem unerläßlichen Umfang nach wie vor durchgeführt werden, nur auf die Einwilligung der Betroffenen gestützt werden können - eine äußerst fragwürdige Situation, da völlig unklar ist, welche Folgen die Verweigerung der Einwilligung hat. In einem besonders interessant gelagerten Fall - es handelt sich um die Erforderlichkeit von Sicherheitsüberprüfungen bei der Datenverarbeitung - hat sich die Senatskanzlei selbst zu einer Kündigung berechtigt gefühlt.

Es ist zwingend geboten, daß die ausstehende rechtliche Regelung noch in dieser Legislaturperiode vorgenommen wird.

Nachdem der Landesbeauftragte für den Datenschutz von Mecklenburg-Vorpommern eine eklatante Benachteiligung von Bürgern der ehemaligen DDR festgestellt hatte, befaßte sich auch die vor Jahren von Berlin initiierte Arbeitsgruppe der Datenschutzbeauftragten der Neuen Länder mit der Durchführung von Sicherheitsüberprüfungen. Auf ihrer Sitzung am 20. September 1994 in Erfurt bekräftigten sie die Forderung nach Schaffung von Landesgesetzen.

105 BGBl. I, 867 f.
106 Jahresbericht 1993, 4.5.2
107 GMBl. 1994, 550 ff. und 624 ff.
108 Jahresbericht 1993, 4.5.2
109 Kleine Anfrage Nr. 5100, LPD vom 6. April 1994

Sie hatten ferner Anlaß, die ja eigentlich selbstverständlichen Forderungen zu erheben, daß

- die Verarbeitung und Nutzung von Daten für Zwecke der Sicherheitsüberprüfung durch die Landesämter für Verfassungsschutz nur erfolgen darf, soweit diese hierfür tatsächlich benötigt werden,
- keine Ungleichbehandlung von Bürgern der ehemaligen DDR im Rahmen von Sicherheitsüberprüfungen erfolgt und
- Datenerhebungen zu Sicherheitsüberprüfungen nur im Rahmen des SÜG erfolgen dürfen.

Neue Verwaltungsvorschriften für den Verfassungsschutz: Wenig Fortschritt

Die Verarbeitung personenbezogener Daten in dem durch Bundes- und Landesämter genutzten Verbundsystem NADIS wird durch Richtlinien geregelt, die vor dem Hintergrund der neuen Verfassungsschutzgesetze neu zu fassen waren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich (bei Stimmenthaltung von Thüringen und Bayern) vor der Sitzung der Innenministerkonferenz am 5./6. Mai 1994 in einer Entschließung gegen den Entwurf der NADIS-Richtlinien als zu weitgehend gewandt[110]. Sie hat gefordert, die in NADIS zu speichernden Daten zu verringern und insbesondere die Daten zu streichen, die nicht Identifizierungszwecken dienen. Weiterhin wurde die Klarstellung verlangt, daß für Datenübermittlungen das Recht des Landes, das die Daten eingegeben hat, zu beachten ist. Weitere Forderungen betrafen die Aufbewahrung von Protokolldaten und deren Zweckbindung sowie die Beteiligung der Datenschutzbeauftragten bei Durchführung und Fortentwicklung des Nachrichtendienstlichen Informationssystems[111].

Sowohl die Leiter der Verfassungsschutzbehörden des Bundes und der Länder als auch die Mitglieder des AK IV der Innenministerkonferenz hatten zuvor bereits im März 1994 einvernehmlich festgestellt, daß auf Grund der Stellungnahme des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz sachliche Änderungen des Entwurfes der NADIS-Richtlinie nicht erforderlich seien. Die Innenministerkonferenz ist in ihrer Sitzung am 5./6. Mai 1994 dem Beschlußvorschlag des AK IV gefolgt und hat die Neufassung der NADIS-Richtlinien unverändert gelassen. Damit traten die NADIS-Richtlinien mit Wirkung vom 6. Mai 1994 bundeseinheitlich ohne datenschutzrechtliche Verbesserungen in Kraft.

Am 1. März 1994 ist die neue *Auskunftsanweisung* des Landesamtes für Verfassungsschutz in Kraft getreten.

Danach entscheidet nicht mehr die - inzwischen aufgelöste - Arbeitsgruppe Auskunft, sondern das zuständige Fachreferat über die Auskunftserteilung. Die Auflösung der Arbeitsgruppe Auskunft ist bedauerlich. Wir hatten den Eindruck, daß die Bearbeitung der Auskunfts- und Akteneinsichtsanträge durch eine nur für diese Aufgabe zuständige Stelle die Bedeutung des Auskunftsrechts der Bürger beim Landesamt für Verfassungsschutz betonte und eine vertrauensbildende Maßnahme darstellte. Zudem war hierdurch eine einheitliche Auskunftspraxis, die auch die Interessen der Betroffenen im Auge hat, gewährleistet. Dies erscheint uns bei der Bearbeitung durch die Fachreferate nicht in dem Maße gesichert.

Unsere Anregungen[112] zur Änderung der Auskunftsanweisung blieben überwiegend unberücksichtigt.

Wenn von Betroffenen in dem Auskunftsantrag kein oder kein aus Sicht des Landesamtes für Verfassungsschutz hinreichendes Interesse dargelegt wird, wird der Antrag schematisch und ohne weitere Prüfung abgelehnt. Eine Prüfung, ob nicht doch Auskunft erteilt werden kann - insbesondere in den Fällen, in denen kein Geheimhaltungsinteresse besteht -, soll nicht erfolgen, obwohl das LfVG in diesen Fällen eine Auskunft vorsieht. Auch die für die Darlegung des besonderen Interesses genannten Beispielsfälle deuten auf eine zu enge Auslegung dieses Begriffes hin.

Das Landesamt für Verfassungsschutz ist jedoch bemüht, dem informationellen Selbstbestimmungsrecht der Betroffenen weitgehender Rechnung zu tragen, indem jedes nachvollziehbare Interesse als ausreichend anerkannt wird. Der Rückgang von Beschwerden Betroffener bei uns scheint dies zu belegen.

Die Unterlagen, die von der Polizei an das Landesamt für Verfassungsschutz übermittelt worden sind, sollen von der Akteneinsicht ausgenommen werden, obwohl die Betroffenen gegenüber der Polizei nach dem ASOG einen Ermessensanspruch auf Akteneinsicht haben. Dies geht auf einen Wunsch der Polizei zurück. Nachdem der Polizeipräsident zur Begründung zunächst darauf hingewiesen hat, daß er grundsätzlich keine Akteneinsicht an Betroffene mehr gewähre, da das Einsichtsrecht des ASOG „nur als Möglichkeit zur Arbeitserleichterung gedacht sei", wurde später klargestellt, daß bei jedem Akteneinsichtsantrag eine Einzelfallprüfung erfolge. Wir gehen davon aus, daß hierbei das Recht auf informationelle Selbstbestimmung des Betroffenen hinreichend berücksichtigt wird.

Probleme mit alten Verfassungsschutzakten

In allen Verwaltungsbereichen macht es Schwierigkeiten, die von den Datenschutzgesetzen bei verschiedenen Voraussetzungen vorgeschriebene *Sperrung von Daten* zu realisieren. Besonders heikel ist dies beim Verfassungsschutz.

Sperren von Daten bedeutet, daß eigentlich zu löschende Daten nicht vernichtet, sondern im Interesse des Betroffenen weiter gespeichert werden. Das kann z. B. bei Rehabilitationsinteressen oder Beweisinteressen des Betroffenen der Fall sein. Da die Löschung der Daten nur im Interesse des Betroffenen unterblieben ist, dürfen die Daten grundsätzlich nicht mehr verarbeitet, insbesondere übermittelt oder sonst von der speichernden Stelle genutzt werden. Nur in Ausnahmefällen und wenn der Betroffene eingewilligt hat, darf auf diese Daten zurückgegriffen werden[113].

Das Landesamt für Verfassungsschutz entnimmt § 15 Abs. 2 LfVG die Rechtfertigung, auf gesperrte Daten für seine Aufgabenerfüllung wieder zurückgreifen zu können, auch ohne den Betroffenen zu fragen oder zu unterrichten. Dieses Verfahren widerspricht dem Sinn und Zweck der Sperrung von Daten. Da von der Löschung ausschließlich im Interesse des Betroffenen abgesehen wurde, sollte auch die Nutzung nur für Zwecke, die im schutzwürdigen Interesse des Betroffenen liegen, erfolgen. Jedenfalls sind die Sperrungsvoraussetzungen unter diesem Gesichtspunkt besonders sorgfältig zu prüfen, da fraglich ist, ob die Sperrung im Interesse des Betroffenen liegt, wenn das Landesamt für Verfassungsschutz auf die gesperrten Daten jederzeit zurückgreifen kann.

Wir haben dem Landesamt für Verfassungsschutz empfohlen, vor einer Entscheidung über eine Sperrung personenbezogener Daten möglichst den Betroffenen zu befragen, ob dies auch seinem Interesse entspricht. Sollte hinsichtlich der gespeicherten Daten wegen überwiegender Geheimhaltungsinteressen eine Anfrage beim Betroffenen nicht möglich sein, könnte auch der Berliner Datenschutzbeauftragte unterrichtet werden. Eine derartige Lösung wurde abgelehnt.

Das Landesamt für Verfassungsschutz hat die nach Aufhebung des vor Jahren in Zusammenhang mit der Arbeit eines Untersuchungsausschusses verhängten Löschungs- und Vernichtungsverbotes gesperrten *Altakten*[114] dem Landesarchiv zur Übernahme angeboten. Die im Zusammenhang mit der Alternativen Liste (AL) vom Verfassungsschutz gesammelten Unterlagen[115] wurden dem Landesarchiv bereits übergeben. Die weiteren Altakten werden derzeit vom Archiv gesichtet. Die Akten, die von dem Landesarchiv nicht übernommen werden, wird das Landesamt für Verfassungsschutz vernichten.

110 Anlage 2.7
111 vgl. auch Jahresbericht 1992, 4.5.2
112 Jahresbericht 1993, 3.1
113 § 17 Abs. 2 BlnDSG
114 Jahresbericht 1993, 4.5.2
115 Jahresbericht 1989, 2.2

Auch Jubilare wollen gefragt sein

Beim Durchblättern der Tageszeitung finden sich insbesondere unter der Rubrik „Aus den Bezirken" immer wieder Mitteilungen, daß ein betagtes Ehepaar Diamantene Hochzeit oder ein Bürger seinen 90. Geburtstag feiern wird und daß der Bezirksbürgermeister den namentlich (zum Teil unter Angabe der Adresse) genannten Jubilaren hierzu persönlich gratulieren wird.

Derartige *Mitteilungen an die Presse* haben sowohl bezirkliche Pressestellen als auch der Landespressedienst bis in die jüngste Zeit gemacht, ohne daß die Betroffenen zuvor um ihre Einwilligung gebeten worden waren. Dies wäre aber Voraussetzung für eine Weitergabe personenbezogener Daten an die Presse nach dem Berliner Datenschutzgesetz gewesen. Es ist nichts dagegen einzuwenden, wenn der Bezirksbürgermeister einen persönlichen Geburtstagsbesuch bei älteren Bürgerinnen und Bürgern macht. Verständlich ist auch, daß er dies in Anwesenheit von Pressevertretern tut. Gerade diesen zusätzlichen Eingriff in die Privatsphäre muß das ältere Geburtstagskind allerdings nicht hinnehmen. Es sollte rechtzeitig um sein Einverständnis gebeten werden, und wenn dies verweigert wird, so muß der Bürgermeister seinen Geburtstagsbesuch ohne Pressevertreter machen.

Auf Anregung der Senatskanzlei haben wir den bezirklichen Pressestellen und dem Landespressedienst ein Verfahren empfohlen, nach dem in Zukunft eine personenbezogene Bekanntgabe von Geburtstagen und des Besuchs des Bürgermeisters gegenüber der Presse nur dann erfolgen darf, wenn die Betroffenen zuvor auf einem Merkblatt über die beabsichtigte Veröffentlichung informiert worden sind und schriftlich ihr Einverständnis erklärt haben.

4.2 Arbeit und Frauen

62 PCs und keine Daten

Mehr Transparenz der Datenverarbeitung war eine der Zielsetzungen der Novellierung des Berliner Datenschutzgesetzes im Jahre 1990. Wesentliche Voraussetzung dafür ist, daß der Bürger auf einfache Weise erkennen kann, welche Dateien die Verwaltung führt und mit welchen Mitteln dies geschieht. Während das Datenschutzgesetz von 1978 lediglich eine Verpflichtung der datenverarbeitenden Stellen zur *Meldung von Dateien* an den Datenschutzbeauftragten vorsah, also eine Meldung der Inhalte der Datenverarbeitung, schreibt das neue Datenschutzgesetz nunmehr auch die Führung eines *Geräteverzeichnisses* sowohl in der Dienststelle (§ 19 Abs. 4 BlnDSG) als auch beim Datenschutzbeauftragten (§ 25 BlnDSG) vor. Sinn macht dies für den Bürger gleichwohl nur, wenn in dem beim Datenschutzbeauftragten geführten öffentlichen Register beide Arten von Meldungen vorliegen.

Wenig sinnvoll ist es dagegen, wenn zum Register nur Angaben zum Geräteverzeichnis, nicht aber zu den Dateien gemacht werden: Der Bürger weiß dann zwar, daß Daten verarbeitet werden, welche dies sind, bleibt ihm dagegen verborgen. Den Vogel in dieser Hinsicht schoß die Senatsverwaltung für Arbeit und Frauen ab: Sie meldete zwar 62 Personalcomputer zum Geräteverzeichnis an, nicht eine einzige Mitteilung erfolgte dagegen zum Dateienregister - Informationstechnik um ihrer selbst willen?

Unsere Nachfrage ergab, daß weder behördlicher Datenschutzbeauftragter noch Organisationsstelle mehr über die Datenverarbeitung wußten.

Frauenförderung und Datenverarbeitung

Die Frauenförderung ist eine der großen politischen Zielsetzungen, die die aktuelle Diskussion über die Umgestaltung der Verwaltung beherrschen. Darüber hinaus ist die Verwaltung verpflichtet, darauf hinzuwirken, daß auch im Bereich der Privatwirtschaft die Belange der Frauen hinreichend berücksichtigt werden. Die Umsetzung dieses Programms wirft unter verschiedenen Aspekten datenschutzrechtliche Probleme auf. Einige davon seien unabhängig davon, ob die Senatsverwaltung für Arbeit und Frauen davon direkt berührt ist, an dieser Stelle erwähnt.

Während das Landesgleichstellungsgesetz teilweise einschneidende Regelungen zur Frauenförderung innerhalb der Verwaltung enthält, steht eine gesetzliche Regelung der *Frauenförderung in allen Lebens- und Arbeitsbereichen* noch aus. Diese soll im wesentlichen von Frauenbeauftragten geleistet werden, die in den Bezirken eingerichtet werden. Ein entsprechender Gesetzentwurf lag im vergangenen Jahr zwar vor, er hat bislang jedoch die erforderliche politische Abstimmung nicht erfolgreich hinter sich gebracht. Aus datenschutzrechtlicher Sicht war es erforderlich, die Frauenbeauftragte zur Verarbeitung personenbezogener Daten zu ermächtigen - auch über Personen außerhalb der Verwaltung (z. B. über betriebliche Frauenbeauftragte); sie sollte auch die Befugnis haben, ohne Beteiligung der Betroffenen Daten zu erheben, wenn nur auf diese Weise festgestellt werden kann, ob Benachteiligungen und Diskriminierungen von Frauen vorliegen.

Eine wesentliche Arbeitsvoraussetzung für die Frauenbeauftragte ist es, in Unterlagen der Bezirksverwaltung Einsicht zu nehmen, um möglichen Benachteiligungen auf die Spur zu kommen. Allerdings stoßen derartige Befugnisse an die Grenzen der Landeskompetenz: So ist die Einsicht der Frauenbeauftragten in Unterlagen der Sozial- und Jugendverwaltung nur mit Einwilligung der Betroffenen zulässig.

Unsere Anregungen zur Präzisierung des Gesetzentwurfs wurden in vollem Umfang aufgegriffen.

Immer noch nicht endgültig geklärt sind die Befugnisse der *Frauenvertreterinnen* in den einzelnen Verwaltungen zur Einsicht in Personalunterlagen bei Bewerbungsverfahren. Insbesondere im Schulbereich besteht weiterhin Klärungsbedarf: Hier wurde im Gegensatz zur Senatsverwaltung für Arbeit und Frauen und uns die Auffassung vertreten, daß der Frauenvertreterin weder das Recht zur Teilnahme an Unterrichtsbesuchen noch die Einsicht in dienstliche Beurteilungen oder andere Personalunterlagen zusteht. Inzwischen hat sich auch der Hauptpersonalrat dieses Problems angenommen und sich sehr dezidiert auf die Seite der Frauenvertreterinnen gestellt.

Auch die konkreten Arbeitsbedingungen der Frauenvertreterinnen werfen datenschutzrechtliche Probleme auf. So wurde die Frage gestellt, welche Sicherungsmaßnahmen getroffen werden müssen, wenn eine Frauenvertreterin sich eines *eigenen PCs* bedient. Die Sensibilität der von der Frauenvertreterin verarbeiteten Daten (Schriftwechsel zu Bewerbungsvorgängen, Förderungsmaßnahmen, sexuellen Belästigungen u. ä., ggf. entsprechende Aufstellungen und Dateien) ist zumindest ebenso hoch zu veranschlagen wie bei Personaldaten. Daraus folgt, daß bei der Nutzung eines PCs triviale Sicherungsmaßnahmen wie Verschluß des Raumes nicht ausreichen. Vielmehr ist der Zugang zum PC durch hinreichenden Paßwortschutz zu sichern sowie bei besonders sensiblen Anwendungen ein Verschlüsselungsverfahren einzusetzen.

Im Laufe des Gesetzgebungsverfahrens zum Landesantidiskriminierungsgesetz, dem Vorgänger des Landesgleichstellungsgesetzes, hatten wir auf die Probleme hingewiesen, die bei der Behandlung *sexueller Belästigungen am Arbeitsplatz* entstehen könnten. Nach unserer Auffassung muß vermieden werden, daß die Beteiligung der Frauenvertreterin sowie die von ihr vorzunehmenden Mitteilungen (§ 17 Abs. 4 i.V.m. § 12 LGG) zu einem Instrument willkürlicher Anprangerung werden: Das im Rahmen des zweiten Gleichberechtigungsgesetzes vom 24. Juni 1994 verabschiedete Gesetz zum Schutz der Beschäftigten vor sexueller Belästigung am Arbeitsplatz (Beschäftigtenschutzgesetz)[115a] bestimmt nunmehr, daß außer bei Sexualstraftaten eine sexuelle Belästigung nur dann vorliegt, wenn die betroffenen Personen diese erkennbar abgelehnt haben. Das Risiko, daß entsprechende Mitteilungen dazu genutzt werden, Betroffene anzuprangern, ohne daß diese sich ihrer Verfehlungen bewußt sind, wird dadurch deutlich gemildert.

115a BGBl. I, 1412

Frauenforschung

Auf dem Hintergrund der allgemeinen politischen Diskussion erfreuen sich frauenspezifische Themen auch bei der *Forschung* einer gewissen Beliebtheit. Wie in allen anderen Bereichen auch, wirft hier insbesondere der Zugang zu den Daten Probleme auf. Das Landesgleichstellungsgesetz oder andere Vorschriften enthalten keine über die allgemeinen Forschungsklauseln hinausgehenden Privilegierungen. Dies bedeutet, daß dann, wenn die Forschung mit anonymen Daten nicht möglich ist, die Einwilligung der betroffenen Frauen eingeholt werden muß. Daß gewisse Forschungsprojekte an dieser Barriere scheitern können, muß im Hinblick auf die informationelle Selbstbestimmung hingenommen werden. So fand sich bisher kein gangbarer Weg, mit Hilfe der Daten der Geschlechtskrankenfürsorge Forschungsvorhaben über ausländische Prostituierte durchzuführen.

Hingegen waren andere Forschungsvorhaben, die zunächst auf erhebliche datenschutzrechtliche Probleme stießen, mit Einwilligung der betroffenen Frauen möglich. Dort, wo die Frauen für die Zusammenarbeit mit den Forschern gewonnen wurden und auch durch transparente Datenschutzregelungen die Akzeptanz des Projekts untersetzt wurde, gelang es, erfolgreich Frauenforschung zu betreiben. Zu nennen sind beispielsweise die Themen:

- Gewalt gegen Frauen (eine Befragung von Bewohnerinnen von Frauenhäusern)
- Armut und Sozialhilfe - Lebenssituation von Sozialhilfeempfängerinnen
- Evaluierung unterstützender Maßnahmen bei Ausstieg aus der Prostitution
- Alterssicherung Berliner Frauen.

Geheimhaltung für Frauenhäuser

Der Träger eines Frauenhauses, dessen Adresse geheimgehalten werden muß, unterhält einen PKW. Die Mitarbeiterinnen haben den Verdacht, daß Männer, die ihre Frauen mißhandelt haben, über das Kennzeichen die Adresse des Frauenhauses herausfinden können.

In der Tat läßt das Straßenverkehrsgesetz (StVG) die Herausgabe von Halterdaten an Privatpersonen zu, wenn der Empfänger darlegt bzw. glaubhaft macht, daß er die Daten zur Verfolgung oder Abwehr von Rechtsansprüchen benötigt, die im Zusammenhang mit der Teilnahme am Straßenverkehr entstanden sind, unter gewissen Voraussetzungen sogar ohne diese Einschränkung (§ 39 StVG). Mit Hilfe einer Schutzbehauptung bestände tatsächlich die Möglichkeit, die Halteradresse in Erfahrung zu bringen. Allerdings schreibt das Straßenverkehrsgesetz eine Protokollierung der Übermittlung vor, über die Auskunft zu erteilen ist.

Dies zeigt, daß ein durchgängiger Schutz der Geheimhaltung der Adresse derartiger Einrichtungen nur schwer sicherzustellen ist. Weitere Beispiele, die an uns herangetragen wurden, sind die Möglichkeit öffentlicher Stellen, trotz einer im Melderegister beantragten Auskunftssperre Daten über die Wohnung zu erhalten, oder die Weigerung der Telekom, Frauenhäusern das Privileg einzuräumen, daß beim Telefonieren in Einzelentgeltnachweisen die Telefonnummer unterdrückt wird (§ 6 Abs. 9 Telekom-Datenschutzverordnung).

Zu erwägen ist, ob nicht eine (bundesweite) Initiative sinnvoll wäre, den Einrichtungen zum Schutz von Frauen vor der Verfolgung durch ihre (früheren) Partner eine besondere Geheimhaltung zuzubilligen. Dies könnte eine sinnvolle Ergänzung zu den aktuellen Erörterungen über die Strafbarkeit der Vergewaltigung in der Ehe sein.

Kindermißbrauch durch Adressenhandel

Empörung löste im Ausschuß für Frauenfragen des Abgeordnetenhauses folgender Sachverhalt aus: Eine Frankfurter Initiative zur Verschärfung der Strafbarkeit der Abtreibung versandte Briefe, in denen u. a. die verschiedenen Abtreibungsmethoden auf höchst abstoßende Weise geschildert und die Adressaten aufgefordert wurden, ihre Meinung zum Schwangerschaftsabbruch kundzutun sowie an einer Postkartenaktion an den Bundeskanzler teilzunehmen. Adressaten der Briefe waren auch Kinder.

Der in der Öffentlichkeit und im Ausschuß geäußerte Verdacht, die Adressen von Kindern seien von öffentlichen Stellen des Landes Berlin an die Initiative gelangt, hat sich nicht bestätigt. Vielmehr ergaben die Nachforschungen der zuständigen Aufsichtsbehörde, daß die Initiative die Berliner Adressen über den Adressenhandel von einem Verlag bezogen hatte, der neben Erwachsenen- auch Kinderzeitschriften veröffentlicht. Von der Aufsichtsbehörde wurde die Rechtswidrigkeit der Einbeziehung der Adressen von Kindern festgestellt.

4.3 Bau- und Wohnungswesen

Automatisierter Abruf und Datenübermittlung aus dem Liegenschaftskataster

§ 28 Abs. 1 Nr. 2 Gesetz über das Vermessungswesen in Berlin[116] ermächtigt die Senatsverwaltung für Bau- und Wohnungswesen, Rechtsverordnungen zur Benutzung des Liegenschaftskatasters zu erlassen. Ein Entwurf für eine Verordnung über die Abgabe digitaler Angaben aus dem Liegenschaftskataster (Lika-AbgabeVO) liegt vor. Ein Entwurf für eine Verordnung über die Benutzung des Liegenschaftskatasters mit Hilfe automatisierter Abrufverfahren (LikA-AbrufVO) wurde ebenfalls erstellt. Während durch die Lika-AbgabeVO geregelt werden soll, daß auch andere Behörden, sonstige öffentliche Stellen und Unternehmen zur Erfüllung ihrer Aufgaben sowie Grundstückseigentümer, Erbbauberechtigte und Nutzungsberechtigte für die Verwaltung ihrer Liegenschaften auf maschinenlesbaren Datenträgern Angaben aus dem Liegenschaftskataster erhalten dürfen, soll durch die Lika-AbrufVO vorgeschrieben werden, daß Vermessungsstellen und andere öffentliche Stellen zur Erfüllung ihrer Aufgaben sowie Unternehmen zur Erfüllung öffentlicher Aufgaben mit Hilfe automatisierter Abrufverfahren auf die Daten des Liegenschaftskatasters zugreifen dürfen.

Wir haben empfohlen, die Datenempfänger bzw. Abrufberechtigten, die Übermittlungszwecke und die zu übermittelnden Daten zu konkretisieren. Die Empfänger der Datenübermittlung sind so genau wie möglich zu bezeichnen und der Verwendungszweck abschließend und so konkret wie möglich anzugeben. Insbesondere war zu prüfen, ob stets die Angaben über die Eigentümer, Erbbauberechtigten und andere Personen bei der Übermittlung erforderlich sind. Bei der Abgabe oder dem Abruf von reinen Grundstücks- und Flächendaten sind weniger detaillierte Regelungen ausreichend.

Ein Online-Zugriff auf die Daten des Liegenschaftskatasters kommt nur für die Stellen in Betracht, die so häufig auf die personenbezogenen Daten zurückgreifen müssen, daß eine ständige Abrufmöglichkeit erforderlich ist. Dabei ist fraglich, ob die Stellen, die ohnehin Daten auf maschinenlesbaren Datenträgern erhalten, überhaupt noch einen Online-Zugriff benötigen. Die Erörterungen dauern noch an.

Akteneinsicht für Betroffenenvertreter in Sanierungsgebieten

Das Baugesetzbuch (BauGB) schreibt vor, daß städtebauliche Sanierungsmaßnahmen mit den Eigentümern, Mietern, Pächtern und sonstigen von der Sanierung Betroffenen möglichst frühzeitig erörtert werden sollen. Die Betroffenen sollen zur Mitwirkung bei der Sanierung und zur Durchführung der erforderlichen baulichen Maßnahmen angeregt und hierbei im Rahmen des Möglichen beraten werden (§ 137 BauGB). Zu diesem Zweck werden Betroffenenvertretungen gebildet, die den betroffenen Personen neben ihrer unmittelbaren Mitwirkung in geeigneter Form auch eine mittelbare Mitwirkung ermöglichen sollen. Fraglich ist, unter welchen Voraussetzungen die Sprecher dieser Betroffenenvertretungen Einsicht in Akten über das Sanierungsverfahren erhalten können.

116 Gesetz über das Vermessungswesen in Berlin (VermGBln) vom 8. April 1974 (GVBl. S. 806), zuletzt geändert durch Artikel III des Gesetzes vom 26. Januar 1993 (GVBl. S. 40).

Die Betroffenenvertretung ist eine nicht-öffentliche Stelle, der personenbezogene Daten nur dann übermittelt werden dürfen, wenn eine Rechtsvorschrift dies erlaubt oder der (datenschutzrechtlich) Betroffene eingewilligt hat. Als Rechtsvorschriften, die dies in bestimmtem Umfang erlauben, können die Richtlinie des Rates der Europäischen Gemeinschaften über den freien Zugang zu Informationen über die Umwelt und das dazu in der Bundesrepublik inzwischen in Kraft getretene Umweltinformationsgesetz (UIG)[117] angesehen werden. Diese Vorschriften enthalten eine weite Bestimmung des Begriffs „Informationen über die Umwelt" und schließen deshalb auch Informationen über Sanierungsvorhaben nach dem Baugesetzbuch ein. Allerdings gestatten auch diese keinen unbeschränkten Zugang zu personenbezogenen Daten, die in umweltrelevanten Verwaltungsvorgängen enthalten sein können. Ein Anspruch auf Akteneinsicht besteht nicht, soweit durch das Bekanntwerden der Informationen personenbezogene Daten offenbart *und* dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden (§ 8 UIG). Die aktenführenden Stellen haben deshalb im Einzelfall zu prüfen, wann aus diesem Grund ein Anspruch auf Informationszugang ausnahmsweise nicht besteht. Soweit schutzwürdige Interessen der Betroffenen durch die Einsichtnahme oder Auskunftserteilung nicht beeinträchtigt werden, ist auch der Zugang zu personenbezogenen Daten zu ermöglichen. In allen anderen Fällen ist zu prüfen, ob mit verhältnismäßigem Aufwand Akten anonymisiert werden können. Erst wenn dies verneint werden muß, darf den Betroffenenvertretern der Zugang zu personenbezogenen Umweltinformationen verwehrt werden.

Allerdings ist in all den Fällen, in denen die Betroffenenvertreter Einsicht in personenbezogene Sanierungsunterlagen erhalten, sicherzustellen, daß die von den auskunftspflichtigen Personen nach dem Baugesetzbuch erhobenen Daten nur zu Zwecken der Sanierung verwendet werden. Die Behörde hat durch geeignete Maßnahmen zu gewährleisten, daß auch die Betroffenenvertreter sich (z. B. vertraglich) verpflichten, die personenbezogenen Daten, die sie durch Akteneinsicht erhoben haben, nicht für andere Zwecke zu verwenden und nach Aufhebung der förmlichen Festlegung des Sanierungsgebiets zu löschen.[117a]

Rechte von Vermietern und Mietern

Ein Petent beschwerte sich, daß ein Bezirksamt von ihm verlangte, daß er seine Einkommensnachweise, die er im Rahmen des Freistellungsverfahrens mit Ausgleichszahlungen nach § 7 Abs. 3 Wohnungsbindungsgesetz (WoBindG) vorzulegen hat, erst dem Vermieter überlassen sollte, bevor dieser sie an das Wohnungsamt weiterleitet.

Neugeschaffener, öffentlich geförderter Wohnraum kann auch nichtberechtigten Personen überlassen werden, wenn das Wohnungsamt nach Abwägung der verschiedenen Interessen einer Freistellung zugestimmt hat. Gemäß § 7 Abs. 3 WoBindG kann die Freistellung mit Nebenbestimmungen, z. B. einer Befristung, Bedingung oder Auflage, versehen werden. Als Auflage wird wegen Überschreitung der maßgeblichen Einkommensgrenze eine laufende monatliche Ausgleichszahlung festgesetzt. Adressat des Freistellungsbescheides und somit zahlungspflichtig gegenüber dem Wohnungsamt ist der Verfügungsberechtigte über den Wohnraum, also der Vermieter. Dieser hat die Möglichkeit, die festgesetzte Ausgleichszahlung als Zuschlag zur Einzelmiete auf den Mieter abzuwälzen. Die Höhe der Ausgleichszahlung wird alle drei Jahre überprüft. Auf entsprechende Aufforderung des Wohnungsamtes sind die persönlichen und die *Einkommensverhältnisse der Wohnungsnutzer* neu nachzuweisen.

Gegenüber dem Petenten bestand das Wohnungsamt darauf, die Unterlagen bzw. Nachweise zur Einkommenssituation nur über den Vermieter dem Bezirksamt zu übermitteln. Es ist datenschutzrechtlich geboten, personenbezogene Daten unmittelbar beim Betroffenen zu erheben, wenn eine Rechtsvorschrift nichts anderes vorsieht (§ 10 Abs. 1 BlnDSG). Daraus folgt, daß Mieter bei einer Freistellung mit Ausgleichszahlung nach § 7 WoBindG die Möglichkeit haben müssen, ihre Daten unmittelbar und nicht auf dem Wege über den Vermieter an das Wohnungsamt zu übermitteln. Auf unsere Bedenken erläuterte das Wohnungsamt, daß es dem betroffenen Mieter gestattet ist, die geforderten Unterlagen in einem verschlossenen Umschlag über den Verfügungsberechtigten oder direkt bei dem zuständigen Wohnungsamt einzureichen.

Wegen des Widerspruchs zwischen dem angeblichen Verfahrensablauf und dem tatsächlichen Verhalten des Wohnungsamtes haben wir eine Änderung der im Verfahren verwendeten Formblätter gefordert. Das Wohnungsamt ist unserer Anregung gefolgt und hat den entsprechenden Vordruck modifiziert. Der Verfügungsberechtigte wird darin nunmehr ausdrücklich darauf hingewiesen, daß „auch keine Bedenken bestehen, wenn Ihr Mieter diese Unterlagen direkt bei uns einreicht".

In unserem Jahresbericht 1993 haben wir berichtet, daß für die Unterrichtung der Mieter über die Antragstellung des Eigentümers auf eine Abgeschlossenheitsbescheinigung die nach § 13 BlnDSG erforderliche Rechtsgrundlage fehlt[118].

Ein Gesetzentwurf der Fraktion Bündnis 90/GRÜNE, der die *Unterrichtung der Mieter* auf eine rechtliche Grundlage stellen sollte, fand im Abgeordnetenhaus keine Mehrheit. Im Bauausschuß wurde beschlossen, testweise für ca. ein Jahr bei Anträgen auf Abgeschlossenheitsbescheinigung die Einwilligung des Vermieters zur Information des Mieters auf freiwilliger Basis zu erbitten. Das Verfahren sieht vor, daß der betroffene Vermieter vom zuständigen Wohnungsamt des Bezirksamtes angeschrieben und um Zustimmung zur Mieterinformation gebeten wird. Bei Zustimmung soll die Informationsbroschüre zur Umwandlung an die betroffenen Mieter verteilt werden. Nach Abschluß der einjährigen Testphase soll erneut geprüft werden, ob weiterhin Bedarf an einer bereichsspezifischen Regelung besteht und ob entsprechende gesetzgeberische Maßnahmen auf Bundesebene anzuregen sind.

Wohnungsleerstand ist ein soziales Übel in einer Zeit, in der erheblicher Mangel an - bezahlbaren - Wohnungen herrscht. Der Baustadtrat eines Bezirksamtes kam auf die Idee, die Briefzusteller könnten mithelfen, leerstehende Wohnungen aufzuspüren.

Die *Erfassung einer leerstehenden Wohnung* betrifft immer die Anschrift, die Angabe, daß die Wohnung mit großer Wahrscheinlichkeit nicht bewohnt ist, und in der Regel den Namen des bisherigen Mieters. Somit werden personenbezogene Daten erhoben. Die Erhebung dieser Daten ist für die Erfüllung der Aufgaben des Postdienstes nicht erforderlich und auch durch die Postdienstdatenschutzverordnung nicht gedeckt.

Zwischen dem Bundesdatenschutzbeauftragten und der Generaldirektion der Deutschen Bundespost - Postdienst - bestand Einvernehmen, daß Anschriftenermittlungen nicht zu den Aufgaben des Postdienstes gehören. Bei ihrer Tätigkeit erhalten Postzusteller zum Teil tiefgehende Einblicke in die Lebensverhältnisse ihrer Zustellbereiche und deren Bewohner. Diese Kenntnisse unterliegen der Amtsverschwiegenheit. Eine aufgabenfremde Ermittlungstätigkeit würde dagegen verstoßen.

Weil schon die Übermittlung der Daten nicht rechtmäßig erfolgt, wäre auch eine Nutzung dieser Daten durch die empfangende Stelle unzulässig. Nach § 42 Abs. 1 ASOG können die Ordnungsbehörden nur rechtmäßig erhobene personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist. Dies gilt auch für personenbezogene Daten, die die Ordnungsbehörden unaufgefordert durch Dritte erlangt haben. Bei allem Verständnis für die Aufgabe, Wohnungsleerstand zu beseitigen, dürften damit Mitteilungen der Briefzusteller vom Wohnungsamt nicht genutzt werden.

117 siehe dazu oben 1.1

117a § 138 Abs. 3 BauGB gilt insofern entsprechend.

118 Jahresbericht 1993, 4.2

4.4 Finanzen

Fehlende Gesetze

Die Abgabenordnung (AO) ist das Verfahrensgesetz der Steuerverwaltung, in dem die bereichsspezifischen Besonderheiten präzise geregelt sein sollten. Dies wäre um so naheliegender, als das in § 30 AO verankerte Steuergeheimnis von jeher eine besonders strenge Vorschrift zum Schutz von Bürgerdaten darstellt. Gleichwohl fehlt es an detaillierten Bestimmungen zum Datenschutz. Im Gegenteil: Die Vagheit der vorhandenen Regeln führt immer wieder zu Auseinandersetzungen mit der Finanzverwaltung. Nicht verständlich ist daher die Auffassung des Senats[119], bereichsspezifische Datenschutznormen fehlten nicht.

Trotz alledem ist die dringend erforderliche Änderung der Abgabenordnung in diesem Jahr nicht weiterverfolgt worden. Ganz im Gegenteil: Das Bundesministerium für Finanzen hatte Ende 1993 den Vorschlag unterbreitet, den Entwurf eines *Abgabenordnungsänderungsgesetzes 1994* nicht weiterzuverfolgen. Es sah nach der Verabschiedung des Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetzes „keinen Handlungsbedarf mehr in datenschutzrechtlicher Hinsicht"[120]. 1994 hat sich tatsächlich in diesem Bereich nichts getan. Zu hoffen bleibt, daß das Gesetzesvorhaben 1995 wieder aufgenommen wird.

Nach langen Diskussionen ist es dagegen in diesem Jahr noch zur Verabschiedung des umstrittenen *Entschädigungs- und Ausgleichsleistungsgesetzes*[121] gekommen. Außer den von vielen erwarteten Entschädigungs- und Ausgleichsregelungen brachte es eine Änderung des *Gesetzes zur Regelung offener Vermögensfragen.* Die von der Berliner Verwaltung für Datenübermittlungen lange erwarteten, notwendigen Übermittlungsbefugnisse sind jedoch auch diesmal nicht geschaffen worden, so daß die Berliner Ämter für Offene Vermögensfragen (LAROV, ÄROV) sowie andere betroffene Behörden nach wie vor auf ein Landesausführungsgesetz warten müssen, das die fehlenden bereichsspezifischen Regelungen für die Datenverarbeitung der Ämter schafft.

Vorfeldermittlungen der Steuerfahndung

Auch öffentliche Stellen erhalten manchmal Post von der Steuerfahndung. Diese wandte sich an mehrere Krankenhäuser des Landes Berlin mit dem Ersuchen, Daten über bestimmte Personen zu übermitteln. Die Anfrage erfolgte ohne nähere Begründung und unter Angabe einer langen Kette von Rechtsgrundlagen, die eine Vielzahl von Fallgestaltungen betreffen können. Welche Ermittlungen die Steuerfahndung durchführen wollte, blieb für die Krankenhäuser unklar.

Bei den Anfragen handelte es sich um Vorfeldermittlungen, die die Steuerfahndung nach § 208 Abs. 1 Nr. 3 AO durchführen wollte. Vorfeldermittlungen dienen der Aufdeckung und Ermittlung unbekannter Steuerfälle, also von Fällen, in denen die Täter oder die Tatbestandsverwirklichung unbekannt sind. Sie sind dann zulässig, wenn zwar keine konkreten Anhaltspunkte für eine Straftat oder Ordnungswidrigkeit gegeben sind, jedoch die Möglichkeit einer Steuerverkürzung vermutet wird.

Die um Auskunft ersuchte Behörde ist nach § 12 Abs. 3 BlnDSG verpflichtet, die Zulässigkeit der erbetenen Datenübermittlung zu überprüfen. Dazu ist es erforderlich, daß die um Auskunft ersuchende Stelle ihre Anfrage auch begründet und die Rechtsgrundlagen für das Ersuchen benennt.

Um Fahndungsmaßnahmen der Steuerfahndung ins Blaue hinein zu verhindern, setzt nach der Rechtsprechung des Bundesfinanzhofs ein auf eine Vorfeldermittlung gestütztes Auskunftsersuchen voraus, daß auf Grund von Ermittlungserfahrungen Erkenntnisse darüber vorliegen, daß von einer bestimmten Gruppe von Steuerpflichtigen verhältnismäßige viele Steuern verkürzen.[122]

Die Steuerfahndungsstelle hat im vorliegenden Fall bei ihren Anfragen keine Begründungen abgegeben, die es den Krankenhäusern ermöglicht hätte, ihre Übermittlungspflichten zu prüfen. Die Anfragen dürfen jedoch erst dann beantwortet werden, wenn dies erfolgt ist. Die Senatsverwaltung für Finanzen hält weitere Begründungen der Steuerfahndung nicht für erforderlich. Sie meint, daß das Berliner Datenschutzgesetz nicht anwendbar ist, sondern will das Bundesdatenschutzgesetz heranziehen. Danach trägt derjenige, der um Auskunft ersucht, die Verantwortung für die Zulässigkeit seines Ersuchens und muß dieses daher nicht weiter begründen.

Dieser Rechtsauffassung liegt ein falsches Verständnis des § 2 Abs. 1 BlnDSG zugrunde. Danach findet das Berliner Datenschutzgesetz Anwendung bei allen Behörden und öffentlichen Stellen des Landes Berlin und damit unzweifelhaft auch auf die Datenverarbeitung der Finanzämter und deren Steuerfahndung. Die Anwendbarkeit des Berliner Datenschutzgesetzes wird auch nicht dadurch ausgeschlossen, daß § 2 Abs. 3 BlnDSG besagt, daß – soweit personenbezogene Daten im Anwendungsbereich des Gesetzes über das Verfahren der Berliner Verwaltung (Verwaltungsverfahrensgesetz) verarbeitet werden – die Vorschriften des Berliner Datenschutzgesetzes gelten. Diese Regelung stellt vielmehr lediglich klar, daß das Verwaltungsverfahrensgesetz nicht als gegenüber dem BlnDSG vorrangige und dieses daher ausschließende Materie zu betrachten ist.

Kontoauszüge mit Steuerdaten und das Steuergeheimnis

Die Freude über seine Steuerrückerstattung verging einem Bürger, als er sah, daß sich auf seinem Kontoauszug außer dem Betrag einer Gutschrift durch das Finanzamt auch einzelne Daten seines Rückzahlungsbescheides wiederfanden. Das Finanzamt hatte auf dem Überweisungsträger z. B. Angaben zur Steuerart und den konkreten Steuerbeträgen gemacht.

Seit Dezember 1993 erscheinen auf den *Überweisungsträgern* bei Arbeitnehmerveranlagungen nur noch die Steuernummer und der Veranlagungszeitraum. Weitere Daten aus dem Rückerstattungsbescheid werden nicht mehr angegeben. Entsprechend wird bei der Erstattung von Kraftfahrzeugsteuer verfahren. Bei allen anderen Veranlagungsarten werden auf dem Überweisungsträger der Betrag, die Steuerart und der Zeitraum der Veranlagung erläutert. Einen solchen Überweisungsträger hatte auch der Petent erhalten. Bei der beschriebenen Verfahrensweise handelt es sich um ein bundeseinheitlich abgestimmtes Verfahren.

Der Bürger war das Opfer eines Fehlers, der den Finanzbehörden bei der seit Anfang 1992 in Berlin durchgeführten Überführung des Arbeitnehmerbesteuerungsverfahrens auf Speicherkonten unterlaufen ist. Dabei war übersehen worden, daß nur noch in bestimmten Erstattungsfällen auf den Überweisungsträgern differenzierte Angaben gemacht werden sollen.

Entgegen der Auffassung der Oberfinanzdirektion und der Senatsverwaltung für Finanzen halten wir auch bei den Veranlagungsarten, bei denen weiterhin differenzierte Angaben zur Steuererstattung auf dem Überweisungsträger der Bank erscheinen, eine Beschränkung der Daten auf die Angabe der Steuernummer und des Veranlagungszeitraumes für erforderlich. Gegebenenfalls muß eine gesonderte Erstattungsmitteilung für den Steuerschuldner gefertigt werden. Nur so ist sichergestellt, daß die Banken nicht mehr an Informationen erhalten, als für die Überweisung erforderlich ist. Die Senatsverwaltung für Finanzen hält dagegen ein solches Verfahren für zu kostenaufwendig und unpraktikabel, da der Steuerschuldner häufig buchführungspflichtig sei und ein detaillierter Überweisungsbeleg für ihn das Verfahren erleichtere. Wir haben empfohlen, sich für eine Änderung des abgestimmten Verfahrens einzusetzen. Dies ist jedoch abgelehnt worden mit dem Hinweis, daß der Bund und die Länder der Ansicht seien, daß das praktizierte Verfahren zulässig sei.

Neukonzeption Automatisiertes Haushaltswesen (NK-AHW)

Eines der größten Automatisierungsprojekte der Berliner Verwaltung ist die Neukonzeption des ADV-Verfahrens für das Haushaltswesen. Es soll künftig ermöglichen, daß Haushaltsplanung und -bewirtschaftung vom Arbeitsplatz der zuständigen Mitarbeiter aus on line bearbeitet werden können.

119 Stellungnahme des Senats zum Jahresbericht 1993, Abghs.-Drs. 12/4655,40
120 Jahresbericht 1993, 4.3
121 BGBl. 1994 I, 2624
122 beispielsweise BFH in BStBl. II 1987, 448, 485

Die Neukonzeption erfolgt auf der Grundlage des Programmsystems ProFISKAL, das im Rahmen einer Ausschreibung als Sieger hervorging. Zu einem von einer Unternehmensberatung erarbeiteten IT-Sicherheitskonzept sowie den entsprechenden Entwürfen von Verwaltungsvorschriften und Richtlinien für den Einsatz des Programmsystems haben wir Stellung bezogen.

Die datenschutzrechtliche Verantwortung bei der Verarbeitung von personenbezogenen Daten im Rahmen des NK-AHW tragen als datenverarbeitende Stellen die für das Haushaltswesen zuständigen Untergliederungen der Senats- oder Bezirksverwaltungen. Die Senatsverwaltung für Finanzen und das LIT sind - soweit sie administrierend, betreuend oder im Rahmen der Datensicherung oder Wartung beteiligt sind - als Datenverarbeiter im Auftrag (§ 3 BlnDSG) tätig.

Das vorgelegte IT-Sicherheitskonzept enthielt zwar eine Bedrohungs- und Risikoanalyse, die die Sicherheitsmaßnahmen, das Zugriffskontrollkonzept, das Datenschutzkonzept und die Anforderungen an die Kommunikationsinfrastruktur begründeten, verzichtete jedoch auf eine Restrisikobetrachtung, die sich auf den Zustand des Verfahrens nach Umsetzung der vorgeschlagenen Maßnahmen zu beziehen hätte. Somit war nicht analysiert worden, ob die Maßnahmen in allen Fällen, in denen untragbare Risiken konstatiert wurden, hinreichend greifen. Die Senatsverwaltung für Finanzen hat angekündigt, daß die Restrisikobetrachtungen erfolgen werden, wenn hinreichende Betriebserfahrungen aus der Einführungsphase vorliegen, die noch zu Änderungen des Sicherheitskonzeptes führen könnten.

Unklar blieb zunächst, wie die Senatsverwaltung für Finanzen die Umsetzung des Sicherheitskonzeptes vor Ort unterstützen wollte. Das vorgelegte Konzept konnte nur einen Rahmen für die einsetzenden Stellen bilden, weil die jeweiligen Verhältnisse nicht vollständig berücksichtigt werden konnten. Für die Erstellung und Umsetzung spezifischer Sicherheitskonzepte bedarf es z. B. der Bereitstellung von Checklisten. Die Senatsverwaltung für Finanzen will den Vorschlag aufgreifen und vor der flächendeckenden Einführung des Verfahrens solche Hilfsmittel bereitstellen.

Ein wesentliches Problem für ProFISKAL ergibt sich aus den Sicherheitsdefiziten, die allgemein bei UNIX-Systemen auftreten, wenn diese nicht um zusätzliche Sicherheitsfunktionen ergänzt worden sind. Hierzu gehören die allumfassenden Rechte der Superuser, die faktisch nicht kontrollierbar sind.

Die vorgesehenen Maßnahmen, die vor allem auf einer Funktionentrennung zwischen den einsetzenden Stellen und dem LIT/SAZ beruhen und erst nach einer Übergangszeit bis zur Funktionsbereitschaft des SAZ wirksam werden, mindern zwar die Risiken, ob dies jedoch ausreicht, muß noch zum Gegenstand einer Restrisikobetrachtung gemacht werden.

4.5 Gesundheit

Krebsregister wird eingerichtet

Mit dem Gesetz über Krebsregister (Krebsregistergesetz - KRG) des Bundes[123] hat eine jahrelange Auseinandersetzung über Sinn und Zulässigkeit der Registrierung von Krebserkrankungen ein vorläufiges Ende gefunden. Das Gesetz, das nur eine Geltungsdauer von fünf Jahren hat, verpflichtet seit dem 1. Januar 1995 alle Bundesländer, bis zum 1. Januar 1999 flächendeckend bevölkerungsbezogene Krebsregister einzurichten und zu führen. Das Gesetz enthält konkrete Vorgaben für die *Voraussetzungen der Datenerhebung und -verarbeitung.* Ob dies verfassungskonform ist oder ob der Bund hier über seine Kompetenzen hinausging, blieb bis zum Ende umstritten und wurde erst am Ende des Gesetzgebungsverfahrens durch einen Kompromiß im Vermittlungsausschuß zugunsten der Bundeszuständigkeit entschieden.

Während in der ehemaligen DDR ein zentrales Krebsregister geführt wurde, an das Daten über Krebserkrankungen hinter dem Rücken der Patienten gemeldet werden mußten, bestanden in den alten Bundesländern bisher nur in Hamburg und im Saarland landesweite Krebsregister, an die patientenbezogene Daten gemeldet wurden. Das neue Krebsregistergesetz des Bundes sieht jetzt vor, daß Ärzte lediglich berechtigt, nicht aber verpflichtet sind, dem jeweiligen Krebsregister patientenbezogene Daten zu übermitteln. Der Arzt hat den Patienten von der beabsichtigten oder erfolgten Meldung zum frühestmöglichen Zeitpunkt zu *unterrichten.* Die Unterrichtung darf nur unterbleiben, solange zu erwarten ist, daß dem Patienten durch sie gesundheitliche Nachteile entstehen könnten. Der Patient kann der Meldung *widersprechen;* auf dieses Widerspruchsrecht ist er vom Arzt hinzuweisen. Auf Wunsch ist er auch über den Inhalt der Meldung zu unterrichten. Widerspricht der Patient, so hat der Arzt die Meldung zu unterlassen oder zu veranlassen, daß die gemeldeten Daten gelöscht werden.

Die Meldungen an das Krebsregister werden in einem zweistufigen Verfahren verarbeitet. In den unter ärztlicher Leitung stehenden *Vertrauensstellen* werden die gemeldeten Daten auf Schlüssigkeit und Vollständigkeit überprüft, etwaige Rückfragen vorgenommen sowie die Identitätsdaten und die epidemiologischen Daten auf getrennte Datenträger übernommen. Die Vertrauensstellen übermitteln anschließend den *Registerstellen* verschlüsselte Identitätsdaten und epidemiologische Daten; anschließend löschen sie alle bei ihnen vorhandenen patientenbezogenen Daten. Unter bestimmten Voraussetzungen dürfen für Maßnahmen des Gesundheitsschutzes und für wichtige Forschungsaufgaben personenbezogene Daten mit Daten des Krebsregisters abgeglichen und bereits verschlüsselte Identitätsdaten wieder entschlüsselt werden.

Die Krebsregister der Länder haben einmal jährlich epidemiologische Daten in anonymisierter Form an die beim Robert-Koch-Institut in Berlin eingerichtete *„Dachdokumentation Krebs"* zu übermitteln.

In Berlin wurde bisher auf der Grundlage des Krebsregistersicherungsgesetzes der Datenbestand des ehemaligen Krebsregisters der DDR im Auftrag Berlins und der neuen Bundesländer verwaltet. Durch ein ebenfalls am 1. Januar 1995 in Kraft getretenes *Verwaltungsabkommen* hat Berlin mit den neuen Ländern vereinbart, ein „Gemeinsames Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen" einzurichten, das als flächendeckendes Krebsregister i. S. d. Krebsregistergesetzes gilt. In dieses Gemeinsame Krebsregister wird der vorhandene Datenbestand einbezogen. Das Gemeinsame Krebsregister unterliegt dem Datenschutzrecht des Landes Berlin, soweit nicht im Krebsregistergesetz etwas anderes bestimmt ist. Das Verwaltungsabkommen über das Gemeinsame Krebsregister muß bis spätestens 1999 durch eine landesgesetzliche Regelung in allen beteiligten Ländern abgelöst werden.

Chipkarten halten ihren Einzug

Abgesehen von den anonymen Telefonkarten wurden die Bürger im Berichtsjahr erstmals in großem Umfang mit der Chipkartentechnik konfrontiert, über die wir im vergangenen Jahr ausführlich berichtet haben[124]: In Ausführung des § 291 SGB V, der zwar die Einführung einer einheitlichen Krankenversichertenkarte für die gesetzlichen Krankenversicherungen vorsieht, aber über die technische Ausführung schweigt, wurden die Versicherten im vergangenen Jahr mit einer Karte ausgestattet, die in bescheidenem Umfang die Mikrochiptechnologie nutzt.

Auf der Karte sind nur diejenigen Daten enthalten, die § 291 SGB V vorsieht; die Möglichkeit, weitere Daten zu speichern, ist technisch ausgeschlossen. Damit dient die Karte nur dem Nachweis der Berechtigung, Leistungen in Anspruch zu nehmen, sowie der Arbeitserleichterung der Ärzte - wenn auch mit der Einführung der Karte für viele Arztpraxen der Einstieg in die Praxisautomation verbunden ist, die eine der Bausteine zu einer umfassenden Vernetzung aller an der Gesundheitsversorgung beteiligten Stellen darstellt.

Es zeichnet sich allerdings ab, daß im Bereich des Gesundheitswesens die Chipkarte eine erheblich größere Bedeutung erhalten wird. Der AOK-Bundesverband („VitalCard") sowie der BKK Landesverband Sachsen („BKK-Card") erproben die Einführung von Gesundheitskarten mit einer ganzen Reihe medizinischer

123 BGBl. 1994 I, 3351

124 Jahresbericht 1993, 2.3

Daten, die Bundesvereinigung deutscher Apothekerverbände möchte die Versorgung mit Medikamenten mit einer „A-Card" unterstützen, in Zusammenarbeit der Universität Freiburg und einer hessischen Klinik wird als Alternative zur Chipkartentechnik eine auf optoelektronischer Basis arbeitende Karte getestet, die es gestattet, auch Abbildungen wie z. B. Röntgenaufnahmen zu speichern („DiagnostiX Card").

Die Einführung derartiger Techniken ist mit weitreichenden Konsequenzen und Risiken für die betroffenen Bürger verbunden, denen mit hinreichenden Maßnahmen des Datenschutzes und der Datensicherung begegnet werden muß. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu einigen Aspekten auf ihrer Sitzung am 9./10. März in Potsdam einen Beschluß mit entsprechenden Forderungen gefaßt.[125]

AOK bewirkt Verlust des Arbeitsplatzes

Ein Arbeitnehmer, der gerade einen neuen Arbeitsplatz angetreten hatte, litt an Lungenkrebs, was seinem Arbeitgeber bekannt war. Er war so weit geheilt, daß die Behandlung in der Klinik beendet werden konnte und drei Nachuntersuchungen gute Befunde gebracht hatten. Während der Probezeit wurde er wegen einer weiteren Behandlung krankgeschrieben. Nachdem der Petent die Arbeit wieder aufgenommen hatte, erhielt der Arbeitgeber von der AOK die Nachricht, daß „Anlaß zu der Annahme besteht, daß die ärztlich festgestellte Arbeitsunfähigkeit bereits bei der Arbeitsaufnahme bestanden hat". Im Ergebnis mußte der Arbeitgeber, der eigentlich zu einer Weiterbeschäftigung bereit war, dem Petenten kündigen, weil die AOK sich weigerte, ein Versicherungsverhältnis mit dem Petenten einzugehen.

Die AOK erklärte dazu, daß die Krankenkassen nicht nur berechtigt, sondern sogar verpflichtet sind, in Einzelfällen zu prüfen, ob ein versicherungspflichtiges Beschäftigungsverhältnis zustande gekommen ist. Voraussetzung ist die Arbeitsfähigkeit zum Zeitpunkt der Arbeitsaufnahme. Durch Anfrage bei dem behandelnden Arzt seien erforderlichenfalls Angaben zum Gesundheitszustand zu erfragen. Wenn diese Auskünfte den Verdacht eines „mißglückten Arbeitsversuches" ergeben, sei eine entsprechende Mitteilung an den Arbeitgeber zu richten. Der Arbeitnehmer werde dabei nicht beteiligt.

Im vorliegenden Fall war die Mitteilung an den Arbeitgeber erfolgt, bevor die medizinischen Daten geklärt waren. Eine unzulässige Offenbarung von Sozialdaten lag demnach darin, daß die AOK schon bei der Anfrage erklärte, daß Anlaß für die Annahme eines mißglückten Arbeitsversuchs bestehe. Wir haben bemängelt, daß dadurch das Ergebnis der noch nicht beendeten ärztlichen Prüfung vorweggenommen worden sei, und haben empfohlen, erst nach dem Abschluß aller für die Prüfung relevanten Gesichtspunkte dem Arbeitgeber die gesetzlich notwendigen Mitteilungen zukommen zu lassen.

Denn richtig ist zwar, daß die AOK befugt ist, vom Arbeitgeber Auskunft über Art und Dauer der Beschäftigung zu verlangen (§ 98 SGB X). Eine Mitteilung über den mißglückten Arbeitsversuch kann jedoch erst dann erfolgen, wenn er medizinisch feststeht. Es kann nicht zulässig sein, hinter dem Rücken des Patienten die Arbeitsunfähigkeit attestieren zu lassen, ohne daß der Patient davon erfährt.

Wenn die Arbeitsunfähigkeit strittig ist, ist die Stellungnahme des medizinischen Dienstes der Krankenversicherungen vorgesehen, der gemäß § 275 Abs. 1 Ziffer 3 SGB V eine gutachterliche Stellungnahme zur Arbeitsfähigkeit oder Arbeitsunfähigkeit abzugeben hat. Der Versicherungsnehmer ist unverzüglich aufzufordern, sich einer Untersuchung durch den medizinischen Dienst zur Verfügung zu stellen, damit die Arbeitsfähigkeit eindeutig festgestellt werden kann. Hierbei besteht eine Mitwirkungspflicht des Versicherten. Unsere Stellungnahme hat die AOK Berlin dazu bewogen, das Verfahren grundsätzlich zu überdenken und die einschlägigen Vordrucke durch die AOK-Vordruckkommission ändern zu lassen. Insbesondere soll nunmehr die Einwilligung des Betroffenen zur Beiziehung weiterer ärztlicher Informationen eingeholt werden.

125 vgl. Anlage 2.2

Ärztliche Schweigepflicht und Strafverfolgung

Zwei Fragestellungen, die im vergangenen Jahr an uns herangetragen wurden, zeigen das problematische Verhältnis zwischen dem Schutz der ärztlichen Schweigepflicht und dem staatlichen Interesse auf Strafverfolgung.

In der DDR wurde mit hoher Wahrscheinlichkeit das Dopingwesen durch verschiedene Stellen der SED und durch staatliche und sportmedizinische Einrichtungen zentral gesteuert. Es besteht der Verdacht, daß es durch Verwendung einiger Dopingsubstanzen zu Gesundheitsbeschädigungen insbesondere auch bei Minderjährigen gekommen ist. Die Arbeitsgruppe Regierungskriminalität der Staatsanwaltschaft sowie die Zentrale Ermittlungsstelle Regierungs- und Vereinigungskriminalität des Polizeipräsidenten begehrten Einsicht in alle bei der Senatsverwaltung für Gesundheit archivierten Patientenakten des ehemaligen Sportmedizinischen Dienstes der DDR.

Diese Akten enthalten Informationen, die ursprünglich der ärztlichen Schweigepflicht unterlagen, weil sie einem Arzt in dieser Eigenschaft anvertraut oder bekannt geworden waren. Sie reicht über den Tod des behandelnden Arztes hinaus, auch dann, wenn sich die Unterlagen nicht mehr in ärztlicher Hand befinden. Bei der Übernahme der sportärztlichen Untersuchungs- und Behandlungsunterlagen der DDR handelte es sich um eine Rechtsnachfolge mit der Folge, daß die rechtlichen Pflichten der abgebenden Stelle gegenüber dem Patienten als Schutzpflichten der übernehmenden Stelle, also der zuständigen Behörden, fortgelten.

Die ärztliche Schweigepflicht soll jedoch nur den Patienten und nicht strafrechtlich relevantes Verhalten eines Arztes vor der Strafverfolgung schützen. Daher kann die Staatsanwaltschaft die Anordnung der Beschlagnahme des Aktenbestandes durch den Richter gemäß §§ 97, 98 StPO beantragen. Bei der Prüfung hätte der Richter Zweifel zu berücksichtigen, ob tatsächlich jeder einzelne Vorgang strafrechtlich relevant ist.

Unbedenklich ist es natürlich, Auskunft über die Gesamtheit der verwalteten Materialien sowie über die Verfahrensweisen allgemeiner Art beim sportärztlichen Dienst zu geben, soweit keine personenbezogenen Daten übermittelt werden. Darüber hinaus hat jeder Sportler die Möglichkeit, Strafanzeige gegen einzelne Ärzte oder leitende Bedienstete des Sportärztlichen Dienstes der DDR zu erstatten.

Ein türkischer Mitbürger begab sich freiwillig mit einer Schußverletzung zur Behandlung in ein Krankenhaus. Aus Furcht vor weiterer Verfolgung veranlaßte er eine Auskunftssperre über seinen Aufenthalt. Eine Benachrichtigung der Polizei durch das Krankenhaus erfolgte nicht.

Dieser Sachverhalt wurde zum Anlaß für eine Nachfrage genommen, ob es möglich sei, eine Meldepflicht der Krankenhäuser zumindest bei Schußverletzungen einzuführen, um Maßnahmen zum Schutz der Betroffenen, sicherlich aber auch zur Verfolgung der Straftat – möglicherweise eines Mordversuchs – ergreifen zu können.

Die Anfrage mußte von uns verneint werden. Die ärztliche Schweigepflicht soll das Vertrauensverhältnis zwischen Arzt und Patient schützen und damit die Funktionsfähigkeit des Gesundheitswesens gewährleisten. Da Leib, Leben und Gesundheit die obersten verfassungsrechtlichen Werte darstellen, müssen andere öffentliche Interessen hinter der ärztlichen Schweigepflicht zurücktreten. Dies gilt grundsätzlich auch für den staatlichen Strafverfolgungsanspruch. In der höchstrichterlichen Rechtsprechung ist dieser Grundsatz wiederholt bestätigt worden.[126]

Die Schweigepflicht des Arztes kann jedoch dann durchbrochen werden, wenn die strikte Einhaltung ihrerseits zu einer Gefährdung menschlichen Lebens, der menschlichen Gesundheit oder anderer höherwertiger Rechtsgüter führen würde. Wesentlich dabei ist, daß die Offenbarung unmittelbar geeignet ist, der Gefährdung direkt entgegenzuwirken. Diese Sachlage ist jedoch bei der Behandlung einer Schußverletzung nicht gegeben,

126 vgl. z. B. Urteil des Bundesgerichtshofes vom 15. April 1985, Az 2 StR 561/84

jedenfalls solange nur das Opfer dem Arzt bekannt ist, nicht jedoch der Täter. Von dem Opfer, das sich in Behandlung befindet, geht keinerlei unmittelbare Gefahr aus, so daß eine Meldung der Schußverletzung auch nicht erforderlich ist, eine Gefahr abzuwenden.

Vielmehr würde eine Meldepflicht die Behandlungsbereitschaft eines verletzten Opfers drastisch mindern; dies zeigte gerade der dargestellte Fall besonders deutlich. Davon unberührt bleibt natürlich, daß es eine selbstverständliche Pflicht des Arztes sein sollte, auf das Opfer dahingehend einzuwirken, daß es einen eigenen Beitrag zur Aufdeckung der Straftat leistet.

Immer wieder: Medizinische Akten auf der Straße

Erneut seien Fälle geschildert, in denen durch Unachtsamkeit oder bösen Willen medizinische Unterlagen unsachgemäß behandelt und damit unbefugt Dritten zugänglich gemacht wurden.

Von Straßenpassanten wurden in Wedding etwa 13 Blechbehälter mit Röntgenfilmrollen eines Krankenhauses aus Stendal nebst den Resten eines Pappkartons gefunden. Eine zufällig vorbeigekommene Polizeistreife wurde von den Passanten gebeten, den Fund zu übernehmen, was von dieser jedoch angeblich abgelehnt wurde. Erst nach längerem Zureden gelang es den Passanten, der Polizeistreife wenigstens eine der Rollen aufzureden und um Aufklärung des Vorgangs zu bitten. Den Rest brachten sie uns.

Die Röntgenrollen waren zwei Tage zuvor als Paketsendung aufgegeben worden waren. Bemerkenswert war, daß dieser Fall verbunden war mit einem weiteren Fund von Röntgenaufnahmen aus einem kirchlichen Krankenhaus, welches umfangreiche Röntgenunterlagen über einen Berliner Patienten an dessen behandelnden Arzt übersandt hatte. Diese Sendung war bereits ein Jahr zuvor aufgegeben worden, aber zusammen mit den Röntgenfilmrollen gefunden worden. Wir haben von der Vorschrift des § 32 Abs. 3 BlnDSG Gebrauch gemacht und Strafantrag gestellt. Die Ermittlungen sind noch nicht abgeschlossen.

Es erscheint allerdings fraglich, ob die Ermittlungen noch wesentlich neue Erkenntnisse bringen werden, da bei dem derzeitigen Paketversandsystem eine Kontrolle des Verbleibs von Paketpostsendungen nur möglich ist, wenn die Sendung als „Wertpaket" über 3 000 DM deklariert wird. Trotz der Paketkarte und des Abgangsabschnitts, der beim Absender bleibt, scheint der Postdienst nicht imstande zu sein, den Weg einzelner Paketsendungen zu verfolgen, wenn diese falsch geleitet worden sind. Daraus ergibt sich, daß die Verpflichtung zur Transportsicherung (§ 5 Abs. 2 BlnDSG) bedeutet, daß so hochsensible Daten wie Röntgenfilme nur als Wertsendung verschickt werden dürfen.

Aus dem Klinikum Rudolf Virchow stammende Röntgenbefunde und Patientenkarteien wurden auf dem Ackerland in der Nähe eines Umspannwerkes zwischen den Ortschaften Neuenhagen und Altlandsberg gefunden. Es handelte sich um Patientenunterlagen, deren Aufbewahrungsfrist abgelaufen war oder bei denen es sich um fehlerhafte Vorentwürfe handelte.

Die Unterlagen wurden im Auftrag des Klinikums von einer Privatfirma entsorgt, die unter anderem auch für die Abfuhr von Bauschutt zuständig ist. Bei der Vernichtung von personenbezogenen Unterlagen ist die Einschaltung einer Fremdfirma nur dann zulässig, wenn bis zum Zeitpunkt der Vernichtung die Aufsicht durch die verantwortliche Stelle sichergestellt ist. Dies ist offensichtlich hier nicht der Fall gewesen.

Ein ausführlicher Arztbericht eines Spandauer Krankenhauses wurde in einer Mülltonne in einem anderen Bezirk aufgefunden. Eine Mitarbeiterin des Krankenhausschreibdienstes hatte sich Schreibarbeiten unerlaubt mit nach Hause genommen und die nicht mehr benötigten Vorentwürfe in die Mülltonne geworfen, wo sie von einem Hausbewohner gefunden wurden.

Dieser Fall zeigt zumindest zweierlei: Werden Schriftstücke in Heimarbeit erstellt (ob befugt oder unbefugt spielt insoweit keine Rolle), muß auf die Datensicherheit höchster Wert gelegt werden. Die in Zusammenhang mit der Frauenförderung sowie der Flexibilisierung der Arbeitsabläufe künftig vermehrt wahrgenommenen Möglichkeiten der Heimarbeit sind nur akzeptabel, wenn gleichzeitig hinreichende Sicherungskonzepte entwickelt werden.

4.6 Inneres

4.6.1 Polizei

Neues zum Polizeirecht

Am 1. November 1994 trat das Gesetz zur Neuregelung der Vorschriften über den *Bundesgrenzschutz* (Bundesgrenzschutzneuregelungsgesetz - BGSNeuRegG) vom 19. Oktober 1994 in Kraft.[127] Danach kommt bei der Unterstützung eines Landes durch den Bundesgrenzschutz grundsätzlich das für das Land geltende Recht zur Anwendung. Wird der Bundesgrenzschutz daher zur Unterstützung der Berliner Polizei bei der Aufrechterhaltung oder Wiederherstellung der öffentlichen Sicherheit oder Ordnung in Fällen von besonderer Bedeutung tätig, gelten die Bestimmungen des Berliner Allgemeinen Sicherheits- und Ordnungsgesetzes.

Datenschutzrechtlich problematisch ist die Befugnis zur Nutzung personenbezogener Daten auf Grund von Anfragen der Verfassungsschutzbehörden, des MAD und des BND über grenzpolizeiliche Angelegenheiten.[128] Nach dem Wortlaut des Gesetzes könnte der Bundesgrenzschutz die personenbezogenen Daten für einen anderen Zweck als den, für den die Daten erlangt worden sind, nutzen, soweit er die Daten für diesen Zweck erheben durfte.

Damit wäre eine Zweckentfremdung der auf Grund von Ersuchen der Nachrichtendienste gespeicherten Daten für eigene Zwecke des Bundesgrenzschutzes möglich. Durch die nicht eingeschränkte Befugnis zum Datenabgleich[129] könnte des weiteren ein Informationsverbund zwischen Datenspeicherungen beim Bundesgrenzschutz und den Verfassungsschutzbehörden entstehen. Um der Gefahr einer Aufhebung der informationellen Trennung zwischen Polizei und Verfassungsschutzbehörden entgegenzuwirken, müssen diese Bestimmungen insoweit restriktiv ausgelegt werden. Datenabgleiche im Zusammenhang mit der Beantwortung von Ersuchen der Nachrichtendienste dürfen ebenfalls nicht erfolgen.

Der Bundesminister des Innern hat einen Referentenentwurf eines *Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten* den Ländern vorgelegt. Der Gesetzentwurf räumt dem Bundeskriminalamt (BKA) zusätzliche Befugnisse ein, die auch Länderkompetenzen berühren.

So soll das BKA die Möglichkeit erhalten, den *Anfangsverdacht* (zureichende tatsächliche Anhaltspunkte) einer in § 110 a Strafprozeßordnung (StPO) bezeichneten Straftat festzustellen. Im Unterschied zu den entsprechenden Regelungen in den Landespolizeigesetzen erhält das BKA damit die Befugnis zu ermitteln, ohne daß tatsächliche Anhaltspunkte dafür vorliegen, daß Straftaten begangen werden sollen.

Die Kompetenzen des BKA zu einer länderübergreifenden, internationalen Kriminalitätsbekämpfung sollen ergänzt werden um die Bekämpfung der Kriminalität „von erheblicher Bedeutung". Die Definition dieses Begriffes ist unklar und wird auch durch die Begründung zum Gesetzentwurf nicht in ausreichendem Maße erläutert. Dem BKA soll ferner die Befugnis zum aktiven Sammeln von Informationen eingeräumt werden, auch wenn die Sache selbst noch keine länderübergreifende, internationale oder erhebliche Bedeutung hat. Damit erhält das BKA eine eigene, allein auf seine Zentralstellenfunktion gestützte Ermittlungskompetenz.

Der Entwurf läßt allgemein eine deutliche Differenzierung zwischen den vom Bundeskriminalamt als Zentralstelle geführten Datensammlungen (Zentraldateien, Dateien der Zentralstelle) und dem *INPOL-Verbundsystem* vermissen. Durch eine Generalklausel soll das BKA vielmehr pauschal zu jeglicher Art von Datenverarbeitung ermächtigt werden. Eine Zweckbindung ist nicht vorgesehen. Das Bundeskriminalamt soll Daten bei den Länderpolizeien erheben können, ohne daß daran weitere Voraussetzungen geknüpft sind.

127 BGBl. 1994 I, 2978 f.
128 § 29 Abs. 1 Sätze 2 und 4 BGSNeuRegG
129 § 34 Abs. 1 Nr. 2 BGSNeuRegG

Grunddaten von Beschuldigten soll das BKA ohne weitere Voraussetzungen speichern dürfen. Anders als im ASOG[130] soll keine „Negativ-Prognose" über künftige Straftaten gefordert werden.

Die Voraussetzungen für die Speicherung von personenbezogenen Daten von potentiellen Zeugen, Gefährdeten, Kontakt- und Begleitpersonen werden in bedenklicher Weise vermischt. Die Möglichkeiten zur Speicherung erkennungsdienstlicher Unterlagen sollen erheblich erweitert werden. Bedenklich ist hier insbesondere, daß ed-Unterlagen zu allen denkbaren Zwecken der Gefahrenabwehr erhoben, in Dateien gespeichert, verändert oder genutzt werden dürfen. Die weitere Speicherung inaktueller Haftdaten soll legitimiert werden. Die Erforderlichkeit dieser Datenspeicherungen, insbesondere nach Wegfall der Haftanordnung, wird nicht begründet. Die Übermittlung von Daten, die von Landespolizeibehörden angeliefert werden, soll dem BKA erlaubt werden, ohne daß deren Zustimmung eingeholt werden muß.

Die konkrete gesetzliche Ausgestaltung des INPOL-Systems bleibt völlig unklar. Statt dessen werden das Bundesministerium des Innern sowie die Innenministerien und -senatoren der Länder ermächtigt, die Architektur des Systems zu gestalten; angesichts der Bedeutung dieses Systems für die Freiheitsrechte wäre hier der Gesetzgeber gefragt!

Die Europapolizei kommt

Die zukünftige informationelle Zusammenarbeit verschiedener europäischer Behörden, insbesondere der Polizei, ist im *Schengener Durchführungsübereinkommen (SDÜ)* vom 19. Juni 1990 geregelt. Dem Abkommen sind bisher Belgien, Deutschland, Frankreich, Luxemburg, Niederlande, Spanien, Portugal, Italien und Griechenland beigetreten. Ein Teil des SDÜ befaßt sich mit dem Aufbau und der Einrichtung des Schengener Informationssystems (SIS). Als von den genannten Staaten gemeinsam geführte *Fahndungsdatei* soll das SIS die Folgen, die mit dem Wegfall der Grenzkontrollen an den Binnengrenzen verbunden sind, ausgleichen. Ein abschließender Katalog der personenbezogenen Daten, die zum Zweck der Ausschreibung von Personen und Sachen zur Fahndung im SIS gespeichert werden dürfen, ist in Art. 94 Abs. 3 SDÜ enthalten. Danach dürfen die zur Identifikation erforderlichen Daten, Hinweise auf Bewaffnung oder Gewalttätigkeit, der Ausschreibungsgrund und die zu ergreifenden Maßnahmen - im Regelfall für einen Zeitraum von drei Jahren (vgl. Art. 112 SDÜ) - gespeichert werden.

Als Ausschreibungsgründe kommen in Betracht: die Festnahme mit dem Ziel der Auslieferung; eine Einreiseverweigerung gegenüber Drittausländer/-innen; die Aufenthaltsermittlung von Zeugen, Vermißten oder angeklagten Personen; die verdeckte Registrierung von Personen und Fahrzeugen, soweit konkrete Anhaltspunkte dafür vorliegen, daß z. B. außergewöhnlich schwere Straftaten geplant werden; Gegenstände, die zur Sicherstellung oder Beweissicherung in einem Strafverfahren benötigt werden.

Vorläufige Schätzungen gehen davon aus, daß Deutschland ca. 600 000 Datensätze über Personen in den gemeinsamen Fahndungsdatenbestand eingeben wird. Darüber hinaus werden sogenannte fahndungsbegleitende Daten zwischen den jeweiligen nationalen Zentralstellen („SIRENEN") ausgetauscht. Die deutsche SIRENE ist beim Bundeskriminalamt angesiedelt.

Als Korrektiv zur umfangreichen Verarbeitung von personenbezogenen Daten im SIS und bei den SIRENEN wurden in das SDÜ datenschutzrechtliche Bestimmungen aufgenommen. So sind zum Beispiel Ansprüche der Betroffenen auf Auskunft, Berichtigung, Löschung oder Schadensersatz geregelt. Darüber hinaus kann ein Betroffener seine Rechte in jedem Vertragsstaat seiner Wahl geltend machen. Die weiteren datenschutzrechtlichen Bestimmungen über die Verantwortung, die Richtigkeit und Aktualtität der im SIS gespeicherten Daten, Zweckbindung, Protokollierung der Abrufe und Datensicherung sind grundsätzlich den in der Bundesrepublik geltenden Vorschriften vergleichbar.

Die Anlieferung und die Weiterverwendung der Angaben durch die Beitrittsstaaten unterliegen dem jeweiligen nationalen Recht. Das hat zur Folge, daß die in Deutschland geltenden, strengen Weiterverarbeitungsregelungen bei einer Abgabe der Daten in das Ausland teilweise leerlaufen, da noch nicht alle Beitrittsstaaten einen vergleichbaren hohen Standard hinsichtlich der nationalen datenschutzrechtlichen Bestimmungen aufweisen.

Als Termin für das Inkraftsetzen des SDÜ ist für die Erstunterzeichnerstaaten Belgien, Deutschland, Frankreich, Luxemburg, Niederlande sowie für die Beitrittsstaaten Spanien und Portugal der 26. März 1995 vorgesehen. Zu diesem Termin soll auch das SIS für die abfrageberechtigten Behörden geöffnet und für betriebsbereit erklärt werden.

Die Errichtung eines *Europäischen Polizeiamtes (EUROPOL)* ist in einem Entwurf für ein Übereinkommen der EU-Staaten vorgesehen, dessen datenschutzrechtliche Aspekte im vergangenen Jahr beraten wurden.

In dem Entwurf werden EUROPOL Aufgaben, Befugnisse und Kompetenzen zugewiesen, die erhebliche Auswirkungen auf die Datenverarbeitung der Bundes- und Länderpolizeien haben werden.

EUROPOL soll die Befugnis erhalten,

- unabhängig von den Mitgliedstaaten Daten im Informationssystem zu speichern und hieraus abzurufen;
- in großem Umfang weitere Dateien zu führen, zu denen die Mitgliedstaaten keinen Zugang haben; diese wären jedoch verpflichtet, auf Ersuchen von EUROPOL Daten anzuliefern, die dann in den EUROPOL-Dateien gespeichert werden;
- regelmäßige Datenübermittlungen an Dritte nach eigenem Ermessen vorzunehmen; die vorherige Beteiligung der Mitgliedstaaten und ihrer Polizeibehörden ist in dem Entwurf nur in Ausnahmefällen vorgesehen;
- allein Auskünfte an Betroffene zu erteilen;
- Daten, die in den Mitgliedstaaten bereits gelöscht sind, weiter zu speichern.

Durch diese Regelungen erhält EUROPOL gegenüber den Mitgliedstaaten eine selbständige Position. Sie ist stärker als die, die das BKA gegenüber den Länderpolizeien selbst nach der weitesten Auslegung der Zentralstellenkompetenz beansprucht. Der zentralistische Ansatz des Entwurfs kommt insbesondere dadurch zum Ausdruck, daß die Zusammenarbeit zwischen den nach innerstaatlichem Recht zuständigen Polizeibehörden - in der Bundesrepublik Deutschland sind dies insbesondere die Länderpolizeien - und EUROPOL bei der nationalen Zentralstelle monopolisiert werden soll. Die Datenübermittlung zwischen den einzelnen Länderpolizeien und der nationalen Zentralstelle - für die Bundesrepublik Deutschland also dem BKA - wird ausschließlich im Interesse dieser Zentralstelle geschehen. Das BKA als nationale Zentralstelle wird durch das Übereinkommen verpflichtet, die für EUROPOL erforderlichen Informationen anzuliefern. Durch diese Verpflichtung erhält das BKA indirekt eine Befugnis gegenüber den Länderpolizeien zur Datenübermittlung. Ausschließlich das BKA darf gegenüber EUROPOL als berechtigter Teilnehmer des EUROPOL-Informationssystems fungieren.

Durch diese Bestimmungen werden wesentliche Bereiche der *Polizeihoheit der Bundesländer* tangiert. Maßgebliche Regelungen der Landespolizeigesetze, die die polizeiliche Datenverarbeitung betreffen, werden durch das EUROPOL-Übereinkommen ersetzt. Darüber hinaus besteht die Gefahr, daß eigene Befugnisse des BKA durch die von EUROPOL überlagert werden und das BKA dadurch nur noch eine unselbständige Funktion als Informationsschnittstelle zwischen den Länderpolizeien und EUROPOL hat.

Nach § 44 Abs. 3 ASOG ist die Berliner Polizei befugt, personenbezogene Daten an ausländische öffentliche Stellen zu übermitteln, soweit dies zur Erfüllung einer polizeilichen Aufgabe oder zur Abwehr einer erheblichen Gefahr für oder durch den Empfänger erforderlich ist. Dabei liegt die Verantwortlichkeit für die Daten bei der übermittelnden Polizeibehörde, also dem Polizeipräsidenten in Berlin. Nur dieser kann auf Grund der in Berlin vorliegenden Erkenntnisse und Unterlagen darüber entscheiden,

130 § 16 Abs. 3 ASOG

ob die gespeicherten Informationen vollständig und richtig sind, eine Löschung der gespeicherten Daten zu erfolgen hat oder ob eine Datenübermittlung erforderlich ist. Diese Verantwortlichkeit ist durch die Bestimmungen des Entwurfs für ein EUROPOL-Übereinkommen in Frage gestellt. Mit der Weitergabe der Daten an EUROPOL entwickeln diese ein Eigenleben, das von den Begehrlichkeiten und Handlungsmöglichkeiten der abfragenden Stellen bestimmt ist. Dadurch wird die Verantwortlichkeit der Polizeibehörde, die die Daten ursprünglich zur Gefahrenabwehr oder Strafverfolgung erhoben hat, unterlaufen.

An den Aufbau eines gemeinsamen Informationssystems im EUROPOL-Übereinkommen sind daher folgende Anforderungen zu stellen:

- Eine Speicherung von personenbezogenen Daten im Informationssystem von EUROPOL darf nur durch diejenige Stelle veranlaßt werden, die materiell für die dafür zugrundeliegende Aufgaben der Strafverfolgung oder Gefahrenabwehr zuständig ist.
- Die Verantwortlichkeit für die Eingabe in das Informationssystem von EUROPOL muß sich auch auf die daran anschließenden weiteren Verarbeitungsschritte - insbesondere die Berichtigung und Löschung der Daten - erstrecken. Kommt die für die Eingabe in das Informationssystem zuständige Behörde zu dem Ergebnis, daß eine Berichtigung oder Löschung der Daten erforderlich ist, muß sie diese auch direkt vornehmen können.
- EUROPOL darf keine Datenbestände aufbauen, die nicht im Zusammenhang mit Aufgaben der Strafverfolgung und Gefahrenabwehr stehen.
- Die Auskunftserteilung über Daten im Informationssystem von EUROPOL hat sich nach dem Recht des Mitgliedstaates zu richten, in dem der Auskunftsantrag gestellt wird. Der Rechtsweg zu den ordentlichen Gerichten der Mitgliedstaaten ist zu gewährleisten.

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen die verfassungsrechtliche Kompetenzverteilung in Bund und Ländern beachtet wird. Die Zuständigkeit und die Befugnisse des BKA als nationaler Stelle für den Informationsverkehr mit EUROPOL sollen unberührt bleiben. Weiterhin haben die Datenschutzbeauftragten darauf hingewiesen, daß die Regelungen zur Verarbeitung personenbezogener Daten präzise sein und der Verhältnismäßigkeit entsprechen müssen. Die vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen entsprechen diesen Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder trifft, z. B. durch eine Protokollerklärung zum EUROPOL-Übereinkommen.[131]

Datenübermittlung der Polizei an die Medien

Die Polizei gibt in Pressemeldungen oft sehr sensible Daten, z. B. über Verdächtige oder Opfer von Straftaten, an die Öffentlichkeit weiter. Dies ist datenschutzrechtlich als Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereiches zu qualifizieren. Nach § 13 BlnDSG ist eine derartige Datenübermittlung nur dann zulässig, wenn eine Rechtsvorschrift diese Übermittlung erlaubt oder der Betroffene darin eingewilligt hat.

§ 45 Abs. 1 ASOG kann bei rein *informativen Pressemeldungen* für die Übermittlung nicht als Rechtsgrundlage herangezogen werden, da diese nicht zur Erfüllung polizeilicher Aufgaben, zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer Person erforderlich sind.

Anders verhält es sich bei *Fahndungen* nach bekannten oder unbekannten Tatverdächtigen, bei der Suche nach Zeugen oder Vermißten oder der Identifizierung von unbekannten Toten. Zwar ist auch hierzu in der Strafprozeßordnung keine normenklare Rechtsgrundlage vorhanden. Die bestehende Gesetzeslücke kann jedoch mit Hilfe der Bestimmungen des ASOG geschlossen werden. Eine Übermittlung von personenbezogenen Daten an Stellen außerhalb des öffentlichen Bereiches ist so nach § 45 Abs. 1 Nr. 1 ASOG i. V. m. § 163 StPO zulässig, wenn dies zur Erfüllung von polizeilichen Aufgaben in strafrechtlichen Ermittlungsverfahren erforderlich ist. Hierzu gehört die Mithilfe von Publikationsorganen bei Fahndungsmaßnahmen.

Dem entsprechen auch die Bestimmungen der „Allgemeinen Verfügung über die Inanspruchnahme von Publikationsorganen zur Fahndung nach Personen bei der Strafverfolgung" der Senatsverwaltung für Justiz vom 11. November 1992. Nach Nr. I 2 Abs. 4 der Verfügung dürfen Publikationsorgane in der Regel allerdings nur dann in die Fahndung eingeschaltet werden, wenn andere, den Betroffenen weniger beeinträchtigende Fahndungsmittel nicht genügend erfolgversprechend erscheinen und die Inanspruchnahme der Fahndungshilfe nicht außer Verhältnis steht zu der Bedeutung der Sache und zu den zu erwartenden Rechtsfolgen der Tat. Gemäß Nr. I 3 der Verfügung entscheidet grundsätzlich der Staatsanwalt - in der Regel nach Anhörung der Polizei - über die Inanspruchnahme der Fahndungshilfe durch Publikationsorgane. Die Zustimmung der Staatsanwaltschaft ist lediglich bei Gefahr im Verzug entbehrlich.

In der Presse machte der Mord an einem Taxifahrer Schlagzeilen. Ein zunächst unter dringendem Tatverdacht festgenommener Beschuldigter wurde nur wenig später, nachdem die Ermittlungen in wesentlichen Punkten zu seiner Entlastung geführt hatten, aus der Untersuchungshaft entlassen. In der Berichterstattung zu diesem Fall war der Beschuldigte in einigen Zeitungen unter Nennung des Vor- und Zunamens und Abdruck seines Lichtbildes als „Taxi-Mörder" bezeichnet worden. Die personenbezogenen Daten des Beschuldigten waren der Presse in einer Polizeilichen Tagesmeldung übermittelt worden.

Der Polizeipräsident hat die Übermittlung mit einer Fahndungsmaßnahme begründet. Die Datenübermittlung sei nach Inkenntnissetzung der Staatsanwaltschaft erfolgt, weil ein weiterer Beschuldigter gesucht worden sei und dieser als ein möglicher Beteiligter des inhaftierten Beschuldigten nur über dessen Porträtveröffentlichung und volle Namensnennung hätte ermittelt werden können.

Die Tagesmeldung war nicht erforderlich. Sie enthielt für den Empfänger keine erkennbaren Hinweise, daß es sich um eine Bitte der Polizeibehörden um Hilfeleistung in einem Mordfall anläßlich einer Öffentlichkeitsfahndung handelt. In dem Text wurden nicht - wie sonst üblich - konkrete Fragen (Wer hat was wann wo bemerkt?) an die Öffentlichkeit gerichtet. Er gab ausschließlich den Sachverhalt wieder. Danach war die Übermittlung nicht erforderlich und damit unzulässig.

Den geschilderten sowie andere Fälle haben wir zum Anlaß genommen, die *Polizeilichen Tagesmeldungen* einer besonderen Prüfung zu unterziehen.

Polizeiliche Tagesmeldungen werden nach einer Auswertung der wichtigsten Ereignisse der letzten 24 Stunden vom Dezernat Lagedienst - Dauerdienst - des Polizeipräsidenten erstellt. Sie dienen der Information der Polizeiführung, der Fachaufsicht der Senatsverwaltung für Inneres und der Staatsanwaltschaft bei dem Landgericht Berlin. Ein Exemplar der jeweiligen Tagesmeldung, das um einen nicht für die Öffentlichkeit bestimmten Teil reduziert wird, erhält die Polizeipressestelle. In der Vergangenheit hat diese die Tagesmeldungen unverändert dem *Polizeilichen Pressedienst* beigefügt, der an alle interessieren Publikationsorgane versandt wird.

Nach einer Verfahrensänderung ist es nunmehr Praxis, daß die Pressestelle die Informationen aus den ihr übersandten Tagesmeldungen redaktionell überarbeitet und in einer eigenen Textfassung im Pressedienst an die Medien herausgibt. Dieses Verfahren realisiert ein gesteigertes Maß an redaktioneller Kontrolle bei der Weitergabe von Daten an Publikationsorgane.

131 Anlage 2.11

Allerdings blieb es dabei, daß im Regelfall der Vorname, der Anfangsbuchstabe des Familiennamens, Alter und Wohnbezirk bzw. -straße des Beschuldigten/Tatverdächtigen oder Zeugen/Opfers, zum Teil Berufsangaben sowie Angaben zu Hergang und Ort des Ereignisses im Polizeilichen Pressedienst veröffentlicht wurden.

Die Durchsicht von mehreren Ausgaben des Polizeilichen Pressedienstes hat ergeben, daß sich insbesondere durch die teilweise sehr ausführlichen Angaben über den Hergang und den Ort der Ereignisse im Zusammenhang mit den weiteren übermittelten Informationen Schlüsse auf die Identität der Betroffenen ziehen lassen.

Auf unsere Empfehlung hat nunmehr der Polizeipräsident angeordnet, daß Namenskürzel sowie nähere Angaben über die Wohnung der Betroffenen unterbleiben.

Polizei, Sport und Datenschutz

Im vergangenen Jahr haben wir bereits über die informationellen Maßnahmen der Polizei anläßlich der Olympiabewerbung Berlins berichtet.[132] Im Laufe der weiteren Überprüfung stellten wir fest, daß Daten über 101 Personen auch in der „Arbeitsdatei PIOS Innere Sicherheit" (APIS) im Rahmen von INPOL gespeichert und damit potentiell an alle Polizeibehörden des Bundes und der Länder übermittelt wurden.

Nach § 42 Abs. 1 Satz 1 ASOG darf die Polizei zur Strafverfolgung erhobene personenbezogene Daten nur speichern, soweit dies hierfür erforderlich ist. Nach Abschluß des jeweiligen Ermittlungsverfahrens sind die Daten grundsätzlich zu löschen. Eine weitere Speicherung dieser Daten zur Gefahrenabwehr, einschließlich der vorbeugenden Straftatenbekämpfung, ist nach § 42 Abs. 3 ASOG nur zulässig, soweit dies für diesen weitergehenden Zweck benötigt wird. Auch die Übermittlung der Daten an Polizeibehörden eines anderen Landes oder des Bundes ist nur zulässig, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich ist (§ 44 Abs. 1 Satz 2 ASOG).

Als Maßstab für die Erforderlichkeit der Verarbeitung von Daten in APIS können die „Richtlinien für den kriminalpolizeilichen Meldedienst in Staatsschutzsachen" (KPMD-S) von 1987 und die Errichtungsanordnung zu APIS von 1993 herangezogen werden. Danach dürfen Daten nur dann in APIS gespeichert werden, wenn die Straftat dem Katalog der Staatsschutzdelikte zugeordnet werden kann oder wenn bei anderen Straftaten wegen der Angriffsrichtung, des Motivs des Täters oder dessen Verbindung zu einer Organisation der Verdacht besteht, daß mit der Tat Ziele i. S. d. Nr. 1 der Richtlinien KPMD-S verfolgt werden. Dort werden Straftaten genannt, „die gegen die freiheitlich demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder eines Landes gerichtet sind oder die eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes oder eines Landes zum Ziele haben ...".

Ein großer Teil (39 Fälle) der in der APIS-Anwendung „Olympia 2000" gespeicherten personenbezogenen Daten stand im Zusammenhang mit politisch motivierter Kleinkriminalität. Den Beschuldigten wurden Sachbeschädigungen (z. B. Farbschmierereien, Abreißen oder Ankleben von Plakaten), Beleidigungen (z. B. das In-die-Höhe-Strecken des rechten Armes und des Mittelfingers gegen Polizeibeamte, wobei der Beschuldigte unter Einfluß von Alkohol [2,00 ‰] stand), Diebstähle (z. B. von Fahnen oder Aufklebern) und Hausfriedensbruch vorgeworfen.

Bereits im Jahresbericht von 1987[133] haben wir darauf hingewiesen, daß die Erstreckung eines technischen Instrumentariums wie APIS, das speziell zur Bekämpfung des Terrorismus entwickelt worden ist, auf die politisch motivierte Kleinkriminalität problematisch ist.

Die Eingabe von personenbezogenen Daten in APIS ermöglicht deren Übermittlung an das Bundeskriminalamt und eine Vielzahl von anderen Landespolizeibehörden. Eine derartige Datenübermittlung ist nur im erforderlichen Umfang zulässig. Für Daten über Sachbeschädigungen wegen Farbschmiererei, Abreißen von Plakaten oder anderer vergleichbarer Kleinkriminalität ist dies nicht ersichtlich, da diese Straftaten in der Regel keine überörtliche, sondern nur eine regionale Bedeutung haben. Auf Grund der breitgestreuten Übermittlung der Daten an eine Vielzahl von Empfängern sowie der stigmatisierenden Wirkung, die mit einer Datenspeicherung in APIS verbunden ist - der Beschuldigte wird verdächtigt, ein Staatsfeind/Terrorist zu sein -, ist die Erstreckung von APIS auf den Bereich der Bagatelldelikte zudem als unverhältnismäßig anzusehen.

Auch die anderen Datensätze konnten nicht dem Bereich der Schwerkriminalität zugeordnet werden. Bei Verstößen gegen das Versammlungsgesetz handelt es sich um Handlungen, wie sie bei einer Vielzahl von Demonstrationen zu beobachten sind (Verstoß gegen das Vermummungsgebot, Mitführen von als gefährlich eingestuften Gegenständen wie z. B. nietenbesetzte Armbänder oder Schienbeinschützer). Vorwürfe wegen Widerstands gegen Vollstreckungsbeamte standen im Zusammenhang mit dem Widerstand der Betroffenen anläßlich ihrer Festnahme durch Polizeibeamte im Rahmen ungenehmigter Demonstrationen gegen „Olympia 2000". Ebensowenig konnten die Tatvorwürfe dem Katalog der Staatsschutzdelikte (vgl. Nr. 2.1.1 bis Nr. 2.1.9 der Richtlinien KPMD-S) zugeordnet werden. Anhaltspunkte dafür, daß sich die den Beschuldigten vorgeworfenen Handlungen gegen die freiheitlich demokratische Grundordnung richten, lagen nicht vor.

Insgesamt betrachtet war die Nutzung von APIS in diesem Bereich nicht zulässig.

Über die US-Botschaft war das FBI an deutsche Behörden mit dem Ersuchen herangetreten, den USA zur Vorbereitung der Fußballweltmeisterschaft 1994 personenbezogene Erkenntnisse über Fußballrowdies zu übermitteln.

Die Informationen sollten in standardisierter Form übermittelt werden. Für jede Person sollte ein eigenes Blatt angelegt werden, und die Personen sollten einer der folgenden Kategorien zugeordnet werden:

- Personen, die dafür bekannt sind, zu anlaßbezogenen Gewaltdelikten anzustiften und/oder Delikte der allgemeinen Kriminalität zu begehen (Hooligans);
- Personen, die im Verdacht stehen, anlaßbezogene Straftaten zu begehen;
- Einzelpersonen, Gruppen oder Cliquen, die dafür bekannt sind, daß sie bei der Begehung anlaßbezogener Gewaltdelikte oder bei der Begehung von Delikten der allgemeinen Kriminalität zusammenwirken oder diese heimlich planen und ausführen;
- andere Personen von Interesse für die Sicherheitsbehörden.

Darüber hinaus sollten ein aktuelles Foto, sämtliche Namen - auch Alias -, Geburtsdatum, Anschrift, Telefonnummer, Rasse, Größe, Gewicht, Haarfarbe, Augenfarbe, besondere Merkmale (Narben oder Tätowierungen), Paßnummer (ausstellendes Land, ausstellende Behörde), allgemeine polizeiliche Erkenntnisse bzw. Verurteilungen, Steckbriefe und Vollstreckungsbefehle, anlaßbezogene Erkenntnisse zur Person, Ansprechpartner ausländischer Polizeibehörden, zusätzliche Informationen (z. B. Mittäter, benutzte Fahrzeuge), personengebundene Hinweise („Bewaffnet" und „Gefährlich") übermittelt werden.

Die Übermittlung von personenbezogenen Daten an ausländische öffentliche Stellen ist nach § 44 Abs. 3 Nr. 1 und 2 ASOG zulässig, wenn dies zur Erfüllung einer Aufgabe der Berliner Polizei oder zur Abwehr einer erheblichen und konkreten Gefahr für oder durch den Empfänger der Daten erforderlich ist.

Die vom FBI erbetene Übermittlung von Daten über Fußballrowdies erfüllt die genannten Tatbestandsvoraussetzungen nicht. Die Datenübermittlung war nicht zur Erfüllung einer der Berliner Polizei zugewiesenen Aufgabe erforderlich. Sie war auch nicht erforderlich, um in den USA eine erhebliche und konkrete Gefahr abzuwenden, sie sollte vielmehr der allgemeinen Gefahrenvorsorge dienen. Konkrete Erkenntnisse oder Anhaltspunkte über geplante Ausschreitungen im Zusammenhang mit der Fußballweltmeisterschaft wurden von den US-Behörden nicht vorgetragen.

132 Jahresbericht 1993, 4.5.1
133 Drs 10/1883, 23

Eine Berechtigung oder Verpflichtung der Berliner Polizei, die vom FBI erbetenen Daten zu übermitteln, konnte auch nicht aus einer über- oder zwischenstaatlichen Vereinbarung zwischen den USA und der Bundesrepublik Deutschland abgeleitet werden.

Die erbetene Übermittlung der Daten durch die Berliner Polizei wäre danach unzulässig gewesen. Das Ersuchen wurde abschlägig beschieden.

4.6.2 Meldewesen

Falsche Daten für die Kirchensteuer

Ein konfessionsloser Bürger aus Pankow fand auf seiner Lohnsteuerkarte 1992 den Eintrag vor, daß er Mitglied der Evangelischen Kirche sei. Er vermutete eine absichtliche Datenmanipulation mit dem Ziel, der Kirche ungerechtfertigte Steuereinnahmen zukommen zu lassen.

Der Bürger empörte sich weniger über die versehentliche Falscherfassung seiner Daten, wie sie leider immer mal vorkommen kann, weil Menschen Fehler machen, sondern vielmehr über die Schwierigkeiten, die es machte, das Datum, das 1991 noch korrekt auf der Lohnsteuerkarte seine Nichtangehörigkeit zu einer Kirche verzeichnete, wieder korrigieren zu lassen. Das zuständige Bezirkseinwohneramt verwies auf die Kirchensteuerstelle der Evangelischen Kirche und forderte von dem Bürger, der in jungen Jahren aus der Katholischen Kirche ausgetreten war, die Vorlage einer Austrittserklärung aus der Evangelischen Kirche. Hilfsweise wurde dem Finanzamt die Verantwortung für die Eintragung in die Lohnsteuerkarte zugeordnet.

Die Kirchensteuerstelle verwies auf die Schuld des Einwohneramtes, das Büro des Bischofs auf die des Finanzamtes, da andererseits evangelische Pfarrer Lohnsteuerkarten erhalten hatten, die sie als Nichtmitglieder ihrer Kirche auswiesen. Das Finanzamt sah die Verantwortung bei der Kirchensteuerstelle, diese beim Landeseinwohneramt.

Die Verwirrung des Bürgers wurde dadurch nicht geringer, daß nach der deutschen Vereinigung im Herbst 1990 eine Erhebung seiner Lohnsteuermerkmale einschließlich der Kirchensteuermerkmale bei ihm selbst erfolgt war, so daß er annehmen durfte, daß die von ihm selbst angegebenen Daten dem Staat glaubhaft genug waren, um damit weiter zu arbeiten.

Was war geschehen? Für die Lohnsteuerkarten 1991 waren die Kirchensteuermerkmale der Ost-Berliner Bürger bei diesen selbst erhoben worden, weil entsprechende Daten in den von der DDR übernommenen Meldedaten nicht enthalten waren. Diese Vorgehensweise entsprach dem datenschutzrechtlichen Gebot, daß der Staat Daten bei den Bürgern grundsätzlich selbst zu erheben hat, nicht aber hinter ihrem Rücken; Ausnahmen bedürfen einer gesetzlichen Ermächtigung. Die so erhobenen Daten wurden mit Personalcomputern erfaßt, da ein On-line-Zugriff auf das ADV-Verfahren Einwohnerwesen (EWW) noch nicht möglich war. Diese auf Disketten gespeicherten Daten wurden zur Vorbereitung des Drucks der Lohnsteuerkarten 1992 in das EWW-Verfahren eingelesen.

Inzwischen hatten aber auch die Kirchen ihre Mitgliederdaten an das Landeseinwohneramt auf Datenträgern übermittelt. Eine Woche nach dem Einlesen der beim Bürger erhobenen Daten wurden diese durch die von den Kirchen übermittelten Daten überschrieben. Abweichungen von den Angaben der Bürger wurden ignoriert, Rückfragen beim Bürger gab es nicht. Die Senatsverwaltung für Inneres hatte die Bezirkseinwohnerämter darauf hingewiesen, daß grundsätzlich die Angaben der Kirchen als zutreffend anzusehen seien - offensichtlich in vielen Fällen ein Irrtum, wie die in diesem Fall betroffene Evangelische Kirche später auch einräumte. In einigen Fällen wurden alle Familienangehörigen als evangelisch geführt, sofern nur ein Familienmitglied evangelisch war. In Beschwerdefällen über falsche Daten sei der Bürger auf die Kirchensteuerstellen und die Religionsgesellschaften selbst zu verweisen. Dabei übersah die Senatsverwaltung für Inneres, daß das Landeseinwohneramt nach der pauschalen Übernahme der Daten für die Richtigkeit selbst datenschutzrechtlich verantwortlich war.

Nach Auffassung der Senatsverwaltung für Inneres war das Landeseinwohneramt zu der Datenübernahme berechtigt, weil die Erhebung durch die Herstellung der deutschen Einheit erforderlich gewesen sei und somit die übliche Datenerhebung durch An- und Abmeldung nicht habe erfolgen können, die Meldebehörde jedoch zu einer Berichtigung oder Fortschreibung des Melderegisters verpflichtet sei. Die Erfassung beim Bürger selbst wurde als nicht ausreichend erklärt, weil angenommen wurde, daß viele Bürger des Beitrittsgebietes sich über ihre Mitgliedschaften in den Kirchen nicht im klaren wären und darüber hinaus unterstellt wurde, daß viele sich durch Falschangaben der Kirchensteuer entziehen wollten.

So geschah es dann umgekehrt: Die Kirchen übermittelten Daten, in denen Nichtmitglieder als Mitglieder enthalten waren, und es wurde den Betroffenen überlassen, sich um die Korrektur dieser Daten zu kümmern, wenn man ungerechtfertigte Kirchensteuern vermeiden wollte.

Dieses Verfahren wurde als Verstoß gegen §§ 6 und 11 BlnDSG beanstandet, denn zumindest hätten die Betroffenen bei Abweichungen gehört werden müssen. Wir empfahlen, die Betroffenen, deren Angaben geändert wurden, in analoger Anwendung von § 17 Abs. 1 Satz 2 BlnDSG wenigstens im nachhinein zu hören. Dazu wurde erklärt, dies sei nicht mehr möglich, da das Bandmaterial der Kirchen bereits gelöscht worden sei und eine Auswertung des Einwohnerdatenbestandes mangels geeigneter Deskriptoren nicht möglich sei.

Da das Landeseinwohneramt jedoch gemäß § 5 Abs. 3 Nr. 7 BlnDSG bei der Umsetzung technisch-organisatorischer Maßnahmen zur Eingabekontrolle verpflichtet ist und somit zu gewährleisten hat, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind, sind wir dieser Aussage nachgegangen. Es stellte sich heraus, daß im Landesamt für Informationstechnik das Protokollband noch vorliegen müßte, das die im August 1991 vorgenommene Überschreibung der Kirchensteuermerkmale durch die Kirchendaten mit den Daten vor und nach der Änderung dokumentiert. Es hätte also nur geeigneter Auswertungsprogramme einfacher Struktur bedurft, um festzustellen, bei welchen Personen bei dem präzise benennbaren Vorgang die Daten tatsächlich verändert worden sind.

Keine Sperre für öffentliche Stellen

Eine mit einem Ausländer verheiratete Mutter kehrte mit ihren Kindern nach Deutschland zurück. Weil sie damit rechnen mußte, daß eine frühere Lebensgefährtin ihres Ehemannes aus Eifersucht ihre Privatsphäre stört, stellte sie bei der Meldebehörde einen Antrag auf Auskunftssperre, dem stattgegeben wurde. Seitdem ist zwar jede Melderegisterauskunft an Private - also auch die ehemalige Lebensgefährtin des Ehemannes - unzulässig. Die Nebenbuhlerin erinnerte sich jedoch an ihren früheren Arbeitgeber - eine öffentliche Stelle - und an eine ehemalige Kollegin. Diese führte aus Gefälligkeit auf dem Kopfbogen der öffentlichen Stelle eine Melderegisteranfrage durch und gab die Anschrift weiter.

Der Fall zeigt ein Problem des Melderechts, das häufig übersehen wird: Die Sperre im Melderegister, die jedermann beantragen kann, der sich durch eine Melderegisterauskunft gefährdet glaubt, wirkt nicht gegenüber öffentlichen Stellen. Hier stand die Sperre also einer Datenübermittlung nicht entgegen.

Der Meldebehörde kann damit kein Vorwurf gemacht werden. Sie mußte davon ausgehen, daß die Meldedaten zur ordnungsgemäßen Aufgabenerfüllung der anfragenden Stelle erforderlich waren. Für Zweifel bestand bei der Form der Anfrage kein Anlaß.

Auf seiten der öffentlichen Stelle liegt dagegen ein datenschutzrechtlicher Mangel vor, da die Erhebung personenbezogener Daten nur zulässig ist, wenn sie zur rechtmäßigen Erfüllung der durch Gesetz der datenverarbeitenden Stelle zugewiesenen Aufgabe und für den jeweils damit verbundenen Zweck erforderlich ist. Im vorliegenden Fall wurden die Daten der Petentin dagegen ausschließlich zu privaten Zwecken abgefragt.

Natürlich liegt auch ein Verstoß gegen § 8 BlnDSG (Datengeheimnis) vor. Danach ist es den Dienstkräften öffentlicher Stellen untersagt, personenbezogene Daten unbefugt zu verarbeiten.

Kein Computer - mehr Daten

Ein Bürger, der sich für eine Wohnung im Ostteil der Stadt angemeldet hat, beschwerte sich darüber, daß die Mitarbeiter der Meldestelle auf dem Anmeldeformular trotz energischen Widerspruchs seine Personalausweisnummer festgehalten haben.

Die Meldebehörde begründet dies damit, daß bei Anmeldungen bei Meldestellen im Ostteil der Stadt, die noch nicht mit ADV ausgestattet sind, sowohl das Melderegister als auch das Personalausweisregister zentral fortgeschrieben werden. Nur in solchen Fällen werde die Personalausweisnummer im Meldeschein eingetragen. Dies erfolge nicht im Rahmen des Melde-, sondern des Ausweisrechts und diene der Überprüfung des Ausweisregisters. In der Übergangszeit bis zur vollständigen Installation der ADV im Ostteil der Stadt müsse die Personalausweisnummer auf der Anmeldung notiert werden, um erheblichen Arbeitsaufwand zu vermeiden. Der Eintrag der Personalausweisnummer auf dem Meldeschein sei keine dem Personalausweisgesetz widersprechende Nutzung. Die Ausweisnummer werde von demselben Mitarbeiter, der die Meldeangelegenheiten bearbeitet, ausschließlich für das Personalausweisregister genutzt. Übermittlungen an andere Stellen seien nicht beabsichtigt.

Nach § 14 Meldegesetz hat der Betroffene auf Verlangen der Meldebehörde die Auskünfte zu erteilen, die für die ordnungsgemäße Führung des Melderegisters benötigt werden, und die zum Nachweis der Angaben erforderlichen Unterlagen vorzulegen. Die Speicherung der Personalausweisnummer ist für den melderechtlichen Vorgang der Ummeldung nicht erforderlich und nach § 12 i. V. m. § 2 Abs. 1 Nr. 16 Meldegesetz damit nicht zulässig.

Inzwischen verwendet die Meldebehörde ein gesondertes Formular, auf dem die Personalausweisnummer festgehalten wird.

Davon unabhängig ist die Verpflichtung nach § 6 Abs. 1 Nr. 5 Landespersonalausweisgesetz, der *Ausweisbehörde* bei der Änderung der Wohnanschrift den Ausweis vorzulegen. Diese Vorlagepflicht dient dem Zweck, die Anschrift im Ausweis zu berichtigen, nicht aber dazu, daß die Meldebehörde über den zulässigerweise gespeicherten Umfang an Meldedaten melderechtsfremde Ausweisdaten festhält.

Geburtsland im Personalausweis

Ein Bürger wurde aus der iranischen Staatsbürgerschaft entlassen und als Deutscher eingebürgert. Mit seiner Einbürgerung hat er einen deutschen Personalausweis erhalten, der neben Datum und Ort der Geburt auch die Angabe seines Geburtslandes Iran enthält. Der Petent fühlt sich dadurch diffamiert.

Rechtsgrundlage für die Speicherung personenbezogener Daten im Personalausweis ist § 1 Abs. 2 Satz 2 PAuswG. Neben dem Lichtbild des Ausweisinhabers sind danach u. a. Angaben zum Tag und Ort der Geburt im Personalausweis zu vermerken (§ 1 Abs. 2 Satz 2 Nr. 5 PAuswG). Form, Art und Umfang dieser Angaben sind den Bestimmungen des PAuswG nicht zu entnehmen. Bundeseinheitliche Verwaltungsvorschriften, die diesen Bereich konkretisieren, existieren - im Gegensatz zu Pässen - für Personalausweise nicht. Auch das Landespersonalausweisgesetz Berlin enthält keine Regelungen darüber. Hinweise sind jedoch dem Erlaß über behelfsmäßige Personalausweise (Personalausweiserlaß) vom 8. März 1988 zu entnehmen, der nach wie vor gilt.

Dort ist festgelegt, daß der Geburtsort im Personalausweis genau - gegebenenfalls unter Angabe des Kreises oder Landes oder eines der geographischen Bestimmung dienenden Zusatzes - zu bezeichnen ist. Bei Geburtsorten im Ausland ist auch der Staat anzugeben, wenn dies zur Klarstellung erforderlich ist.

Danach sind Angaben im Personalausweis zum Geburtsland grundsätzlich zulässig. Sie werden z. B. auch bei Deutschen, die im Ausland geboren sind, vermerkt. Eine spezielle Diffamierung eines Ausweisinhabers allein durch diesen Zusatz kann darin demnach nicht gesehen werden.

Es ist jedoch denkbar, daß persönliche Gründe (z. B. Zwangsausbürgerung) den Betroffenen veranlassen, jeglichen Hinweis auf sein Geburtsland im Ausweis abzulehnen.

Eine Nachfrage bei der Senatsverwaltung für Inneres, ob in begründeten Einzelfällen von der genannten Praxis abgesehen werde, ergab, daß derartige Anträge regelmäßig abgelehnt werden, da dem Ausweisinhaber durch den Zusatz beim Geburtsort keine rechtlichen Nachteile entstehen könnten. Subjektive Vorstellungen, Befürchtungen oder Ängste könnten keine Berücksichtigung finden. Das Verwaltungsgericht habe dies in mehreren Entscheidungen ebenso gesehen.

Für die Personenstandsbehörden, für die entsprechende Regelungen gelten, ist dies verständlich: Der Schriftverkehr mit dem Standesamt des Geburtsortes wird durch eine derartige Angabe erleichtert. Für den Personalausweis, bei dem der Geburtsort lediglich der zusätzlichen Individualisierung dient, ist der Sinn nicht ohne weiteres einsichtig. Die Übernahme der Bestimmung für die Standesbeamten ist wohl eher der Ausfluß eines gewissen Perfektionierungsdranges.

Allerdings läßt auch die Formulierung „wenn dies zur Klarstellung erforderlich ist" einen gewissen Ermessensspielraum. Sie bedeutet praktisch, daß die Mitarbeiter in den Meldestellen selbst entscheiden, ob der Geburtsstaat aufgenommen wird. Dies heißt überspitzt, daß es auf die geographischen Kenntnisse der Bediensteten ankommt. Dieser Spielraum kann dazu genutzt werden, subjektiv empfundenen Beeinträchtigungen bei der Angabe des Geburtslandes entgegenzuwirken.

Vor dem Hintergrund dieser Überlegungen haben wir empfohlen, daß bei Personen, die sich durch die Angabe ihres Geburtslandes diskriminiert fühlen, hierauf verzichtet wird. Die Senatsverwaltung für Inneres hat unsere Empfehlung zum Anlaß einer bundesweiten Abstimmung genommen.

4.6.3 Ausländerwesen

Ausländerzentralregistergesetz

Am 1. Oktober 1994 ist das Gesetz über das Ausländerzentralregister (AZR-Gesetz) vom 2. September 1994 in Kraft getreten.[134] Damit wurde für das bereits seit 40 Jahren beim Bundesverwaltungsamt in Köln geführte Ausländerzentralregister endlich eine Rechtsgrundlage geschaffen. Die Datenschutzbeauftragten des Bundes und der Länder haben in der Vergangenheit mehrfach darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist.[135]

Inhaltlich bestehen gegen das AZR-Gesetz allerdings aus datenschutzrechtlicher Sicht erhebliche Bedenken. Diese haben die Datenschutzbeauftragten des Bundes und der Länder veranlaßt, in einem Beschluß darauf hinzuweisen, daß das Ausländerzentralregister zukünftig nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.[136]

Diese Funktionserweiterung ergibt sich daraus, daß Erkenntnisse der Sicherheitsbehörden mit Bezug zu Ausländern in das Register eingespeichert werden.

So ist es künftig zulässig, daß der *INPOL-Fahndungsbestand* des Bundeskriminalamtes - soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält - in das Ausländerzentralregister übernommen wird (§ 2 Abs. 2 Nr. 6 AZR-Gesetz). Diese Doppelspeicherung ist überflüssig. Die Polizei hat die erforderlichen Daten bereits im INPOL-System erfaßt und damit jederzeit Zugriff auf diese Daten. Darüber hinaus steht diese Regelung im Widerspruch zum BKA-Gesetzentwurf, da die dort vorgesehenen Zugriffsbeschränkungen auf den polizeilichen Fahndungsdatenbestand aufgehoben werden.

134 BGBl. I, 2265
135 Jahresbericht 1991, 3.4.3
136 vgl. Anlage 2.6

Eine weitere bedenkliche *Funktionserweiterung* des Ausländerzentralregisters ergibt sich daraus, daß Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehen, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben, gespeichert werden dürfen (§ 2 Abs. 2 Nr. 7 AZR-Gesetz). Diese Informationen dienen nicht ausländerbehördlichen Aufgaben, sondern dem Zweck der Kriminalitätsbekämpfung. Zur Verfolgung und vorbeugenden Bekämpfung von Straftaten sind diese Angaben jedoch bereits im INPOL-System, für Drittländer im Schengener Informationssystem und bei Staatsschutzdelikten im NADIS gespeichert. Eine zusätzliche Speicherung im Ausländerzentralregister ist daher überflüssig und eine weitere Umgehung der bereichsspezifischen Regelungen für die Strafverfolgungsbehörden und den Verfassungsschutz.

Die im AZR-Gesetz vorgesehenen Voraussetzungen, unter denen für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste *automatisierte Abrufverfahren* eingerichtet werden können, stellen keine wirksame Vorkehrung für die erforderliche Begrenzung der Abrufe dar.[137] Besonders problematisch ist der automatisierte Zugriff durch die Nachrichtendienste auf einen - wenn auch reduzierten - Datensatz. Die Erforderlichkeit derartiger Abrufe durch die Dienste ist in keiner Weise belegt. Die Datenschutzbeauftragten haben sich daher dafür ausgesprochen,[138] zumindest auf den automatisierten Abruf von Daten aus dem Ausländerzentralregister durch die Nachrichtendienste zu verzichten.

Ausländergesetz

Obwohl das Ausländergesetz (AuslG) bereits seit mehreren Jahren in Kraft ist, liegen die bereits mehrfach angekündigten bundeseinheitlichen *Verwaltungsvorschriften zur Durchführung der dort vorgesehenen Übermittlungsvorschriften* immer noch nicht vor. Wir haben in den vergangenen Jahresberichten bereits mehrfach gefordert, daß für die Übergangszeit Verwaltungsvorschriften für Berlin in Kraft gesetzt werden.[139]

Das Abgeordnetenhaus hat nunmehr den Senat mit Beschluß vom 23. Juni 1994 aufgefordert, die im Sommer 1991 im Zusammenwirken mehrerer Senatsverwaltungen, der Ausländerbeauftragten und des Datenschutzbeauftragten erarbeiteten Anwendungshinweise zu den §§ 75, 76 und 77 AuslG in Kraft zu setzen. Diesem Beschluß ist die Senatsverwaltung für Inneres nachgekommen, indem sie die betroffenen Behörden gebeten hat, diese Hinweise als verbindliche Vorabregelung zu behandeln, die erst mit dem Erlaß der Allgemeinen Verwaltungsvorschriften zum Ausländergesetz auf Bundesebene hinfällig werden.

Erkennungsdienstliche Behandlung von Bürgerkriegsflüchtlingen

Presseberichten entnahmen wir, daß beabsichtigt sei, alle Bürgerkriegsflüchtlinge aus dem ehemaligen Jugoslawien erkennungsdienstlich zu behandeln, denen eine Duldung erteilt werden soll und die ein bosnisches Identitätspapier vorlegen. Die erkennungsdienstliche Behandlung dieses „abgrenzbaren Personenkreises" sei gerechtfertigt wegen genereller Zweifel an der Identität des Antragstellers und vor dem Hintergrund, daß den bosnischen Behörden 16 000 Paß- und Ausweisformulare nebst Stempeln abhanden gekommen seien sowie daß in den letzten Monaten in Berlin über 500 Ermittlungsverfahren wegen Totalfälschung oder Verfälschung bosnischer Legitimationspapiere oder wegen Benutzung der entwendeten bosnischen Paß-Blankette eingeleitet werden mußten.

Vor einer Gesetzesänderung, zu der die Bundesregierung von der Innenministerkonferenz am 6. Mai 1994 aufgefordert worden ist, ist eine erkennungsdienstliche Maßnahme gegen Ausländer nur unter den Voraussetzungen der §§ 41 Abs. 1 Nr. 2 i. V. m. 41 Abs. 2 AuslG zulässig. Danach kann - wenn eine Duldung erteilt werden soll - diese nur zur Feststellung seiner Identität durchgeführt werden, wenn im Einzelfall Zweifel an der Person des Ausländers bestehen.

Erkennungsdienstliche Maßnahmen können in erheblichem Maß in das allgemeine Persönlichkeitsrecht und die körperliche Unversehrtheit des Betroffenen eingreifen. Insofern müssen strenge Anforderungen auch an die Notwendigkeit derartiger Eingriffe gestellt werden. Bei jedem einzelnen Betroffenen, der nach § 41 AuslG einer erkennungsdienstlichen Behandlung unterzogen werden soll, ist somit konkret festzustellen, auf Grund welcher Tatsachen Zweifel daran bestehen, daß die vom Betroffenen angegebenen Personalien zutreffen. Eine pauschale erkennungsdienstliche Behandlung aller bosnischen Flüchtlinge - ohne Berücksichtigung des Einzelfalls - widerspricht damit dieser Bestimmung.

Bereits im Jahresbericht 1991[140] haben wir gegen die Praxis, Asylbewerber aus bestimmten Herkunftsländern generell erkennungsdienstlich zu behandeln, erhebliche Bedenken geäußert. Diese Bedenken lassen sich auf den vorliegenden Fall übertragen. Auch der Umstand, daß es sich hier um einen „abgrenzbaren Personenkreis" handelt und Hinweise auf einen verstärkten Mißbrauch von Paß- und Ausweisformularen vorliegen, die ein erhöhtes Mißtrauen hinsichtlich der Angaben zur Identität der Betroffenen rechtfertigen, macht eine Prüfung der Erforderlichkeit von erkennungsdienstlichen Maßnahmen in jedem Einzelfall nicht entbehrlich.

Die Senatsverwaltung für Inneres hält demgegenüber ihr Vorhaben angesichts der konkreten Anhaltspunkte für massenhafte Fälschungen und damit mißbräuchliche Nutzung sowohl des Aufenthaltsrechts als auch der entsprechenden Sozialleistungen für gerechtfertigt. Über das endgültige Vorgehen ist noch nicht entschieden.

4.6.4 Statistik

Europäische Statistik - Datenschutz mangelhaft

Die Europäische Kommission hat einen Vorschlag über eine EG-Statistikverordnung vorgelegt. Die datenschutzrechtliche Entwicklung bei der EU hat mit dem Aufbau der Europäischen Statistik keineswegs Schritt gehalten. So werden nationale datenschutzrechtliche Grundsätze und Standards des Statistikrechts weitgehend nicht berücksichtigt. Die Datenschutzbeauftragten des Bundes und der Länder unterstützten nachdrücklich einen Beschluß des Bundesrates,[141] der diese Mängel bloßlegt, und fordern, daß die Bundesregierung entsprechende Bedenken gegen diesen Vorschlag geltend macht.

Insbesondere ist eine selbständige und unabhängige Stellung des Statistischen Amtes der Europäischen Gemeinschaften (EUROSTAT) nicht gewährleistet. Nur eine solche Stellung kann die für die amtliche Statistik unabdingbaren Grundsätze von Objektivität und Neutralität sichern. In dem Vorschlag ist vorgesehen, daß das statistische Programm von der Kommission beschlossen wird. Grundlegende Entscheidungen über die Bürger belastende Datenerhebungen sollten jedoch dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Auch wird eine generelle Befugnis der Kommission, statistische Einzelmaßnahmen einschließlich der Verpflichtung, vorhandene Daten an EUROSTAT zu übermitteln, als zu weit gehend kritisiert. Dem Grundsatz der Subsidiarität widerspricht die vorgesehene Übertragung der Befugnis zur Organisation der Verarbeitung der statistischen Daten auf die Kommission. Grundsätzlich sollten nach Auffassung der Datenschutzbeauftragten die Mitgliedstaaten nach ihrem nationalen Recht zur Verarbeitung der statistischen Daten zuständig sein.

Die Möglichkeit der Übermittlung vertraulicher statistischer Daten an Stellen außerhalb des Statistischen Amtes der EG widerspricht dem Gebot der Abschottung. Nicht hinreichend klar ist die Abgrenzung vertraulicher und nicht vertraulicher Daten. Des weiteren fehlt eine Regelung zur Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen sowie der alsbaldigen Löschung personenbezogener Hilfsmerkmale, wie sie in der Bundesrepublik Deutschland zum Kernbereich des Statistikrechts gehört. Sieht man diese Mängel in Zusammenhang mit nach wie vor fehlenden unabhängigen und effektiven Datenschutzkontrollinstanzen für die Organe der Europäischen Union,

137 s. o. 3.2
138 vgl. Anlage 2.6.
139 Jahresbericht 1992, 4.2.5; Jahresbericht 1991, 3.4.3

140 Jahresbericht 1991, 3.4.3, zur ED-Behandlung von Asylbewerbern
141 BR-Drs 283/94; vgl. Anlage

wird die Problematik noch deutlicher. Einerseits sieht sich die deutsche Statistik auch im Interesse ihrer eigenen Akzeptanz beim Bürger im Land erheblichen datenschutzrechtlichen Schranken und Begrenzungen gegenüber, andererseits sollen diese Schranken auf der Ebene der Europäischen Union für faktisch gleiche Datenbestände weitgehend außer Kraft gesetzt werden.

Prüfung des Statistischen Landesamtes

Eine Kontrolle der technischen und organisatorischen Maßnahmen bei Personalcomputern sowie der eingesetzten Netz- und Großrechnertechnik im Statistischen Landesamt führte zu recht unterschiedlichen Ergebnissen. Während die Maßnahmen zum Datenschutz bei dem Einsatz der Personalcomputer unzureichend waren, fiel die Bewertung bei Großrechner- und Netztechnik besser aus.

Obwohl die Historie im Statistischen Landesamt eine wichtige Rolle zu spielen scheint („das haben wir schon immer so gemacht"), erfordert der Einsatz moderner Rechner- und Kommunikationstechnologie auch moderne technische und organisatorische Schutzmechanismen.

Insbesondere benötigen vernetzte *Einzelplatzrechner* verstärkte *Sicherheitsmechanismen*. Im Statistischen Landesamt wurde nur auf einem Teil der PCs eine Datenschutzsoftware vorgefunden. Die Installation war dabei nur mangelhaft durchgeführt worden, so daß die wesentlichen Schutzmechanismen nicht installiert oder aktiviert waren. So war auf allen PCs für die Anwender ein ungehinderter Betriebssystemzugang oder der Zugang zum Diskettenlaufwerk möglich.

Auf keinem der PCs, mit denen personenbezogene Daten verarbeitet werden, wurde eine hinreichende *Eingabekontrolle* nach § 5 Abs. 3 Nr. 7 BlnDSG durchgeführt. In Einzelfällen war zwar die Protokollfunktion der Datenschutzsoftware aktiviert, jedoch wurden nur Login-Versuche im Ringmodus protokolliert, das heißt, nach einer bestimmten Anzahl von Protokollereignissen werden die ersten Ereignisse überschrieben.

Bei allen kontrollierten PCs war eine ungenügende *Datenträgersicherung, -verwaltung und -organisation* festzustellen. Immerhin war eine Kennzeichnung von Datenträgern durch die Aufschrift „Statistisches Landesamt Berlin" zeitweilig vorgenommen worden. Allerdings ist dies mittlerweile eingestellt worden. Die Vollständigkeit und Authentizität der Datenträger kann daher nicht mehr überwacht werden. Wegen des umfangreichen internen Datenträgeraustausches sollte aber durch die Verwendung gekennzeichneter und katalogisierter Disketten einer Systemgefährdung durch unbefugte Entnahme, Verwendung oder Einbringung von Disketten vorgebeugt werden.

In mehreren Räumen fanden wir Datenträger, die zwar gekennzeichnet waren, jedoch offen herumlagen und auch zum Feierabend nicht weggeschlossen wurden, obwohl die Raumreinigung nicht oder nicht immer unter Aufsicht der Mitarbeiter stattfindet. Ein Laptop wurde in einem unverschlossenen Schreibtisch aufbewahrt; er enthielt personenbezogene Echtdaten zu *Testzwecken* für eine Datenbankprogrammierung. Die Vertraulichkeit dieser Daten war angesichts des erhöhten Diebstahlrisikos eines Laptops besonders gefährdet, abgesehen davon, daß die Verwendung personenbezogener Daten für Testzwecke gemäß § 11 Abs. 4 Satz 3, 2. Halbsatz BlnDSG ohnehin unzulässig ist.

Das Auffinden eines Schlüssels auf einem Türrahmen ermöglichte den Zugang in ein Dienstzimmer, in dem ein verlassener, jedoch eingeschalteter PC vorgefunden wurde. An diesem mit Hard- und Software besonders gut ausgestatteten PC wurden zwar keine personenbezogenen Daten verarbeitet, die mangelhafte Zugangskontrolle kann jedoch Risiken für die anderen am Netz angeschlossenen Rechner bedeuten, da über diesen Rechner der Zugang an das Netz möglich ist.

Fast sämtliche PCs sind über ein Netzwerk mit dem Rechnerverbund des Landesamtes und einem Rechner des LIT verbunden. Auf diesen Hauptrechnern werden die wesentlichen Statistikanwendungen bearbeitet. Die PCs dienen einerseits dem Zugriff auf Daten dieser Rechner und andererseits der weiteren Aufbereitung der Ergebnisse.

Die Kopplung der unterschiedlichen Systeme ermöglicht nicht nur das interaktive Arbeiten auf den verschiedenen Systemen, sondern auch den Austausch von Dateien untereinander. Prinzipiell ist jede Datei, für die eine Zugriffsberechtigung existiert, auf einen PC übertragbar und ablegbar. Die Kontrolle darüber, was kopiert werden kann, ist also abhängig von den Benutzerprofilen der Großrechner. Eine Protokollierung findet nicht statt.

Die Systemadministration und Sicherheit der *Hauptrechner* wurde positiv bewertet. Dies ist in erster Linie den vorhandenen Sicherheitsmechanismen der eingesetzten traditionellen Systeme zu danken. Proprietäre Systeme bieten immer noch ein wesentlich höheres Sicherheitsniveau als die „modernen" Client-Server-Systeme. So ist in dem Betriebssystem VMS bereits ein Security-Management-System enthalten, das es erlaubt, alle verfügbaren Ressourcen durch die Vergabe von dedizierten Zugriffsrechten zu schützen. Sämtliche sicherheitsrelevanten Ereignisse wurden protokolliert. Auch das auf dem Rechner im LIT eingesetzte Betriebssystem MVS mit der Datenschutzsoftware TopSecret bietet einen hohen Sicherheitsstandard.

Die hier festgestellten Mängel sind organisatorischer Natur:

Das Landesamt nutzt das Rechenzentrum des LIT als *Datenverarbeitung im Auftrag* (§ 3 BlnDSG). Es existieren jedoch weder vertragliche Vereinbarungen, noch wurde bisher eine vom LIT vorgegebene Servicevereinbarung abgeschlossen. Auch eine Dokumentation hinsichtlich der Schnittstellen zwischen StaLa und LIT existiert nicht. Zur Rechtfertigung wurde auf die historisch gewachsene Zusammenarbeit zwischen beiden Dienststellen verwiesen. Das Fehlen revisionsfähiger und verbindlicher Weisungen zur Auftragsdatenverabeitung verstößt gegen § 3 Abs. 2 BlnDSG.

Auch in den anderen Fällen, in denen externe Stellen Aufgaben des Landesamtes durchführen, wie z. B. bei der Datenerfassung oder der Vernichtung der Erfassungsbelege, konnten uns keinerlei Verträge vorgelegt werden.

Problematisch ist die Verfahrensweise, daß in den Fachreferaten diejenigen Mitarbeiter, die Auswertungsprogramme erstellen, auch gleichzeitig „Herren der Daten" sind. Auf diese Weise ist kaum mehr zu kontrollieren, ob die programmierten Auswertungen dem tatsächlichen Arbeitsauftrag entsprechen. Die fehlende Funktionentrennung widerspricht auch der Pflicht zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung (§ 19 Abs. 1 BlnDSG). So ist eine Kontrolle bezüglich der Einhaltung von § 8 Abs. 1 BlnDSG (Datengeheimnis) bzw. § 18 LStatG und § 21 BStatG (Reidentifizierungsverbot) kaum möglich. Wir haben daher eine strikte personelle und datenmäßige Trennung von Verfahrensentwicklung und -anwendung mit entsprechenden Freigabeverfahren empfohlen.

Volkszählungsboykotteure - für immer gespeichert?

Auch die Computer der Bußgeldstelle des Statistischen Landesamtes wurden geprüft. Dabei fanden wir eine Datei mit fast 4700 Datensätzen von Volkszählungsverweigerern. Die Datensätze enthielten neben dem Namen, der Straße und Hausnummer, dem Geschlecht und der Postleitzahl den Nachweis der zugestellten Mahnungen und der Bußgeldbescheide und endeten mit dem Datum der Verfahrenseinstellung (in der Regel 1990) auf Grundlage von Gnadenerlassen. Neben dieser Datei existierte auch eine manuelle Datei mit Tausenden von Mahnvorgängen anläßlich der Volkszählung 1987. Nachfragen ergaben, daß im Archiv des Statistischen Landesamtes überdies Tausende von durch Begleichung oder Begnadigung erledigten Bußgeldvorgängen über einen Zeitraum von ca. 8 Jahren aufbewahrt werden. Mit Ausnahme der Kassenbelege, die nach Haushaltsrecht aufzubewahren sind, gibt es sowohl für die Aufbewahrung der Computerdatei als auch für die Kartei der Volkszählungsverweigerer und den sonstigen in den Akten vorhandenen Schriftverkehr kein Erfordernis mehr. Das Vorhalten dieser Daten entbehrt überdies einer Rechtsgrundlage. Dies wurde von uns beanstandet. Das Landesamt hat die beanstandeten Dateien inzwischen gelöscht.

Immer noch Gesetzesmängel

Das Statistische Landesamt war auch 1994 gezwungen, die *Bevölkerungsstatistik* aufgrund einer datenschutzrechtlich äußerst bedenklichen gesetzlichen Grundlage durchzuführen. Die vergangene Legislaturperiode des Bundestages ging ohne die von den Datenschutzbeauftragten angemahnte Novellierung des Gesetzes über die Bevölkerungsstatistik zu Ende.

Wegen Fristablauf ist 1995 auch das *Mikrozensusgesetz* durch den Bundesgesetzgeber neu zu fassen. Ein Arbeitsentwurf ist geprägt von einer erheblichen Ausweitung des Merkmalkataloges, einer weitgehenden Reduzierung der bislang freiwillig erhobenen Merkmale, einer Erweiterung des Stichprobenumfangs und einer Verkürzung der Periodizität der Erhebung einer Reihe von Merkmalen. So sieht der Entwurf beispielsweise eine Verfünffachung der mit Auskunftspflicht erhobenen Merkmale im Komplex Tourismus vor. Dies würde zu einer wesentlichen Vertiefung des mit dem Mikrozensus verbundenen Eingriffs in das informationelle Selbstbestimmungsrecht verbunden sein. Die Innenverwaltung teilte unsere Auffassung und machte diese auf Bundesebene geltend. Im Ergebnis wurde der Arbeitsentwurf in dieser Form nicht für akzeptabel erklärt und zur Überarbeitung empfohlen.

Schulung tut not

Eine Reihe von statistischen Erhebungen (wie der Mikrozensus und die Wohnungsstichprobe 1993) werden mit Hilfe von Interviewern durchgeführt. Jährlich nehmen wir stichprobenhaft an Interviewerschulungen teil und überprüfen, ob die Auswahl der Interviewer und deren Schulung als besonders zur Geheimhaltung verpflichteten Personen mit der entsprechenden Sorgfalt erfolgt. Dies ist in der Regel der Fall. Ein im vergangenen Jahr aufgetretener Fall unterstreicht die Sorgfaltspflicht des Statistischen Landesamtes.

Ein Interviewer bemühte sich nach Abschluß der Erhebung durch das Statistische Landesamt, zuvor von ihm interviewte Bürger aufgrund seiner durch die statistische Erhebung erlangten Kenntnisse für eine andere wissenschaftliche Befragung zu gewinnen. Das Statistische Landesamt zog die notwendigen Konsequenzen und kündigte das Vertragsverhältnis mit dem Interviewer.

4.6.5 Personalwesen

Wie oben dargelegt[142], stellt das Fehlen landesrechtlicher gesetzlicher Regelungen zur Führung von Personalakten das wesentliche Defizit spezialrechtlicher Regelungen zum Datenschutz in Berlin dar. Derzeit findet die Verarbeitung von Personaldaten wegen einer entsprechenden Verweisung im Berliner Datenschutzgesetz (§ 34 Abs. 2) ihre Rechtsgrundlage im Bundesdatenschutzgesetz (insbesondere § 28), wobei die Bestimmungen des Beamtenrechtsrahmengesetzes zur Konkretisierung der dort enthaltenen Generalklauseln heranzuziehen sind.

Großzügiger Umgang mit Personaldaten

In einem Berliner Bezirksamt war innerhalb der Abteilung Personal und Verwaltung Streit darüber entstanden, ob dem Rechtsamt zur Erfüllung seiner Aufgaben (u. a. Durchführung von Prozeßvertretung für das Land Berlin) Personalakten von Beschäftigen ausgehändigt werden dürfen.

Dabei verwies das Rechtsamt auf seine Aufgabe, die Abteilung Personal und Verwaltung in Arbeitsstreitigkeiten optimal vertreten zu müssen, woraus zwangsläufig folge, daß der jeweilige Referent zwecks wirksamer Prozeßvertretung Kenntnis von dem gesamten beruflichen Werdegang des Beschäftigten und somit vom kompletten Inhalt der Personalakte haben müsse. Im übrigen sei das Rechtsamt laut Organisationsrecht Teil der Abteilung Personal und Verwaltung, so daß lediglich eine abteilungsinterne Datenübermittlung vorliege und die juristischen Referenten zudem auf Grund ihrer verantwortungsvollen Tätigkeit einer gesteigerten Schweigepflicht unterlägen.

Maßgebende Rechtsvorschrift für die Beantwortung der Frage, ob und in welchem Umfang Personalakten von der Abteilung Personal und Verwaltung an das Rechtsamt weitergegeben werden dürfen, ist unter den genannten Voraussetzungen § 56 d Beamtenrechtsrahmengesetz (BRRG). Bei der Abteilung Personal und Verwaltung einerseits und dem Rechtsamt andererseits handelt es sich um *verschiedene Organisationseinheiten* und damit um verschiedene datenverarbeitende Stellen (§ 4 Abs. 3 Nr. 1 BlnDSG), weil sie funktional verschiedene Aufgaben wahrnehmen.

Nach den genannten Vorschriften ist es zulässig, Personalakten ohne Einwilligung des Betroffenen an Behörden desselben Geschäftsbereichs weiterzugeben, soweit die Vorlage zur Vorbereitung oder Durchführung einer Personalentscheidung notwendig ist. Es ist daher in jedem Einzelfall zunächst zu prüfen, ob die Vorbereitung oder Durchführung einer Personalentscheidung (z. B. Höhergruppierung, Disziplinarverfahren etc.) gegeben ist. Wird diese Frage bejaht, so ist weiterhin zu prüfen, ob die Überlassung der Personalakte an das Rechtsamt im konkreten Fall notwendig ist. Dabei ist von dem Grundsatz auszugehen, daß die Personalakten sowohl im dienstlichen als auch im persönlichen Interesse des Beamten einen besonderen Vertrauensschutz genießen, der sich auch auf den Verkehr der Behörden untereinander erstreckt.

Dies bedeutet, daß das Rechtsamt im jeweiligen konkreten Einzelfall darzulegen hat, ob die Überlassung der gesamten Personalakte für eine ordnungsgemäße Prozeßführung erforderlich ist oder ob die Übersendung nur eines Teils daraus hierfür ausreicht. Die Erforderlichkeit ist nur dann zu bejahen, wenn die Kenntnis der Daten notwendig ist, um die Vorbereitung und die Durchführung des Rechtsstreits rechtmäßig, vollständig und in angemessener Zeit erledigen zu können. Dabei wird nicht verkannt, daß im Interesse einer wirksamen Prozeßvertretung die Kenntnis von dem gesamten beruflichen Werdegang des Beschäftigten und somit die Kenntnis des kompletten Inhalts der Personalakte nicht selten erforderlich sein wird. Dies ist jedoch in jedem Einzelfall zu prüfen.

Im Zuge eines Verwaltungsstreitverfahrens zwischen einer Berliner Hochschule und einem dort beschäftigten Lehrer wegen Herabsetzung einer Lehrverpflichtung wurde von dem geschäftsführenden Direktor des Instituts der vollständige anwaltliche Schriftsatz an einen Kollegen des Beschäftigten mit der Bitte um Stellungnahme weitergeleitet.

Die Erforderlichkeit der Datenübermittlung war hier zu verneinen. Bei Vorgängen, die Rechtsstreitigkeiten aus dem Beamten- oder Arbeitsverhältnis betreffen und somit nicht der Personalakte im materiellen Sinne zuzuordnen sind, finden die Vorschriften des § 6 BlnDSG i. V. m. § 2 Abs. 1 *Informationsverarbeitungsgesetz* (IVG) Anwendung.

Danach dürfen personenbezogene Daten im Rahmen allgemeiner Verwaltungstätigkeit (zu der auch die Durchführung von Rechtsstreitigkeiten gehört) ohne Einwilligung des Betroffenen nur verarbeitet werden, soweit dies für die allgemeine Verwaltungstätigkeit erforderlich ist und schutzwürdige Belange des Betroffenen wegen der Art der Daten, wegen der Art der Verwendung oder wegen ihrer Offenkundigkeit nicht entgegenstehen. Hier hätte es ausgereicht, dem Kollegen des Klägers auszugsweise lediglich die ihn betreffenden Ausführungen zur Stellungnahme zu übersenden.

Ein Bezirksamt nahm ein von der Staatsanwaltschaft im Rahmen der Mitteilungspflichten in Strafsachen (MiStra) übersandtes Urteil eines Strafgerichts wegen Fahrerflucht eines Beschäftigten zu dessen Personalakte, obwohl es sich zum einen um eine Privatfahrt gehandelt hatte und es zum anderen nicht zu seinen beruflichen Aufgaben gehörte, Kraftfahrzeuge zu führen.

142 vgl. 1.2

Dies war gemäß § 34 Abs. 2 BlnDSG i. V. m. §§ 28, 13 BDSG unzulässig. Nach § 2 Abs. 4 Nr. 2 Verwaltungsvorschrift über die Führung der Personalakten der Dienstkräfte des Landes Berlin - Teilregelung (Fn: Anlage zum Rundschreiben Sen Inn 88/1986 vom 3. Dezember 1986) sind Vorgänge oder Vermerke über *strafrechtliche oder berufsgerichtliche Verurteilungen*, staatsanwaltliche Ermittlungsverfahren oder sonstige Entscheidungen in einem Straf- oder Ermittlungsverfahren in eine Beiakte aufzunehmen, es sei denn, daß der Gegenstand ein außerdienstliches Verhalten ist und offensichtlich kein Bezug zum Beamten- oder Arbeitsverhältnis besteht.

Aufgrund unserer Intervention räumte die Personalverwaltung ein Fehlverhalten bezüglich der Anlage einer Beiakte ein und entfernte diese aus der Personalakte des Beschäftigten, teilte jedoch gleichzeitig mit, daß nach der Gemeinsamen Geschäftsordnung für die Berliner Verwaltung - Allgemeiner Teil (GGO I) verfügt worden sei, den Vorgang als *„Weglegevorgang"* gesondert und verschlossen für die Dauer eines Jahres zu archivieren.

Eine weitere Aufbewahrung des Schriftstücks war jedoch ebenfalls unzulässig. Gemäß § 55 Abs. 2 Satz 3 Nr. 4 bzw. § 78 Abs. 1 Nr. 2 GGO I ist „weglegen" dann zu verfügen, wenn der Vorgang wegen seines unwesentlichen Inhalts nicht in den Akten aufbewahrt zu werden braucht. Das in Rede stehende Schriftstück war jedoch keineswegs unwesentlich und hatte darüber hinaus keinen Bezug zu dem zugrunde liegenden Arbeitsverhältnis des Beschäftigten. Gemäß § 56 Abs. 1 Satz 2 BRRG gehören zur Personalakte alle Unterlagen einschließlich der in Dateien gespeicherten, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Andere Unterlagen dürfen gemäß § 56 Abs. 1 Satz 3 BRRG nicht in die Personalakte aufgenommen werden und sind gem. § 56 e BRRG analog zu vernichten.

Eine weitere Aufbewahrung des Urteils wäre auch gem. § 34 Abs. 2 BlnDSG i. V. m. § 28 BDSG unzulässig, da die Speicherung nicht im Rahmen der Zweckbestimmung des Vertragsverhältnisses erfolgte und darüber hinaus unverhältnismäßig war. Gemäß § 35 Abs. 2 Nr. 1 BDSG sind personenbezogene Daten zu löschen bzw. zu vernichten, wenn ihre Speicherung wie im vorliegenden Fall unzulässig war.

Eine Senatsverwaltung ist an uns mit der Frage herangetreten, inwieweit der Wahlvorstand für die Wahl der Schwerbehindertenvertretung das Recht hat, von der Personalverwaltung die Privatadressen der Schwerbehinderten zu verlangen, wenn er die schriftliche Stimmabgabe beschlossen hat.

Nach der Schwerbehindertenwahlordnung sind dem Schwerbehinderten vom Wahlvorstand die erforderlichen Unterlagen zu übersenden (§ 11 Abs. 2 i. V. m. § 11 Abs. 1 Nr. 4).

Wenn von der Dienststelle sichergestellt wird, daß die Wahlunterlagen bei Versendung als Dienstpost an die entsprechende Beschäftigungsstelle des Schwerbehinderten diesen in jedem Fall erreichen, so hat der Wahlvorstand kein Recht auf Herausgabe der Privatadresse, da eine Übermittlung nicht erforderlich ist. Ist dies nicht gewährleistet, so besteht ein Anspruch des Wahlvorstandes auf Herausgabe nur insoweit, als alle Schwerbehinderten der Herausgabe der Adresse zustimmen.

Bei Widersprüchen bzw. Widerständen gegen die Weitergabe ist im Wege der Adreßmittlung (Umschläge bzw. Unterlagen werden vom Wahlvorstand geordnet an das Personalamt zwecks Adressierung abgegeben und von dort an die Wahlberechtigten versandt) zu verfahren. Der Schwerbehinderte sollte dann darüber informiert werden, daß die Wahlunterlagen nicht vom Wahlvorstand, sondern vom Personalamt verschickt wurden.

Probleme mit dem Telefon

Ein Mitarbeiter der Berliner Polizei beantragte mit Erfolg eine Geheimnummer für seinen privaten Telefonanschluß, leugnete jedoch gegenüber dem Dienstherrn, einen solchen zu besitzen. Nachdem er in verschiedensten Funktionen auf mehreren Dienststellen der Polizei, zuletzt im Führungsstab einer Direktion tätig war, stellte die Dienststelle eine telefonische Anfrage bei der TELEKOM, ob der Beschäftigte einen Telefonhauptanschluß besitzt. Die TELEKOM bejahte dies und teilte die Geheimnummer mit. Die Polizei begründete ihr Vorgehen mit der Notwendigkeit der Aufstellung eines Alarmierungsplans und der schnellen Erreichbarkeit des Bediensteten.

Die Anfrage bei der TELEKOM verstieß gegen § 34 Abs. 2 BlnDSG i. V. m. §§ 28, 13 BDSG. Danach ist das Erheben personenbezogener Daten nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.

Zwar hat die Polizei im Rahmen der Gefahrenabwehr die erforderlichen Vorbereitungen für die Hilfeleistungen und das Handeln in Gefahrenfällen zu treffen, wozu das Aufstellen von Alarmierungsplänen und die Pflicht gehört, die schnelle *Erreichbarkeit nach Dienstschluß* auch durch Angabe des privaten Telefonanschlusses zu gewährleisten, soweit ein solcher Anschluß vorhanden ist. Die Tatsache jedoch, daß der Bedienstete Angehöriger des Führungsstabes werden konnte, obgleich er keinen Nachweis über das Vorhandensein eines privaten Telefonanschlusses erbrachte und somit nur persönlich alarmiert werden konnte, belegte, daß die Kenntnis eines (geheimgehaltenen) privaten Telefonanschlusses eben nicht zur Aufgabenerfüllung der Beschäftigungsstelle erforderlich war.

Ein Beschäftigter der Technischen Universität wurde von seinem Vorgesetzten sowie dem stellvertretenden Leiter der Einrichtung in seinem Dienstzimmer aufgesucht und nach dem Namen des Gesprächspartners sowie dem dienstlichen Grund des soeben beendeten Telefonats befragt. Nachdem sich der Beschäftigte geweigert hatte, den Namen des Betreffenden preiszugeben, drückte der stellvertretende Leiter die Wiederholungstaste und las die Telefonnummer vom Display des Telefons ab.

Das eigenmächtige Ablesen der Rufnummer auf dem Display des Telefonapparats des Beschäftigten war unzulässig. Das Grundrecht auf *Wahrung des Telefongeheimnisses* hat wegen seiner hohen Bedeutung für die Persönlichkeitsrechte auch Auswirkungen auf die Ausgestaltung des Arbeitsverhältnisses. Nach der Rechtsprechung kommt es dabei nicht darauf an, ob jemand berechtigt die Einrichtung (z. B. Telefon) benutzt. Schutzgut ist das gesprochene Wort. Im übrigen war im vorliegenden Fall der Einsatz von Kommunikationsanlagen auch Gegenstand einer Dienstvereinbarung, in der Verhaltens- und Leistungskontrollen durch Vorgesetzte ausdrücklich ausgeschlossen sind.

Medizinische Daten von Dienstkräften

Bislang war es landesweit üblich, ärztliche Atteste (z. B. Arbeitsunfähigkeitsbescheinigungen) den jeweiligen Büroleitungen, Einsatzstellen usw. vorzulegen, die ihrerseits die Atteste dann der personalaktenführenden Stelle übermittelten. Dies war datenschutzrechtlich bedenklich, da durch den Stempelaufdruck des behandelnden Arztes unschwer dessen Fachrichtung erkennbar ist, die Rückschlüsse auf die Art der Erkrankung ermöglicht und breiten Raum zu Spekulationen eröffnet.

Nach längeren Schriftwechseln hat sich die Senatsverwaltung für Inneres unserer Auffassung angeschlossen und verfügt[143], daß der ärztliche Nachweis einer Erkrankung nicht mehr dem jeweiligen Fachvorgesetzten, sondern unmittelbar der Büroleitung oder der personalaktenführenden Stelle zuzuleiten ist, welche den Fachvorgesetzten nur über die voraussichtliche Dauer der Erkrankung in Kenntnis setzt.

In einem Streitfall zwischen dem Personalrat und der Personalabteilung einer Senatsverwaltung über ein amtsärztliches Gutachten im Rahmen des § 77 LBG hat die Senatsverwaltung für Inneres dem Hauptpersonalrat gegenüber die Auffassung vertreten, daß die Dienstbehörden „ganz allgemein daran interessiert sein müssen, möglichst ausführliche ärztliche Stellungnahmen zu erhalten".

143 Rundschreiben II Nr. 30/1994 vom 16. März 1994

Mit der Novellierung des § 77 LBG vom 20. April 1993 ist die Übermittlung des Untersuchungsbefundes an die Dienstbehörde nur in dem eng abgesteckten Rahmen des Absatzes 1 Satz 4 LBG zulässig. Voraussetzung für eine solche Übermittlung durch den untersuchenden Arzt ist zum einen das Vorliegen *konkreter Zweifel* an dem festgestellten Ergebnis der ärztlichen Beurteilung und zum anderen die *Erforderlichkeit der Kenntnisnahme* für die von der Dienstbehörde zu treffende Entscheidung unter Wahrung des Verhältnismäßigkeitsgebots.

Insofern ist der Hinweis der Senatsverwaltung für Inneres auf das allgemein bestehende Interesse der Dienstbehörde an der möglichst ausführlichen ärztlichen Stellungnahme datenschutzrechtlich in hohem Maße bedenklich.

Erforderlich, aber auch ausreichend ist die Unterrichtung der Dienstbehörde über die Art der Funktionseinbuße zur Feststellung der Dienstunfähigkeit. Insoweit können Erkenntnisse vom Amtsarzt an die Dienstbehörde übermittelt werden. Hierbei sollte jedoch eine zurückhaltende Formulierung gewählt werden. Ergänzend dazu könnte (möglicherweise spezifiziert für einzelne Arbeitsbereiche) ein Kriterienkatalog entwickelt werden, den der Amtsarzt bei seiner Untersuchung zugrunde legt. Die Mitteilung des Untersuchungsergebnisses würde damit gleichzeitig das Zutreffen bzw. Nichtzutreffen der einzelnen Kriterien beinhalten. Im übrigen muß auch hier die ausdrückliche Einwilligung eingeholt werden.

Die „Gauckung"

Die Überprüfung der aus dem Ostteil der Stadt übernommenen öffentlichen Bediensteten daraufhin, ob sie hauptamtlich oder inoffiziell für den Staatssicherheitsdienst tätig waren (§ 21 Abs. 1 Ziff. 6 Stasiunterlagengesetz - StUG -), wurde in den Bezirksämtern und den meisten Senatsverwaltungen zu 90 bis 95 % abgeschlossen; damit findet eine in Umfang und Intensität bislang nicht dagewesene Datenerhebungsaktion im öffentlichen Bereich ihr Ende. Ihre Durchführung war von einer Vielzahl von Unsicherheiten begleitet, die vor allem darauf zurückzuführen sind, daß die Schaffung präziser Rechtsgrundlagen für entbehrlich gehalten wurde. Wir haben darüber mehrfach berichtet.

Es wird nunmehr zu beobachten sein, wie mit den angefallen Daten, seien es die von den Bediensteten in den ersten Fragebogenaktionen selbst angegebenen oder die vom Bundesbeauftragten für die Unterlagen der Staatssicherheit („Gauck-Behörde") übermittelten Angaben, umgegangen wird.

Im Fall eines positiven Gauck-Bescheides kann es zu einer Kündigung kommen. Dabei erhebt sich die Frage, inwieweit der Personalvertretung ein Recht auf Einsichtnahme in die Personalakte, insbesondere jedoch in die Unterlagen der Gauck-Behörde zusteht, wenn der Betroffene hierzu keine Einwilligung gibt.

Der Gauck-Bescheid enthält Personaldaten und ist auch bei Aufnahme in die Personalakte im materiellen Sinne deren Bestandteil. Die Weitergabe des Bescheides an den Personalrat/Hauptpersonalrat verstößt bei Vorliegen eines Einverständnisses des Beschäftigten nach § 73 Abs. 1 Satz 3 Personalvertretungsgesetz (PersVG) nicht gegen § 29 StUG, da seine Beteiligung zwingend vorgeschrieben ist.

Liegt ein Einverständnis jedoch nicht vor, so ist zu beachten, daß § 73 Abs. 1 Satz 3 PersVG das Recht des Beschäftigten normiert, selbst zu entscheiden, ob er dem Personalrat Einblick in seine höchstpersönlichen Angelegenheiten gestatten will. Insoweit genießt hier das Recht auf informationelle Selbstbestimmung des Beschäftigten Vorrang vor dem Recht des Personalrats auf kollektive Interessenwahrnehmung. In aller Regel wird zwar die einzelne Dienstkraft an einer Vorlage der Personalakten an die Personalvertretung schon deshalb interessiert sein, weil diese sich ein objektives Bild im Zusammenhang mit der beabsichtigten Personalmaßnahme machen kann. Es darf jedoch nicht übersehen werden, daß Personalakten Auskunft über höchstpersönliche Angelegenheiten der einzelnen Dienstkraft geben und daher ein schutzwürdiges Interesse an der Entscheidungsfreiheit über das Einsichtsrecht anerkannt werden muß. Dies muß um so mehr gelten, als es sich bei den Gauck-Unterlagen um hochsensibles und komplexes Aktenmaterial handelt. Hier muß dem Betroffenen die Möglichkeit gelassen werden, selbst zu entscheiden, ob er einem Gremium wie der Personalvertretung den Zugang bzw. Umgang damit gestatten soll oder sich besser zur Wahrnehmung seiner Rechte eines Anwalts bedient.

Verweigert der Betroffene sein Einverständnis, so ist dem Personalrat von der Dienststelle lediglich mitzuteilen, daß ein Bescheid der Gauck-Behörde vorliegt, der die Kündigung nach dem Einigungsvertrag zuläßt. Keinesfalls darf der konkrete Inhalt des Gauck-Bescheides vorgetragen oder gar aus ihm passagenweise zitiert werden.

Fortgeführt wird die Überprüfung von Bediensteten, die nicht aus dem Ostteil der Stadt stammen. An der rechtlichen Zulässigkeit hatten wir Zweifel geäußert[144] *und eine Beanstandung ausgesprochen, die der Senat jedoch zurückgewiesen hat.*

Auch die Durchführung dieser Überprüfung wies erhebliche Mängel auf: So wurden gedankenlos die gleichen Erhebungsformulare verwendet wie bei Bediensteten aus dem Osten. Von allen in die Überprüfung einbezogenen Bediensteten wurde z. B. die Angabe der Anschriften innerhalb der letzten 10 Jahre verlangt, obwohl die Gauck-Behörde damit gar nichts anfangen konnte. Auch die „Wessis" wurden nach ihrer PKZ gefragt; auf die Freiwilligkeit der Angabe dieses Merkmals[145] wurde nicht hingewiesen. Daß (West-)Berlin gleich der DDR zugeschlagen wurde, war nur das Tüpfelchen auf dem i (Frage nach den früheren Wohnanschriften von West-Berlinern, „wenn diese sich *in einem anderen Bezirk der DDR* befanden").

4.7 Jugend und Familie

Das Zusammenwirken von Gesundheitsamt, Jugendamt und Sozialamt

In einem Bezirksamt waren im Rahmen der Durchführung der ambulanten Hilfen im Rahmen der Hilfe zur Erziehung nach § 27 Kinder- und Jugendhilfegesetz (KJHG - SGB VIII) die fachdienstlichen Stellungnahmen der Kinder- und Jugendpsychiatrischen Beratungsstelle gegenüber dem Jugendamt strittig.

Die Stellungnahmen waren ursprünglich von der Tendenz getragen, möglichst umfassend und vollständig über die Gesundheitssituation an das Jugendamt zu berichten. Unbestritten war, daß das Jugendamt die Angaben für das Bewilligungsverfahren erhalten muß, soweit der Hilfebedürftige den Antrag aufrechterhält. Nach §§ 60, 65 SGB I hat das Jugendamt einen Anspruch darauf, daß der Antragsteller im Rahmen der Mitwirkung die erforderlichen *Tatsachen* offenbart. Somit hat der Antragsteller u. U. auch dem Jugendamt Tatsachen mitzuteilen, die im Rahmen einer vertrauensärztlichen Untersuchung unter die ärztliche Schweigepflicht fallen. Hierbei ist jedoch auf das Verhältnismäßigkeitsprinzip besonders zu achten, so daß nur die anspruchsbegründenden Tatsachen zu übermitteln sind. Das gesamte ärztliche Gutachten und weitergehende Befunde gehen weit darüber hinaus und sind im übrigen auch für die Jugendämter nicht hilfreich. Sinnvoll ist allein eine Plausibilitätsbegründung für das Vorliegen oder Nichtvorliegen der anspruchsbegründenden Tatsachen.

Eine ähnliche Problematik stellte sich in einem anderen Bezirk beim Eingliederungsprojekt „Betreutes Wohnen", wo ebenfalls Stellungnahmen des sozialpsychiatrischen Dienstes des Gesundheitsamtes an das Sozialamt abzugeben sind, um die Finanzierung des betreuten Wohnens sicherzustellen. Auch hier muß dem Erforderlichkeitsprinzip Rechnung getragen werden, so daß Informationen, die nicht der Bewilligung oder der Weiterbewilligung des Antrags dienen, vom Sozialpsychiatrischen Dienst nicht übermittelt werden dürfen.

144 Jahresbericht 1993, 4.5.5
145 Jahresbericht 1992, 3.1

Probleme der Verwaltungsreform

Vom Sprecherrat der Kinder- und Jugendgesundheitsdienste wurde uns das Problem der Rückverlagerung von Aufgaben nach dem KJHG aus dem Jugendgesundheitsdienst für Säuglinge und Kleinkinder auf die Abteilung Jugend und Sport vorgetragen. Dazu wurde ein Teil der Stellen des Gesundheitsamtes auf das Jugendamt übertragen.

Nicht bedacht wurde dabei, daß die für die Arbeit grundlegenden Geburtsmeldungen durch Meldeämter bzw. Standesämter aufgrund der rechtlichen Festschreibung im Berliner Melderecht (Anlage 4 DVO-Meldegesetz) an das Gesundheitsamt zu gehen hatten, so daß dem Jugendamt die Arbeitsgrundlage für ein Tätigwerden fehlte, dem Gesundheitsamt die Meldungen zwar noch zugingen, dort man aber nicht tätig werden konnte, weil die erforderlichen Mitarbeiter abgezogen waren.

Datenschutz hat auch etwas mit rationaler Behördenorganisation zu tun, so daß die richtige Information an die richtige Stelle kommt und dort effizient verwertet werden kann. So hatten wir in früherer Zeit die Meldungen an die Gesundheitsämter mit der Begründung befürwortet, daß gerade bei Neugeborenen die ärztliche Versorgung sichergestellt werden muß und vor allem aus ärztlichem Bereich etwaige Defizite in der Sozialstruktur aufgedeckt und bewertet werden können, um im erforderlichen Falle Jugendämter für die weitere Familienbetreuung einzuschalten.

4.8 Justiz

Bundesrecht: Defizite

Nach wie vor klaffen im Bereich der Justiz erhebliche Lücken datenschutzrechtlicher Regelungen des Bundesrechts. In der Entschließung, die die Datenschutzbeauftragten des Bundes und der Länder anläßlich des zehnten Jahrestages des Volkszählungsurteils faßten[146], stellten sie fest, daß ausreichende gesetzliche Regelungen nach wie vor fehlen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z. B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz), .
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Verfahren.

Verbrechensbekämpfungsgesetz

Das am intensivsten diskutierte Gesetz beinhaltet eher Rückschritte: Am 21. September 1994 hat der Bundestag das Gesetz zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz) verabschiedet, nachdem sich Bundesrat und Bundestag im Vermittlungsausschuß über die strittigen Punkte geeinigt hatten. Es ist am 1. Dezember 1994 in Kraft getreten[147].

Bis zuletzt war über die Aufgabe der bisherigen Beschränkung der strategischen Telefonüberwachung des *Bundesnachrichtendienstes* (BND) auf die Gewinnung von Erkenntnissen über das Ausland, die von sicherheitspolitischer Bedeutung sind, gestritten worden.

Nach dem Gesetzentwurf der Bundesregierung soll der BND künftig insbesondere auch die Einfuhr von Betäubungsmitteln, Aktivitäten des internationalen Terrorismus, die internationale Geldfälschung und die damit zusammenhängende Geldwäsche aufklären[148]. Mit einigen Änderungen ist diese Regelung in dieser Form auch in Kraft getreten.

Trotz der Kritik an der beginnenden Aufhebung des Trennungsgebotes hat sich der Vermittlungsausschuß auf eine nicht unbedenkliche Kompetenzerweiterung für den BND geeinigt. Gestrichen wurde zwar die Möglichkeit des BND, gezielt Suchbegriffe zu Personen zu verwenden, geblieben ist aber die Einschaltung des „elektronischen Staubsaugers" des BND, wenn bestimmte, für die Strafverfolgung interessante Stichworte fallen. Dann schaltet sich das Aufzeichnungsgerät ein.

Aus dem BND wurde damit ein Zulieferer für die Strafverfolgung. Die vom Gesetz bisher verriegelte Tür zwischen Polizei und Geheimdienst ist aufgesperrt.

Die Erweiterung der Befugnisse des BND führt faktisch zu einer Mitwirkung des BND bei der Verbrechensbekämpfung, obwohl dieser Bereich strikt von dem Einsatzbereich von Geheimdiensten zu trennen ist. Im Gegensatz zu den Geheimdiensten sind die Strafverfolgungsbehörden einer Vielzahl von rechtsstaatlichen Verfahrensregelungen unterworfen, die neben dem Recht des Beschuldigten auf Verteidigung auch in besonderer Weise dessen informationelle Selbstbestimmung sichern. Durch die Ausdehnung des Anwendungsbereiches nachrichtendienstlicher Mittel ist diese Trennlinie verwischt worden. Darauf haben die Datenschutzbeauftragten des Bundes und der Länder hingewiesen und die strikte Einhaltung des Trennungsgebotes bei der Zusammenarbeit von Nachrichtendiensten und Polizei gefordert[149].

Mit dem Inkrafttreten des Verbrechensbekämpfungsgesetzes ist auch der Weg frei geworden für ein *bundesweites staatsanwaltschaftliches Informationssystem* (SISY).

In dem Informationssystem sollen alle staatsanwaltschaftlichen Vorgänge ohne Differenzierung erfaßt werden. Der bundesweite Zugriff auf alle staatsanwaltschaftlichen Vorgänge, unabhängig von der Schwere und Bedeutung der Straftaten, ist im Hinblick auf den Verhältnismäßigkeitsgrundsatz bedenklich. Wir hatten in den Gesetzesberatungen deshalb empfohlen, das Informationssystem auf schwere und überregional bedeutsame Straftaten zu beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat darauf hingewiesen, daß bei Einstellungen mangels hinreichenden Tatverdachts und rechtskräftigem Freispruch in der Regel eine Registrierung nicht gerechtfertigt ist, es sei denn, tatsächliche Anhaltspunkte für eine Straftat liegen auch noch nach Abschluß des Verfahrens vor. Weiterhin hat die Konferenz eine Abstimmung der Datei mit den bestehenden polizeilichen Informationssystemen und dem Bundeszentralregister, das ebenfalls Daten zu Zwecken der Strafverfolgung speichert, gefordert[150].

Zu SISY liegt bereits der Entwurf einer *Errichtungsanordnung* vor. Hier finden sich insbesondere Regelungen über den Zweck der Datei, den betroffenen Personenkreis, die zu verarbeitenden Daten und Übermittlungsregelungen. Entgegen dem Wortlaut des § 474 Abs. 3 Satz 2 StPO sieht die Errichtungsanordnung auch sogenannte *Spontanübermittlungen,* d. h. solche Übermittlungen vor, die ohne ein vorheriges Ersuchen einer Staatsanwaltschaft erfolgen. Derartige Übermittlungen sind vom Gesetz nicht gedeckt. Nach § 474 Abs. 3 Satz 2 StPO dürfen aus dem Register nur Auskünfte erteilt werden für Zwecke eines Strafverfahrens. Der Gesetzgeber hat damit klargestellt, daß nur auf ein Ersuchen hin Daten übermittelt werden dürfen, da eine Auskunft grundsätzlich ein Ersuchen voraussetzt.

Nicht von der gesetzlichen Grundlage gedeckt ist auch die Einbeziehung der von den Finanzbehörden geführten *steuerstrafrechtlichen* Verfahren. Nach der Vorstellung des Gesetzgebers teilen nach § 474 Abs. 3 StPO nur die Staatsanwaltschaften die einzutragenden Daten mit. Das Gesetz ist an dieser Stelle hinreichend bestimmt, so daß wir eine andere Auslegung, die auch die Finanzbehörden mit einbezieht, nicht für möglich halten.

146 vgl. Anlage
147 BGBl. I, 3186
148 vgl. § 3 Abs. 1 G-10-Gesetz (E), Art. 12 Nr. 1, 3 und 4 Verbrechensbekämpfungsgesetz, BT-Drs 12/6853
149 vgl. Anlage 2.12
150 vgl. Anlage 2.3

Es gibt auch Fortschritte

Am 1. Januar 1995 trat das Gesetz zur Änderung von Vorschriften über die *Prozeßkostenhilfe* (PKHÄndG)[151] in Kraft. Das Gesetz enthält datenschutzrechtliche Verbesserungen.

Die Erklärung einer Partei im Prozeßkostenhilfeantragsverfahren über ihre persönlichen und wirtschaftlichen Verhältnisse und die entsprechenden Belege dürfen zukünftig dem Antragsgegner nur noch dann zugänglich gemacht werden, wenn die Partei dem vorher auch zugestimmt hat.

Das Gericht darf dem Prozeßgegner bei der Entscheidung über den Prozeßkostenhilfeantrag die Gründe der Entscheidung, wenn diese Angaben über die persönlichen und wirtschaftlichen Verhältnisse enthalten, nur noch mit vorheriger Zustimmung der Antragspartei zugänglich machen.

Ebenfalls am 1. Januar 1995 trat das Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis in Kraft, eine Regelung, die seit Bestehen der Datenschutzbeauftragten regelmäßig angemahnt worden war. Darin ist nun eine detaillierte Zweckbindung für die Verwendung von Daten aus dem Schuldnerverzeichnis enthalten. Um der Verwechslungsgefahr zwischen verschiedenen Schuldnern vorzubeugen, sollen, soweit bekannt, auch die Geburtsdaten der Personen im Schuldnerverzeichnis eingetragen werden.

Besonders hervorzuheben sind die neugefaßten Regelungen zur Löschung der Eintragung im Schuldnerverzeichnis, die jetzt auch eine vorzeitige Löschung von Amts wegen neben der weiterhin geltenden dreijährigen Löschungsfrist vorsehen, in den Fällen, in denen das Vollstreckungsgericht vom Wegfall des Eintragungsgrundes erfährt.

Ausdrücklich geregelt wurden die Voraussetzungen für die Erteilung von Abdrucken zum laufenden Bezug aus dem Schuldnerverzeichnis an im Gesetz benannte öffentliche und private Stellen wie beispielsweise die Industrie- und Handelskammern oder die privaten Schuldnerverzeichnisse. Hierzu wurde eine Verpflichtung zur vertraulichen Behandlung der übermittelten Daten aufgenommen.

Durch das Gesetz wird das Bundesministerium für Justiz ermächtigt, eine Rechtsverordnung zur Ausgestaltung der Regelungen des Schuldnerverzeichnisses zu erlassen. Die Verordnung über das Schuldnerverzeichnis (SchuVVO) ist ebenfalls am 1. Januar 1995 in Kraft getreten[152].

Das Dauerthema des Strafverfahrensänderungsgesetzes

Nichts Entscheidendes ist hinsichtlich der Novellierung der StPO geschehen. Die Länder Bayern, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland und Thüringen hatten dem Bundesrat den Entwurf eines *Strafverfahrensänderungsgesetzes 1994* (StVÄG 1994) zugeleitet. In unserem Jahresbericht 1993[153] hatten wir über diesen Entwurf berichtet. Die Datenschutzbeauftragten des Bundes und der Länder sind der Auffassung, daß der Entwurf einer grundlegenden Überarbeitung bedarf[154]. Der Bundesrat hat dennoch beschlossen, den Gesetzentwurf ohne wesentliche Änderungen im Bundestag einzubringen. Der Gesetzentwurf[155] trägt dem Recht auf informationelle Selbstbestimmung nur unzureichend Rechnung; er fällt weit hinter den Standard der allgemeinen Datenschutzgesetze und der Polizeigesetze der Länder zurück.

Alle an einem Strafverfahren Beteiligten, Verdächtige, Verbrechensopfer, Tatzeugen, aber auch Unbeteiligte müssen nach dem Entwurf damit rechnen, daß Daten über ihre Person aus Strafakten nicht nur an andere Rechtspflegeorgane, sondern auch an viele andere Behörden weitergegeben werden können. Ein nicht näher definiertes „berechtigtes Interesse" soll private Personen und Unternehmen zur Auskunft aus oder zur Einsicht in Strafakten legitimieren. Damit wird die besondere Schutzwürdigkeit gerade des Inhaltes von Strafakten schwer mißachtet. Geändert worden ist inzwischen die ursprünglich vorgesehene Löschungsregelung, nach der Angaben in Justizdateien, abweichend vom allgemeinen Datenschutzrecht, nur nach dem Zufallsprinzip aus Anlaß einer Einzelfallbearbeitung gelöscht werden sollten. Jetzt ist eine Löschung vorgesehen, wenn die Speicherung der Daten unzulässig war oder aber ihre Kenntnis nicht mehr zur Aufgabenerfüllung der Strafverfolgungsbehörde erforderlich ist, allerdings ohne daß im Gesetz Löschungs- oder Prüfungsfristen genannt sind.

Auch die Diskussion um den *„Großen Lauschangriff"* hält an. Bayern hat eine Bundesratsinitiative zur Ergänzung des Gesetzes gegen die organisierte Kriminalität (OrgKG) gestartet und dem Bundesrat den Entwurf eines Gesetzes zur Ergänzung des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG ErgG) zugeleitet[156]. Mit diesem Gesetzesentwurf soll das heimliche Abhören von Gesprächen in Wohnungen und damit auch das heimliche Betreten der Wohnungen (Änderung des § 100 c StPO und der §§ 100 d, 101 StPO) zum Installieren der Abhörgeräte ermöglicht werden. Zugleich soll die Möglichkeit der Herstellung von Lichtbildern und Bildaufzeichnungen sowie der Einsatz sonstiger technischer Observationsmittel in Wohnungen geschaffen werden. Da der Lauschangriff in Wohnungen mit dem Grundrecht der Unverletzlichkeit der Wohnung, das aus Art. 13 Grundgesetz (GG) folgt, nicht vereinbar wäre, soll auch Art. 13 Abs. 3 GG geändert werden[157].

Das OrgKG ErgG sieht außer dem Lauschangriff in Wohnungen die Einbeziehung des Straftatbestandes der Geldwäsche in den Katalog des § 100 a StPO vor, der die Straftatbestände nennt, bei deren Verdacht die Überwachung und Aufzeichnung des Fernmeldeverkehrs angeordnet werden darf. Ungeklärt ist, ob dann nicht schon jede Meldung einer Bank als ausreichend für die Anordnung der Überwachung des Fernmeldeverkehrs angesehen werden könnte.

Weiterhin sollen nach dem Entwurf verdeckte Ermittler in bestimmten Fällen selbst Straftaten begehen dürfen - nämlich dann, wenn „das Interesse an dem Einsatz des verdeckten Ermittlers das beeinträchtigte Interesse wesentlich überwiegt".

Diese Gesetzesinitiativen sind unvereinbar mit dem Grundrecht auf freie Entfaltung der Persönlichkeit. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich bereits 1992 gegen eine Ausweitung des Lauschangriffes auf Privatwohnungen für Zwecke der Strafverfolgung ausgesprochen mit dem Hinweis, „daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis nicht geben darf".

Datenschutz macht nicht vor Strafvollzug Halt

Ein Untersuchungshäftling aus der Justizvollzugsanstalt Moabit beschwerte sich darüber, daß die Gefangenen zur Vorstellung beim Arzt für jedermann laut hörbar ausgerufen werden. Derselbe Untersuchungshäftling mußte feststellen, daß auch seine Post an den Berliner Datenschutzbeauftragten der Postkontrolle unterzogen wurde.

Durch ein Ausrufen des Gefangenen zur Vorstellung bei der *Arztgeschäftsstelle* oder beim Arzt werden Informationen über den Betroffenen unbefugt an andere Mitgefangene offenbart. Dies stellt einen Verstoß gegen § 8 und § 13 BlnDSG dar, der nicht damit zu rechtfertigen ist, daß möglicherweise Verzögerungen entstehen könnten, wenn der Gefangene nicht in seinem Haftraum oder auf seiner Arbeitsstelle ist. Dies gilt besonders für so sensible Daten wie den Arztbesuch, der schließlich auch in den strafbewährten Schutzbereich des § 203 StGB fällt.

Bei der *Überwachung des Postverkehrs* der Gefangenen in der Untersuchungshaft ist eine verfassungskonforme Auslegung der Nr. 30 Untersuchungshaftvollzugsordnung (UVollzO) für die Beschränkung des Schriftverkehrs eines Gefangenen an den Datenschutzbeauftragten geboten. Nr. 30 UVollzO, die die Schreiben des Gefangenen an Volksvertretungen des Bundes und

151 BGBl. I 1994, 2954
152 vgl. 1.1
153 Jahresbericht 1993, 4.7
154 vgl. Anlage
155 BR-Drs 620/94 vom 14. Oktober 1994
156 BR-Drs 494/94
157 BR-Drs 493/94

der Länder sowie an deren Vertreter und Schreiben an die Europäische Kommission für Menschenrechte von der Überwachung durch den Richter ausnimmt, ist verfassungskonform dahin auszulegen, daß auch die Schreiben an die Datenschutzbeauftragten des Bundes und der Länder von der Überwachung des Schriftverkehrs ausgenommen sind. Bei Schreiben an den Datenschutzbeauftragten können daher auch nur die durch Nr. 30 UVollzO vorgesehenen Beschränkungen durch den Richter gebilligt werden.

Die Senatsverwaltung für Justiz verweist darauf, daß die Ausnahme der Post vom und an den Datenschutzbeauftragten von der Postkontrolle in ein künftiges Untersuchungshaftvollzugsgesetz aufgenommen werden soll. Da für die Entscheidungen zum Vollzug der Untersuchungshaft auch Strafverfolgungsbehörden anderer Länder zuständig sein könnten, wird von der Senatsverwaltung für Justiz eine landesspezifische Regelung abgelehnt.

Mitteilungen in Zivilsachen - MiZi -

Die Gerichte sind verpflichtet, Behörden in bestimmten Fällen Mitteilungen über Urteile zu machen. Wann dies der Fall ist und was mitzuteilen ist, regelt die Anordnung über Mitteilungen in Zivilsachen (MiZi). Dort ist beispielsweise geregelt, daß Urteile in Kindschaftssachen, sofern sie eine Eintragung im Personenstandsbuch erforderlich machen, dem zuständigen Standesbeamten mitzuteilen sind. Eine Mitarbeiterin eines Gerichtes fragte sich, ob für die Eintragung in das Personenstandsbuch die Übersendung des gesamten Urteils in Kindschaftssachen erforderlich sei, denn ein solches Urteil enthält sehr intime Informationen zu den betroffenen Personen.

Nach § 29 Abs. 2 Ausführungsgesetz zum Gerichtsverfassungsgesetz (AGGVG) sind Mitteilungen nach den MiZi bis zum Inkrafttreten eines bundeseinheitlichen Justizmitteilungsgesetzes zulässig. Der in § 9 Abs. 1 BlnDSG hervorgehobene Verfassungsgrundsatz der Erforderlichkeit ist damit bei der Datenverarbeitung in der Berliner Justiz ausgeschlossen. Er ist jedoch auch bei der Anwendung der MiZi zu beachten[158], und es ist nur das zu übermitteln, was zur rechtmäßigen Aufgabenerfüllung durch das Standesamt benötigt wird.

Die Senatsverwaltung für Justiz vertritt dagegen die Auffassung, daß eine besondere Erforderlichkeitsprüfung im Rahmen der MiZi nicht angezeigt sei. Diese Auffassung hat der Senat bereits in seiner Stellungnahme zu unserem Jahresbericht 1992[159], in dem wir das Problem schon einmal aufgegriffen hatten, vertreten.

Nach Auskunft der Senatsverwaltung für Inneres als Aufsichtsbehörde für die Standesämter dürfte in der überwiegenden Zahl der mitzuteilenden Entscheidungen eine Ausfertigung des Urteils ohne vollständigen Tatbestand und ohne Entscheidungsgründe in Verbindung mit den Angaben im jeweiligen Mitteilungsvordruck für den Standesbeamten zur Erfüllung seiner Aufgaben ausreichend sein. Damit verstößt die angesprochene Praxis trotz der anderweitigen Ansicht der Justizverwaltung gegen geltendes Datenschutzrecht.

4.9 Kulturelle Angelegenheiten

Zögerliche Aufbereitung von Datenbeständen der DDR

Mit dem Berliner Archivgesetz wurde, wie im Jahresbericht 1993 erörtert, eine abschließende Regelung für den Umgang mit Datenbeständen ehemaliger Einrichtungen der DDR geschaffen. Danach sind personenbezogene Daten derartiger Einrichtungen, wenn sie zur Erfüllung von Verwaltungsaufgaben nicht mehr erforderlich sind, zunächst dem *Landesarchiv* anzubieten. Verzichtet das Landesarchiv auf eine Archivierung, so sind diese Daten zu löschen oder zu vernichten. Diese Regelung führte im Jahr 1994 erst in Einzelfällen zu Angeboten. Lediglich in drei Fällen wurden archivarisch bedeutende Datenbestände übernommen.

Im Juni 1994 wandte sich der Berliner Datenschutzbeauftragte mit einer Presseerklärung an die Öffentlichkeit. Wir haben darauf hingewiesen, daß alle Privatpersonen und nicht-öffentlichen Stellen, die noch im Besitz von Unterlagen ehemaliger Einrichtungen der DDR sind, nach dem Landesarchivgesetz verpflichtet wurden, diese an die zuständigen öffentlichen Stellen herauszugeben. Insbesondere wurde darauf verwiesen, daß noch nicht alle Unterlagen der 162 ehemaligen Schiedskommissionen, die einfache zivilrechtliche Streitigkeiten und geringfügige Strafsachen zu DDR-Zeiten verhandelten, bei den Amtsgerichten abgeliefert worden waren. Des weiteren bemühten wir uns um Aufklärung, inwieweit in den Depots der Treuhandanstalt, die Unterlagen der ehemaligen volkseigenen Betriebe der DDR aufbewahren, auch Unterlagen der ehemaligen Konfliktkommissionen, die einfache Arbeitsrechtsstreitigkeiten und auch geringfügige Strafsachen verhandelten, Eingang fanden. Die Treuhandanstalt teilte daraufhin mit, daß Unterlagen der Schieds- und Konfliktkommissionen in Depots ihrer Niederlassungen (Dresden, Magdeburg und Schwerin) eingelagert sind. Betroffenen Bürgern wird grundsätzlich Auskunft aus den archivierten Unterlagen erteilt. Einzelanfragen können auch direkt an das jeweilige Depot gerichtet werden.

Im Jahresbericht 1992 machten wir auf das Problem des Umgangs mit *Studentenaltakten* aufmerksam. Im Jahr 1994 wurde durch die im Ostteil liegenden Hochschulen begonnen, die Altaktenbestände zu sichten und nach den im Archivgesetz festgelegten Grundsätzen dem Landesarchiv anzubieten bzw. im Hochschularchiv zu verwahren oder zu vernichten.

Auch an den *Schulen im Ostteil Berlins* hat auf Grundlage eines - vor Erlaß des Landesarchivgesetzes - von der Senatsverwaltung für Schule, Berufsbildung und Sport herausgegebenen Rundschreibens die Bereinigung der aus DDR-Zeiten stammenden Archivbestände eingesetzt.

Das zentrale *Totenscheinarchiv* der ehemaligen DDR wurde zum 1. Januar 1994 entsprechend dem Gebietsstand der neuen Bundesländer aufgeteilt und diesen übergeben. Dieses Archiv umfaßt alle Totenscheine des Zeitraums von 1969 bis 1990, wobei ab 1979 die Sortierung nach dem Sterbeort erfolgte. Dies hat zur Folge, daß die übernehmenden Bundesländer zwangsläufig Daten von Verstorbenen mit ehemaligen Wohnsitzen haben, die heute zu anderen neuen Bundesländern bzw. zu Berlin gehörten. In Berlin hat diesen Datenbestand das Landesamt für Zentrale Soziale Aufgaben - Landesversorgungsamt - übernommen. Als Aufbewahrungsfrist wird von einem Zeitraum von 30 Jahren ausgegangen.

Diese Ausführungen machen deutlich, daß noch nicht von einer den Regelungen des Archivgesetzes entsprechenden Aufbereitung personenbezogener Datenbestände aus DDR-Zeiten ausgegangen werden kann. Gerade im Interesse der zeitgeschichtlichen Forschung müssen diese Unterlagen - soweit sie als archivwürdig eingestuft werden - in den Archiven Berlins gesichert werden.

Automation in den Berliner Bibliotheken

Die Automation in den Berliner Bibliotheken befindet sich derzeit in einem Umbruch, um die Medienversorgung der Berliner Bürger effizienter und schneller sicherzustellen.

Mit erheblicher Verspätung sind wir über den geplanten *Verbund der Öffentlichen Bibliotheken* des Landes mit prüffähigen Unterlagen unterrichtet worden, so daß eine fundierte datenschutzrechtliche Stellungnahme noch nicht abgegeben werden konnte. Immerhin liegt mit § 4 des Gesetzes über Datenverarbeitung im Bereich der Kulturverwaltung seit 1993 eine bereichsspezifische gesetzliche Regelung für die Verarbeitung personenbezogener Daten in Bibliotheken vor, so daß der automatisierten Datenverarbeitung keine grundsätzlichen rechtlichen Einwände mehr entgegenstehen. Ob das geplante Projekt vollständig von dieser Regelung abgedeckt wird, wird noch zu ermitteln sein.

Schwerpunkt datenschutzrechtlicher Betrachtungen ist dabei nicht der bibliographische Verbund, der allen Benutzern dazu dienen kann, festzustellen, wo ein von ihm gewünschtes Werk für ihn verfügbar ist und von ihm entliehen werden kann. Vielmehr muß das Augenmerk auf die Speicherung und Übermittlung von

158 Abgeordnetenhaus-Drs 12/3081, 4.3
159 Jahresbericht 1992, 4.3

benutzerbezogenen Daten aus der Ausleihverbuchung gerichtet werden, denn diese Daten können bei längerer Aufbewahrung zur Beobachtung der Lesegewohnheiten geeignet sein; solche Persönlichkeitsprofile gehören zu den schutzbedürftigsten Daten, die zu einer Person existieren können.

Sicherheitsbedenken können auftreten, wenn das MAN[160] für den externen Zugang an den bibliographischen Verbund benutzt werden soll. Es ist zu prüfen, ob das IT-Sicherheitskonzept für das MAN stark genug ist, um die sicherheitsempfindlichen Verfahren, die über das MAN vernetzt werden sollen, auch dann ausreichend zu schützen, wenn es auch für den öffentlichen Zugang an Informationsangebote der öffentlichen Verwaltung genutzt werden soll.

Für die Automation in der *Senatsbibliothek* hat eine Unternehmensberatung ein Konzept erstellt und vorgeschlagen, dieses im Rahmen von Outsourcing[161] umzusetzen. Die Klärung der für das Projekt wichtigen datenschutzrechtlichen Aspekte war Gegenstand des Gutachtens.

Neben einer Reihe von Nachlässigkeiten im Umgang mit dem Berliner Datenschutzgesetz wurden grobe Fehler festgestellt:

Die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten waren falsch und unvollständig dargestellt. Das Berliner Datenschutzgesetz wurde selbst als Rechtsgrundlage herangezogen. Es verlangt aber gerade in § 6 Abs. 1, daß eine besondere Rechtsvorschrift die Verarbeitung erlauben muß, wenn eine Einwilligung nicht vorliegt. Das Erforderlichkeitsprinzip in § 9 BlnDSG ergänzt die gesetzlichen Anforderungen, ersetzt sie aber nicht. Rechtsgrundlage ist vielmehr § 4 des Gesetzes über die Datenverarbeitung im Bereich der Kulturverwaltung. Diese spezialgesetzliche Vorschrift wurde von den Gutachtern unberücksichtigt gelassen. Dies bedeutet, daß alle Ausführungen des Gutachtens neu zu betrachten sind, insbesondere jene, die die längerfristige Speicherung von Ausleihdaten nach Rückgabe von Medien betrafen.

Die aus § 3 Abs. 4 BlnDSG folgenden Konsequenzen für die Gestaltung des Outsourcing-Vertrages in dem beigelegten Vertragsentwurf für das Outsourcing sind unberücksichtigt geblieben (Unterwerfung unter das Berliner Datenschutzgesetz und die Kontrolle des Berliner Datenschutzbeauftragten).

4.10 Schule, Berufsbildung und Sport

Schuldatenverordnung in Kraft

Auf Grundlage der Anfang 1993 ins Schulgesetz aufgenommenen Datenschutzregelungen wurde durch die Senatsverwaltung für Schule, Berufsbildung und Sport eine Schuldatenverordnung[162] erlassen. In die Verordnung sind die in der Vergangenheit gesammelten guten Erfahrungen der Ausführungsvorschriften über die Führung schriftlicher Unterlagen über Schüler *(AV-Schülerunterlagen)* eingeflossen. Unsere vielfältigen Hinweise, insbesondere zum praktikablen Umgang mit Schülerdaten im täglichen Schulleben, zu den Akten der Sozialpädagogen, zur Tätigkeit der Förderausschüsse und zur *Schulstatistik* wurden berücksichtigt. Die auf unsere Anregung zurückgehende Regelung, die es nunmehr erlaubt, auch Leistungsdaten von Schülern auf privaten Computern der Lehrer zu verarbeiten, wurde in den vergangenen Monaten von vielen Lehrern begrüßt. Um auch durch die Schüler und deren Eltern die notwendige Akzeptanz solcher Datenverarbeitungen zu erhalten, sind die Berliner Schulen gefordert, in nächster Zeit die noch ausstehenden Meldungen zum Berliner Dateienregister, insbesondere auch für die Verarbeitung auf privaten Computern, vorzunehmen.

Für einige sich aus der Schuldatenverordnung ergebenden praktischen Probleme sind künftig noch konkret ausgestaltete Verfahrensweisen festzulegen. Dies betrifft die von der Senatsverwaltung beabsichtigte und nach der Schuldatenverordnung zulässige Umgestaltung der Schulstatistik sowie auch die Verwendung personenbezogener Daten der Sozialpädagogen für Aufsichts- und Kontrollaufgaben.

Mit der vorliegenden Schuldatenverordnung dürfte der Prozeß der datenschutzrechtlichen Ausgestaltung des Berliner Schulwesens im wesentlichen abgeschlossen sein.

160 vgl. 2.2
161 vgl. 2.4.3
162 GVBl. 1994, 435 ff.

Datenschutz im Unterricht

Darf ein Lehrer vor der Klasse die Noten einzelner Schüler bekanntgeben? Ist das nicht ein Verstoß gegen den Datenschutz? Warum gibt der Lehrer bei der Rückgabe von Klassenarbeiten nicht die Noten der einzelnen Schüler bekannt? Sogar ein Notenspiegel wird von ihm als ein Verstoß gegen den Datenschutz angesehen.

Eingaben von Eltern mit solchen und ähnlichen Fragen erreichen uns immer wieder. Offenbar sind einige Lehrer unsicher, was bei der Gestaltung ihres Unterrichts zulässig ist und was nicht. Mit der Schuldatenverordnung lassen sich jedoch eine Reihe von datenschutzrechtlichen Problemen, die im praktischen Unterricht auftreten, nicht greifen.

Nach § 1 Schulgesetz ist es die Aufgabe der Schule, alle wertvollen Anlagen der Kinder und Jugendlichen zur vollen Entfaltung zu bringen und ihnen ein Höchstmaß an Urteilskraft, gründliches Wissen und Können zu vermitteln. In diesem Rahmen wurde durch § 10 Berliner Schulverfassungsgesetz den Lehrern die Aufgabe zugewiesen, die ihnen anvertrauten Schüler zu unterrichten und zu erziehen. Dabei beurteilen die Lehrer die Leistungen der Schüler gemäß ihrer fachlichen Ausbildung und in eigener Verantwortung im Rahmen der geltenden Vorschriften und Konferenzbeschlüsse. Somit hat die Schule nicht nur den Auftrag, Wissen zu vermitteln, sondern auch die Verpflichtung, pädagogisch auf die ihr anvertrauten Kinder und Jugendlichen einzuwirken und ihnen eine Einordnung der eigenen Leistung zu ermöglichen.

Damit ist es durchaus zulässig, im Rahmen des Unterrichts die Noten aller Schüler vor der Klasse bekanntzugeben und mit Hilfe eines Notenspiegels die Eltern über die leistungsmäßige Einordnung ihrer Kinder zu informieren. Das Schulverfassungsgesetz gibt mit § 14 den Schulen jedoch die Möglichkeit, auf Grund von Beschlüssen der Gesamtkonferenz Regelungen zu treffen, die beispielsweise ein Verlesen der Noten oder auch einen Zensurenspiegel ausschließen. Nach dieser Rechtsvorschrift berät und beschließt die Gesamtkonferenz auch über die Grundsätze zur Sicherung einer einheitlichen Leistungsbeurteilung der Schüler. Schränkt die Gesamtkonferenz die Verantwortung der Lehrer nicht ein, so bleibt es dem pädagogischen Ermessen des jeweiligen Lehrers überlassen, Noten in dieser Weise oder anders den Schülern bekanntzugeben.

Zu beanstanden wäre hingegen das Vorgehen eines Lehrers, der bewußt nur die (schlechten) Noten einzelner Schüler verliest oder anderweitig Schülern bzw. Eltern mitteilt, um diese einzelnen Schüler vor den Mitschülern bloßzustellen. Die pädagogischen Freiräume des Lehrers enden dort, wo gezielt oder unbewußt Maßnahmen mit Prangerwirkung ergriffen werden.

Als datenschutzrechtlich nicht zulässig, da durch den Erziehungsauftrag von Schulgesetz und Schulverfassungsgesetz nicht gedeckt, sehen wir die Bekanntgabe der Noten aller oder einzelner Schüler anläßlich einer Elternversammlung an. Gleiches gilt, wenn den Eltern Listen mit Namen und Noten der Schüler übergeben werden.

Der Datenschutz im Unterricht hat auch noch eine weitergehende Dimension. Bereits früher[163] wiesen wir auf die Problematik bei Aufsätzen und Unterrichtsgesprächen hin. Nicht selten offenbaren die Kinder hier Informationen über ihre Familie und ihre Lebensumstände, die sehr viel Schutzwürdiges aus der Privatsphäre beinhalten. Hier sind die Lehrer gefordert, steuernd einzugreifen. In der konkreten Unterrichtsgestaltung hat der Lehrer den Widerspruch zwischen der einerseits von den Rahmenthemenplänen geforderten Entwicklung der Kommunikations- und Ausdrucksmöglichkeiten der Schüler und der auf der anderen Seite stehenden Verpflichtung zum Respektieren der Privatsphäre zu meistern. Daß sich hier Probleme mitunter nicht ausschließen lassen, ist offenkundig. Der Lehrer muß jedoch den Eltern die Gewähr dafür bieten, daß Informationen aus dem privaten Bereich, die durch ihre Kinder im Unterricht offenbart werden, von ihm mit hoher Sensibilität gegen eine Offenbarung an Dritte, also auch an andere Eltern, geschützt werden.

163 Jahresberichte 1983, 3.4; 1986, 4.4; 1992, 4.4

Leider, so mußten wir im vergangenen Jahr feststellen, bieten dem Anschein nach nicht alle für die Berliner Schulen zugelassenen Unterrichtsmittel die Gewähr dafür, daß keine weitgehenden Informationen aus dem Privatbereich der Familie in den Unterricht einfließen. Für bedenklich hielten wir insbesondere einen Fragebogen für den Englischunterricht. Es wurde nicht nur nach Name und Adresse des Schülers sowie für alle Schüler der Klasse nach Alter, Staatsangehörigkeit und Geschwisterzahl sondern auch nach den Eltern, Frühstücksgewohnheiten, der Wohnungsausstattung und bestehenden Freundschaften gefragt. Hier wird der Grundsatz der Erforderlichkeit bei der Verarbeitung personenbezogener Daten im Unterricht deutlich überschritten.

4.11 Soziales

Berliner Automatisiertes Sozialhilfe-Interaktions-System (BASIS)

Über die Weiterentwicklung des Projekts BASIS zur Automationsunterstützung der Sachbearbeitung bei der Gewährung von Sozialhilfe und wirtschaftlicher Hilfe für Jugendliche und über die datenschutzrechtlichen Auseinandersetzungen um dieses Projekt haben wir in den letzten Jahren immer wieder berichtet. Das Projekt wurde mittlerweile zügig weiterentwickelt und in den ersten Bezirken erprobungshalber eingeführt.

Die Auseinandersetzung über die Rechtsgrundlagen für einen bezirksübergreifenden Datenabgleich zur Erkennung von mißbräuchlichen, weil mehrfach in verschiedenen Bezirken gestellten Sozialhilfeanträgen ist inzwischen durch eine Änderung des Gesetzes zur Ausführung des Bundessozialhilfegesetzes (BSHG) beendet worden[164]. Damit wurde unserer Empfehlung gefolgt, die unbefriedigende Situation, die darin bestand, daß mit der Einfügung von § 117 in das BSHG zwar eine Rechtsgrundlage für den Datenabgleich zwischen Kommunen als Träger der Sozialhilfe geschaffen wurde, aber damit kein Datenaustausch zwischen den Bezirken begründet werden konnte, mit einer Änderung des Berliner Ausführungsgesetzes zu beenden. Nunmehr wurde festgelegt, daß § 117 Abs. 2 BSHG auch innerhalb des Landes Berlin für die Erhebung und Ermittlung der erforderlichen personenbezogenen Daten durch verschiedenene datenverarbeitende Stellen Anwendung findet, soweit diese an der Gewährung der Sozialhilfe beteiligt sind (§ 3 Gesetz zur Ausführung des Bundessozialhilfegesetzes). Dies setzt allerdings voraus, daß die Rechtsverordnung des Bundes zu § 117 BSHG zuvor erlassen wird.

Für die Planung und Umsetzung der technischen und organisatorischen Maßnahmen zum Datenschutz in den Bezirken hat die Projektgruppe BASIS eine „Checkliste Datenschutz und Datensicherheit" erarbeitet. Auf ihrer Grundlage sollen in den Bezirken Datenschutz- und Datensicherheitskonzepte entwickelt werden. Für das Bezirksamt Weißensee und für die Zentrale Sozialhilfestelle für Asylbewerber beim Landesamt für Zentrale Soziale Aufgaben wurden uns ausgefüllte Checklisten, die in Verbindung mit internen Regelungen das Datenschutz- und Datensicherheitskonzept bilden, vorgelegt.

Die Checklisten bilden ein geeignetes Instrument, um Sicherheitskonzepte für den Einsatz von BASIS zu entwickeln. Im Detail war jedoch einzuwenden, daß

- Maßnahmen zur *Kontrolle der Systemverwaltung* noch nicht berücksichtigt waren, obwohl die Befugnisfülle eines UNIX-Systemverwalters zu den wichtigsten Risikopotentialen solcher Systeme gehören;
- dem *Einsatz diskettenloser Arbeitsplatzrechner* nur eine geringe Priorität eingeräumt wurde;
- die *Datenträgerkontrolle* noch nicht detailliert geregelt war;
- die Regelungen für den *Paßwortwechsel* noch nicht präzisiert worden waren.

Weitere Empfehlungen betrafen die *Zugangskontrolle* bei den Akten und für den Serverraum und den Zugriff auf die Protokolldateien.

Die Projektgruppe BASIS der Senatsverwaltung für Soziales kündigte an, das Sicherheitsrisiko bei der Systemverwaltung nach den Vorgaben des Datenschutzkonzeptes für das Automatisierte Haushaltswesen beherrschbar zu machen[165]. Zu den übrigen Punkten wurde auf ein zu entwickelndes verfahrensübergreifendes Gesamtkonzept verwiesen, das vom Landesamt für Informationstechnik vorbereitet würde.

Wir hatten schon sehr frühzeitig gefordert, daß die Verarbeitung von Echtdaten in den Bezirken erst erfolgen sollte, wenn ein bezirksspezifisches Datenschutz- und Datensicherheitskonzept erarbeitet und umgesetzt wurde. In der Zwischenzeit wurde in verschiedenen Bezirken mit unterschiedlicher Intensität mit der Echtverarbeitung begonnen, ohne daß Datenschutz- und Datensicherheitskonzepte vorlagen.

Wir haben dies zum Anlaß genommen, in einem Bezirksamt eine erste datenschutzrechtliche Kontrolle durchzuführen, um ein Bild über das Datenschutzniveau bei der BASIS-Erprobung zu gewinnen, die noch vorhandenen Probleme zu erfassen und einen Anstoß zu geben, sich den Problemen des Datenschutzes und der informationstechnischen Sicherheit auch in den bezirklichen Projektgruppen zu stellen.

In dem Bezirksamt erfolgte bisher noch keine Direktverarbeitung bei der Sozialhilfeantragstellung, sondern erst die Erfassung der Altfälle, um den Umgang mit dem System zu erproben. Infolgedessen mußte ein Konzept noch nicht vorliegen, das auch die direkte Antragsbearbeitung betraf. Die Fertigstellung des Datenschutz- und Datensicherheitskonzeptes war für Ende 1994 vorgesehen.

Unter diesen Umständen erwartungsgemäß, trafen wir auf diverse Provisorien, die auf Dauer nicht akzeptierbar wären. So existierte noch kein gewidmeter Serverraum. Wenigstens war der Server aber in der ebenfalls zugangsgeschützten Telefonzentrale untergebracht.

Die Arbeitsplatzrechner sind mit Diskettenlaufwerken ausgestattet, weil bei der Ausschreibung noch nicht daran gedacht wurde, Systeme ohne Laufwerke zu beschaffen. Allerdings waren die Laufwerke durch programmtechnische Maßnahmen deaktiviert. Ob diese Maßnahme ausreichend wirksam ist, ist noch ungeklärt und bleibt einer weiteren Untersuchung vorbehalten.

Zur angesprochenen Problematik der Systemverwalterkontrolle beim UNIX-Server standen noch keine Lösungen zur Verfügung. Das auch von der Projektgruppe BASIS angestrebte Sicherheitsniveau entsprechend der Kategorie C 2 der amerikanischen Sicherheitskriterien (Orange Book) wurde mit der derzeit eingesetzten Betriebssystemversion noch nicht erreicht.

Sozialdaten und Strafverfolgung

Die datenschutzrechtlichen Bestimmungen des SGB X sind mit erheblicher Verzögerung an das BDSG 1990 angepaßt worden[166]. Dabei wurden auch inhaltliche Änderungen vorgenommen, zu denen eine Lockerung der strengen Vorschriften über die Übermittlung von Sozialdaten für Zwecke der Strafverfolgung gehören.

> *Ein Mitarbeiter eines Sozialamtes fragte, ob auf die Anfrage der Polizei Angaben über den Leistungsbezug von Vietnamesen übermittelt werden dürfen, die namentlich aufgelistet waren und unter dem Verdacht des Schwarzhandels standen. Die Vietnamesen hatten hohe Geldbeträge ins Ausland überwiesen; die Polizei wollte insbesondere wissen, ob diese Beträge als Einkommen angegeben worden waren.*

Nach § 73 SGB X in der Form der Neufassung vom 13. Juni 1994 wäre auf Grund einer richterlichen Anordnung die Übermittlung der erforderlichen Sozialdaten wegen der „erheblichen Bedeutung" der Straftaten möglich gewesen. Die richterliche Anordnung fehlte jedoch, so daß die Übermittlung auf Grund dieser Vorschrift nicht in Frage kam.

164 vgl. 1.2

165 vgl. 4.4
166 vgl. 1.1

Folgende rechtliche Überlegungen sind jedoch anzustellen: Die Übermittlung der Namensliste durch die Polizei an das Sozialamt war im Wege der Ermittlungstätigkeit der Polizei zulässig. Das Sozialamt konnte daraufhin bei den genannten Personen überprüfen, ob die gezahlten Sozialleistungen zu Recht erfolgt waren und ob die Vermögensverhältnisse zutreffend angegeben waren. Bei denjenigen Personen, bei denen Ungereimtheiten und unwahre Angaben festgestellt wurden, war das Amt befugt, von Amts wegen ein Ermittlungsverfahren einzuleiten. In diesem Fall enthält § 69 Abs. 1 Satz 2 SGB X auch eine Offenbarungsbefugnis, soweit die Übermittlung der Daten zur Durchführung eines mit der Erfüllung einer Aufgabe nach dem Sozialgesetzbuch zusammenhängenden Strafverfahrens erforderlich ist. Das Amt konnte nach eigenem Ermessen in dem Zusammenhang auch eine Strafanzeige wegen Unterstützungsbetruges stellen und dabei die von der Polizei erwünschten Angaben machen. Im Unterschied zu den Rechtswirkungen des § 73 steht bei § 69 SGB X die Datenermittlung und Datenübermittlung im Ermessen des Sozialamtes, wogegen bei der Erfüllung der richterlichen Anordnung nach § 73 dem Sozialamt kein Ermessen zusteht. Vielmehr muß es sich der richterlichen Anordnung fügen, soweit nicht prozeßrechtlich im Wege der Beschwerde Schritte unternommen werden können.

Die Problematik der Neufassung des § 73 SGB X zeigt folgender Fall:

Aus einem Bezirksamt wurde berichtet, daß in einem Beschluß des Amtsgerichts Tiergarten angeordnet wurde, die Diensträume zu durchsuchen und etwaige Beweismittel wegen eines zur Anzeige gebrachten sexuellen Mißbrauchs zu beschlagnahmen.

Von den Mitarbeitern der Jugendverwaltung wird zurecht darauf hingewiesen, daß das Vertrauensverhältnis zwischen den Jugendämtern und den Klienten dadurch gestört werden könnte, daß nach dem neuen Recht die klare Unterscheidung zwischen Verbrechen und Vergehen aufgehoben wurde. Minderschwere Fälle des Mißbrauchs oder der Mißhandlung, die früher als Vergehen und Antragsdelikt dem strafrechtlichen Zugriff aus familienfürsorglichen Gründen entzogen werden konnten, unterliegen nunmehr durch den erweiterten Begriff der Straftat von „erheblicher Bedeutung" der Ermessensentscheidung des erkennenden Gerichtes. Die moderne Jugendarbeit ist gerade in Berlin auf ausgleichende Konfliktstrategien ausgerichtet mit dem Ziel, im Rahmen der gesetzlichen Möglichkeiten der Hilfe für das Kind Vorrang einzuräumen vor dem staatlichen Strafverfolgungsanspruch. Die Veränderung der Rechtslage verschiebt den dafür zur Verfügung stehenden Spielraum zuungunsten der sozialpädagogischen Lösungen.

Gescheitert ist der Versuch, auch die Amtshilfevorschrift des § 68 SGB X aufzuweichen[167].

Kein Schutz für falsche Angaben

Aus der Bevölkerung der östlichen Bezirke erreichten uns wiederholt Anfragen über die Zulässigkeit und den Umfang der Vermögensermittlung durch Vorlage von Sparbüchern und Kontoauszügen. In einer größeren Aktion haben wir überprüft, inwieweit bei den Bezirksämtern die Vorlage von Sparbüchern im sozialen Leistungsverfahren (wirtschaftliche Hilfen) verlangt wird. Das Verfahren wird in allen Bezirksämtern im wesentlichen gleich gehandhabt.

Einen Grund zur Beanstandung hat es dabei nicht gegeben.

Es ist jedoch angebracht, nochmals darauf hinzuweisen, daß die Entscheidung, die Vorlage von Beweisurkunden zu verlangen, in einem angemessenen Verhältnis zu der in Anspruch genommenen Sozialleistung stehen muß (vgl. §§ 60 Abs. 1 Nr. 3, 65 Abs. 1 Nr. 1 SGB I). Dies ist nicht der Fall, wenn beispielsweise bei der Gewährung von laufenden Leistungen die monatliche Vorlage der Beweisunterlagen verlangt wird. Die Leistungsempfänger sollten darüber informiert werden, daß und welche gesetzlichen Regelungen greifen, um die Vermögenslage effizient zu überprüfen (z. B. § 117 BSHG und §§ 20, 21 SGB X). Hierdurch könnte den Antragstellern bewußt gemacht werden, welche Risiken sie eingehen, wenn sie unwahre Tatsachen vortragen. Dadurch wird das Verfahren für die Betroffenen berechenbarer und eine unnötige Kriminalisierung durch Fahrlässigkeit und Nachlässigkeit der betroffenen Antragsteller verhindert.

Ein Antragsteller auf Wohngeld machte zu den von ihm geleisteten Unterhaltszahlungen falsche Angaben. Er hatte nicht berücksichtigt, daß die geschiedene Ehefrau und ihre Kinder beim gleichen Amt zu versorgen waren und daß deswegen durch die gleiche Sachbearbeiterin die beiderseitigen Angaben verglichen werden konnten. Die Unterschrift für die angeblich geleisteten Unterhaltszahlungen war vom Antragsteller gefälscht, was durch einen Schriftvergleich von der Sachbearbeiterin ohne weiteres festgestellt werden konnte.

Auch hier gehörte die Verhinderung des Unterstützungsbetruges zu den Aufgaben des Amtes; die Verwendung und der Abgleich der Daten waren daher zulässig.

4.12 Stadtentwicklung und Umweltschutz

Neue Gesetze

Mitte 1994 wurde das Umweltinformationsgesetz[168] des Bundes verabschiedet. Damit entsprach der Bundesgesetzgeber seiner Pflicht, die EU-Richtlinie über den freien Zugang zu Informationen über die Umwelt in deutsches Recht umzusetzen. In diesem Gesetz wurden erstmals im Bundesrecht Informationsfreiheitsrechte der Bürger und Datenschutzansprüche zueinander ins Verhältnis gesetzt und ein Abwägungsprozedere gefunden. Zwar werden in diesem Gesetz die Ansprüche eines jeden auf freien Zugang zu Informationen über die Umwelt, die bei einer öffentlichen Stelle vorliegen, gewährleistet, sie unterliegen jedoch auch erheblichen Beschränkungen.

Informationen über die Umwelt, die personenbezogene Daten darstellen, dürfen dann offenbart werden, wenn dadurch schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden. Bei Informationen, die als Betriebs- oder Geschäftsgeheimnisse gekennzeichnet sind oder der Behörde vor dem 1. Januar 1993 zugegangen sind, ist der Betroffene vor der Offenbarung anzuhören. Entsprechend wurde auch die Gewerbeordnung geändert. Auch wenn nach Inkrafttreten des Gesetzes der von einigen befürchtete Ansturm von Informationsbegehrenden auf die Umweltbehörden offenbar ausblieb, scheint sich dieses Gesetz aus datenschutzrechtlicher Sicht in der Praxis jedoch zu bewähren. So bestand beispielsweise für die Erarbeitung eines Branchenkonzepts für einen bestimmten Industriebereich die Möglichkeit, Namen und Anschriften von Betrieben, Beschäftigte nach Größengruppen und Tätigkeitsfelder der Unternehmen zu übermitteln.

Inwieweit die von uns im Jahresbericht 1993 kritisierten und im Umweltinformationsgesetz nach wie vor vorhandenen Regelungsdefizite zum Tragen kommen, wird die Zukunft zeigen.

Der Berliner Gesetzgeber verabschiedete im Oktober das in den vergangenen Jahren schon mehrfach von uns angemahnte Gesetz über die *Datenverarbeitung für Zwecke der räumlichen Stadtentwicklung, Stadt- und Regionalplanung und bodenwirtschaftliche Aufgaben* (Stadtplanungsdatenverarbeitungsgesetz)[169]. Dieses Gesetz erlaubt eine normenklare Verarbeitung auch personenbezogener Daten für die mit Stadtplanungsaufgaben betrauten Behörden. Die Datenkataloge sind klar voneinander abgegrenzt, und Daten, die einen unmittelbaren Personenbezug erlauben, sind besonders geschützten Teilen der Dateien zugeordnet. Es bleibt abzuwarten, wie die Berliner Verwaltungen die Möglichkeiten, die der Gesetzgeber für automatisierte Abrufverfahren erlaubt, künftig für eine effektive Vernetzung nutzt. Daten, die nicht bereits nach vorangehenden Vorschriften gespeichert wurden, werden beim Betroffenen mit seiner Kenntnis erhoben. Eine Auskunftspflicht, die wir für einen unverhältnismäßigen Eingriff in das informationelle Selbstbestimmungsrecht hielten, wurde in das Gesetz nicht aufgenommen.

167 vgl. 1.1

168 BGBl. I, 490

169 GVBl. 1994, 444

Auch die *Verordnung über die Verarbeitung von personenbezogenen Daten im Zusammenhang mit nicht genehmigungsbedürftigen Anlagen*[170] ist zwischenzeitlich erlassen worden. Damit wird den Bezirksämtern auch für bereits erhobene Daten eine rechtliche Grundlage gegeben, und die Datenübermittlung an die Umweltverwaltung zur Erstellung des Emissionskatasters ist zulässig.

Auch 1994 wurde noch kein Entwurf eines *Bodenschutzgesetzes* ins Abgeordnetenhaus eingebracht. Überfällig ist des weiteren die vorbereitete 8. Änderung der *Wassergesetze* sowie des Gesetzes über Maßnahmen der *Gewässeraufsicht und -überwachung*. Beide Gesetzesvorhaben wurden bereits im Jahresbericht 1993 angemahnt.

Auftragsdatenverarbeitung beim FNP

Im Zusammenhang mit der Erarbeitung des ersten Gesamtberliner Flächennutzungsplanes stand die Aufgabe, Zehntausende von Vorschlägen der Bürger zu prüfen. Die Senatsverwaltung für Stadtentwicklung und Umweltschutz beauftragte eine private Firma, die technische Seite der Datenverarbeitung durchzuführen.

In einem Zeitraum des massenhaften Eingangs derartiger Einwendungen prüften wir vor Ort den Umgang mit diesen Daten und stellten keine gravierenden Mängel fest. Als wir im Nachgang allerdings die vertragliche Grundlage dieser Datenverarbeitung im Auftrag überprüften, traten Mängel zutage. Es existierte kein den Anforderungen des § 3 BlnDSG entsprechender Vertrag. Es war lediglich ein Auftragsformular vorhanden, in dem als einzige datenschutzrechtliche Regelung der Auftragnehmer verpflichtet wurde, über alle ihm und seinen Mitarbeitern bekanntgewordenen Angelegenheiten Stillschweigen zu bewahren. Es fehlte eine Verpflichtung des Auftragnehmers, die Vorschriften des Berliner Datenschutzgesetzes zu befolgen und sich der Kontrolle des Berliner Datenschutzbeauftragten zu unterwerfen.

Lärm und Datenschutz

Wird ein Bürger in seiner Nachtruhe durch Lärm massiv gestört, so greift er mitunter zum Telefon und bittet die Polizei, die Ruhe wieder herzustellen. Auch dies ist eine Aufgabe der Polizei zur Gefahrenabwehr im Wege ihrer Eilzuständigkeit. Die sachliche Zuständigkeit liegt hingegen beim jeweiligen Bezirksamt (Amt für Gesundheit und Umweltschutz). Nachdem die Polizei tätig geworden ist, übergibt sie das Verfahren dem jeweiligen Umweltamt. Damit ist das polizeiliche Verfahren abgeschlossen.

In der Vergangenheit hatte sich die Praxis herausgebildet, der Polizei eine Rückmeldung über den Abschluß des Ordnungswidrigkeitsverfahrens, insbesondere in der Form der Durchschrift von Bußgeldbescheiden, zu übersenden. Dies ist nicht erforderlich. Eine einfache Rückmeldung „Verfahren abgeschlossen" durch die Bezirksämter wäre völlig ausreichend, damit die Polizei den bei ihr angelegten Vorgang vernichten kann. Da für die bisherige Praxis keine Rechtsgrundlage erkennbar war, wurde sie zwischenzeitlich eingestellt. In ähnlicher Weise wurden bislang erteilte Ausnahmegenehmigungen nach der Lärmverordnung ohne Einwilligung der Betroffenen pauschal der Polizei übermittelt. Auch hier wurde eine Änderung erwirkt: Im Rahmen der Anhörung wird der Antragsteller darauf hingewiesen, daß dem Polizeipräsidenten die Ausnahmegenehmigung übermittelt wird, wenn der Betroffene nicht widerspricht.

4.13 Verkehr und Betriebe

Verkehr ...

Die Bundesregierung hat den Entwurf eines *Gesetzes zur Änderung des Fahrlehrergesetzes und anderer Gesetze* vorgelegt[171]. Bei der Vorlage handelte es sich um den ersten Teil des Referentenentwurfes eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze, über den wir in unserem Jahresbericht 1993[172] berichtet hatten. Die Umsetzung des damaligen Referentenentwurfes soll jetzt in zwei Abschnitten erfolgen. Es ist vorgesehen, in der ersten Stufe das Fahrlehrerrecht zu ändern. In der zweiten Stufe soll dann die Novellierung der Führerscheinregelung, einschließlich der Einführung eines Zentralen Fahrerlaubnisregisters, die Novellierung der Vorschriften über das Verkehrszentralregister und das Punktesystem erfolgen.

Der von der Bundesregierung vorgelegte Entwurf enthält auch Änderungen des Straßenverkehrsgesetzes. So ist die Erhebung von Gebühren für Auskünfte aus dem Verkehrszentralregister vorgesehen, auch wenn ein Bürger Auskunft über die zu seiner Person gespeicherten Daten verlangt. Damit wird von dem Grundsatz der Gebührenfreiheit für Auskünfte über eigene Daten, wie sie § 19 Abs. 7 BDSG vorschreibt, abgewichen. Es ist nicht abzeptabel, daß die Wahrnehmung des aus dem Grundrecht auf informationelle Selbstbestimmung folgenden Auskunftsanspruchs[173] von der Zahlung einer Gebühr abhängig gemacht wird.

Abzuwarten bleibt, wann die Bundesregierung den Entwurf eines Gesetzes zur Regelung des *Zentralen Fahrerlaubnisregisters* vorlegt.

Die Senatsverwaltung für Verkehr und Betriebe schloß einen Gestattungsvertrag mit der Münchener Co-Pilot GmbH & Co. KG für ein *elektronisches Verkehrsleit- und Informationssystem* ab, mit dessen Hilfe der Autofahrer staufrei sein Ziel erreichen soll.

Dafür werden an ca. 500 Stellen – verteilt über das gesamte Stadtgebiet und am Autobahnring – sogenannte Baken installiert. Das *bakengestützte Leitsystem* verfügt über ein eigenständiges Rechnersystem, das nicht mit dem Berliner Verkehrszentralrechner vernetzt ist. Allerdings ist vorgesehen, Mittelwerte von Verkehrsdaten, die bei den Gebietsrechnern für Lichtsignalanlagen anfallen, in das System einzuspeisen und dort für Leitempfehlungen zu nutzen.

Eine Fahrt mit dem Verkehrsleitsystem beginnt mit der Eingabe eines Zieles. Das individuelle Leiten setzt beim Passieren der ersten im Straßennetz vorhandenen Bake ein. Im Fahrzeuggerät wird eine neue, zufällige und temporäre Identifikation erzeugt, mit deren Hilfe eine Verknüpfung aller Einzelnachrichten („Telegramme") dieses Fahrzeuges für die aktuelle Fahrt im Leitrechner ermöglicht werden soll. Diese Identifikation bleibt bis zum Ende der jeweiligen Fahrt gültig und unverändert. Nach Beendigung der Fahrt sind die während der Fahrt empfangenen Telegramme einem bestimmten Fahrzeug nicht mehr zuzuordnen. Die Kennzahl für die Identifikation wird mittels eines Zufallsgenerators ermittelt. Sobald ein neues Fahrziel im Bordgerät des Fahrzeuges eingegeben wird, erfolgt ein neuer Start des Zufallsgenerators. Die Fahrt erfolgt dann unter einer neuen, zufallsbedingten Kennzahl. Der Benutzer kann das System jederzeit vor, während oder nach der Fahrt ein- oder ausschalten.

Das System ist schon einmal in einer Testphase Ende der 80er Jahre erprobt worden. Die Testphase war damals mit uns abgestimmt worden. Gegen die jetzt gewählte Konzeption haben wir keine datenschutzrechtlichen Bedenken.

... und Betriebe

Am 17. Juni 1993 war das *Eigenbetriebsreformgesetz* verabschiedet worden. Damit sind ab 1. Januar 1994 die bisherigen Eigenbetriebe BEHALA, BSR, BVG und BWB in rechtlich selbständige, landesunmittelbare Anstalten öffentlichen Rechts umgewandelt worden. Nach § 19 Abs. 1 Berliner Betriebegesetz dürfen diese Anstalten personenbezogene Daten verarbeiten, soweit dies für die Erfüllung ihrer satzungsgemäßen Aufgaben sowie zur Verfolgung ihrer und zur Abwehr fremder Forderungen erforderlich ist. Nach Absatz 2 sollte dabei Näheres durch Rechtsverordnung geregelt werden. Diese Rechtsverordnung ist am 30. Juni 1994 in Kraft getreten.

170 GVBl. 1994, 464
171 BT-Drs 12/3251
172 Jahresbericht 1993, 4.11
173 vgl. Jahresbericht 1993, 3.1

Von besonderem Interesse sind die Vorschriften für die BVG. Danach darf die BVG folgende personenbezogene Daten von Fahrgästen, die ohne gültigen Fahrausweis angetroffen werden, verarbeiten: Name, Geburtsdatum und -ort, Geschlecht, Anschrift, Name und Anschrift gesetzlicher Vertreter, Zeit, Ort und sonstige für die Rechtsverfolgung erhebliche Umstände des Vorfalls. Darüber hinaus ist die BVG berechtigt, diese Daten zur Wahrnehmung ihrer Rechte an Dritte, insbesondere an die Strafverfolgungsbehörden und an Inkassofirmen weiterzugeben. Die Daten werden spätestens zwei Jahre nach dem letzten Vorfall gelöscht.

Mehrere Petenten verfügten über einen gültigen Fahrausweis, konnten diesen jedoch bei der Kontrolle nicht vollständig vorlegen. So wurde zum Beispiel eine Schülerin, die zwar im Besitz einer gültigen Schülermonatskarte war, jedoch den Schülerausweis vergessen hatte, erfaßt, da nach III Ziffer 3 der Tarifbestimmungen der BVG i. V. m. § 8 Abs. 3 der gemeinsamen Beförderungsbedingungen der Verkehrsgemeinschaft Berlin-Brandenburg (VBB) nur bei Vorlage beider Legitimationspapiere ein gültiger Fahrausweis vorliegt.

In einem anderen Fall war auf einer Seniorenkarte das Gültigkeitsdatum aufgrund eines Mitverschuldens der BVG nicht lesbar. Die personenbezogenen Daten des Petenten wurden dennoch gespeichert, da auch hier gem. IV der Tarifbestimmungen i. V. m. § 8 Abs. 1 Nr. 1 bzw. 3 der Fahrausweis nicht anerkannt wurde, obwohl sich der Petent anhand der beigebrachten Unterlagen als rechtmäßiger Inhaber des Fahrausweises legitimieren konnte.

Dieses Vorgehen der BVG verstieß gegen die Bestimmungen des Berliner Datenschutzgesetzes. Zwar findet sich eine Befugnisnorm in § 19 Abs. 1 Berliner Betriebegesetz i. V. m. der genannten Rechtsverordnung, nicht dagegen eine Legaldefinition, wann ein gültiger Fahrausweis vorliegt. Diese Klarstellung findet sich erst in den Tarifbestimmungen der BVG, die jedoch keine Gesetzesqualität genießen.

Tarifbestimmungen, die eine Speicherung der Daten von Fahrgästen zulassen, obwohl sich diese nachweisbar im Besitz eines gültigen, nicht übertragbaren Fahrausweises befinden, den Berechtigungsnachweis für einen vorgezeigten Fahrschein nicht nachweisen können, dies aber fristgemäß nachholen, sind rechtswidrig: Es mangelt an der Erforderlichkeit der Datenspeicherung, die eine zwingende Voraussetzung für jegliche Art der Datenverarbeitung darstellt.

Die BVG wird auf Grund unserer Intervention diese und ähnlich gelagerten Fälle zukünftig nicht mehr speichern und die Daten der in diesem Zusammenhang erfaßten Personen aus dem Speicher löschen.

4.14 Wirtschaft und Technologie

Am Ende doch Novellierung der Gewerbeordnung

Das Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften wurde verabschiedet.[173a] Mit dieser Gesetzesänderung werden endlich datenschutzrechtliche Vorschriften in die Gewerbeordnung aufgenommen. Die bisherigen Vorschriften stellten keine ausreichende Rechtsgrundlage für die Datenverarbeitung der Gewerbeämter dar. Es gab nur wenige Normen, die datenschutzrechtliche Regelungen enthielten – wie beispielsweise die Regelungen zum Gewerbezentralregister in den §§ 149 ff. Gewerbeordnung (GewO).

In § 11 GewO sind Regelungen zur Datenerhebung, Datenübermittlung, Sperrung, Löschung und Nutzung enthalten. Der Grundsatz, daß Daten in erster Linie beim Betroffenen selbst zu erheben sind und nur in gesetzlich geregelten Fällen bei anderen Stellen erhoben werden dürfen[174], ist hier übernommen worden. Von großer Bedeutung sind die Datenübermittlungsregelungen bei den anzeigepflichtigen Gewerben in der Neufassung des § 14 GewO. Hier werden differenzierte Regelungen zur Datenübermittlung getroffen, die insbesondere auch die regelmäßig stattfindenden Datenübermittlungen bei *Gewerbeanzeigen* an die Industrie- und Handelskammer, die Handwerkskammer, die für den Immissionsschutz zuständigen Behörden und andere benannte Stellen auf eine rechtliche Grundlage stellt. Von Bedeutung ist auch die Ergänzung des § 35 Abs. 4 GewO, d. h. die Regelung der *Gewerbeuntersagung bei Unzuverlässigkeit.* Durch eine Ergänzung der Norm ist jetzt sichergestellt worden, daß bei der Anhörung von Aufsichtsbehörden, der IHK oder eines Prüfungsverbandes in Untersagungsverfahren wegen Unzuverlässigkeit nur die zur Abgabe einer Stellungnahme erforderlichen Unterlagen übersandt werden dürfen. Damit wird der üblichen Praxis, den gesamten Vorgang zu übersenden, ein datenschutzrechtlicher Riegel vorgeschoben.

Bei den Vorschriften zum *Gewerbezentralregister* wird mit § 150 b GewO eine Regelung für die *wissenschaftliche Forschung* getroffen. Hier wurde die beabsichtigte Regelung des § 42 Bundeszentralregistergesetz (BZRG) übernommen. Eine Auskunft aus dem Register zu Forschungszwecken ist danach nur dann zulässig, wenn das Interesse an der Forschungsarbeit das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Auskunft erheblich überwiegt. Wenn es möglich ist, soll die Auskunft zudem in anonymisierter Form erteilt werden.

Ein Wermutstropfen ist die Regelung über das Inkrafttreten des Gesetzes. § 11 GewO sowie die Änderungen der §§ 35, 150 b GewO werden drei Monate nach der Verkündung des Gesetzes in Kraft treten. Dagegen wird der geänderte § 14 GewO erst 13 Monate nach Verkündung in Kraft treten, ebenso die Änderungen des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern.

Die verlorengegangenen Gewerbeakten

Bei der Renovierung der neu angemieteten Räume eines Radiosenders machten Handwerker einen Fund: In unverschlossenen Schränken und einigen Umzugskartons fanden sie ca. 200 recht alte Gewerbeakten. Die Akten enthielten sensible personenbezogene Daten wie Gaststättenerlaubnisse, Mietverträge oder Strafregisterauszüge. Die Akten stammten aus den 40er, 50er, 60er und 70er Jahren. Die meisten Akten waren in den 60er Jahren abgeschlossen worden.

Nach § 17 Abs. 3 BlnDSG sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die datenverarbeitende Stelle zur rechtmäßigen Erfüllung der ihr übertragenen Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Die Akten waren zur Aufgabenerfüllung des Gewerbeamtes nicht mehr erforderlich. Auch die internen Aufbewahrungsfristen des Gewerbeamtes waren längst überschritten. Zur Kontrolle der Aufbewahrungsfristen sieht § 86 Abs. 3 Gemeinsame Geschäftsordnung der Berliner Verwaltung (GGO I) eine regelmäßige Kontrolle der Aufbewahrungsfristen und nach § 86 Abs. 1 Satz 1 GGO I die Führung eines Aktenverzeichnisses vor. Diese regelmäßige Aktenkontrolle hatte nicht stattgefunden.

IHK und Steuerdaten

Zahlreiche Gewerbetreibende erhielten in diesem Jahr einen Beitragsbemessungsbescheid der IHK, der einen deutlich höheren Beitrag als in den vergangenen Jahren auswies. Sie stellten bei genauerem Hinsehen fest, daß der Beitrag sich auf Steuerdaten bezog, die sie gegenüber der Industrie- und Handelskammer nicht angegeben hatten. Für viele stellte sich daher die Frage, ob die IHK auf dem Steuergeheimnis unterliegende Steuerdaten für die Beitragsbemessung zurückgreifen darf.

Die IHK ist berechtigt, zur Festsetzung der Kammerbeiträge die erforderlichen Bemessungsgrundlagen bei den Finanzämtern zu erheben. Als Bemessungsgrundlage für den Mitgliedsbeitrag dient nach § 3 Abs. 3 Satz 3 Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHK-G) der Gewerbeertrag nach dem Gewerbesteuergesetz oder der nach dem Einkommensteuer- oder Körperschaftsteuergesetz ermittelte Gewinn aus dem Gewerbebetrieb. Die IHK kann diese Daten zur

173a BGBl. I, 3475, vgl. 1.1

174 vgl. § 10 Abs. 1 und Abs. 3 BlnDSG

Berechnung des Kammerbeitrages entweder nach § 9 Abs. 2 IHK-G bei den Finanzbehörden erheben oder nach § 3 Abs. 3 Satz 5 IHK-G die Kammermitglieder um Auskunft ersuchen. Die IHK ist sogar berechtigt, Geschäftsunterlagen einzusehen, die sich auf Grundlagen beziehen, die der Festsetzung des Kammerbeitrages dienen.

Auf der anderen Seite sind die Finanzbehörden nach § 31 Abgabenordnung (AO) berechtigt, Besteuerungsgrundlagen und Steuermeßbeträge Körperschaften des öffentlichen Rechts – und dazu zählt auch die IHK – mitzuteilen, sofern sie zur Festsetzung solcher Abgaben dienen, die an diese Besteuerungsgrundlagen anknüpfen.

Zwar waren auf den Beitragsbescheiden der IHK einige Rechtsgrundlagen angegeben, es fehlten jedoch die Rechtsgrundlagen der für die Bürger ja besonders gravierenden Erhebung der Steuerdaten.

4.15 Wissenschaft und Forschung

Bummelstudenten werden zur Kasse gebeten

Unter dieser und ähnlichen Schlagzeilen wies die Presse Ende 1993 auf eine beabsichtigte Änderung des Berliner Hochschulgesetzes hin. Die schließlich vom Abgeordnetenhaus beschlossene Gesetzesänderung beinhaltete jedoch keine an die Überschreitung der Regelstudienzeiten gebundenen erhöhten Studiengebühren, sondern verpflichtete die Hochschulen, ein System von Pflichtberatungen aufzubauen. Daraufhin erließ der Akademische Senat der Freien Universität im Januar 1994 eine Satzung für Studienangelegenheiten. Sie verpflichtete die Studenten, an bestimmten besonderen Prüfungsberatungen teilzunehmen. Für das Wintersemester 1994/1995 wurden 15 500 „Langzeitstudenten", also Studenten, die die gesetzlich vorgeschriebene Regelstudienzeit um mehr als zwei Semester überschritten haben, zu einer obligatorischen Prüfungsberatung aufgefordert.

Dieses Beratungsverfahren ist durch die Änderung des Hochschulgesetzes und die ergänzenden Regelungen in der Satzung zum Bestandteil des Rückmeldeverfahrens geworden. Die Prüfungsberatungen wurden durch „prüfungsberechtigte Hochschulangehörige", in der Regel also durch Professorinnen und Professoren, durchgeführt. Die als Nachweis für die durchgeführte Prüfungsberatung vom Prüfungsberechtigten und vom Dekan auszustellende Bescheinigung ist, was die Pflichtangaben betrifft, ausschließlich auf den Nachweis von Studien- und Prüfungsleistungen beschränkt. Zwei Zeilen sind für freiwillige Angaben des Studierenden vorgesehen, auf denen er auf persönliche, den Studienablauf beeinträchtigende Umstände verweisen kann. Die von uns geprüften Unterlagen deuteten auf eine sparsame, lediglich den Nachweis des stattgefundenen Gesprächs vermerkende Datenerhebung hin. Inhalt und Dauer des Gesprächs wurden nicht dokumentiert. Generell wiesen die Unterlagen sowohl auf einen datenschutzgerechten Umgang der beratenden Professorinnen und Professoren mit den personenbezogenen Daten als auch auf ein großzügiges Herangehen an die Problematik hin. Dazu wird auch beigetragen haben, daß die Studenten ihre Berater selbst wählen durften bzw. diese ihnen durch eine Buchstabenzuordnung zugewiesen wurden. Selbst bei einer Zuweisung war die Wahl eines anderen Beraters nicht ausgeschlossen.

Nach erfolgter Beratung und anschließender Rückmeldung wurden die Unterlagen an die Studenten verschickt. Die Beratungsnachweise wurden anschließend, wenn sich nicht durch den Abschluß des Studiums oder eine Exmatrikulation auf eigenen Wunsch die nach Jahresfrist vorgeschriebene erneute Prüfungsberatung erübrigt, an die Fachbereiche zurückgesandt. Hier werden diese Nachweise als Grundlage für die nach einem Jahr zu wiederholende Prüfungsberatung verwahrt. Gegenstand dieser erneuten Beratungen, die erstmals zum Wintersemester 1995/1996 einsetzen werden, ist dann der Nachweis eines Studienfortschritts des Studenten. Dann ist eine Exmatrikulation von Amts wegen vorgesehen, wenn durch den Studierenden weder ein Studienfortschritt noch persönliche einen Studienfortschritt behindernde Gründe nachgewiesen werden. Wir werden auch dieses Verfahren datenschutzrechtlich überprüfen.

Studentendaten

Die *Technische Universität* hat entsprechend den Anforderungen des Berliner Hochschulgesetzes den Entwurf einer *Rahmenordnung über die Diplom- und Magisterprüfungen* vorgelegt. Der behördliche Datenschutzbeauftragte wurde frühzeitig einbezogen, so daß der vorliegende Entwurf eine aus unserer Sicht vorbildliche Datenschutzregelung zum Umgang mit Prüfungsakten enthält. Darin werden zunächst die Datenverarbeitungsbefugnis der Prüfungsausschüsse, darüber hinaus aber auch Löschungsfristen und Einsichtsrechte geregelt. Überdies wird der Forderung nach einer anonymisierten Geschäftsstatistik entsprochen.

Ein Hinweis war Anlaß für uns, die *Promotionsordnungen* der Berliner Universitäten und der Hochschule der Künste hinsichtlich ihrer Befugnisse zum Erheben personenbezogener Daten zu überprüfen. Dabei stellten wir zum Teil erhebliche Unterschiede beim Umfang der zu erhebenden Daten fest. Auch der Zeitpunkt, zu dem diese Daten erhoben werden, differierte stark. So waren in einigen Fällen die Erhebungen an den Zulassungsantrag, in anderen wieder an die einzureichende Dissertation sowie mitunter auch an beide Zeitpunkte gebunden. Wir baten die Hochschulen, die Erforderlichkeit zu überprüfen. Für unverhältnismäßig halten wir es, den Lebenslauf zu einem festen und damit unbegrenzt öffentlich zugänglichen Bestandteil der Dissertation zu machen sowie allgemeine, nicht auf den wissenschaftlichen Werdegang zielende Lebensläufe und Lichtbilder zu verlangen. Wir gehen davon aus, daß die in den Promotionsordnungen festgelegten Datenerhebungen fallweise mit anderweitig anstehenden Änderungen der Promotionsordnungen bereinigt und vereinheitlicht werden können.

Polizei in der Hochschule

Mitunter wenden sich Polizeibehörden an Hochschulen und bitten diese im Rahmen von strafrechtlichen Ermittlungsverfahren um Auskünfte zu einer bestimmten Person. Zu solchen Auskünften an die Polizei ist die Hochschule *berechtigt*, soweit sie der Auffassung ist, daß die verlangten Informationen zur Durchführung des Ermittlungsverfahrens erforderlich sind. *Verpflichtet* zur Auskunftserteilung ist die Hochschule aber nur gegenüber der Staatsanwaltschaft bzw. den in ihrem Auftrag handelnden Polizeibeamten.

In einem Fall verlangte die Staatsanwaltschaft von einer Hochschule, die Daten aller Studenten aufzuliefern, auf die ein bestimmtes Geburtsjahr, ein bestimmtes Studienfach und ein Bezirk in Berlin zutreffen. Die Universität hat festgestellt, daß diese Merkmale nicht auf eine Person, sondern eine große Zahl von Personen zutreffen. Ein solches Ansinnen bezieht sich jedoch nicht auf eine Auskunftserteilung im Einzelfall, sondern auf eine Rasterfahndung nach § 98 a der Strafprozeßordnung, die einer richterlichen Anordnung, zumindest aber einer schriftlichen Anordnung der Staatsanwaltschaft bei Gefahr im Verzuge und anschließender richterlicher Bestätigung bedarf. § 98 a Strafprozeßordnung ist auch dann anwendbar, wenn eine datenverarbeitende Stelle anhand von Merkmalen, welche die Polizei oder die Staatsanwaltschaft liefern, auf Grund einer maschinellen Recherche in den eigenen Datenbeständen Informationen zur Übergabe an die Staatsanwaltschaft finden soll.

Forschung

Einen erheblichen zeitlichen Aufwand erforderte von unserer Dienststelle im vergangenen Jahr wiederum die Beratung von Forschern. Aus diesem Grunde hielten wir es für notwendig, zum *Datenschutz in Wissenschaft und Forschung*[175] erneut eine eigene Veröffentlichung herauszugeben. Mit diesem Heft sollen den Forschern Wege aufgezeigt werden, wie die Kollision der Grundrechte Forschungsfreiheit und informationelle Selbstbestimmung auf dem Wege der praktischen Konkordanz überwunden werden kann. Nicht selten hängt der Erfolg eines wissenschaftlichen Forschungsvorhabens davon ab, wie es dem Forscher gelingt, den „Beforschten" als Partner zu sehen und einzubeziehen. Auch wenn das einzelne Forschungsvorhaben nicht auf anonymisierte Daten oder die Einwilligung des Betroffenen gestützt

175 vgl. die vorgesehene Checkliste zum Datenschutz bei Forschung und Planung

werden kann, sind unter bestimmten Bedingungen gesetzlich fixierte Forschungsklauseln (auch Forschungsprivilegien genannt) anwendbar.

Einen Schwerpunkt unserer Beratung bildete die *Forschung in der Schule.* Nach den Datenschutzregelungen im Schulgesetz bedarf es hier der Einwilligung der Erziehungsberechtigten bzw. volljährigen Schüler und der Genehmigung durch die Senatsschulverwaltung. Im Rahmen des Genehmigungsverfahrens wurden wir frühzeitig eingeschaltet; die Erhebungen konnten von den Wissenschaftlern weitgehend ohne Probleme durchgeführt werden. Seitens der Eltern trifft dieses Verfahren auf breite Zustimmung.

Ein Viertel der Schülerbefragungen hatte die Gewaltproblematik zum Gegenstand. Eine Schwierigkeit dieser Untersuchungen bestand darin, solche Fragestellungen zu finden, mit denen die Schüler sich bei richtiger Beantwortung nicht einer Straftat bezichtigen. Eine wesentliche Voraussetzung für die Akzeptanz ist eine konsequente und für die betroffenen Schüler wie auch für die Eltern nachvollziehbare Anonymisierung. Um dies zu sichern, nahmen die Lehrer die Einwilligungserklärungen der Eltern entgegen und verwahrten diese für einen bestimmten Zeitraum. Die Lehrer stellten sicher, daß nur Kinder und Jugendliche an den Befragungen teilnahmen, deren Eltern ihre Einwilligung gegeben hatten. Die Wissenschaftler erhoben nachfolgend die Daten unmittelbar bei den Kindern und Jugendlichen in Abwesenheit der Lehrer. Damit war schon zum Zeitpunkt der Erhebung eine weitgehende Anonymisierung gegeben, die durch die Wissenschaftler in der nachfolgenden Aufbereitung verstärkt wurde.

Von den etwa 70 im vergangen Jahr beratenen Forschungsvorhaben entfiel neben dem Drittel Schulforschung ein weiteres Drittel auf den Bereich Gesundheit. Darüber hinaus ging es vor allem um zeitgeschichtliche und historische Forschungen sowie um Untersuchungen zur Stadtentwicklung und sozialen Struktur. Als besonders schwierig erwiesen sich Forschungsvorhaben, die entweder zu Beginn der Untersuchungen ohne Einwilligung oder gänzlich ohne diese durchgeführt werden mußten. Neben der Beratung der Forscher war es notwendig, mit der betreffenden Behörde, deren Daten ohne Einwilligung der Betroffenen zu Forschungszwecken verwendet werden sollten, eng zusammenzuarbeiten. Es galt, ein Prozedere zu finden, das den mildesten Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen darstellt. So konnte beispielsweise im Auftrag der Senatsverwaltung für Soziales eine Evaluationsstudie zur *Wirksamkeit der Maßnahmen der „Hilfe zur Arbeit"* des gesamten im Jahre 1989 betroffenen Personenkreises durchgeführt werden. Über die Ergebnisse wurde in der Presse berichtet. Ähnlich schwierig gestaltete sich ein Forschungsvorhaben, das die staatlichen *Unterstützungsmaßnahmen für aussteigewillige Prostituierte* untersucht.

Bei den bisher erwähnten wissenschaftlichen Vorhaben stand ein von Anfang an klar bestimmter wissenschaftlicher Zweck im Vordergrund. Anders ist die Situation, wenn im Vorfeld der eigentlichen wissenschaftlichen Forschung zunächst „nur" *Register* bestimmter Personengruppen aufgebaut werden sollen. Im Unterschied zum Krebsregister sollen diese Daten mit Einwilligung der Betroffenen vorgehalten werden. Hier müssen jedoch die Einwilligungserklärungen den Betroffenen eine hinreichende Absicherung gegen mißbräuchliche Nutzungen gewährleisten sowie Widerspruchsrechte einräumen.

In Vorbereitung befinden sich gegenwärtig in Berlin ein *Nierenbehandlungsregister,* ein *Register der Lippen-, Kiefer- und Gaumenspaltenpatienten* und ein *Zentralregister für kindliche Hörstörungen.* Überdies soll durch anonymisierte Datenübermittlung eine retrospektive Datenbank mit den genetischen Daten von nach der Tschernobylkatastrophe aufgetretenen *Chromosomenanomalien* (Trisomie 21/Mongolismus) entstehen. Hierfür sollen weitgehend anonymisierte Daten der Gesundheitseinrichtungen übermittelt werden. Ähnlich ist auch die nach dem „Mainzer Modell" vorgesehene Erfassung von *Fehlbildungen bei Neugeborenen.* In beiden Fällen sollen die Datensätze jedoch entweder nachträglich um die vollständige alte (vierstellige) Postleitzahl ergänzt werden oder von vornherein die vollständige neue (fünfstellige) Postleitzahl enthalten. Schon vor Einführung der neuen Postleitzahl hatten wir eine räumliche Zuordnung von Datensätzen (ohne Namen und Anschrift) nur durch die erste Ziffer der alten Postleitzahl für zulässig gehalten, um eine Reidentifizierung weitgehend auszuschalten. Um so problematischer ist die Verwendung der gegenwärtigen fünfstelligen Postleitzahlen, als diese mitunter nur für wenige Einwohner zutreffen. In einer Untersuchung durch das Statistische Landesamt wurde festgestellt, daß zwar in Hellersdorf unter einer Postleitzahl fast 50 000 Einwohner leben, jedoch unter einer anderen Berliner Postleitzahl weniger als 150 Personen melderechtlich registriert sind. Damit bieten die neuen Postleitzahlen in keiner Weise eine hinreichende Sicherheit, eine Deanonymisierung auszuschließen. Dies gilt insbesondere, wenn andere Daten wie Geburtsdatum, Geschlecht und gesundheitliche Besonderheiten zusätzlich gespeichert sind. Lediglich eine um die letzten drei Ziffern gekürzte Postleitzahl würde damit Bedingungen einer faktischen Anonymisierung entsprechen.

5. Telekommunikation und Medien

5.1 Telekommunikation in Deutschland und Europa

Postreform II - Gesetz zur Neuordnung des Postwesens und der Telekommunikation

Der Bundestag hat im September 1994 das *Gesetz zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz -PTNeuOG*[176]) beschlossen, das neben den Weichenstellungen für die Umwandlung der Deutschen Bundespost in drei Aktiengesellschaften auch zahlreiche Änderungen des materiellen Datenschutzrechts im Bereich der Telekommunikation enthält. Das Gesetz ist am 1. Januar 1995 in Kraft getreten. Zu den aus Datenschutzsicht wichtigsten Änderungen zählen insbesondere folgende:

Nach Art. 13 § 1 Nr. 3 PTNeuOG tritt das Postverfassungsgesetz zum 1. Januar 1995 außer Kraft. Damit entfällt insbesondere die Verordnungsermächtigung aus § 30 Abs. 2 Postverfassungsgesetz, auf Grund deren die *TELEKOM-Datenschutzverordnung (TDSV) und die Teledienstunternehmen-Datenschutzverordnung (UDSV),* die gegenwärtig den Datenschutz in diesem Bereich regeln, erlassen worden sind. Gleichzeitig ermächtigt das Gesetz über die Regulierung der Telekommunikation des Postwesens (PTRegG, Art. 7 PTNeuOG) in § 10 die Bundesregierung, eine entsprechende Rechtsverordnung zum Schutz personenbezogener Daten der am Fernmeldeverkehr oder am Postverkehr Beteiligten zu erlassen, welche die Erhebung, Verarbeitung und Nutzung dieser Daten regelt. Eine solche Rechtsverordnung, die der Zustimmung des Regulierungsrates und damit auch der Bundesländer bedarf, steht noch aus.

Für die Übergangszeit gelten die Regelungen von TDSV und UDSV mit den im Fangschaltungsbeschluß des Bundesverfassungsgerichts[177] getroffenen Einschränkungen fort.

Der Gesetzgeber hat in § 10 PTRegG gleichzeitig versucht, die Konsequenzen aus dem Fangschaltungsbeschluß zu ziehen, und Vorgaben für den Inhalt der zu erlassenen Rechtsverordnung im Gesetz formuliert.

Es ist leider nicht gelungen, im Rahmen der Postreform II eine wesentliche Verbesserung des Datenschutzes in der Telekommunikation zu erreichen. Teilweise bewirkt das Postneuordnungsgesetz sogar eine Verschlechterung der Positionen der Betroffenen.

So ist die dringend *notwendige Erstreckung des Post- und Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG auf die Rechtsnachfolger der Deutschen Bundespost* nicht erfolgt. Das Post- und Fernmeldegeheimnis schützt den Bürger bisher ausschließlich vor Eingriffen des Staates und der Deutschen Bundespost. Die Geltung des Fernmeldegeheimnisses ist lediglich einfachgesetzlich (durch § 10 Fernmeldeanlagengesetz - FAG -) auf private Betreiber einer für den öffentlichen Verkehr bestimmten Fernmeldeanlage erstreckt worden. Durch die vollständige Privatisierung der bisher in Behördenform geführten Unternehmen der Deutschen Bundespost fällt ein Hauptadressat des ausschließlich staatsgerichteten

176 BGBl. I, 2325 ff.

177 BVerfGE 85, 386; dazu vgl. Jahresbericht 1992, 1.1

Grundrechts aus Art. 10 Abs. 1 GG weg. Die gesetzliche Erstrekkung des Fernmeldegeheimnisses auf alle Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, wird außerdem befristet, denn das gesamte Fernmeldeanlagengesetz tritt mit Ablauf des 31. Dezember 1997 außer Kraft (§ 23 PTRegG). Wie der Grundrechtsschutz des Bürgers nach dem Wegfall des Monopols der Deutschen Telekom AG gesichert wird, ist gegenwärtig völlig offen.

Bereits in früheren Jahresberichten hatten wir darauf hingewiesen, daß § 12 FAG, der eine Auskunftserteilung über Verbindungsdaten für jedes beliebige Strafverfahren zuläßt, dringend änderungsbedürftig ist.[178] Auch diese Änderung ist im Rahmen der Postreform II unterblieben.

Das Postneuordnungsgesetz stellt auch nicht die einheitliche Kontrolle der Einhaltung von Datenschutzbestimmungen bei allen Nachfolgeunternehmen der Deutschen Bundespost sicher. Artikel 12 Abs. 16 PTNeuOG beschränkt die Kontrollkompetenz des Bundesbeauftragten für den Datenschutz vielmehr auf die „aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen ...". Dies hat bereits jetzt zur Folge, daß nicht durch Gesetz entstandene Tochterunternehmen der Deutschen Bundespost TELEKOM, wie z. B. die DeTeMobil und die DeTeMedien zum 1. Januar 1995 nicht mehr in die Kontrollkompetenz des Bundesbeauftragten für den Datenschutz (BfD), sondern in die der lokal zuständigen Aufsichtsbehörde fallen. Darüber hinaus fällt die Kontrollbefugnis des BfD mit dem Wegfall der Monopole ebenfalls den jeweiligen Aufsichtsbehörden zu, wenn im Zuge der jetzt bevorstehenden *Postreform III* keine anderen Entscheidungen getroffen werden. Damit bleibt eine wesentliche Forderung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder unberücksichtigt, die die Sicherstellung einer bundesweit einheitlichen Kontrolle gefordert hatten.[179] Im Rahmen der Beratungen im Bundestagsausschuß für Post und Telekommunikation bestand jedoch Einigkeit darüber, „... daß für die Zeit, wenn DBP TELEKOM und DBP Postdienst über keine Monopole mehr verfügen und daher § 2 Abs. 1 BDSG für die Zuständigkeit des Bundesbeauftragten für den Datenschutz bei den Unternehmen seine Wirkung verlieren wird, in Absprache mit den Bundesländern eine zentrale Kontrollstelle für den Datenschutz bestimmt werden soll".[180]

Auch die von uns bereits mehrfach kritisierte Regelung zur *Anzeige der Rufnummer des Anrufers bei telefonischen Beratungsstellen* sowie der Aufnahme der Rufnummern dieser Stellen in *Einzelentgeltnachweise*[181] ist eher noch zu Lasten des Bürgers verändert worden. Die im Gesetz bezüglich der telefonischen Beratungsstellen getroffenen Festlegungen sind jedenfalls nach wie vor unzureichend. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat demgegenüber in ihrer Entschließung[182] das „holländische Modell" favorisiert, bei dem jeder Kunde selbst darüber entscheiden kann, ob seine Rufnummer in Einzelentgeltnachweise von Anrufern aufgenommen wird oder nicht.

Bisherige Dauer der Speicherung von Verbindungsdaten bei der TELEKOM rechtswidrig?

Das Oberverwaltungsgericht Bremen[183] hat die TELEKOM verpflichtet, Rufnummern von angerufenen Teilnehmern aus dem digitalen Telekommunikationsnetz ISDN nur höchstens vier Tage in voller Länge zu speichern. Danach müssen die letzten drei Ziffern des angerufenen Anschlusses gelöscht werden. Die Kläger hatten die sofortige Löschung der Telefondaten aus dem digitalen Telefonnetz ISDN gefordert und angeführt, für eine weitergehende Speicherung und den damit verbundenen Eingriff in das Fernmeldegeheimnis bestehe gegenwärtig keine gesetzliche Grundlage. Nach Auffassung des Gerichts ist zur Aufrechterhaltung des Telefonverkehrs eine kurzfristige Speicherung jedoch weiterhin zulässig.

Die TELEKOM hat gegen das Urteil Revision eingelegt. Sollte diese Entscheidung vor dem Bundesverwaltungsgericht Bestand haben, so wäre die entsprechende Regelung der TDSV, die eine Speicherung der Zielnummern bis zu 80 Tagen vorsieht und ohnehin ersetzt werden muß, rechtswidrig.

Daten der Telefonauskunft auf CD-ROM

Bereits mehrfach haben wir in vergangenen Jahresberichten über das Angebot von Teilnehmerverzeichnissen der TELEKOM auf elektronisch lesbaren Datenträgern berichtet[184]. Dabei hatten wir kritisiert, daß der Benutzer der Eintragung seiner Daten in das Telefonbuch (§ 10 Abs. 3 TDSV) nicht so differenziert widersprechen kann, daß lediglich eine Eintragung auf elektronischen Datenträgern ausgeschlossen wird[185]. Die Einführung eines solchen differenzierten Widerspruchsrechts ist um so dringlicher, als die DeTeMedien (ehem. Deutsche Postreklame GmbH) künftig neben der bereits bestehenden Möglichkeit, eine zu einem Namen gehörige Telefonnummer aufzufinden, weitere Suchmöglichkeiten plant, wie z. B. die „invertierte Suche", bei der der Name des Benutzers zu einer eingegebenen Telefonnummer aufgefunden wird. Damit werden die bereits bisher bestehenden erheblichen Auswertungsmöglichkeiten elektronischer Telefonbücher nochmals erweitert. Die TELEKOM hat es auch in den neuen Telefonbüchern 1994/95 unterlassen, die Kunden über die Folgen einer Weitergabe ihrer Daten auf elektronischen Datenträgern umfassend aufzuklären.

Telekommunikation in Europa

Im Rahmen der *Europäischen Union* sind im Berichtszeitraum zahlreiche Initiativen im Bereich der Telekommunikations- und Medienpolitik ergriffen worden. Verbindliche Regelungen zum Schutz der Daten von Telekommunikationskunden und Mediennutzern stehen allerdings nach wie vor aus. Die Konferenz der Europäischen Datenschutzbeauftragten hat bei ihrer Sitzung in Madrid[186] darauf hingewiesen, daß die zahlreichen Initiativen der Europäischen Kommission zur schnellen Einführung neuer Telekommunikationsdienste und transeuropäischer Telekommunikationsnetze den Datenschutz bisher nur unzureichend berücksichtigen und sehr viel weiter gediehen sind, als die Beratungen über die allgemeine Datenschutzrichtlinie und die ISDN-Richtlinie. Insofern besteht ein erheblicher *Harmonisierungsbedarf* zwischen Maßnahmen zur Öffnung der Märkte und der europäischen Datenschutzgesetzgebung. Die Datenschutzbeauftragten sehen die konkrete Gefahr, daß die beiden Datenschutzrichtlinien, wenn sie verabschiedet werden, möglicherweise bereits von den zahlreichen umgesetzten Maßnahmen zur Einführung neuer Dienste und Netze überholt sein könnten. Sie haben deshalb die Europäische Union aufgefordert, schon jetzt spezielle Datenschutzvorschriften in diejenigen Rechtsakte aufzunehmen, die im Telekommunikationsbereich vor Verabschiedung der Datenschutzrichtlinien beschlossen werden.

Fast vier Jahre nachdem die Europäische Kommission einen ersten Vorschlag für eine *ISDN-Richtlinie* gemacht hatte, hat die Kommission im Juni 1994 einen geänderten Vorschlag für diese Richtlinie vorgelegt[187], nachdem zeitweise die Gefahr bestanden hatte, daß die Kommission ihr ursprüngliches Vorhaben völlig aufgeben würde. Die Änderungen werden von der Kommission in erster Linie mit dem Hinweis auf das vom Europäischen Rat in Edinburgh als Maßstab für die Unionsgesetzgebung festgelegte Subsidiaritätsprinzip und mit einer Beschränkung des Richtlinieninhalts auf telekommunikationsspezifische Fragen begründet, während allgemeine datenschutzrechtliche Fragen von der bereits weiter fortgeschrittenen Datenschutzrichtlinie beantwortet werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung[188] die Bundesregierung aufgefordert, noch unter der deutschen Ratspräsidentschaft diesen

178 vgl. Jahresbericht 1992, 5.2 sowie Jahresbericht 1991, 2.3
179 Jahresbericht 1993, Anlage 2.4
180 vgl. den Anschlußbericht BT-Drs. 12/8060, S. 200, Anm. zu § 10
181 vgl. Jahresbericht 1991, 2.3
182 vgl. Anlage
183 Az. OVG 1 BA 30/92 v. 14. 7. 94
184 vgl. z. B. Jahresbericht 1991, 2.3
185 vgl. Jahresbericht 1992, 5.2
186 vgl. Anlage 3.1
187 KOM (94) 128 endg. - COD 288
188 vgl. Anlage 2.13

geänderten Vorschlag vordringlich zu behandeln, damit er möglichst bald vom Rat und vom Europäischen Parlament beschlossen werden kann. Dies ist deshalb nicht gelungen, weil sich die Beratungen über die allgemeine Datenschutzrichtlinie im Rat bis Ende 1994 hingezogen haben. Auch inhaltlich haben sowohl die deutschen als auch die europäischen Datenschutzbeauftragten[189] Verbesserungsvorschläge zum geänderten Richtlinienentwurf der Kommission gemacht.

Die „Gruppe von Persönlichkeiten zur Informationsgesellschaft" hat unter dem Vorsitz von Kommissionsmitglied Bangemann in ihren Empfehlungen für den Europäischen Rat *„Europa und die globale Informationsgesellschaft"*[190] zwar die rasche Verabschiedung des Richtlinienvorschlags der Kommission über allgemeine Prinzipien des Datenschutzes durch die Mitgliedstaaten als erforderlich bezeichnet, weil ohne die rechtliche Sicherheit eines unionsweiten Konzepts für den Datenschutz der Vertrauensmangel auf seiten des Verbrauchers einer raschen Entwicklung der Informationsgesellschaft im Wege stehe. Bedauerlicherweise wird der Vorschlag für eine ISDN-Richtlinie aber nicht erwähnt. Demgegenüber hat die Kommission in ihrem Dokument *„Europas Weg in die Informationsgesellschaft – ein Aktionsplan"*[191] deutlich gemacht, daß im einzelnen durch unionsweite Regelungen festzulegen ist, wie die allgemeinen Datenschutzgrundsätze auf spezifische Situationen anzuwenden sind, die sich aus der Einführung neuer Technologien ergeben. Gerade diesem Zweck dient der Entwurf für eine erste bereichsspezifische Richtlinie über den Datenschutz im ISDN.

Die Europäische Kommission hat ein *Grünbuch über ein gemeinsames Konzept für Mobilkommunikation und Personal Communications in der Europäischen Union*[192] vorgelegt, das eine europäische Gesetzgebung vorbereiten soll. In diesem Grünbuch wird erstmals umfassend beschrieben, in welche Richtung sich die Telekommunikation in Europa und auch weltweit in den nächsten Jahren bewegen wird: Es wird in absehbarer Zeit keine Unterschiede mehr zwischen dem herkömmlichen Festnetz und den Mobilfunknetzen geben, jeder Teilnehmer kann in beiden Netzen erreicht werden und seinerseits anrufen, wenn er eine entsprechende Chipkarte in ein beliebiges (stationäres oder mobiles) Telefon steckt. Damit wird die Mobilität und Erreichbarkeit erhöht. Die Telekommunikation gleicht sich immer mehr der persönlichen, unmittelbaren Kommunikation an, auch wenn die Unterschiede noch auf absehbare Zeit überwiegen werden.

Gleichzeitig entstehen qualitativ neue Gefahren für die Privatsphäre. Im „persönlichen Kommunikationsnetz" der Zukunft werden nämlich nicht mehr Telefone, sondern Personen direkt angewählt, unabhängig davon, ob sie zu Hause oder mit einem Mobilfunkgerät unterwegs sind. Damit erhält die Telefonnummer den Charakter eines Personenkennzeichens. Das Recht jedes Nutzers, unbeobachtet zu kommunizieren, könnte entscheidend verkürzt werden. Das vor kurzem gegründete Europäische Amt für Numerierung in Kopenhagen hat zwar gegenwärtig nur die Aufgabe, nationale und europäische Numerierungspläne für die Telekom-Gesellschaften zu koordinieren und neu zu konzipieren. Sobald diese oder eine andere Institution aber beginnt, sich mit der *Numerierung von Menschen* zu befassen, ist dies keine Frage der Verteilung knapper Ressourcen mehr, sondern in erster Linie eine Frage der grundrechtlich geschützten Privatsphäre. Dies haben die europäischen Datenschutzbeauftragten in ihrer von uns initiierten Stellungnahme zum Grünbuch der Kommission[193] deutlich gemacht. Auch in einem zukünftigen universellen Telekommunikationsnetz muß zumindest die Möglichkeit für den einzelnen Teilnehmer erhalten bleiben, mit anderen zu kommunizieren, ohne sich selbst identifizieren zu müssen.

Die Europäische Kommission hat unsere Stellungnahme aufgegriffen und in ihrer Mitteilung an das Europäische Parlament und den Rat[194] betont, daß das Konzept der Anrufe von Person zu Person, der einheitlichen Nummernvergabe an Individuen und der personalisierten Karten unter dem Aspekt des Schutzes der Privatsphäre untersucht werden muß. Die Kommission hat erklärt, sie werde noch vor dem 1. Januar 1996 einen Bericht darüber vorbereiten, ob weitere Maßnahmen bezüglich eines Schutzes personenbezogener Daten notwendig sind.

Für den Telekommunikationssektor und insbesondere für das immer weiter verbreitete *Teleshopping* von Bedeutung ist der geänderte Vorschlag der Kommission für eine *Richtlinie des Rates über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz*[195]. Dieser Vorschlag ist – im Gegensatz zur ISDN-Richtlinie – bereits Gegenstand der Beratung im Rat. Wir haben im Rahmen der Europäischen Datenschutzkonferenz gemeinsam mit der französischen Datenschutzkommission und dem britischen Datenschutzbeauftragten eine Stellungnahme zu diesem Entwurf aus datenschutzrechtlicher Sicht formuliert, die dem Rat zugeleitet wurde. Auch wenn der Schwerpunkt dieser Richtlinie beim Verbraucherschutz liegt, so hat es doch zugleich Auswirkungen auf den Schutz der Privatsphäre, ob etwa das Telefon oder die elektronische Post zum Abschluß von Kaufverträgen im Fernabsatz ohne vorherige Zustimmung des Käufers benutzt werden darf. Der Richtlinienvorschlag enthält auch eine Regelung über kartengestützte Zahlungsverfahren im Fernabsatz.

In diesem Zusammenhang ist auch das von der Kommission im April 1994 vorgelegte *Grünbuch zu strategischen Optionen für die Stärkung der Programmindustrie im Rahmen der audiovisuellen Politik der Europäischen Union* zu erwähnen. Zwar nennt das Grünbuch die Wahrung des Datenschutzes und der Privatsphäre als ein Ziel der europäischen Strategie; dennoch spielen Datenschutzaspekte bei der Entwicklung neuer audiovisueller Dienste bisher offenbar nur eine untergeordnete Rolle.

Zu diesen neuen Diensten zählen vor allem Pay-per-View, Video-on-Demand und Shopping-Channels, mit denen Angebote immer stärker individualisiert werden. In dem Maße, wie der herkömmliche Rundfunk vom Massenmedium zum individuellen Bestell- und Konsummedium wird, bei dem über einen Rückkanal Daten der Nutzer an den Anbieter übermittelt werden, entstehen neue Gefährdungen für die Privatsphäre. Die Anbieter solcher Dienste haben ein starkes wirtschaftliches Interesse daran, Informationen über das Konsum- und Nutzungsverhalten der Kunden zu erhalten und individuelle Nutzungsprofile zu erstellen.

Demgegenüber haben wir die Kommission darauf hingewiesen, daß bereits bei der Konzeption audiovisueller interaktiver Dienste die Verarbeitung personenbezogener Daten auf ein möglichst geringes Maß reduziert werden muß *(Grundsatz der Datensparsamkeit)*. Eine Speicherung von (zwingend erforderlichen) Daten sollte soweit wie möglich dezentral und unter der Kontrolle des Benutzers erfolgen. Gebühren sollten von Guthabenkarten (prepaid cards) abgebucht werden können. Die Datenverarbeitung muß für den Benutzer transparent sein. Schließlich sind diejenigen Daten, die Systembetreiber und Diensteanbieter erhalten müssen, einer strikten Zweckbindung zu unterwerfen.

Die verschiedenen *Richtlinien über den offenen Netzzugang*, die bereits seit mehreren Jahren in Kraft sind, sollen im Laufe des Jahres 1995 aktualisiert werden. Zu diesem Zweck erstellt die Europäische Kommission einen Bericht, für den wir eine Stellungnahme der Europäischen Datenschutzkonferenz koordiniert haben[196]. Die Datenschutzbeauftragten dringen in diesem Zusammenhang darauf, daß dem Datenschutz ein höherer Stellenwert beigemessen wird, als dies in der ursprünglichen Rahmenrichtlinie über den offenen Netzzugang der Fall war. Nachdem der Entwurf einer *Richtlinie über den offenen Netzzugang im Sprachtelefondienst* zunächst am Widerstand des Europäischen Parlaments gescheitert ist, besteht außerdem die Möglichkeit, diese Richtlinie von vornherein datenschutzgerechter zu gestalten, als es der ursprüngliche Kommissionsvorschlag vorsah. Dieser Richtlinienvorschlag muß auch besser als bisher mit dem Vorschlag für eine ISDN-Richtlinie abgestimmt werden.

189 vgl. Anlage 3.4
190 sog. Bangemann-Bericht vom 26. Mai 1994, erstellt für die Tagung des Europäischen Rats am 24./25. Juni 1994 auf Korfu.
191 KOM (94) 347 endg.; BR-Drs. 792/94
192 KOM (94) 145 endg.
193 vgl. Anlage 3.2
194 KOM (94) 492 endg. v. 23. November 1994
195 KOM (93) 396 endg. SYN 411
196 vgl. Anlage 3.3

Das Programm des offenen Netzzugangs, das von der Kommission bereits verfolgt wurde, bevor spezielle Datenschutzrichtlinien vorgeschlagen wurden, sieht die *Schaffung eines allgemeinen Basistelekommunikationsdienstes* in allen Mitgliedstaaten vor, der jedem Unionsbürger den Zugang zu bestimmten unionsweiten Dienstemerkmalen ermöglichen soll. Der Entwurf für eine Ratsentschließung über diesen Basisdienst[197] erwähnt das Problem des Persönlichkeitsschutzes mit keinem Wort und nimmt noch nicht einmal Bezug auf die grundlegenden Anforderungen der Rahmenrichtlinie über den offenen Netzzugang, zu denen - wenn auch in schwacher Form - der Datenschutz zählt. Die europäischen Datenschutzbeauftragten haben es in ihrer Stellungnahme als entscheidend bezeichnet, daß Datenschutzmaßnahmen Teil jedes allgemeinen Basisdienstes werden, der in der Europäischen Union angeboten wird.

Die Liberalisierung auf dem europäischen Telekommunikationsmarkt wird in naher Zukunft weitergehen, nachdem zunächst im Bereich des Mobilfunks das Netzmonopol abgeschafft wurde. Als nächstes wird das Monopol für den Sprachtelefondienst auch im Festnetz zum Ende des Jahres 1997 fallen, und spätestens zu diesem Zeitpunkt wird es in der Europäischen Union auch kein Netzmonopol der Telekommunikationsorganisationen mehr geben. Dann werden auch andere Unternehmen, die über „alternative Netze" verfügen (z. B. Energieversorgungsunternehmen), Telekommunikationsnetze betreiben; der Unterschied zwischen Diensteanbietern und Netzbetreibern wird weitgehend bedeutungslos werden. Die damit verbundenen Auswirkungen für den Persönlichkeitsschutz der Bürger sind noch nicht im einzelnen absehbar. Es wird entscheidend darauf ankommen, daß der einzelne Unionsbürger sowohl im Verhältnis zu den Netzbetreibern als auch zu den Diensteanbietern nicht schlechter gestellt ist, als er gegenwärtig im Verhältnis zu den herkömmlichen Telekommunikationsorganisationen steht.

5.2 Telekommunikation in der Berliner Verwaltung

Vielfach besteht Unklarheit in der Verwaltung darüber, ob - und, wenn ja, welche - Daten in *Telefonnebenstellenanlagen* gespeichert werden dürfen.

Nach der Rahmendienstvereinbarung über den Einsatz und den Betrieb von digitalen Nebenstellenanlagen vom 15. August 1991[198] ist die Speicherung von Verbindungsdaten, wie beispielsweise die Rufnummer der anrufenden und angerufenen Teilnehmer, nach Beendigung der Verbindung unzulässig (§ 5 Abs. 2).

Darüber hinaus ist der Einsatz digitaler Telefonanlagen nur gestattet, wenn zwischen dem örtlich zuständigen Personalrat und der Behördenleitung eine besondere Dienstvereinbarung über die eingesetzten Leistungsmerkmale getroffen worden ist (§ 4 Rahmendienstvereinbarung). Wir haben gegenüber den öffentlichen Stellen des Landes Berlin auf diesen Umstand hingewiesen. Daraufhin sind in mehreren Dienststellen Dienstvereinbarungen zwischen örtlichen Personalräten und Behördenleitungen zum Einsatz der dortigen digitalen Telefonnebenstellenanlagen nachträglich getroffen worden.

> *Sowohl bei analogen als auch bei digitalen Nebenstellen steht vielfach die Funktion „Lauthören/Freisprechen" zur Verfügung. Dabei kann mit aufgelegtem Telefonhörer über ein Mikrofon gesprochen werden, die Stimme des Gesprächspartners wird über einen Lautsprecher übertragen. Mehrfach haben uns Behördenmitarbeiter um Stellungnahme gebeten, unter welchen Voraussetzungen die Nutzung dieser Funktion möglich ist.*

Die Nutzung der *Funktion „Freisprechen/Lauthören"* ist nur mit Einwilligung aller am Gespräch beteiligten Personen zulässig. Die Einwilligung muß vor Aktivierung der Funktion eingeholt werden. Die heimliche Nutzung kann strafrechtliche Konsequenzen nach sich ziehen, da das heimliche Mithören des Telekommunikationsverkehrs unter Strafe gestellt ist (§ 201 Abs. 1 StGB). Auch die Rahmendienstvereinbarung über den Einsatz und den Betrieb von digitalen Telefonnebenstellenanlagen enthält eine entsprechende Regelung (§ 5 Abs. 5 Satz 3).

> *Im Unterausschuß Kommunikations- und Informationstechnik des Hauptausschusses wurde der Senat aufgefordert, ein Konzept zur Abrechnung privater Telefongespräche vorzulegen. Gleichzeitig war die Verwaltungsvorschrift, die das Verfahren bisher regelt, außer Kraft getreten. Dies haben wir zum Anlaß genommen, das bisherigen Verfahren der Abrechnung zu überprüfen, insbesondere in welchem Umfang bisher Daten über die Gespräche aufgezeichnet werden.*

Kernstück des Verfahrens ist bisher ein *Sammelformular,* das vierteljährlich in den Verwaltungen zirkuliert und in das die Mitarbeiter die Anzahl der privat geführten Telefoneinheiten eintragen. Hierdurch wird zumindest die Häufigkeit privater Telefongespräche einzelner Mitarbeiter dienststellenweit bekannt. Wir haben daher empfohlen, für die Erfassung der Gebühren für jeden Mitarbeiter ein gesondertes Formular zu verwenden, so daß die Kenntnisnahme seiner personenbezogenen Daten durch nicht mit dem Abrechnungsverfahren befaßte Dritte ausgeschlossen wird.

Vielfach werden in den Dienststellen bei dienstlichen (und - obwohl grundsätzlich nicht zulässig - auch bei privaten) Ferngesprächen die *Zielnummern der angerufenen Personen* in Fernsprechbüchern oder -listen der Vermittlungsstellen der einzelnen Dienststellen gespeichert. Für diese Speicherung existiert bisher keine Rechtsgrundlage. Wir haben angeregt, auf die Speicherung der Zielnummer bei privaten Telefongesprächen künftig ganz zu verzichten und die Zielnummer bei dienstlichen Ferngesprächen nur noch unter Verkürzung um die letzten drei Ziffern zu speichern. Durch die Verwendung von Büchern bei der Speicherung der Daten wird eine *zeitnahe Löschung* der Daten nach dem Wegfall der Erforderlichkeit erheblich erschwert. Daher haben wir gegenüber den betroffenen Stellen die Verwendung von Einzelbelegen angeregt.

Auf dem Hintergrund der Beschlußfassung des Unterausschusses KIT plant die Verwaltung, eine *automatisierte Erfassung der Gebühren für Privatgespräche von Dienstapparaten* einzuführen. Der Bericht der Senatsverwaltung für Inneres sieht dazu folgendes Verfahren vor:

Bei dienstlichen Ortsgesprächen werden für jede Kostenstelle die Anzahl der Gebühreneinheiten und die daraus resultierenden Gesprächskosten ohne Personenbezug aufsummiert. Zur Erfassung dienstlicher Ferngespräche wird den zur Führung solcher Gespräche berechtigten Personen eine *Identifikationsnummer* zugeordnet. Über die Eingabe dieser Nummer wird die Freischaltung für dienstliche Ferngespräche erteilt und zugleich der entstehende Gebührendatensatz (Identifikationsnummer, Name, Datum/Uhrzeit, Gesprächseinheiten, Kosten) gespeichert. Für die Abrechnung privater Orts- und Ferngespräche wird allen Mitarbeitern eine weitere persönliche Identifikationsnummer zugeordnet. Nach Eingabe dieser Nummer werden die Gebührendaten registriert und bilden die Grundlage für die Erstattung der Kosten für die Gespräche. Auch hier soll die Identifikationsnummer als Teil des Datensatzes abgelegt werden.

Die Speicherung der Nummer des Angerufenen (Zielnummer) soll nach den Plänen der Innenverwaltung grundsätzlich unterbleiben. Um zu überprüfen, ob Mitarbeiter privat geführte Gespräche auch ordnungsgemäß angeben, soll die zuständige Dienststelle im *Verdachtsfall* für die Dauer von längstens drei Monaten die Speicherung der Verbindungsdaten der Dienstgespräche bestimmter Beschäftigter mit den ungekürzten Rufnummern der angerufenen Anschlüsse anordnen können. Die zuständige Personalvertretung soll vorher, der Betroffene nachher über die Maßnahme informiert werden.

Allerdings bedarf die Verarbeitung personenbezogener Daten des Anrufers einer *bereichsspezifischen Rechtsgrundlage,* in der Art und Umfang der Datenspeicherung und -nutzung sowie deren Dauer, Verwendungszweck und der Kreis der Zugriffsberechtigten festgelegt werden. Wir haben hierzu einen entsprechenden Vorschlag zur Änderung des Informationsverarbeitungsgesetzes unterbreitet.[199]

197 KOM (93) 543 endg. v. 15. November 1993
198 Dienstblatt des Senats von Berlin I, 305 ff.; vgl. auch Jahresbericht 1991, 2.3

199 vgl. Anlage 4

Problematisch ist die Nutzung einer Identifikationsnummer in der geplanten Form: Jedes Verfahren, mit dem die von einzelnen Teilnehmern verursachten Gebühren ermittelt werden sollen, setzt eine verläßliche Identifizierung und Authentifizierung des jeweiligen Mitarbeiters voraus (vgl. § 5 Abs. 3 Nr. 4 BlnDSG). Das zu diesem Zweck vorgeschlagene Verfahren, bei dem der Benutzer eine Identifikationsnummer am Telefon eingibt, die dann im Gebührendatensatz abgelegt wird, erfüllt diese Anforderungen nicht, da nicht ausgeschlossen werden kann, daß andere Mitarbeiter Kenntnis von der Identifikationsnummer des Bediensteten erhalten und auf dessen Kosten telefonieren. Die persönliche Identifikationsnummer darf daher nur dem Beschäftigten bekannt sein und muß – wenn sie anderen Mitarbeitern bekannt geworden ist – für den Administrator der Telefonanlage (besser für den Beschäftigten selbst an einem Endgerät) änderbar sein. Von einer Speicherung in den Gebührendatensätzen sollte abgesehen werden. Besonders problematisch ist ferner die geplante ungekürzte Speicherung der Zielnummer. Hier bestehen erhebliche Bedenken, ob die Verhältnismäßigkeit im Hinblick auf das informationelle Selbstbestimmungsrecht des Angerufenen noch gewahrt ist.

Telefondienstleistungen der Berliner Sparkasse

Telekommunikationsunternehmen und Geldinstitute bieten zunehmend Dienstleistungen an, die eine Abrechung von Telefongebühren über besondere sogenannte *„Calling Cards"* oder bereits vorhandene *Kreditkarten* ermöglichen. Das Funktionsprinzip ist in beiden Fällen das gleiche:

Der Benutzer wählt die gebührenfreie Nummer eines Telekommunikationsanbieters. Er identifiziert sich durch Eingabe der Kartennummer (beispielsweise der Kreditkartennummer) sowie einer zusätzlichen, meist vierstelligen Geheimzahl. Danach kann die gewünschte Telefonnummer gewählt werden. Die Abrechnung der Gespräche erfolgt im Falle der Kreditkartennutzung über das Kreditkartenkonto, ansonsten werden die Kosten durch das Telekommunikationsunternehmen direkt dem Anrufer in Rechnung gestellt.

Die Berliner Sparkasse, ein Geschäftsbereich der Landesbank Berlin, bietet im Zusammenhang mit einer von ihr vertriebenen Kreditkarte eine derartige Dienstleistung an. Mehrere Petenten hatten uns darauf hingewiesen, daß die vierstellige Geheimzahl standardmäßig mit den ersten vier Ziffern des Geburtsdatums des Benutzers belegt sei und darüber hinaus der Service automatisch für alle Inhaber dieser Kreditkarten freigeschaltet werde, ohne daß diese gesondert informiert würden.

Diese Sicherungsmaßnahme war nicht ausreichend, da sowohl die Kreditkartennummer als auch Geburtstag und -monat nicht nur den Benutzern, sondern einem nicht näher bestimmbaren Kreis weiterer Personen bekannt sein kann und eine mißbräuchliche Nutzung des Angebots damit nicht wirksam ausgeschlossen ist. Damit sind die Anforderungen des Berliner Datenschutzgesetzes an technische und organisatorische Maßnahmen zur wirksamen Speicher- und Benutzerkontrolle (§ 5 Abs. 3 Nr. 3, 4 BlnDSG) nicht erfüllt.

Das Verfahren wurde insofern geändert, als eine automatische Freischaltung unterbleibt und das Paßwort durch den Kunden künftig frei gewählt werden kann.

Zunehmend bieten auch Berliner Kreditinstitute sogenannte *„Phone-Banking"-Dienste* an, bei denen Bankkunden verschiedenste Bankgeschäfte – wie z. B. Abfragen des Kontostandes und Überweisungen – über Telefon abwickeln können.

Ein Petent wandte sich an uns, der bei der Berliner Sparkasse eine telefonische Beratung zu Phone-Banking in Anspruch genommen hatte. Im Laufe des Gesprächs teilte ihm der Berater der Sparkasse mit, daß aus Sicherheitsgründen alle Transaktionen, die von Bankkunden telefonisch abgewickelt werden, bei der Sparkasse aufgezeichnet würden. Dies gelte auch für das gerade geführte Informationsgespräch.

Die *Aufzeichnung von Beratungsgesprächen* im Rahmen des Phone-Banking war zu beanstanden, da es hier an der für die Aufzeichnung personenbezogener Daten erforderlichen Rechtsgrundlage mangelt. Die Speicherung kann insbesondere nicht auf § 28 BDSG gestützt werden, da die Erforderlichkeit der Speicherung bei Beratungsgesprächen regelmäßig nicht gegeben ist. Unabhängig davon, ob sich die von der Landesbank gegenwärtig verwendete Klausel im allgemeinen Vertrag zur Errichtung eines Girokontos oder in einem speziellen Vertrag für das Phone-Banking befindet, rechtfertigt diese Klausel nicht das lückenlose Mitschneiden von Anrufen solcher Kunden oder potentieller Kunden, die sich in allgemeiner Form über die Modalitäten des Phone-Banking informieren wollen. Darüber hinaus wird durch die heimliche Aufzeichnung der Telefongespräche das Recht der Betroffenen auf Vertraulichkeit der Kommunikation (dessen Verletzung nach § 201 Strafgesetzbuch strafbar sein kann) verletzt. Schließlich fordert das BDSG, daß personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise zu erheben sind (§ 28 Abs. 1 Satz 2 BDSG). Dies ist bei der heimlichen Aufzeichnung von Telefongesprächen ebenfalls nicht der Fall. Eine Einwilligung der Betroffenen liegt bei der Aufzeichnung von Beratungsgesprächen regelmäßig nicht vor.

Wir haben gegenüber der Berliner Sparkasse angeregt, das Verfahren insoweit zu ändern, als der Kunde zusätzlich zu den Vertragsunterlagen eine gesonderte Einwilligungserklärung erhält, mit der er ausführlich über Umfang und Dauer der Speicherung personenbezogener Daten beim Phone-Banking informiert wird. Ein vom Kunden unterschriebenes Doppel sollte an die Berliner Sparkasse zurückgesandt und dort zu den Kundenunterlagen genommen werden. Dies betrifft jedoch nur die Aufzeichnung einzelner Transaktionen bei telefonischen Bankgeschäften. Die Aufzeichnung von Beratungsgesprächen bleibt unzulässig. Wir haben daher die Berliner Sparkasse aufgefordert, die Speicherung von Beratungsgesprächen einzustellen und bereits aufgezeichnete Beratungsgespräche zu löschen.

5.3 Datenschutz und Medien

Die Medienfreiheit rechtfertigt nicht die Mißachtung der Menschenwürde durch die Zurschaustellung von Unfallopfern oder Menschen in Not in Rundfunksendungen, die ein tatsächliches Geschehen wiedergeben *(Reality TV)*.[200] Es ist deshalb zu begrüßen, daß durch den *Ersten Rundfunkänderungsstaatsvertrag* mit Wirkung vom 1. August 1994[201] ein ausdrückliches Ausstrahlungsverbot für solche Sendungen in den Rundfunkstaatsvertrag aufgenommen worden ist, die Menschen, die sterben oder schweren körperlichen oder seelischen Leiden ausgesetzt sind oder waren, in einer die Menschenwürde verletzenden Weise darstellen und ein tatsächliches Geschehen wiedergeben, ohne daß ein überwiegendes berechtigtes Interesse gerade an dieser Form der Berichterstattung vorliegt. Das Ausstrahlungsverbot gilt auch dann, wenn die Betroffenen eingewilligt haben (§ 3 Abs. 1 Nr. 5 Rundfunkstaatsvertrag). Es bleibt abzuwarten, welche Auswirkungen diese Regelung haben wird. Es gibt Anzeichen dafür, daß Reality-TV-Sendungen vor allem deshalb zunehmend aus dem Programm genommen werden, weil die Einschaltquoten nachgelassen haben.

Die in Köln ansässige *Gebühreneinzugszentrale (GEZ)* zieht seit 1976 im Auftrag der Landesrundfunkanstalten der ARD, also auch des Senders Freies Berlin (SFB), bundesweit Rundfunk- und Fernsehgebühren auf der Grundlage des Rundfunkgebührenstaatsvertrags ein.

Auf den Zentralrechnern der GEZ werden ungefähr 33 Millionen Teilnehmerkonten geführt, an die ca. 800 Endgeräte der Zentral-EDV der GEZ sowie weitere ca. 350 Endgeräte bei den Gebührenabteilungen der einzelnen Landesrundfunkanstalten angeschlossen sind. Neben Teilnehmerstammdaten (wie Name, Vorname, Adresse etc.) werden hier auch Daten über die Zahlungsmodalitäten wie die Bankverbindung des Teilnehmers sowie Angaben zu von der GEZ in Rechnung gestellten Beträgen und eingegangenen Zahlungen des Teilnehmers gespeichert.

200 vgl. Jahresbericht 1991, 5.2
201 GVBl. 1994, 221

Im Jahr 1991 wurden bei der GEZ ca. 155,7 Millionen Geschäftsvorfälle (An-, Ab- und Ummeldungen, eingehende Zahlungen, Mahnverfahren etc.) durchgeführt. Um die Verwaltung der hierbei anfallenden Belegmengen zu erleichtern, werden eingehende Belege und Schreiben der Teilnehmer unmittelbar nach deren Eingang bei der GEZ mikroverfilmt. Die Mikrofilme werden in einem automatisierten Datenträgerarchiv aufbewahrt, aus dem einzelne Belege automatisiert wieder lesbar gemacht werden können.

Der Landesbeauftragte für den Datenschutz Bremen, der Hessische Datenschutzbeauftragte und wir haben eine *gemeinsame Prüfung der Gebühreneinzugszentrale* vor Ort durchgeführt. Die Datenschutzgesetze dieser drei Bundesländer enthalten Kontrollbefugnisse der Landesbeauftragten für den Datenschutz gegenüber ihren jeweiligen Rundfunkanstalten, soweit diese administrativ-wirtschaftlich tätig werden. Damit konnte die Einhaltung der datenschutzrechtlichen Bestimmungen bei der GEZ erstmals durch unabhängige, externe Datenschutzinstitutionen kontrolliert werden.

Im Bereich der Datensicherheit hat die – stichprobenhafte – Untersuchung gezeigt, daß die GEZ die notwendigen Voraussetzungen für eine ordnungsgemäße Datenverarbeitung geschaffen hat. Die getroffenen technischen und organisatorischen Maßnahmen und Regelungen entsprechen der gesetzlichen Vorgaben. Die Dokumentation der Datenträger- und Belegvernichtung konnte auf Anregung der Datenschutzbeauftragten weiter verbessert werden.

Wir hoffen, auch die noch offen gebliebenen Fragen im Zusammenhang mit Aufbewahrungsfristen für Teilnehmerdaten sowie Einzelfragen des Umfangs der Datenspeicherung im Laufe des nächsten Berichtsjahres befriedigend klären zu können.

Zwei Petenten wandten sich an uns, denen die GEZ Aufforderungen geschickt hatte, ihre Rundfunk- und Fernsehgeräte bis zu einer bestimmten Frist anzumelden, obwohl sie ihre Geräte bereits jahrelang ordnungsgemäß angemeldet hatten. Die Petenten fragten nach der Herkunft der Daten.

Die GEZ hatte im Laufe des Jahres 1993 bei der DeTeMedien GmbH (ehemals Deutsche Postreklame GmbH) die *Daten von über 49 000 Berliner Fernsprechteilnehmern angemietet.* Diese Daten wurden mit dem bei der GEZ vorhandenen Datenbestand Berliner Rundfunkteilnehmer abgeglichen; alle Personen, die nicht bereits im Datenbestand der GEZ vorhanden waren, erhielten ein Schreiben mit der Aufforderung, etwa vorhandene Rundfunk- und Fernsehgeräte umgehend anzumelden. Durch Bearbeitungsfehler der GEZ bzw. der bis 1975 für die Beitreibung von Rundfunkgebühren zuständigen Deutschen Bundespost wurden die beiden Petenten nicht als bereits zahlende Rundfunkteilnehmer erkannt und erhielten ebenfalls derartige Schreiben.

Die „Satzung der Rundfunkanstalt Sender Freies Berlin über das *Verfahren zur Leistung von Rundfunkgebühren*[202] enthält in § 8 eine Ermächtigung des SFB, „... andere Rundfunkanstalten oder andere Stellen bei der Erhebung, der Einziehung oder bei Inkassomaßnahmen von Rundfunkgebühren einschließlich Säumniszuschlägen und Kosten ... einzuschalten". Zwar kann dem SFB nicht verwehrt werden, sich wie jedes andere Unternehmen auch des unter bestimmten Voraussetzungen gesetzlich erlaubten Adreßhandels zur Verbesserung des Rundfunkgebührenaufkommens zu bedienen. Die Regelung in § 8 der Satzung entspricht jedoch nicht dem verfassungsrechtlichen Grundsatz der Normenklarheit, da der Bürger aus der dort getroffenen Formulierung nicht mit hinreichender Klarheit entnehmen kann, daß die Beiziehung anderer Stellen sich auch auf die Einschaltung kommerzieller Adressenhändler wie der DeTeMedien GmbH bezieht. Der SFB hat auf unsere Anregung hin eine entsprechende Klarstellung in der Satzung in Aussicht gestellt.

Anläßlich einer weiteren Eingabe stellte sich heraus, daß der SFB bereits seit den 80er Jahren regelmäßig ein *privates Inkassobüro* in Mainz einschaltet, wenn die Beitreibung von Rundfunkgebühren im gesetzlich vorgeschriebenen Verwaltungszwangsverfahren ergebnislos bleibt. Die dazu erforderliche Datenübermittlung an das Inkassobüro bedarf nach § 13 des Berliner Datenschutzgesetzes einer bereichsspezifischen Rechtsgrundlage. Eine solche Rechtsgrundlage bestand jedenfalls bis zum Inkrafttreten der Satzung der Rundfunkanstalt Sender Freies Berlin über das Verfahren zur Leistung von Rundfunkgebühren am 1. Januar 1994 nicht. Ich habe daher das Verfahren für den vorhergehenden Zeitraum gegenüber dem SFB beanstandet.

6. Durchsetzung des Datenschutzes

6.1 Sicherstellung des Datenschutzes in den Behörden

Behördliche Datenschutzbeauftragte

Die Zahl der Bestellungen von *behördlichen Datenschutzbeauftragten* im öffentlichen Bereich hat im Berichtszeitraum deutlich zugenommen. So sind uns bis jetzt ca. 640 behördliche Datenschutzbeauftragte durch Bestellungsschreiben der jeweiligen Behörde mitgeteilt worden. Nicht nur in den großen Verwaltungen, sondern auch in vielen nachgeordneten Einrichtungen wie Schulen, Krankenhäusern, Bibliotheken und Landesinstituten gibt es damit Ansprechpartner, die für Datenschutzfragen zuständig sind und den Datenschutz im Hause koordinieren.

In großen Behörden wie einigen Senatsverwaltungen und Bezirksämtern werden die behördlichen Datenschutzbeauftragten in Schwerpunktbereichen (z. B. Soziales, Gesundheit und Volksbildung) durch Datenschutz-Kontaktpersonen unterstützt.

Es häufen sich allerdings Anfragen zu *Kompatibilitätsproblemen* bei der Auswahl der geeigneten Person, weil Betroffene und Personalvertretungen der Auffassung sind, daß als behördliche Datenschutzbeauftragte Mitarbeiter bestellt werden, die entweder selbst intensiv mit personenbezogenen Daten zu tun haben oder für die Verarbeitung personenbezogener Daten oder für die Durchführung und Gestaltung der automatisierten Datenverarbeitung Verantwortung tragen (z. B. Leiter der EDV-Abteilung, Leiter Personalwesen bzw. Organisation). So wollte an einer Schule der Schulleiter selbst die Funktion des internen Datenschutzbeauftragten übernehmen.

Bei der Beurteilung, ob bestimmte Tätigkeiten wegen ihrer Inkompatibilität der Bestellung zum behördlichen Datenschutzbeauftragten entgegenstehen, muß allerdings berücksichtigt werden, daß diejenigen, die über die ausreichende Fachkunde verfügen und ein notwendiges Durchsetzungsvermögen erwarten lassen, meist in irgendeiner Form im Hauptamt Tätigkeiten ausüben, die zwangsläufig mit dem Umgang mit personenbezogenen Daten oder mit dem Betrieb der IuK-Systeme zu tun haben. Der Kreis der Personen, der zum behördlichen Datenschutzbeauftragten ernannt werden kann, würde bei restriktiver Auslegung der Kompatibilität zu klein werden und den Behörden noch mehr Schwierigkeiten bereiten, einen behördlichen Datenschutzbeauftragten zu benennen, der dieses Amt kompetent ausüben kann.

So wurde in einer Fachhochschule ein Hochschullehrer zum behördlichen Datenschutzbeauftragten benannt, der auch die Betreuung des hauseigenen *Telekommunikationssystems* übernommen hatte. Wir haben hierin keine Interessenkollision gesehen, die so gravierend wäre, daß sie einer Bestellung zum behördlichen Datenschutzbeauftragten entgegenstehen würde. In einer anderen großen öffentlichen Bildungsstätte wurde der *Verwaltungsleiter* zum behördlichen Datenschutzbeauftragten ernannt. Der Verantwortungsbereich des Verwaltungsleiters ist so geschnitten, daß in bestimmten Fällen zwar Interessenkonflikte auftreten können, dies aber nicht der Bestellung entgegenstehen mußte.

Dateienregister

Da wir bei Beratungsgesprächen, Kontrollen und anderen Gelegenheiten verstärkt zur Abgabe von *Dateiregistermeldungen* aufgefordert haben, war im Laufe des Berichtszeitraums eine stetig zunehmende Zahl von neuen Meldungen zu verzeichnen. Ende 1994 waren zum Dateienverzeichnis ca. 1 550 und zum Geräteverzeichnis ca. 1 300 Meldungen eingegangen. Gleichwohl

202 vom 25. November 1993 (ABl. Nr. 2 vom 14. Januar 1994, S. 88)

stehen noch viele Meldungen aus, die mit großem Zeitaufwand angemahnt werden müssen. Dies gilt vor allem dann, wenn Stellen der Meinung sind, daß sie nicht erneut melden müssen, wenn sie bereits früher vor Inkrafttreten des neuen Berliner Datenschutzgesetzes von 1990 nach altem Recht gemeldet hatten.

Insbesondere Gerätemeldungen, die erst seit der Neufassung des Berliner Datenschutzgesetzes dem Berliner Datenschutzbeauftragten zuzuleiten sind, werden vernachlässigt. Obwohl das LIT im Zusammenhang mit dem IT-*Inventar- und Informationssystem INVENT* ein Report-Programm erstellt hat, das es den INVENT-Anwendern erleichtert, eine Meldung zum Geräteverzeichnis zu fertigen, ist bisher nur eine noch zu geringe Anzahl von Meldungen erfolgt. Wir haben aus diesem Grunde im Herbst 1994 ein Rundschreiben an alle öffentlichen Stellen des Landes Berlin gesandt, in dem dieses spezielle Meldeverfahren kurz erläutert wird und die Stellen zur unverzüglichen Abgabe der Meldungen aufgefordert werden. Inzwischen fand ein gesondertes Treffen der INVENT-Anwender statt, das sich ausschließlich mit dieser Problematik befaßte.

Es fällt auf, daß bei vielen Meldungen die Vorgaben des Berliner Datenschutzgesetzes, des Informationsverarbeitungsgesetzes und der Dateienregisterverordnung nicht beachtet werden, so daß eine Weiterbearbeitung der Meldungen bei uns unzumutbar erschwert wird und daher zur Nachbesserung aufgefordert werden muß.

Um bei künftigen Meldungen Fehler beim Ausfüllen zu vermeiden, sei an dieser Stelle auf folgende häufige Mängel hingewiesen:

1. Dateien, die unter das IVG fallen, sind nicht zu melden.

   Dies betrifft sowohl manuelle als auch automatisierte personenbezogene Dateien, die bei der allgemeinen Verwaltungstätigkeit anfallen. Dazu zählen u. a. Aktensammlungen, allgemeine Beratungs- und Betreuungsfälle, Personalkarteien, Urlaubslisten, Telefonverzeichnisse, Geschäftsverteilungspläne, Stellenkarteien.

2. Karteien (nichtautomatisierte Dateien) sind nur zu melden, wenn aus ihnen an Dritte übermittelt wird.

3. Stellen, die Dateien vor dem Inkrafttreten des neuen Berliner Datenschutzgesetzes auf alten Formularen gemeldet hatten, haben Änderungsmeldungen auf neuen Formularen, hier aber nur die tatsächlich geänderten Seiten, abgegeben. Aus Gründen der Einheitlichkeit und der besseren Lesbarkeit für den einsichtsberechtigten Bürger sind stets die neuen Formulare zu verwenden.

4. Viele Meldungen werden immer noch handschriftlich ausgefüllt. Dies führt stets dazu, daß die Meldungen zurückgesandt werden und um Ausfüllung mit Maschinenschrift gebeten werden muß.

5. Oft erreichen uns Meldungen nur unvollständig ausgefüllt. Vermutlich sind die Ausfüllanleitungen nicht an nachgeordnete bzw. Außenstellen weitergegeben worden. Treten Zweifelsfälle auf, kann bei uns jederzeit telefonisch nachgefragt werden.

6. Manche Stellen haben das Meldeformular auf ihrem Computer entworfen, um das Ausfüllen zu erleichtern und um nicht stets beim Vordrucklager des Landesverwaltungsamtes neue Formulare anfordern zu müssen. Neben den Disketten, die uns für die Weiterverarbeitung zugesandt werden, sind die Meldungen auch in Papierform mitzuschicken, damit der Bürger sein Einsichtsrecht wahren kann. Dabei ist darauf zu achten, daß die Formularangaben aus dem Originalformular originalgetreu umgesetzt werden und beim Eintragen gängige Schrifttypen gewählt werden, da sonst die automatische Lesbarkeit stark beeinträchtigt ist.

7. Durch die nachlässige Handhabung interner Ordnungsmerkmale wird oft die genaue Zuordnung von Dateien zum verarbeitenden Gerät erschwert.

8. Abgegebene Meldungen müssen aktualisiert werden, wenn Veränderungen der Dateien und Systeme erfolgen. Um zu vermeiden, daß der Aufwand bei Systemen, die häufigen Veränderungen ausgesetzt sind, zu groß wird, reicht es, wenn ca. alle 6 Monate eine Änderungsmeldung erfolgt, die die inzwischen eingetretenen Änderungen berücksichtigt.

9. Einige Stellen haben uns Meldungen in doppelter Ausfertigung zugesandt. Dies ist nicht erforderlich. Es genügt die einfache Meldung.

10. Änderungen von Meldungen, die auf Grund von Anmahnungen an uns zurückgeschickt werden, haben mitunter keinen Bezug zur Erstmeldung. Es ist unbedingt die Datei- bzw. Gerätebezeichnung oder wenigstens das Ordnungsmerkmal anzugeben.

Aufgabenentwicklung

Die Zahl der Eingaben ist im Berichtszeitraum auf dem hohen Niveau der Vorjahre geblieben. Die meisten Beschwerden richten sich gegen Einrichtungen der Leistungsverwaltung (Sozial- und Gesundheitswesen), gefolgt von der Ordnungsverwaltung (wobei der Bereich Meldewesen wiederum am häufigsten betroffen war) und dem Sicherheitsbereich (Justiz, Polizei und Landesamt für Verfassungsschutz). Die schon im vergangenen Jahr beachtliche Zahl von Eingaben gegen die Verarbeitung von Personaldaten ist in etwa gleichgeblieben, noch weiter gestiegen sind die Beschwerden in Geschäftsordnungsangelegenheiten (Zusatzdaten im Adreßfeld, Formulare, Versand von Schriftstücken).

Die Beratungsersuchen der Verwaltung sind im Zusammenhang mit der Planung und Einführung der Großprojekte und des MAN noch weiter gestiegen. Bei den Rechtsfragen stehen die Bereiche Bildung und Forschung sowie Gesundheit und Soziales weiter vorn, wobei aber auch die Ordnungsverwaltung immer stärker von der Möglichkeit der Beratung Gebrauch macht.

6.2 Der Berliner Datenschutzbeauftragte

Die Dienststelle

Am 30. November 1994 lief die dritte Amtsperiode des Berliner Datenschutzbeauftragten aus. Der bisherige Amtsinhaber Dr. Hansjürgen Garstka wurde am 19. Januar 1995 vom Abgeordnetenhaus wiedergewählt und am 9. Februar 1995 erneut für fünf Jahre ernannt.

Trotz der äußerst schwierigen Haushaltslage verschloß sich das Abgeordnetenhaus unserem Hinweis nicht, daß eine Kontrolle der bevorstehenden Umwälzungen im IT-Bereich der Berliner Verwaltung[203] mit dem vorhandenen Personal nicht mehr gewährleistet werden könne, und bewilligte für den Doppelhaushalt 1995/96 eine zusätzliche Stelle im Bereich Technik und Organisation; für den Bereich der inneren Verwaltung wurde eine (niedrig dotierte) Stelle des gehobenen Dienstes bewilligt, mit der zusätzlich die Verwaltungsaufgaben bewältigt werden sollen, die für den in unseren Geschäftsbereich eingegliederten Landesbeauftragten für die Unterlagen des Staatssicherheitsdienstes anfallen. Auch hinsichtlich der Sachmittel brachte das Abgeordnetenhaus hohes Verständnis für unsere Aufgaben auf.

Ein kurzer Überblick über unsere Geschäftsverteilung zum Ende des Berichtszeitraums befindet sich in den Anlagen.[204]

Abgeordnetenhaus

Erneut hat der Berliner Datenschutzbeauftragte anläßlich der parlamentarischen Beratung des Jahresberichts 1993 von seinem Rederecht vor dem Abgeordnetenhaus Gebrauch gemacht.[205]

Intensiv und mit großer Sachlichkeit hat der Unterausschuß Datenschutz des Innenausschusses in sechs Sitzungen anstehende Probleme beraten. Unter den erörterungsbedürftigen Problemen der Jahresberichte 1992 und 1993 befand sich vor allem die ausstehende Verwaltungsvorschrift zum Ausländergesetz, die auf Grund einer harten Terminsetzung nunmehr endlich in Kraft gesetzt wurde.[206]

203 siehe oben 2.2
204 vgl. Anlage 6
205 vgl. Anlage 1
206 vgl. 4.6.3

Auch eine Reihe anderer Ausschüsse bat uns um Beratung; für den Petitionsausschuß wurden wiederum einige Gutachten gefertigt.

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 Landesdatenschutzbeauftragten, die nach der Wahl der Thüringischen Datenschutzbeauftragten im vergangenen Jahr nunmehr auch in allen neuen Ländern eingesetzt sind. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in zwei Sitzungen, diesmal in Potsdam, eine Reihe von Beschlüssen zu grundlegenden Fragen des Datenschutzes gefaßt.[207] Auch die besondere Zusammenarbeit mit den Landesbeauftragten der neuen Länder wurde fortgesetzt, wobei die Kooperation mit dem Landesbeauftragten von Brandenburg besonders intensiv und einvernehmlich war.

Auf nationaler, europäischer und internationaler Ebene wurde die besondere Kooperation auf dem Gebiet des Datenschutzes bei Telekommunikation und Neuen Medien fortgesetzt. Der Berliner Datenschutzbeauftragte hat hier den Vorsitz in den Arbeitskreisen der jeweiligen Konferenzen. Auf Grund der Vorbereitungen in diesen Gremien hat die Europäische Konferenz der Datenschutzbeauftragten mehrere Beschlüsse gefaßt[208]; auf der Internationalen Konferenz in Den Haag im September 1994 wurde über Arbeitsergebnisse berichtet.

Auch die Zusammenarbeit mit den anderen Kontrollinstanzen, insbesondere mit der Aufsichtsbehörde für den Datenschutz bei der Senatsverwaltung für Inneres sowie den behördlichen Datenschutzbeauftragten, wurde in der bewährten Weise fortgeführt.

Aus- und Fortbildung

Wiederum haben wir uns bemüht, durch die Wahrnehmung von Lehraufträgen an Universitäten und Fachhochschulen, durch Unterrichtsbesuche in Schulen, aber auch durch Veranstaltungen und Vorträge bei privaten Fortbildungseinrichtungen die an uns herangetragenen Aus- und Fortbildungswünsche zu befriedigen.

Diese Nebentätigkeiten können - im Gegensatz zur Übung in anderen Verwaltungen - in der Regel nicht in der Arbeitszeit durchgeführt werden, da hierzu die Kapazitäten unserer Dienststelle nicht ausreichen. Dies gilt auch für die Lehrtätigkeit in der Fachhochschule für Verwaltung und Rechtspflege, bei der nach dem Umzug nach Friedrichsfelde mit der Beteiligung an der Lehre ein besonders hoher Aufwand verbunden ist.

Öffentlichkeitsarbeit

Bereits in unserem Jahresbericht 1993 hatten wir das *Berliner Informationsgesetzbuch* vorgestellt. Die Idee zu dieser Publikation ist durch den vielfach an uns herangetragenen Wunsch nach einer einfachen Sammlung der wichtigsten datenschutzrechtlichen Regelungen entstanden. Auf Grund der großen Resonanz, die auf die Vorauflage des ersten Heftes der Reihe, den Text des Berliner Datenschutzgesetzes, erfolgt ist, haben wir dieses nunmehr in einer Neuauflage in auch grafisch überarbeiteter Form herausgebracht. Weitere Hefte mit gleichem Design sind diesem gefolgt.

Insgesamt sind im Berliner Informationsgesetzbuch bisher erschienen:

Teil 1: Datenschutzgesetze
Heft 1 - Berliner Datenschutzgesetz
Heft 2 - Bundesdatenschutzgesetz

Teil 2: Sicherheits- und Ordnungsrecht
Heft 1 - Allgemeines Sicherheits- und Ordnungsgesetz
Heft 2 - Meldegesetz

Teil 3: Gesundheits- und Sozialrecht
Heft 1 - Schutz der Sozialdaten.

Für diejenigen, die häufig mit den Gesetzen arbeiten müssen, gibt es einen einfachen Einband, mit dem die einzelnen Hefte zu einem handlichen Hilfsmittel zusammengeführt werden können.

Nach wie vor greifen wir gerne Anregungen auf, um welche Vorschriften oder andere Texte die Sammlung ergänzt werden könnte.

In unserer Reihe „Materialien zum Datenschutz" ist das Heft mit dem Titel *Datenschutz in Wissenschaft und Forschung* erschienen.

In einer Reihe von Wissenschaftsgebieten wird der Mensch zum Objekt der Forschung. Um aussagekräftige Forschungsergebnisse erzielen zu können, werden die vielfältigsten Daten über einzelne Personen benötigt. Damit greift die Forschung in das allgemeine Persönlichkeitsrecht ein, dem auch das Recht auf informationelle Selbstbestimmung zugeordnet ist. Zwischen den widerstreitenden Grundrechten der informationellen Selbstbestimmung und der Wissenschafts- und Forschungsfreiheit hat insofern ein Ausgleich zu erfolgen.

In Ermangelung von konkreten bereichsspezifischen Regelungen, die diesen Ausgleich vornehmen, kommen für viele wissenschaftliche Forschungen immer noch die Bestimmungen der Datenschutzgesetze des Bundes und der Länder zur Anwendung. Nicht selten sind aber in diesem Zusammenhang auch andere Rechtsbereiche zu beachten.

Den vielen Beratungsgesprächen mit Wissenschaftlern konnten wir entnehmen, daß datenschutzrechtlich gut vorbereitete Forschungsvorhaben einen beachtlichen Vertrauensbonus bei den Betroffenen oder den Behörden erhalten, der die wissenschaftliche Arbeit erleichtern und bereichern kann.

Mit dem Heft „Datenschutz in Wissenschaft und Forschung" wollen wir einige Lösungsansätze vermitteln und unsere Erfahrungen einer breiten, interessierten Öffentlichkeit zur Verfügung stellen.

Die Broschüre *Mobilfunk und Datenschutz* ist als Gemeinschaftsprojekt des Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen, und des Hamburgischen Datenschutzbeauftragten und des Berliner Datenschutzbeauftragten ebenfalls in der Reihe „Materialien zum Datenschutz" erschienen.

Sie befaßt sich mit den datenschutzrechtlichen Risiken der Übertragung personenbezogener oder sonstiger vertraulicher Daten mittels mobiler Kommunikationsdienste, die sich aus den Besonderheiten des eingesetzten Übertragungsmediums ergeben. Eines der Themen, die in dem Heft angesprochen werden, ist z. B. das datenschutzrechtlich relevante Problem, daß die mittels Mobilfunk übertragenen Signale - anders als bei der leitungsgebundenen Kommunikation - nicht physikalisch gegen unbefugtes Mithören und Aufzeichnen abgeschirmt werden können.

Als Vorsitzender des nationalen und internationalen Arbeitskreises „Datenschutz in Telekommunikation und Medien" engagiert sich der Berliner Datenschutzbeauftragte besonders in Fragen des Datenschutzes bei elektronischen Informations- und Telekommunikationsdienstleistungen. In diesem Bereich war in den vergangenen Jahren eine rasante Entwicklung zu beobachten. Auch der von der Deutschen Bundespost Telekom angebotene *Datex-J-Dienst* hat an dem Aufschwung teilgenommen.

Um die Nutzer dieser neuen Medien zu erreichen und für das Anliegen des Datenschutzes zu sensibilisieren, hat der Berliner Datenschutzbeauftragte bereits seit Jahren ein eigenes Programmangebot im „Bildschirmtext" veröffentlicht. Dieses Programmangebot wurde strukturell und inhaltlich völlig neu überarbeitet. Auf ca. 150 Seiten kann der interessierte Datex-J-Teilnehmer unter den Überschriften

1. Berliner Datenschutzbeauftragter. Wir über uns!
2. Aktuelles/Schwarzes Brett

207 vgl. Anlagen zu 2
208 vgl. 5.1; Anlagen zu 3

3. Info-Material zum Datenschutz
4. Datenschutzrecht
5. Technisch-organisatorische Maßnahmen des Datenschutzes
6. Telekommunikation und Medien
7. Datenschutzbehörden
8. Lexikon
9. Mitteilungen an den Berliner Datenschutzbeauftragten

Informationen zum Thema Datenschutz, über unsere Dienststelle, die bei uns zu bestellenden Materialien und die Adressen von weiteren Ansprechpartnern abrufen.

Berlin, 28. März 1995

Dr. Hansjürgen Garstka
Berliner Datenschutzbeauftragter

Anlagen zum Jahresbericht 1994

Anlage 1

1. Rede des Berliner Datenschutzbeauftragten vor dem Abgeordnetenhaus am 15. September 1994

Sehr verehrte Frau Präsidentin,
sehr geehrte Damen und Herren!

Der Berliner Gesetzgeber, und das heißt dieses Haus, hat in beispielhafter Weise das Verfassungsgebot umgesetzt, daß der Bürger bei der Lektüre der Gesetze und der anderen publizierten Rechtsvorschriften erkennen soll, welche öffentlichen Stellen welche Daten über ihn erheben, für die ursprünglichen oder andere Zwecke nutzen oder an wen sie Daten herausgeben. Diesem Beispiel ist übrigens das Land Brandenburg gefolgt. An die Stelle dehnbarer Generalklauseln traten spezialrechtliche Regelungen, die im vergangenen Jahr in weiten Bereichen durch Rechtsverordnungen präzisiert wurden. Verwaltungen, bei denen wir im Jahresbericht das Fehlen derartiger Vorschriften bemängelt hatten, haben dies nachgeholt bzw. werden dies in Kürze tun.

Angesichts dieser der Verfassung in besonderer Weise entsprechenden Lage wäre es ein schwer vertretbarer Rückschritt, würde man den Grundsatz der einzelgesetzlichen Befugnisregelung zugunsten einer gleichmacherischen Generalklausel zurücknehmen. An der Forderung nach einer derartigen Generalklausel hält der Senat gleichwohl fest. Er meint, durch den Verzicht auf bereichsspezifischen Datenschutz würde der Grundrechtsschutz der Bürger besser gewährleistet. Das Gegenteil ist der Fall: Ein solcher Schritt würde die Entscheidungsspielräume der Verwaltung beim Umgang mit den Daten der Bürger wieder zu deren Lasten erweitern. Ich verkenne dabei nicht, und dies wurde im Unterausschuß Datenschutz bereits beraten, daß es gewisse Ausnahmen geben sollte. Vorschläge sind von uns für den Vollzug von Bundesrecht oder für Querschnittsaufgaben der Verwaltung gemacht worden.

Zum Hintergrund dieser Debatte möchte ich zwei Einzelbeispiele darstellen, weil sie meines Erachtens ein Schlaglicht auf grundsätzliche Probleme werfen:

Mit gewisser Häme verweist der Senat darauf, daß das Gesetz über Datenverarbeitung im Bereich der Kulturverwaltung sogar regele, welche personenbezogenen Daten für den Eintrittskartenvertrieb der staatlichen Bühnen verarbeitet werden dürfen. Bei genauem Hinsehen ist die Regelung allerdings erheblich weniger komisch, als dies scheint: Werden die Kultureinrichtungen doch in dieser Bestimmung ermächtigt, nicht nur Daten über Kontonummern, Zahlungsweisen und Zahlungswege zu verarbeiten, sondern auch über Ermäßigungen begründende Sachverhalte, also etwa Behinderungen - mir scheint es nicht ulkig, sondern konsequent, daß der Bürger dies durch Lektüre des Gesetzes in Erfahrung bringen kann: Nicht die Selbstverständlichkeiten, die notwendigerweise auch in einem Gesetz stehen müssen, sondern die Besonderheiten machen den wesentlichen Regelungsgehalt aus.

Zweites Beispiel:

Es wird häufig verkannt, daß die informationelle Selbstbestimmung nicht nur ein Grundrecht der Benachteiligten ist, sondern sich selbstverständlich auch die vom Leben Bevorzugten auf dieses Grundrecht berufen können. Zum Beispiel Eigentümer von Mietshäusern.

Ihnen legt das Bürgerliche Gesetzbuch die Pflicht auf, dem Mieter den bevorstehenden Verkauf einer Wohnung anzuzeigen - damit dieser von seinem Vorkaufsrecht Gebrauch machen kann. Ein fairer Vermieter wird seine Mieter früher benachrichtigen - verpflichtet ist er nach dem BGB dazu nicht. Der Senat hält das Schutzbedürfnis der betroffenen Mieter dabei zur Zeit für nicht genügend berücksichtigt: Weil der Datenschutz zu weitgehend sei, solle man nicht nur „für diese, sondern auch für ähnliche Problemlagen" den Behörden gestatten, die Betroffenen über vorbereitende Verwaltungsvorgänge zu informieren - hinter dem Rükken der Eigentümer, versteht sich. Auch ich meine, der Mieter sollte frühzeitig informiert werden - dann aber auf Grund einer klaren Entscheidung des Gesetzgebers und nicht auf einem datenschutzrechtlichen Schleichweg. Noch mehr entspricht der informationellen Selbstbestimmung natürlich, den Mieter mit Einwilligung des Vermieters zu informieren - wie es die Bauverwaltung demnächst erproben will.

Gegen eine gesetzliche Regelung wird wie in anderen Fällen die fehlende Gesetzgebungskompetenz eingewandt. Darauf ist nur zu sagen: Es kann ja wohl nicht wahr sein, daß die Berliner Verwaltung vom Bundesrecht nicht vorgesehene Verfahren einführen kann, deren gesetzliche Regelung dem Berliner Parlament verwehrt sein soll!

Beide Beispiele machen deutlich, daß der Weg, den dieses Haus bei der Ausgestaltung des Datenschutzrechts eingeschlagen hat, weitergeführt und nicht abrupt und ohne Grund abgebrochen werden sollte.

Allerdings sind auf diesem Weg nicht nur datenschutzrechtliche Errungenschaften erreicht, sondern auch bedauerliche Rückzüge angetreten worden.

In unserem Jahresbericht 1993 haben wir uns ausführlich mit den Auskunfts- und Einsichtsrechten des Bürgers befaßt, der Magna Charta des Datenschutzes, wie diese Rechte zutreffend genannt worden sind. Durch spezialgesetzliche Sonderregelungen ist namentlich das im Datenschutzgesetz großzügig und bürgerfreundlich ausgestaltete Einsichtsrecht in eigene Daten zurückgenommen worden. Ins Leere gehende Verweisungen, wie im Ausführungsgesetz zum Gerichtsverfassungsgesetz, erschwerende Begründungspflichten wie im Verfassungsschutzgesetz oder dem Wortlaut nach anscheinend unverbindliche Kannvorschriften wie im Allgemeinen Sicherheits- und Ordnungsgesetz lassen den Verwaltungen die Möglichkeit, die Akteneinsicht je nach Bedarf zu beschränken - bis auf Null, wie etwa der Fall bei der Polizei, die sich berechtigt fühlt, jede Akteneinsicht zu verweigern mit der dem Charakter des Einsichtsrechts hohnsprechenden Begründung, das Einsichtsrecht des ASOG „sei nur als Möglichkeit zur Arbeitserleichterung gedacht".

[Zitat aus einem Schreiben des Polizeipräsidenten vom 1. Juni dieses Jahres].

Sehr geehrte Damen und Herren Abgeordnete!

Es ist unumstritten, daß unsere Gesellschaft sich von einer Industrie- zu einer Informationsgesellschaft entwickelt. Der Mensch wird seine Würde nur noch wahren und seine Persönlichkeit nur noch entfalten können, wenn er die Möglichkeit hat, sich Kenntnis über seine informationellen Abbilder zu verschaffen und mit dieser Kenntnis sein in der Berliner Verfassung garantiertes Grundrecht auf Datenschutz geltend zu machen. Möglichst umfassende Auskunfts- und Einsichtsrechte sind hierzu ein unerläßliches Instrument. Ich bitte Sie, bei Gesetzgebung und Verwaltungskontrolle dem so weit wie möglich Rechnung zu tragen.

Das Stichwort „Informationsgesellschaft" führt mich zu den technischen Perspektiven.

Die Landesverwaltung steht hier vor einem bisher nicht dagewesenen Umbruch: Die bevorstehende Einführung oder flächendeckende Einsetzung von Großverfahren in wichtigen Verwaltungsbereichen - der Sozialverwaltung, der Personalverwaltung, der Steuerverwaltung, dem Haushaltswesen - wird Tausende von Terminals auf die Schreibtische der Mitarbeiterinnen und Mitarbeiter bringen. Die Einführung eines hochmodernen Verwaltungsnetzes, der Ersatz der bisherigen Telekommunikationstechnologie durch ISDN, die Öffnung der Verwaltung hin zu weltweiten Telekommunikationsdiensten werden an Datenschutz und Informationssicherheit höchste Anforderungen zu stellen haben.

Und am Horizont zeichnen sich bereits weitere Entwicklungen ab. Ich will nur die Revolution erwähnen, die die demnächst zu erwartende Marktreife von Spracherkennungssystemen in Vorzimmer und Schreibdienste hineintragen wird.

All dies ist Voraussetzung für die gewaltigen Personaleinsparungen, die die bestehende Finanznot der Berliner Verwaltung aufzwingt. Für den Datenschutzbeauftragten bringt die Entwicklung allerdings nicht nur eine Erhöhung, sondern eine Vervielfältigung der Aufgaben mit sich, wenn man mit dem Bundesverfassungsgericht davon ausgeht, daß die Kontrolle durch den Datenschutzbeauftragten ein notwendiges Pendant zu den Gefährdungen der informationellen Selbstbestimmung darstellt. Die Einlösung dieses hohen Anspruchs ist nur durch die Gewährleistung eines Mindestmaßes an Kontrolldichte möglich.

Dies wird, und ich sage dies in vollem Bewußtsein, was dies bedeutet, nicht ohne zusätzliche Kosten für den Datenschutz zu bewältigen sein.

Sehr geehrte Damen und Herren,

die dritte Amtsperiode des Berliner Datenschutzbeauftragten geht dem Ende zu. Vieles in den vergangenen Jahren ist von der verspotteten oder gar bekämpften Außenseiterposition zur akzeptierten Verwaltungsroutine geworden. Oder, wie Bertoldt Brecht formulierte, „auf die Mühen der Gebirge folgten die Mühen der Ebenen".

Ich hoffe, die - gemeinsamen - Mühen haben sich für den Bürger gelohnt.

2. Beschlüsse, Entschließungen und Stellungnahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Anlage 2.1

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat

(- bei Stimmenthaltung Bayerns und in Abwesenheit Baden-Württembergs)

- die folgende

Bestandsaufnahme über die Situation des Datenschutzes „10 Jahre nach dem Volkszählungsurteil"

zustimmend zur Kenntnis genommen.

Nach Ablauf von über 10 Jahren seit der Verkündung des Urteils des Bundesverfassungsgerichtes zum Volkszählungsgesetz am 15. Dezember 1983 sieht sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder veranlaßt, eine Bestandsaufnahme der Situation vorzulegen, in der sich der Datenschutz derzeit befindet.

Entwicklung nach dem Volkszählungsurteil:

Bereits unmittelbar nach Inkrafttreten der Datenschutzgesetze in Bund und Ländern war die Frage heftig diskutiert worden, welchen Rang der Datenschutz gegenüber anderen Rechtsgütern habe. Befürwortern der Auffassung, dem Datenschutz komme Grundrechtsqualität zu, standen zurückhaltendere Stimmen gegenüber, die die Subsidiarität des Datenschutzes betonten.

Das Volkszählungsurteil hat den Datenschutz zu einer elementaren Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens erklärt und den Grundrechtscharakter der informationellen Selbstbestimmung festgeschrieben. Dieses Grundrecht gewährleistet die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Damit wurde klargestellt, daß der Datenschutz unter den Bedingungen der modernen Datenverarbeitung das zentrale Mittel zur Gestaltung der Informationsbeziehungen zwischen den einzelnen und den Institutionen in Staat und Gesellschaft ist. Das Bundesverfassungsgericht hat seine Grundposition in der Zwischenzeit in einer Reihe weiterer Urteile eindrucksvoll bestätigt.

Danach ist von dem verfassungsrechtlichen Grundsatz auszugehen, daß die Entscheidung über die Preisgabe und Verwendung personenbezogener Daten zuallererst beim Betroffenen selbst liegt. Einschränkungen der individuellen Dispositionsfreiheit sind für die Rechts- und Gesellschaftsordnung von so wesentlicher Bedeutung, daß sie nur auf einer gesetzlichen Grundlage zulässig sind. Wie mit personenbezogenen Daten umzugehen ist, darf weder administrativer Zweckmäßigkeit noch dem Markt überlassen bleiben, sondern ist im Gesetzgebungsverfahren, d. h. vor den Augen der Öffentlichkeit zu entscheiden.

Bei der Regelung des Informationsumgangs ist von den individuellen Freiheitsrechten auszugehen; doch darf und muß der Gesetzgeber selbstverständlich berücksichtigen, daß der einzelne in vielfältiger Weise auf den Schutz und die Hilfe des Staates angewiesen ist und daß die Tätigkeit des Staates kontrollierbar sein muß. In gesetzlich klar vorgegebenen Fällen ist daher die Verwendung personenbezogener Daten auch ohne selbstbestimmte Mitwirkung des Betroffenen erforderlich.

Das Grundrechtsverständnis mit der Selbstbestimmung des Bürgers als Regelfall und ihre Einschränkung als Ausnahme ist allerdings keineswegs von allen Seiten als Selbstverständlichkeit akzeptiert worden: Nach 10 Jahren ist eine positive, aber auch eine kritische Bilanz zu ziehen.

Nach der Entscheidung des Bundesverfassungsgerichts sind, wenn auch in vielen Fällen in langwierigen Verfahren, viele gesetzgeberische Aktivitäten entfaltet worden. Dabei mußte mancher datenschutzrechtliche Fortschritt hart umkämpft werden.

Neben einer grundlegenden Novellierung der Datenschutzgesetze in Bund und Ländern wurden Spezialbestimmungen in zahlreichen Sondermaterien geschaffen. Auf der Ebene des Bundes zählen dazu:

- einzelne Bücher des Sozialgesetzbuches,
- das Personalaktenrecht für Beamte,
- das Straßenverkehrsrecht,
- die Gesetze über die Nachrichtendienste des Bundes,
- das Telekommunikationsrecht.

Besonderer Handlungsbedarf für die Verwirklichung der informationellen Selbstbestimmung entstand durch die deutsche Einigung. Dabei stellt die Aufarbeitung der Hinterlassenschaft des Staatssicherheitsdienstes der ehemaligen DDR auch für den Datenschutz eine besondere Herausforderung dar.

Noch weitergehend ist der Umfang der datenschutzrechtlichen Neuregelungen in den Ländern, in denen die Vorgaben des Bundesverfassungsgerichtes teilweise konsequenter umgesetzt wurden als im Bund.

Diese Verrechtlichungswelle hat auch Kritik hervorgerufen:

In Dutzenden von Gesetzen ist nunmehr das „Kleingedruckte" des Rechts auf informationelle Selbstbestimmung bereichsspezifisch geregelt. Das so entstandene Normengeflecht ist engmaschig und kompliziert. Dies steht der Intention des Verfassungsgerichtes, der Bürger solle bereits aus normenklaren Gründen erkennen können, mit welcher Verarbeitung seiner Daten er zu rechnen hat, gelegentlich bereits entgegen. Eine weitergehende Kritik stellt in Frage, ob diese Normenflut mit ihren perfektionistischen und detaillistischen Regelungen der Verwirklichung des Grundsatzes der Verhältnismäßigkeit dient und notwendig war. Geäußert wurde auch die Annahme, daß die Effizienz der staatlichen Verwaltung bei der Bewältigung ihrer Aufgaben unter der Last perfektionistischer detaillistischer Regelungen gelitten habe und daß die Kreativität der Gesellschaft und ihre Fähigkeit zur Anpassung und Bewältigung der gegenwärtigen Herausforderungen durch enge, starre Gesetze behindert würden.

Dem muß allerdings entgegengehalten werden, daß die Fülle und Kompliziertheit der Datenverarbeitung in den verschiedensten Verwaltungsbereichen für die Regelungsdichte verantwortlich ist. Sie ist eine Konsequenz des Umstands, daß in allen Verwaltungsbereichen der - zunehmend automatisierten - Informationsverarbeitung immer mehr Bedeutung zukommt: Eine notwendige Folge der Entwicklung hin zur „Informationsgesellschaft".

Ein weiterer Grund für die Komplexität der Gesetzgebung liegt darin, daß die Gesetze häufig nicht darauf abzielen, die Rechtsposition des Bürgers zu stärken, sondern vielmehr die Verarbei-

tung personenbezogener Daten zu ermöglichen, oft über das Maß hinaus, das bislang zulässig war. Viele Vorschriften sind so derart allgemein und umfassend zugunsten der Eingriffsseite formuliert, daß es schwerfällt, sie als „Datenschutzgesetze" im eigentlichen Sinn zu verstehen. Wann immer Verwaltungen sich durch den Datenschutz behindert glaubten, ertönte der Ruf nach dem Gesetzgeber, der – zugunsten der Verwaltung – korrigierend eingreifen soll.

Trotz alledem blieb der Datenschutz in wesentlichen Bereichen ungeregelt. Auf Bundesebene gibt es z. B. bis heute keine hinreichenden datenschutzrechtlichen Vorschriften auf den Gebieten des Arbeitnehmerdatenschutzes, der Justizmitteilungen und der Zwangsvollstreckung, des Abgabenrechts, des Mieterschutzes, der Arbeit von Auskunfteien, Detekteien und privaten Sicherheitsdiensten, der Bundespolizeibehörden, des Ausländerzentralregisters oder – am gravierendsten – des gesamten Strafverfahrens.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, diese Lücken umgehend und im Sinne der informationellen Selbstbestimmung zu schließen.

Zur aktuellen Situation:

Die derzeitige Situation des Datenschutzes wird von den beiden großen Themenbereichen geprägt, die die Innenpolitik beherrschen: Die innere Sicherheit und der Zustand unserer Wirtschafts- und Sozialordnung. Diese Felder ängstigen die Menschen und stärken die Kontrollbedürfnisse des Staates. Auf beiden Gebieten wird die vermeintliche Lösung darin gesucht, daß die gesetzlichen Möglichkeiten zur Verarbeitung personenbezogener Daten erheblich ausgeweitet und auf der anderen Seite die Rechte der Bürger entsprechend eingeschränkt werden.

Auf dem Gebiet der Strafverfolgung haben sich bisher die Ermittlungen auf den Beschuldigten konzentriert, und die prozessuale Aufklärung geschah im wesentlichen offen.

Jetzt setzt man auf Heimlichkeit und interessiert sich für Unbeteiligte. Ermittlungsverfahren ist nicht mehr Aufklärung eines konkreten Tatverdachts, sondern flächendeckende Sammlung personenbezogener Daten. Der Staat hält sich nicht mehr an die Grenzen der Ausforschung, die selbstverständlich waren, und er trifft dabei auf breite öffentliche Zustimmung.

Im Bereich der Wirtschafts- und Sozialordnung wird auf besonders drastische Weise versucht, durch die Einführung neuer Überwachungsverfahren eine Kostenminderung zu erreichen. Die Daten werden einerseits genutzt, durch Plafondierungen und Wirtschaftlichkeitsuntersuchungen eine Kostendämpfung zu erreichen (so etwa bei der Intensivierung der Kontrolle der Ärzte im Gesundheitsstrukturgesetz) oder eine angeblich mißbräuchliche Inanspruchnahme von Sozialleistungen aufzudecken (insbesondere durch regelmäßige Datenabgleiche bei Sozialhilfe und Arbeitsförderung).

Auf den Datenschutz wirkt sich dabei die Tendenz aus, weg von einer angeblichen egozentrischen Selbstbestimmung hin zu einer stärker betonten Gemeinschaftsverantwortung zu kommen. Individualrechte werden vielfach ohne zwingende Gründe zugunsten staatlicher Eingriffsrechte zurückgedrängt. Mehr und mehr begegnet der Staat dem einzelnen Bürger mit Mißtrauen und schafft ein immer dichteres Kontrollnetz. Es ist fraglich, ob dieses Menschenbild dem des Grundgesetzes entspricht.

Hinzu kommt, daß das reine Verwaltungsinteresse, das Bestreben nach größtmöglicher Perfektion und Einzelfallgerechtigkeit ein immer größeres Gewicht erhält. Je mehr Perfektion die Verwaltung anstrebt, desto mehr Daten muß sie erheben, nutzen, abgleichen oder sonst verarbeiten. Das Gespür für den „Mut zur Lücke" geht verloren. Kennzeichnend für den demokratischen Rechtsstaat ist aber nicht seine Allwissenheit, sondern die bewußte Beschränkung seiner Informationsherrschaft.

Besonders gern wird zur Intensivierung der Kontrolle die Wunderwaffe des Datenabgleichs genutzt. Perfektion und Korrektheit lassen sich dadurch auf bequeme Weise erreichen: Auf Knopfdruck lassen sich die verschiedensten Kontrollmechanismen in Gang bringen, ohne daß sich die Behörde unmittelbar mit dem einzelnen Bürger auseinandersetzen muß. Mühelos ist die Prüfung von Zehntausenden in kürzester Frist möglich.

Wird der Weg zu intensiverer Kontrolle und Überwachung, insbesondere zum Abgleich der verschiedensten Datenbestände, ungebremst fortgesetzt, könnte sich aus einer Unsumme von automatisierten Dateien und aus einem Netz von Datenabgleichen, das schließlich alle Bürger und fast alle ihre Lebensbereiche erfaßt, der „gläserne Bürger" ergeben. Selbst wenn jeder einzelne Abgleich und Kontrollvorgang für sich eine gewisse Berechtigung haben sollte, trägt er bei zu einem umfassenden Netz von Überwachungs- und Überprüfungsmöglichkeiten. Jeder Bürger wird dabei potentiell zum Verdächtigen, dessen korrektes Verhalten es zu überprüfen gilt. Damit ändert sich das Verhältnis des Bürgers zum Staat auf grundlegende Weise.

Wie dem begegnen?

Zwar ist die verfassungsrechtliche Dimension des Datenschutzes unbestritten. Gleichwohl fehlt der informationellen Selbstbestimmung das Fundament im Grundgesetz. Eine grundlegende Verbesserung könnte erreicht werden, wenn 10 Jahre nach der Anerkennung des Grundrechts auf Datenschutz durch das Bundesverfassungsgericht dieses Grundrecht auch ausdrücklich in das Grundgesetz aufgenommen würde. Daß die erforderliche Mehrheit in Bundesrat und Bundestag hierfür bisher nicht erreicht werden konnte, bedauert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausdrücklich.

Die verfassungsrechtliche Verbesserung bei einer derartigen Grundgesetzänderung bestünde auch darin, daß bei jedem Gesetzentwurf von Anfang an die Berücksichtigung des Grundrechts auf Datenschutz zu prüfen wäre. Eine Einschränkung des Grundrechts müßte künftig durch ausdrückliche Erwähnung im Gesetz unter Angabe des neuen Grundgesetzartikels kenntlich gemacht werden (sog. Zitiergebot nach Art. 19 GG); anderenfalls wäre das Gesetz nichtig. Dies wäre ein erheblicher „Mehrwert" zugunsten der Bürger.

Für die weitere Ausgestaltung des einfachen Datenschutzrechts sollten folgende Erwägungen zugrunde gelegt werden:

In der Informationsgesellschaft ist der effektive Schutz der personenbezogenen Daten die Voraussetzung für eine breite Teilnahme der Bürger an der Gesellschaft. Nur wenn der Bürger sicher sein kann, daß seine dem Staat und der Wirtschaft überlassenen Daten soweit wie möglich geschützt werden, nimmt er aktiv am Gemeinschaftsleben teil. Der Bürger kann seine Freiheit zur Kommunikation (und umgekehrt ebenso seine Entscheidung zur Freiheit von Kommunikation) nur verwirklichen, wenn der Staat seine Schutzpflichten für die Daten der Bürger ernst nimmt.

Die wichtigste Folge dieser Einsicht ist, daß Datenschutzvorschriften nicht nur Rechtssicherheit, sondern auch materielle Freiheitsräume garantieren müssen. Dies bedeutet, daß bei der Frage, ob der einzelne einer Auskunftspflicht unterworfen werden soll, ob seine Daten außer für den Erhebungszweck auch für andere Zwecke freigegeben werden sollen, wie lange belastende Daten aufbewahrt werden dürfen und welche Datenverarbeitungsvorgänge dem Betroffenen verborgen bleiben dürfen, jeweils strenge Maßstäbe angelegt werden müssen.

Hierfür ist eine neue Grenzziehung für Eingriffe in das Recht auf informationelle Selbstbestimmung erforderlich: Der Begriff des „überwiegenden Allgemeininteresses", der alleine einen Eingriff in die informationelle Selbstbestimmung rechtfertigt, ist inhaltlich mehr aufzufüllen und mehr als bisher im Lichte der informationellen Selbstbestimmung zu interpretieren. In konkreten Konfliktfällen darf die Freiheitssicherung der Bürger gegenüber effektiver Staatstätigkeit nicht ins Hintertreffen geraten.

Für das Bundesverfassungsgericht ist die Beteiligung unabhängiger Datenschutzbeauftragter wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten im Interesse eines vorgezogenen Rechtsschutzes von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung. Dies gilt insbesondere in den Bereichen, in denen ein Auskunfts- oder Einsichtsanspruch des

Bürgers nicht oder nur unvollständig besteht. Daraus folgt, daß Rolle und Kompetenzen der Datenschutzbeauftragten auch im Hinblick auf effektivere Eingriffsmöglichkeiten gestärkt werden müssen. Versuchen, die Kontrollmöglichkeiten der Datenschutzbeauftragten zu beschränken, muß schärfstens widersprochen werden.

Datenschutzrechtliche Verstöße gehen meist auf Unkenntnis und mangelndes Problembewußtsein seitens der öffentlichen Stellen zurück. Aus- und Fortbildung in Fragen des Datenschutzes muß daher erheblich mehr Gewicht beigemessen werden als bisher. Insbesondere sind Bemühungen zu fördern, den Datenschutz in den einschlägigen Ausbildungsplänen (Informatikunterricht in der Schule, Rechts- und Informatikstudium in den Hochschulen) sowie den Fortbildungsveranstaltungen an der öffentlichen Verwaltung als obligatorisches Fach zu verankern.

Die Datenverarbeitungstechniken haben sich gegenüber der Zeit des Volkszählungsurteils geradezu revolutionär verändert. Der Umsetzung des Volkszählungsurteils durch die Schaffung der eigenen Rechtsgrundlagen muß daher verstärkt die Entwicklung geeigneter technisch-organisatorischer Maßnahmen zur Seite gestellt werden. Der Blick des Datenschutzes muß sich stärker auf die Technik des Verarbeitunsprozesses selbst richten. Dies bedeutet nicht nur die Entwicklung spezifischer Datenschutzvorkehrungen für neue informationstechnische Entwicklungen (Miniaturisierung der Rechner, Chipkarten, neue Vernetzungstechniken), sondern auch neuer komplexer Anwendungsformen (z. B. im Bereich des Zahlungsverkehrs, der Straßenbenutzung oder der Textverarbeitung).

Die Europäische Union wird zunehmend zur Informations- und Datengemeinschaft. Dies macht einen europäischen Datenschutz erforderlich. Die Konferenz teilt mit den europäischen Nachbarn nicht nur die Überzeugung, daß der Datenschutz in Europa harmonisiert werden muß, sondern auch, daß die Rechte der Gemeinschaftsbürger auf einem hohen Niveau gesichert werden müssen, damit die Öffnung der Grenzen für Güter, Kapital und Dienstleistungen - und damit auch für persönliche Daten - nicht zu Nachteilen für den einzelnen führt.

Innerhalb von Deutschland wirft die Integration der neuen und der alten Bundesländer nach wie vor Probleme auf. Nach wie vor besteht die Neigung, über Bürger aus den neuen Bundesländern erheblich mehr Daten zu erheben und unter erleichterten Bedingungen Daten zu verarbeiten, als dies in den alten Ländern der Fall wäre.

Die Notwendigkeit für Übergangsregelungen in den neuen Bundesländern wird nicht bestritten; die Eingriffe in Persönlichkeitsrechte müssen aber dennoch verhältnismäßig, erforderlich und darüber hinaus zeitbefristet sein. Aus dem Einigungsprozeß herrührende Sonderregelungen und Verwaltungsvorschriften sind nicht festzuschreiben, sondern auch im Sinne der informationellen Selbstbestimmung schrittweise abzubauen.

Anlage 2.2

Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam

Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten von Bund und Ländern verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern und
- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte „Gesundheitskarten", etwa „Service-Karten" von Krankenversicherungen und privaten Anbietern, „Notfall-Karten", „Apo-(theken)-Cards" und „Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen „Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkartentechnik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkartentechnik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller - etwa ein Krankenversicherungsunternehmen oder eine Krankenkasse - mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z. B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karteninhabern vorbehält bzw. erleichert.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sogenannten Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die „Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkartentechnik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten - wie den Medizinern - und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest - vorbehaltlich weiterer Punkte - die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.
- Die freiwillige Gesundheitskarte darf nicht - etwa durch Integration auf einem Chip - die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.
- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.

- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung - z. B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung - entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.
- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.
- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

Anlage 2.3

Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam

Informationsverarbeitung im Strafverfahren
(bei Stimmenthaltung Bayerns)

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben.

Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiter verarbeitet werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4 §§ 474 ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz - BT-Drucksache 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittlungsakten enthalten eine Vielzahl höchstsensibler Daten insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren - auch mit Zwangsmitteln - erhobenen Daten nicht entsprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten. Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend normenklar festzulegen.

1.1 Insgesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.

1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftserteilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen.

2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z. B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z. B. Spurendokumentations- und Recherchesysteme).

2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden, wenn dies zur Vorgangsverwaltung zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen.

In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrt wird. Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegriffen werden muß.

Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrunde liegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z. B. bei Fahrlässigkeitstaten der Fall sein. Bei laufenden Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach § 154 StPO oder die Gesamtstrafenbildung gegeben sein.

2.3 Für einen Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Daten der jeweils anderen Behörden ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei abstrakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß.

Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§§ 152 Abs. 2, 160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden - also auch von anderen Staatsanwaltschaften - Auskunft verlangen (§ 161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit - ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens - von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktabrufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu begründen sein. Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften. Auf § 78 SGB X ist in diesem Zusammenhang hinzuwei-

sen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.

2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert.

Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./29. September 1981 zu „Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften", vom 24./25. November 1986 „Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" und vom 5./6. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 3. November 1988).

Anlage 2.4

Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam

Abbau des Sozialdatenschutzes
(gegen die Stimme Bayerns)

Der Gesetzgeber hat in den vergangenen Monaten die Möglichkeit der Überprüfung von Sozialleistungsempfängern ohne deren vorherige Befragung oder Kenntnis in drastischem Umfang vermehrt. Insbesondere durch das seit dem 1. Juli 1993 geltende Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms ist das Kontrollinstrumentarium von Sozial- und Arbeitsämtern noch einmal erheblich erweitert worden. Ohne Rücksicht auf konkrete Anhaltspunkte für einen unberechtigten Leistungsbezug im Einzelfall sind künftig automatisierte Datenabgleiche zwischen Sozialhilfeträgern sowie zwischen diesen und der Arbeitsverwaltung bzw. der Kranken-, Unfall- und Rentenversicherung gestattet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist sehr besorgt über diese Entwicklung, die zu einem immer dichteren Datenverbundsystem im Sozialleistungsbereich und zu immer nachhaltigeren Eingriffen in das Recht auf informationelle Selbstbestimmung aller Betroffenen, d. h. auch und gerade der großen Mehrheit rechtstreuer Antragsteller und Leistungsbezieher, führt.

Mit Nachdruck wenden sich die Datenschutzbeauftragten gegen Versuche von Sozialverwaltungen, bei der Umsetzung der neuen Kontrollregelungen durch extensive Interpretation über den gesetzlich vorgegebenen Rahmen hinauszugehen. So erlaubt beispielsweise der neu gefaßte § 117 Abs. 3 des Bundessozialhilfegesetzes entgegen der Handhabung einzelner Kommunen keinen automatisierten Datenabgleich zwischen Sozialhilfedatei und Kraftfahrzeug-Register, sondern nur den Vergleich von Angaben in Verdachtsfällen.

Die dargestellte Entwicklung macht es erneut notwendig, auf die verfassungsrechtliche Qualität des Grundsatzes der Datenerhebung beim Betroffenen hinzuweisen. An dem Prinzip, daß bei der Überprüfung der Leistungsberechtigung und der Nachweise Auskünfte zunächst beim Antragsteller anzufordern sind und nur auf Grund konkreter Verdachtsmomente Nachfragen bei dritten Stellen oder Datenabgleiche erfolgen dürfen, muß für den Regelfall festgehalten werden, soll der einzelne mündiger Bürger bleiben und nicht zum bloßen Objekt staatlicher Verhaltenskontrolle werden.

Sorge äußert die Konferenz auch über die hartnäckigen Bestrebungen, Datenbestände der Sozialverwaltung für immer neue Zwecke und Adressaten zu öffnen. Beispiele dafür sind die im Gesetzgebungsverfahren zum 2. SGB-Änderungsgesetz im letzten Augenblick gescheiterten Anträge, Polizei und Staatsschutz in unvertretbarem Umfang Zugriff auf Daten Arbeitsloser und sonstiger Sozialleistungsempfänger zu geben. Das Sozialgeheimnis muß ein wirksamer Sonderschutz für die besonders sensiblen Daten in der Sozialverwaltung bleiben. Nur dies entspricht der Abhängigkeit des einzelnen von staatlichen Leistungen und der sich daraus ergebenden speziellen Verletzlichkeit seines Rechts auf informationelle Selbstbestimmung.

Anlage 2.5

Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam

Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation
(Postneuordnungsgesetz - PTNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718)

und zu der dafür erforderlichen Änderung des Grundgesetzes
(BR-Drs. 114/94 = BT-Drs. 12/6717)

I.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.

II.

Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom 25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten.

Die Datenschutzbeauftragten halten insbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:

a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.

b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.

c) Das Post- und Telekommunikationswesen muß auf Dauer - auch nach dem Wegfall der Monopole - einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kriterien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.

d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.

e) Die vorgesehene Vorschrift zum Einzelentgeltnachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen, wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufen bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.

f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des § 14 a Fernmeldeanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.

III.

Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des § 12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (BR-Drs. 416/91).

Anlage 2.6

Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam

Ausländerzentralregistergesetz
(gegen die Stimme Bayerns)

Das Ausländerzentralregister beim Bundesverwaltungsamt in Köln existiert seit 40 Jahren ohne gesetzliche Grundlage. Derzeit stehen den verschiedenen Benutzern des Registers Daten zu mindestens 8 Millionen Ausländern, die sich in der Bundesrepublik aufhalten oder aufgehalten haben, zur Verfügung. Gespeichert sind neben Daten zur Identifizierung und weiteren Beschreibung der Person insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 2. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.

Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehen, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern - worauf die Entwurfsbegründung hinweist - der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen, unter denen u. a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen - wenn auch reduzierten - Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

Anlage 2.7

Entschließung der Datenschutzbeauftragten des Bundes und der Länder zu dem Entwurf der NADIS-Richtlinien vom 2. Mai 1994

(mit Stimmenthaltung von Bayern und Thüringen)

Das von den Verfassungsschutzbehörden des Bundes und der Länder betriebene Verbundsystem NADIS-PZD (Nachrichtendienstliches Informationssystem/Personenzentraldatei) ist nach den Vorgaben der in Überarbeitung befindlichen NADIS-Richtlinien und der nunmehr erstellten Dateianordnung als Aktenhinweissystem zu qualifizieren. Die NADIS-Richtlinien und die Dateianordnung haben sich hinsichtlich ihres Regelungsgehaltes an den Bestimmungen der Verfassungsschutzgesetze zu orientieren.

Die Datenschutzbeauftragten des Bundes und der Länder halten den Entwurf der NADIS-Richtlinien und der Dateianordnung für die Personenzentraldatei für zu weitgehend und fordern deshalb:

- Die in der Personenzentraldatei gespeicherten personenbezogenen Daten sind auf das unerläßlich notwendige Maß zu reduzieren. Eine solche automatisierte Datei darf nach den bindenden Vorgaben des Bundesverfassungsschutzgesetzes nur die Daten enthalten, die für das Auffinden der Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Eine Erweiterung für andere Identifizierungszwecke scheidet somit aus.

  Die Dateianordnung enthält darüber hinaus Arten von Daten, die über den Zweck einer Aktenhinweisdatei hinausgehen.

- Alle Rechtsvorschriften, die für die an dem zu übermittelnden Datensatz beteiligten Verfassungsschutzbehörden maßgeblich sind, sind zu beachten. Die in dem Entwurf der NADIS-Richtlinien enthaltenen Regelungen für die Übermittlung personenbezogener Daten sehen hingegen vor, daß hierfür ausschließlich das Recht der übermittelnden Stelle gelten soll.

  Die Dauer der Speicherung von Protokolldatenbeständen ist einheitlich zu regeln. Eine Differenzierung, ob die ursprünglich in der Personenzentraldatei erfaßte Information infolge Fristablaufs oder auf Grund einer Einzelfallentscheidung gelöscht wurde, erscheint nicht sachgerecht.

  Außerdem muß sichergestellt sein, daß Protokolldaten, so wie es die Verfassungsschutzgesetze vorsehen, nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage verwendet werden.

  Die Datenschutzbeauftragten sind im Rahmen der Durchführung und Fortentwicklung des Nachrichtendienstlichen Informationssystems frühzeitig zu unterrichten und zu beteiligen. Dies muß insbesondere bei der Vorbereitung von datenschutzrechtlichen Regelungen gelten.

Anlage 2.8

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. August 1994 in Potsdam

Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik
- EG-Statistikverordnung -
(KOM [94] 78 endg.; Ratsdok. 5615/94 = BR-Drs 283/94)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings darauf hin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs 283/94 - Beschluß -).

Gegen den vorgelegten Vorschlag einer Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:

1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen - insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung - bei dieser Stelle bereits auf Grund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.

   Zugleich sollte EUROSTAT zumindest einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotenen Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht wie in Art. 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189 b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sogenannte Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nichtvertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff „statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 - allerdings mit einem anderen Begriffsinhalt - definiert wird. Der Begriff „statistische Geheimhaltung" sollte an einer Stelle in der Verordnung und so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag.

6. Gemäß dem Grundsatz der Subsidiarität sollte - ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) - auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.

7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag. Dieser gebietet hier, daß - jedenfalls grundsätzlich - die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.

   Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z. B. dem Steuer- oder auch dem Sozialgeheimnis, unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nicht-Gemeinschaftsstatistiken zuständigen Stellen vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen. Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

Anlage 2.9

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer 48. Sitzung

Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

   Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sogenannte Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, d. h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

Anlage 2.10

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer 48. Sitzung

Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als 10 Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Statt dessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z. B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz),
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sogenannten Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes des Bürgers entgegenwirken.

Anlage 2.11

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer 48. Sitzung

Datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (EUROPOL)

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

- Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die materielle Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleiben die Zuständigkeiten und die dazugehörigen Befugnisse des BKA als nationale Stelle für den Informationsverkehr mit EUROPOL unberührt.
- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, zum Beispiel durch eine Protokollerklärung zum EUROPOL-Übereinkommen, trifft.

Anlage 2.12

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer 48. Sitzung

Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und Nachrichtendiensten

Geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse müssen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Dies betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.
- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtssprechung des Bundesverfassungsgerichts sicherzustellen.

Anlage 2.13

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer 48. Sitzung

Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994
(KOM (94) 128 endg. - COD 288)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.
2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei „berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.
3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.
4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte - wie im ursprünglichen Richtlinienentwurf vorgesehen - untersagt werden.
5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte - wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah - auf Unionsebene garantiert werden.
6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinie aufgenommen werden, z. B. indem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.
7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z. B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedstaaten, diese Anregungen zu unterstützen.

3. Gemeinsame Erklärungen und Stellungnahmen der Konferenz der Europäischen Datenschutzbeauftragten

Anlage 3.1

Gemeinsame Erklärung der Konferenz der Europäischen Datenschutzbehörden zu dem Verhältnis zwischen den Datenschutzrichtlinien des Europäischen Parlamentes und des Rates und Maßnahmen zur Entwicklung neuer Telekommunikationsnetze und -dienste
Konferenz in Madrid am 25./26. Mai 1994

Seit der Veröffentlichung des Grünbuchs über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte (KOM (87) 290, 30. Juni 1987) hat die Europäische Kommission zahlreiche Vorschläge für Richtlinien und andere Maßnahmen zur schnellen Einführung neuer Telekommunikationsdienste und zum Aufbau transeuropäischer Telekommunikationsnetze gemacht. Einige dieser Vorschläge sind bereits angenommen worden oder werden bald angenommen.

Während keine dieser vorgeschlagenen oder beschlossenen Maßnahmen selbst ein hinreichendes Niveau zum Schutz personenbezogener Daten und der Privatsphäre von Unionsbürgern vorsieht, werden die wichtigen Vorschläge für eine Richtlinie betreffend den Schutz personenbezogener Daten und der Privatsphäre im Zusammenhang digitaler Telekommunikationsnetze (ISDN-Richtlinie SYN 288) und für eine Rahmenrichtlinie zum

Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Rahmenrichtlinie SYN 287) nur zögerlich beraten.

Die Europäischen Datenschutzbeauftragten sehen die konkrete Gefahr, daß beide Datenschutzrichtlinien schon obsolet sein könnten, wenn sie schließlich in Kraft gesetzt werden, weil zahlreiche spezielle Maßnahmen der Union zur Einführung neuer Telekommunikationsdienste und -netze dann bereits umgesetzt sein werden. Die Datenschutzbeauftragten halten eine Synchronisierung und Harmonisierung zwischen den Datenschutzrichtlinien und Richtlinien sowie anderen Maßnahmen zur Entwicklung von neuen Telekommunikationsdiensten und -netzen für dringend erforderlich.

Es gibt zahlreiche Vorschläge und Dokumente auf europäischer Ebene im Bereich Telekommunikation, die in bisher unbekanntem Ausmaß zu einer Verarbeitung personenbezogener Daten führen werden, die aber Probleme des Persönlichkeitsschutzes und des Datenschutzes nicht einmal erwähnen. Ein aktuelles Beispiel ist die vorgeschlagene Verordnung des Rates über Gemeinschaftszuschüsse für transeuropäische Netze (KOM (94) 62 endg.).

Die Europäischen Datenschutzbeauftragten fordern deshalb die Organe der Europäischen Union auf, spezielle Datenschutzvorschriften in diejenigen Rechtsakte in diesem Bereich aufzunehmen, deren Verabschiedung vor der Annahme der Rahmenrichtlinie und der Richtlinie zum Datenschutz im ISDN für notwendig gehalten wird.

Anlage 3.2

Stellungnahme
der Europäischen Datenschutzbeauftragten
zum Grünbuch
über ein gemeinsames Konzept
für Mobilkommunikation und Personal Communications
in der Europäischen Union
(von der Kommission vorgelegt)
KOM (94) 145 endg.

Es ist zu begrüßen, daß die Kommission in diesem Grünbuch die Bedeutung eines effektiven Schutzes der Privatsphäre und personenbezogener Daten in der Telekommunikation sehr viel stärker betont, als sie es in zwei vorangegangenen Grünbüchern (KOM (87) 290, 30. Juni 1987; KOM (90) 490, 20. November 1990) getan hat. Die Europäischen Datenschutzbeauftragten unterstützen ausdrücklich die Feststellung der Kommission, daß ohne einen wirksamen Schutz der Privatsphäre die öffentliche Akzeptanz unionsweiter Netze und Dienste nicht sichergestellt werden kann. Das Grünbuch zur Mobilkommunikation enthält die klare Botschaft für Netzbetreiber, Diensteanbieter, Hersteller und Standardisierungsgremien, daß Datenschutz ein Problem von hoher Priorität ist.

I.

Ein wirksamer Schutz der Privatsphäre ist um so wichtiger, als dieses Grünbuch eine qualitative Veränderung in der Entwicklung der Telekommunikationsnetze und -dienste einleitet: In einem zukünftigen Personal Communications System werden einzelne Menschen anstelle von Endgeräten adressiert. Gleichzeitig verschwimmt die Trennungslinie zwischen Fest- und Mobilnetzen. Dieser Wechsel zur Adressierung von Personen anstelle von Endgeräten wirft grundlegend neue Fragen des Persönlichkeitsschutzes auf. In einem zukünftigen nahtlosen Telekommunikationsnetz kann das Recht jedes Nutzers, unbeobachtet zu kommunizieren, entscheidend verkürzt werden. Personen, die eine persönliche Nummer benutzen, sollten über die Wirkung einer derartigen Nummer als Personenkennzeichen aufgeklärt werden.

Die Numerierung von Endgeräten ist schon gegenwärtig nicht nur ein Problem der Verteilung knapper Ressourcen und der Begrenzung von Kosten der Programmanpassung (vgl. Grünbuch, IV. 2 VI Numerierung), sondern sie wirft auch datenschutzrechtliche Fragen auf. Dies wird eine der wesentlichen Aufgaben des entstehenden Europäischen Amtes für Numerierung (ENO) sein, das in Kopenhagen eingerichtet werden soll. Mit der Einführung von Personal Communications wird man jedoch Menschen, und nicht nur Endgeräte, numerieren müssen. Die Numerierung von Menschen ist keine Frage der Verteilung knapper Ressourcen, sondern in erster Linie eine Frage des Grundrechtsschutzes und insbesondere des Schutzes der Privatsphäre.

Aus der Sicht des Persönlichkeitsschutzes ist es deshalb entscheidend, daß bei der Entwicklung neuer weltweiter Telekommunikationsnormen wie z. B. für das Universelle Mobile Telekommunikationssystem (UMTS) zumindest die alternative Option erhalten bleibt, ohne Zwang zur Identifizierung kommunizieren zu können. Diese alternative Option kann nicht den Marktkräften überlassen bleiben, sondern muß vom europäischen Gesetzgeber gesichert werden. Sie sollte ohne zusätzliche Kosten für den Benutzer angeboten werden.

II.

Was die Frage freiwilliger Verhaltenskodizes für Diensteanbieter (vgl. Grünbuch, IV. 2 II Bereitstellung von Diensten, Randziffer 4) betrifft, ist darauf hinzuweisen, daß in einigen Mitgliedstaaten spezielle nationale Rechtsvorschriften (nicht nur freiwillige Verhaltenskodizes) zum Datenschutz gelten, die unter anderem auf Diensteanbieter Anwendung finden. Falls das Gemeinschaftsrecht - wie es das Grünbuch vorschlägt - unterscheiden sollte zwischen zwingenden grundlegenden Anforderungen für Netzbetreiber auf der einen Seite und freiwilligen Verhaltenskodizes für Diensteanbieter auf der anderen Seite, könnte nationales Recht, das Diensteanbieter verpflichtet, möglicherweise gegen Gemeinschaftsrecht verstoßen. Bei dem Konsultationstreffen am 16./17. Juni 1994 in Brüssel wurde von seiten der Generaldirektion XIII betont, daß dies nicht der Fall sei und daß das Grünbuch sich lediglich zu zusätzlichen Anforderungen für Diensteanbieter äußere. Die bestehenden rechtlichen Anforderungen sollten unverändert fortgelten, aber zusätzliche Anforderungen sollten nur in freiwillige Verhaltenskodizes aufgenommen werden. Dies sollte zumindest in der zukünftigen Gemeinschaftsgesetzgebung klargestellt werden.

Die zugrunde liegende Unterscheidung des Grünbuchs zwischen Netzbetreibern, die rechtlichen Verpflichtungen und Lizenzvereinbarungen unterliegen sollen, und Diensteanbietern, die lediglich an freiwillige Verhaltenskodizes gebunden sein sollen, überzeugt allerdings nicht völlig. Es mag durchaus sein, daß Netzbetreiber größere Datenbestände verarbeiten, aber Diensteanbieter verarbeiten ebenfalls personenbezogene Daten, insbesondere wenn sie Dienste wie Abrechnung, Mailboxen etc. anbieten. Es erscheint deshalb erforderlich, daß das Gemeinschaftsrecht entweder die gleichen rechtlichen Verpflichtungen für Diensteanbieter und Netzbetreiber vorsieht, soweit es die grundlegende Anforderung „Datenschutz" betrifft, oder zumindest einzelstaatliche Gesetzgebung dieses Inhalts zuläßt. Die Tatsache, daß Netzbetreiber quantitativ mehr personenbezogene Daten verarbeiten als Diensteanbieter, rechtfertigt keine Privilegien für Diensteanbieter. Dies erscheint als Deregulierung vom falschen Ende her, die nicht gerechtfertigt ist durch die Grundsätze der Verhältnismäßigkeit und der Subsidiarität.

III.

Mit der bevorstehenden Überarbeitung der Ratsrichtlinie zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (Open Network Provision - ONP - 90/387/EWG) und der übrigen ONP-Richtlinien sollte die restriktive Bestimmung zum Datenschutz als einer grundlegenden Anforderung, „wo dies angebracht ist" (Art. 3 Abs. 2 ONP-Rahmenrichtlinie), geändert werden. Der Datenschutz, wie er im entstehenden Gemeinschaftsrecht (z. B. in der vorgeschlagenen Rahmenrichtlinie zum Datenschutz und in der ISDN-Richtlinie) vorgesehen ist, ist nicht nur eine grundlegende Anforderung, „wo dies angebracht ist", sondern unter allen Umständen, die das Gemeinschaftsrecht (ebenso wie einzelstaatliches Recht in Übereinstimmung mit dem Gemeinschaftsrecht) vorsieht. Die ONP-Rahmenrichtlinie enthält keine vergleichbaren Einschränkungen anderer grundlegender Anforderungen wie

etwa der Sicherheit des Netzbetriebes oder der Aufrechterhaltung der Netzintegrität. Der Datenschutz hat keine geringere Bedeutung und sollte nicht hintangestellt werden dürfen, wenn Netzbetreiber oder Diensteanbieter dies für angemessen halten.

IV.

Die Frage der gegenseitigen Anerkennung von Lizenzen erhebt sich in bezug auf Netzbetreiber und Diensteanbieter, wie man dem geänderten Vorschlag für eine Richtlinie über die gegenseitige Anerkennung von Lizenzen und anderen nationalen Genehmigungen für Telekommunikationsdienste (KOM (94) 41 endg.) entnehmen kann. Weder die gegenseitige Anerkennung von Lizenzen noch - in Zukunft - ein europäisches Lizenzierungssystem sollte zu einer Absenkung der bestehenden Standards für den Datenschutz und den Schutz der Privatsphäre führen, wie sie durch nationale Gesetzgebung und Lizenzbedingungen festgelegt sind. Das muß auch gelten, wenn die vorgeschlagenen Datenschutzrichtlinien in Kraft treten; die Umsetzung des darin vorgesehenen Datenschutzstandards sollte weder durch die gegenseitige Anerkennung von Lizenzen noch durch ein europäisches Lizenzierungssystem beeinträchtigt werden.

V.

Satellitenkommunikation unter Einsatz von niedrigfliegenden Satelliten (Low earth orbit-satellites/LEOs) wird eine immer wichtigere Rolle im System der weltweiten Personal Communications spielen (vgl. Grünbuch, IV. 2 VII Randziffer 7).

Einerseits kann die Satellitenkommunikation das Risiko der Aufzeichnung präziser Bewegungsprofile begrenzen, soweit ein satellitengestütztes Netz nicht auf kleinen Zellen wie die terrestrischen Mobilfunknetze beruht. Der angerufene Teilnehmer empfängt Signale innerhalb der verhältnismäßig großen Ausleuchtzone des Satelliten und kann deshalb nicht in derselben Weise lokalisiert werden, wie er in terrestrischen Zellularsystemen lokalisiert werden könnte. Auf der anderen Seite birgt die Satellitenkommunikation eine größere Gefahr für die Vetraulichkeit, weil Daten von leistungsstarken Erdfunkstationen zum Raumsegment (uplink) übermittelt werden und dann zurückübermittelt werden zu anderen Erdfunkstationen (downlink). Effektive Verschlüsselungstechniken müssen deshalb schon innerhalb der Erdfunkstation angewandt werden, bevor Daten zum Raumsegment übertragen werden, um das Abhören der Verbindung in der Nähe der Erdfunkstation zu verhindern.

VI.

Diese Stellungnahme kann nicht auf alle Details des Grünbuchs eingehen. Die Europäischen Datenschutzbeauftragten bitten jedoch die Kommission darum, möglichst frühzeitig Gelegenheit zu weiteren Stellungnahmen zu Vorschlägen für eine Gemeinschaftsgesetzgebung oder Normentwicklung zu erhalten, die sich aus diesem Grünbuch und dem anschließenden Konsultationsprozeß ergeben kann.

Anlage 3.3

Stellungnahme der Europäischen Konferenz der Datenschutzbeauftragten zum Analysebericht der Europäischen Kommission (DG XIII) entsprechend der ONP-Rahmenrichtlinie - (Richtlinie des Rates 90/387/WG) -

- Übersetzung aus dem Englischen -

Allgemeine Anmerkungen

Der Rat der Europäischen Gemeinschaften hat die Harmonisierung der Bedingungen für offenen und effizienten Zugang zu Telekommunikationsnetzen und -diensten (Open Network Provision - ONP) vorrangig behandelt.

Die Europäischen Datenschutzbeauftragten sind der Ansicht, daß Datenschutz eine bedeutendere Rolle spielen sollte, als dies jetzt der Fall ist. In seiner ONP-Richtlinie zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (90/387/EWG vom 28. Juni 1990) hat der Rat bestimmt, daß die ONP-Bedingungen „. . . den Zugang zu öffentlichen Telekommunikationsnetzen oder öffentlichen Telekommunikationsdiensten nicht beschränken (dürfen), es sei denn aus Gründen, die auf *grundlegenden Anforderungen* beruhen und die in Übereinstimmung mit dem Gemeinschaftsrecht stehen. Diese *grundlegenden Anforderungen sind . . . Datenschutz, wo dies angebracht ist.*"

Die Europäischen Datenschutzbeauftragten sind der Ansicht, daß diese eingeschränkte Vorstellung über den Schutz personenbezogener Daten revidiert werden sollte. Der Schutz personenbezogener Daten, wie er durch das zukünftige Gemeinschaftsrecht (wie die vorgeschlagene Rahmenrichtlinie über den Schutz personenbezogener Daten und die ISDN-Richtlinie über den Datenschutz) sichergestellt wird, ist nicht nur eine grundlegende Anforderung, „wo dies angebracht ist", sondern unter allen im Gemeinschaftsrecht beschriebenen Umständen (sowie dem nationalen Recht in Übereinstimmung mit dem Gemeinschaftsrecht). Die ONP-Rahmenrichtlinie enthält keine solchen Einschränkungen für andere grundlegende Anforderungen wie die Sicherheit des Netzbetriebs und die Aufrechterhaltung der Netzintegrität. Der Schutz personenbezogener Daten ist nicht von geringerer Bedeutung, und es sollte nicht erlaubt sein, ihn zu beeinträchtigen, wenn Netzbetreiber und Diensteanbieter dies für angemessen halten.

Der Analysebericht schlägt vor, die Anwendung der ONP-Prinzipien auf verschiedene andere Telekommunikationsdienste zu erweitern, insbesondere intelligente Netzfunktionen, Netzmanagement, den Nahverkehrsbereich und die Breitbandkommunikation. Die Europäischen Datenschutzbeauftragten sind der Ansicht, daß spezifische Datenschutzregelungen in jede der zukünftigen ONP-Richtlinien aufgenommen werden sollten. Es ist von großer Bedeutung, die Schaffung neuer Telekommunikationsdienste und -infrastrukturen ohne hinreichende Datenschutzmaßnahmen zu verhindern. Die gegenwärtigen Fassungen der Vorschläge für die ISDN-Richtlinie und die allgemeine Datenschutzrichtlinie decken nur einige der spezifischen Probleme von Telekommunikationsdiensten ab. Besonders der geänderte Vorschlag für die ISDN-Richtlinie ist in seinem Anwendungsbereich im Vergleich mit dem ursprünglichen Vorschlag erheblich eingeschränkt worden. Die Europäischen Datenschutzbeauftragten beabsichtigen, kurzfristig eine Erklärung zu dem geänderten Vorschlag für eine ISDN-Richtlinie abzugeben.

Grundsätzlich sollte die Verarbeitung personenbezogener Daten zur Erbringung von Telekommunikationsdiensten auf ein Minimum reduziert werden. Dies gilt besonders für Verbindungsdaten. Die verbleibenden notwendigen Daten sollten im Prinzip nicht an Dritte weitergegeben werden (Zweckbindungsgrundsatz).

Anwendung von ONP-Prinzipien auf intelligente Netzfunktionen

Der Bericht stellt fest, daß die Kommission sicherstellen wird, daß die relevanten Regelungen der vorgeschlagenen Richtlinie für den Sprachtelefondienst vollständig in diesem Bereich angewendet werden (S. 9). Dies sollte die Datenschutzregelungen der Richtlinie einschließen (weitere Anmerkungen zu dieser Richtlinie siehe unten).

Anwendung der ONP-Prinzipien auf das Netzmanagement

Die NERA-Studie empfiehlt, daß die Kommission die Wettbewerbsgleichheit zwischen Telekommunikationsorganisationen und unabhängigen Mehrwertdienstanbietern sicherstellen sollte (S. A 1-5, Empfehlung 1). Die Europäische Union sollte in diesem Zusammenhang ebenfalls sicherstellen, daß das Prinzip des Fernmeldegeheimnisses - wie in der nationalen Gesetzgebung der Mitgliedstaaten für Telekommunikationsorganisationen niedergelegt - auch in vollem Umfang auf Mehrwertdienstanbieter anwendbar ist.

Die Studie empfiehlt auch die Einführung von einzeln aufgeschlüsselten Rabatten auf den Rechnungen (Tabelle: Open Network Provision Supply Conditions proposed by the study, S. A 1-6). Die Europäischen Datenschutzbeauftragten sind der Auffassung, daß die Informationen über einzelne Rabatte auf den Rechnungen nicht mehr personenbezogene Daten enthalten sollten als die Rechnung selbst, z. B. sollten keine Nummern von Angerufenen aufgenommen werden, wenn der Teilnehmer sich nicht für einen Einzelentgeltnachweis entschieden hat. Der extensiven Datenverarbeitung, die dem gesamten Prozeß der Rechnungsstellung zugrunde liegt, sollte unabhängig von der Option, die der Teilnehmer gewählt hat, mehr Aufmerksamkeit gewidmet werden.

Zugang zum Breitbandnetz

Betreffend die Anwendung von ONP-Prinzipien auf Breitbandkommunikation, besonders Video- und Multimedia-Applikationen, sind die Europäischen Datenschutzbeauftragten der Auffassung, daß hierdurch völlig neue Fragen aufgeworfen werden. Da die Grenze zwischen Telekommunikation und Rundfunk zunehmend verwischt wird, wird es immer wichtiger werden, die Teilnehmer effektiv gegen die Schaffung elektronischer Profile über ihr Verhalten zu schützen.

Anwendung der ONP-Prinzipien auf den Sprachtelefondienst

Der Vorschlag für eine Richtlinie des Rates zur Einführung des offenen Netzzugangs (ONP) beim Sprachtelefondienst ist in diesem Juni vom Europäischen Parlament zurückgewiesen worden. Daher nehmen die Europäischen Datenschutzbeauftragten die Gelegenheit wahr, zu den Datenschutzregelungen des zurückgewiesenen Vorschlags Stellung zu nehmen, um zur Verbesserung der Datenschutzregelung in späteren Vorschlägen beizutragen.

Der geänderte Vorschlag der ONP-Sprachtelefondienstrichtlinie (KOM (93) 182 endg. - SYN 437) enthielt Regelungen zum Einzelentgeltnachweis (Art. 14), zu Teilnehmerverzeichnissen (Art. 15) und die Begründungen, die auf grundlegende Anforderungen in Einklang mit dem Gemeinschaftsrecht gestützt werden (Art. 21 Ziff. 5).

Der geänderte Vorschlag enthielt nur generelle Verweise auf die relevante Gesetzgebung über den Schutz personenbezogener Daten (Art. 14, 15, 21 Ziff. 5 d). In dieser Hinsicht war der Vorschlag unvollständig und bedurfte der Ergänzung durch substantielle Regelungen über den Datenschutz beim Sprachtelefondienst.

Es muß jedoch zur Kenntnis genommen werden, daß der Vorschlag der Kommission ausdrücklich feststellt, daß „Nutzungseinschränkungen, die aus grundlegenden Anforderungen abgeleitet werden, ... mit ordnungspolitischen Mitteln und nicht durch technische Einschränkungen durchzusetzen (sind)". Dieser Vorschlag könnte - wenigstens in der englischen Version - so ausgelegt werden, daß keinerlei technische Einschränkungen zur Sicherstellung des Datenschutzes verhängt werden könnten. Dies würde im Widerspruch zu der Ansicht verschiedener Europäischer Datenschutzbeauftragter stehen, daß effektive Maßnahmen zum Schutz personenbezogener Daten nicht allein auf gesetzliche Regelungen gestützt werden können, sondern auch durch technische Standards unterstützt werden müssen. Daher bedarf wenigstens der englische Text der Klarstellung („... *nicht nur* durch technische Einschränkungen ...").

Darüber hinaus wurde im geänderten Vorschlag der Kommission für eine Sprachtelefondienstrichtlinie die Regelung über Einzelentgeltnachweise derart geändert, daß alle Teilnehmer, die dem nicht widersprochen haben, automatisch Einzelentgeltnachweise erhalten würden (Art. 14). Der Verweis auf die relevante Datenschutzgesetzgebung blieb unverändert. Die Europäischen Datenschutzbeauftragten haben es begrüßt, daß der gemeinsame Standpunkt vom 30. 6. 1993 den ursprünglichen Vorschlag in dieser Hinsicht wiederhergestellt hat, so daß Einzelentgeltnachweise nur auf Verlangen erhältlich sind. Diese Regelung sollte in dem neuen Vorschlag, der durch die Kommission vorbereitet werden wird, erhalten bleiben. Der extensiven Datenverarbeitung, die dem gesamten Verfahren der Rechnungserstellung zugrunde liegt, sollte wiederum mehr Aufmerksamkeit gegeben werden, unabhängig davon, welche Option der Teilnehmer gewählt hat.

Der Rat hat ebenfalls die Regelung aus Art. 15 b gestrichen, nach dem die Benutzer berechtigt sind, sich „ohne zusätzliche Kosten" in öffentliche Telefonverzeichnisse eintragen oder nicht eintragen zu lassen. Dies würde es für die Benutzer schwieriger machen, sich nicht in öffentliche Telefonverzeichnisse eintragen zu lassen, ein Recht, das die meisten Europäischen Datenschutzbeauftragten bisher für wesentlich gehalten haben.

Vorschlag für eine Entscheidung des Rates über Grundsätze für den universellen Dienst im Bereich der Telekommunikation (KOM (93) 543 endg. vom 15. November 1993)

Das Konzept des offenen Netzzugangs sorgt auch für die Schaffung eines universellen Basisdienstes in allen Mitgliedstaaten. Dieser universelle Dienst soll bestimmte gemeinschaftsweite Basismerkmale enthalten, die für jeden Bürger der Gemeinschaft erhältlich sein sollen. Zusätzlich zu diesen Basismerkmalen können Zusatzmerkmale von konkurrierenden Diensteanbietern angeboten werden. In seinem Vorschlag für eine Entscheidung des Rates über Grundsätze für den universellen Dienst im Bereich der Telekommunikation (KOM (93) 543 endg.) hat die Kommission diese Struktur näher ausgeführt, ohne das Problem der Datensicherheit und des Datenschutzes für die Teilnehmer in diesem Bereich überhaupt zu erwähnen. Es gibt nicht einmal einen Verweis auf die grundlegenden Anforderungen aus Art. 3 Ziff. 2 der allgemeinen ONP-Richtlinie, die den Datenschutz enthalten.

Die Europäischen Datenschutzbeauftragten halten es für wesentlich, daß Maßnahmen zum Datenschutz Bestandteil jedes universellen Basistelekommunikationsdienstes werden, der in der Europäischen Union angeboten wird.

Anlage 3.4

Gemeinsame Erklärung der Europäischen Datenschutzbeauftragten 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. Allgemeine Anmerkungen

Die Datenschutzbeauftragten in der Europäischen Union haben in ihrer gemeinsamen Erklärung, die am 25./26. Mai 1994 in Madrid angenommen wurde, betont, daß eine Notwendigkeit für die Schaffung spezifischer Datenschutzregelungen im Bereich der Telekommunikation besteht, in dem gegenwärtig zahlreiche Dienste und transeuropäische Netze eingeführt werden. Der geänderte Vorschlag für eine ISDN-Richtlinie ist ein bedeutender Schritt in diese Richtung. Wie in Madrid dargelegt wurde, müssen andere Gesetzgebungsvorhaben in diesem Bereich mit der ISDN-Richtlinie harmonisiert werden.

B. Einzelne Anmerkungen

1. Artikel 2 - Begriffsbestimmungen

Der Begriff „Telekommunikationsdienste" sollte definiert werden. Dieser Begriff wird in Art. 3 benutzt, um den Anwendungsbereich der Richtlinie festzulegen. Während der Begriff „öffentlicher Telekommunikationsdienst" in Art. 2 Nr. 6 definiert ist, wird in Art. 3 Nr. 2 der Begriff „andere Telekommunikationsdienste, die über das öffentliche Telekommunikationsnetz angeboten werden", benutzt. Beide Regelungen sollten klargestellt werden, indem in Art. 2 eine Definition für „Telekommunikationsdienste" aufgenommen wird.

Art. 2 Nr. 1 und 6 des geänderten Vorschlags beziehen sich auf Telekommunikationsorganisationen und öffentliche Telekommunikationsdienste in nichtliberalisierten Märkten. Unter Berücksichtigung der Tatsache, daß in manchen Mitgliedstaaten die Liberalisierung von Diensten und Netzen unter Umständen schon vor 1998 stattfinden wird, schlagen die europäischen Datenschutzbeauftragten eine flexiblere Formulierung für diese Regelung vor. Wenn die Worte „oder die Europäische Union/Europäische Gemeinschaft" nach den Worten „Mitgliedstaat" und „Mitgliedstaaten" eingefügt würden, wäre die Richtlinie in zukünftig liberalisierten Märkten mit unionsweiten Lizenzierungsverfahren anwendbar.

Die Ausnahme von Rundfunk und Fernsehen in Art. 2 Nr. 2 verstehen die Datenschutzbeauftragten in der Europäischen Union so, daß nur Rundfunk im klassischen Sinne aus dem Anwendungsbereich des Richtlinienvorschlags ausgenommen werden soll. Im Gegensatz dazu sollten interaktive Dienste, die über ein öffentliches Telekommunikationsnetz erbracht, und Telefondienste, die von Kabelfernsehunternehmen angeboten werden, von der Richtlinie erfaßt werden. Sollte es diesbezüglich irgendwelche Zweifel geben, so sollte der Text entsprechend geändert werden.

Es wird allgemein notwendig sein, auf der europäischen Ebene Maßnahmen zu ergreifen, um personenbezogene Daten von Radio- und Fernsehkonsumenten zu schützen, sobald es möglich wird, sie - z. B. im Falle von „Video on demand" - zu identifizieren und elektronische Profile ihres Verhaltens zu erstellen. Die Datenschutzbeauftragten in der Europäischen Union akzeptieren zwar, daß Rundfunk und Fernsehen im klassischen Sinne von diesem Richtlinienvorschlag nicht erfaßt werden, werden aber trotzdem die weitere Entwicklung in diesem Bereich genau beobachten, um Empfehlungen für eventuell notwendige spezifische Maßnahmen durch das Europäische Parlament und den Rat zu geben.

2. Art. 3 - Betroffene Dienste

Das Verhältnis zwischen der zukünftigen allgemeinen Datenschutzrichtlinie (KOM [92] 422 endg. - SYN 287) und dem Vorschlag für eine ISDN-Richtlinie sollte im Text der ISDN-Richtlinie klargestellt und der vorrangige Charakter der allgemeinen Richtlinie bekräftigt werden. Erwägungsgrund 9 sollte überarbeitet werden; die gegenwärtige Formulierung stimmt nicht mit den Regelungen des Art. 3 Nr. 1 überein.

Der geänderte Vorschlag für eine ISDN-Richtlinie (Art. 3 Nr. 2) unterscheidet zwischen Telekommunikationsorganisationen und Diensteanbietern. Während Telekommunikationsorganisationen völlig von der Richtlinie erfaßt werden, gelten für die Diensteanbieter nur die Art. 4, 5, 6, 11, 14 und 16. Die Datenschutzbeauftragten sind der Auffassung, daß einige der übrigen Artikel ebenfalls auf Diensteanbieter angewandt werden sollten. Art. 3 sollte geändert werden, um dies klarzustellen. Die Unterscheidung zwischen Telekommunikationsorganisationen und Diensteanbietern ist nicht gerechtfertigt. Für den Benutzer macht es keinen praktischen Unterschied, ob seine Daten von einer Telekommunikationsorganisation oder einem Anbieter von Telekommunikationsdienstleistungen verarbeitet werden (unabhängig davon, ob diese besonders vertrauenswürdig sind oder nicht). Daher sollte ihm in beiden Fällen ein gleiches Schutzniveau gewährt werden.

Art. 3 Nr. 3 beschreibt die Situation, in der Dienste nicht durch digitale, sondern durch analoge Netzwerke erbracht werden. Es ist zu begrüßen, daß die Mitgliedstaaten die Anwendung der Regelungen dieser Richtlinie auf Dienste, die in analogen Netzwerken erbracht werden, sicherstellen sollen, wo dies technisch möglich ist. Allerdings werden selbst in den Ländern, in denen die Digitalisierung der Netzwerke bereits fortgeschritten ist, überwiegend analoge Endgeräte an digitale Vermittlungsstellen angeschlossen sein (vgl. Art. 12 Nr. 3 des ursprünglichen Vorschlags). Da diese Situation in den meisten Mitgliedstaaten für einige Zeit bestehen bleiben wird, ist es von Bedeutung, daß die vorgeschlagene Richtlinie hier genauso anwendbar ist wie bei Dienstleistungen, die über analoge Netzwerke erbracht werden. Dies könnte erreicht werden, indem die Worte „und Geräte" nach „Netzwerken" in Art. 3 Nr. 3 eingefügt werden.

Bezüglich der Voraussetzung „soweit technisch möglich" sollte bedacht werden, daß eine Reihe von Regelungen der Richtlinie unabhängig von technischen Grenzen angewandt werden können. Dies gilt besonders für Art. 11 bezüglich der Teilnehmerverzeichnisse. „Technische Unmöglichkeit" sollte daher nicht als eine Rechtfertigung zur Abweichung von diesen Regelungen akzeptiert werden. Dies sollte im Text der Nr. 3 entsprechend deutlich gemacht werden.

3. Art. 4 des ursprünglichen Vorschlags - Zweckbindungsgebot/elektronische Profile

Art. 4 Nr. 1 des ursprünglichen Vorschlags enthielt eine Beschränkung für die Erhebung, Speicherung und Verarbeitung personenbezogener Daten durch Telekommunikationsorganisationen auf Telekommunikationszwecke (Zweckbindungsgebot). Die Streichung dieser Regelung im geänderten Vorschlag würde dazu führen, daß nur Art. 7 Buchstabe f des Entwurfs für eine allgemeine Datenschutzrichtlinie anwendbar wäre, der die Befugnis, personenbezogene Daten zu verarbeiten, auf alle Situationen ausdehnt, in denen die Verarbeitung „erforderlich ist zur Verwirklichung des Allgemeininteresses oder des berechtigten Interesses, das von dem Verantwortlichen der Verarbeitung oder von dem Dritten wahrgenommen wird, dem die Daten übermittelt werden, sofern nicht die Interessen des Betroffenen überwiegen". Dies scheint für die Verarbeitung personenbezogener Daten in Telekommunikationsnetzen unzureichend und zu vage zu sein. Aufgrund der spezifischen Beschaffenheit digitaler Nachrichtenübermittlungssysteme sollte das besondere Zweckbindungsprinzip, das in Art. 4 Nr. 1 des ursprünglichen Vorschlags enthalten war, wieder in die ISDN-Richtlinie aufgenommen werden. Das spezifische Zweckbindungsgebot wird an Bedeutung gewinnen, da die Telekommunikationsorganisationen ihre Aktivitäten in zunehmendem Maße diversifizieren. Das Zweckbindungsgebot sollte ebenso für die Verarbeitung personenbezogener Daten durch Diensteanbieter gelten.

Art. 4 Nr. 2 des ursprünglichen Vorschlags verbot die Nutzung personenbezogener Daten, um elektronische Profile der Teilnehmer zu erstellen oder einzelne Teilnehmer nach Kategorien zu sortieren. Diese Regelung ist im geänderten Vorschlag gestrichen worden.

Die Europäischen Datenschutzbeauftragten sind der Auffassung, daß die Nutzung von Verbindungs- und anderen personenbezogenen Daten über das Telekommunikationsverhalten einzelner Teilnehmer zur Erstellung von elektronischen Profilen prinzipiell verboten werden sollte. Die entsprechende Regelung der allgemeinen Datenschutzrichtlinie (Art. 16 Nr. 1 - automatisierte Einzelentscheidungen) bietet in dieser Hinsicht wiederum keinen ausreichenden Schutz für den Teilnehmer. Entsprechend der vom Europäischen Parlament vorgeschlagenen Änderung sollte das Erstellen derartiger elektronischer Profile durch Telekommunikationsorganisationen nur mit der informierten Einwilligung des Teilnehmers erlaubt sein. Die Erbringung von Basisdiensten darf nicht verweigert werden, wenn der Teilnehmer nicht in die Erstellung eines elektronischen Profils einwilligt (vgl. Art. 7 § 3 des ursprünglichen Vorschlags).

4. Art. 5 des ursprünglichen Vorschlags - Speicherung der übertragenen Inhaltsdaten nach dem Ende der Übertragung

Der Vorschlag für eine allgemeine Richtlinie beantwortet die Frage, in welchem Ausmaß die übertragenen Informationen nach dem Ende der Übertragung von Telekommunikationsorganisationen oder Dienstanbietern gespeichert werden dürfen. Daher sollte Art. 5 Nr. 2 des ursprünglichen Vorschlags in einer modifizierten Form wieder aufgenommen werden. Die notwendige spezifische Regelung könnte wie folgt lauten:

„Die Inhalte der übertragenen Informationen dürfen nach Beendigung der Übertragung nicht von der Telekommunikationsorganisation gespeichert werden, es sei denn, dies ist auf Grund von Verpflichtungen erforderlich, die in den Mitgliedstaaten dem Gemeinschaftsrecht entsprechend gesetzlich vorgeschrieben sind."

5. Art. 7 des ursprünglichen Vorschlags – Vertraulichkeit/Geheimhaltung der Telekommunikation

Obwohl viele Mitgliedstaaten für die Vertraulichkeit oder Geheimhaltung der Telekommunikation in ihrer nationalen Gesetzgebung gesorgt haben (einige sogar in ihren Verfassungen) ist es notwendig, dies in die ISDN-Richtlinie aufzunehmen, um einen gemeinschaftsweiten Minimalstandard zu etablieren. Art. 7 Nr. 1 des ursprünglichen Vorschlags sollte daher in einer geänderten Version wieder aufgenommen werden, die wie folgt lauten könnte:

„Die Mitgliedstaaten sollen sicherstellen, daß alle personenbezogenen Daten, die in Verbindung mit Telekommunikationsnetzen und -diensten verarbeitet werden, vertraulich behandelt werden müssen."

Die Vertraulichkeit sollte ausdrücklich auf Verbindungsdaten erstreckt werden, die für die Beobachtung des einzelnen Teilnehmers genausogut genutzt werden können wie Inhaltsdaten. Andererseits könnte es mehr Ausnahmen von der Vertraulichkeit von Verkehrsdaten geben, während der Inhalt der übertragenen Informationen nur unter sehr eingeschränkten Bedingungen Dritten bekanntgegeben werden darf (vgl. Art. 7 Nr. 2 des ursprünglichen Vorschlags).

6. Art. 5 – Abrechnungsdaten

Die Datenschutzbeauftragten betonen nochmals, daß anonyme Zahlungsverfahren den Benutzern in der Europäischen Union als ein Basisdienst angeboten werden sollten. Der Teilnehmer sollte in die Lage versetzt werden, eine informierte Auswahlentscheidung bezüglich der Art der Abrechnung aus einer Reihe von Möglichkeiten einschließlich der Beschränkung auf die Summe der Gebühren zu treffen. Im Falle der Erstellung eines Einzelentgeltnachweises sollte die Speicherung von Daten dem in Erwägungsgrund (10) niedergelegten Prinzip entsprechen, d. h., die Speicherung sollte auf den unbedingt für die Erbringung des Dienstes notwendigen Zeitraum beschränkt werden.

Art. 5 Nr. 1 sollte durch Hinzufügen der Worte „innerhalb der Telekommunikationsorganisation oder des Diensteanbieters" nach dem Wort „Daten" im letzten Satz klarer formuliert werden.

In Art. 5 Nr. 2 sollte das Wort „gesetzlich" gestrichen werden. Dies ist notwendig, da der Zeitraum, innerhalb dessen die Rechnung angefochten werden kann, auch vertraglich festgelegt sein könnte. Datenschutzfreundliche Auswahlmöglichkeiten („privacy options"), wie sie gegenwärtig in den Niederlanden diskutiert werden, wo überhaupt keine Daten für einen längeren Zeitraum als für die Erstellung der Rechnung notwendig gespeichert werden (falls der Benutzer dies wünscht), sollten auch nach der ISDN-Richtlinie erlaubt bleiben.

7. Art. 6 – Verkehrsdaten

Art. 6 sollte wie folgt geändert werden:

„Verkehrsdaten zum Aufbau von Verbindungen, die personenbezogene Daten enthalten, müssen gelöscht werden, sobald ihre Speicherung nicht mehr für die Abrechnung oder andere vertraglich festgelegte Dienste erforderlich ist."

Die gegenwärtige Formulierung von Art. 6 im geänderten Vorschlag ist zu eng, weil Verkehrsdaten nicht nur in den Vermittlungsstellen der Telekommunikationsorganisationen gespeichert werden könnten. Andererseits ist die Formulierung „zur Bereitstellung des entsprechenden Dienstes" im Vergleich zu Art. 10 Nr. 2 des ursprünglichen Vorschlags nicht hinreichend präzise.

8. Art. 8 – Anzeige der Rufnummer des Anrufers

Art. 8 Nr. 1 sollte neu gefaßt werden, um ausdrücklich klarzustellen, daß der anrufende Teilnehmer (oder einzelne Benutzer) in der Lage sein sollte, die Anzeige seiner Rufnummer von seinem Endgerät aus in einfacher Weise in jedem Einzelfall zu unterdrücken, ohne daß die Einschaltung der Telekommunikationsorganisation, des Diensteanbieters oder irgendeines Dritten notwendig ist.

Art. 8 Nr. 2 bezieht sich nur auf Telekommunikationsorganisationen. Die Anwendung dieser Regelung sollte ebenfalls auf Diensteanbieter erstreckt werden.

Die Datenschutzbeauftragten in der Europäischen Union sind generell der Auffassung, daß die Speicherung der übermittelten Rufnummer durch den angerufenen Teilnehmer ohne entsprechende Information des Anrufers eine unfaire Datenverarbeitung darstellt.

In bezug auf den letzten Satz von Art. 8 Nr. 3 gibt es gute Gründe dafür, die Möglichkeit der Beschränkung ankommender Verbindungen auf diejenigen, bei denen die Anzeige der Rufnummer des Anrufers nicht ausgeschlossen worden ist, privaten Einzelpersonen vorzubehalten. Kein Bürger sollte gezwungen werden, sich zu identifizieren, wenn er eine öffentliche Stelle anruft. Telekommunikationsorganisationen, die bisher überhaupt keine derartigen „block-blocking-Einrichtungen" anbieten, sollten damit unter der zukünftigen europäischen Gesetzgebung fortfahren dürfen.

In Art. 8 Nr. 5 sollten die Worte „für den Teilnehmer, der diese Möglichkeit wahrnimmt" nach „kostenfrei" eingefügt werden.

9. Art. 11 – Teilnehmerverzeichnisse

Die Datenschutzbeauftragten in der Europäischen Union unterstützen die in Art. 11 Satz 2 getroffene Regelung, die den Teilnehmer berechtigt, *kostenfrei* ohne Geschlechtsangabe oder überhaupt nicht ins Teilnehmerverzeichnis aufgenommen zu werden. Ein flexibleres System der Nichtaufnahme in Teilnehmerverzeichnissen, wie es in verschiedenen Mitgliedstaaten existiert, sollte erwogen werden (z. B. Nichtaufnahme in das Teilnehmerverzeichnis bei gleichzeitiger Erlaubnis für die Telekommunikationsorganisation oder den Diensteanbieter, die Telefonnummer auf Anfrage weiterzugeben). Diesen Mitgliedstaaten sollte wenigstens gestattet werden, ihre verschiedenen Grade der Nichtaufnahme in Verzeichnisse, die einen höheren Datenschutzstandard ausmachen, beizubehalten.

Art. 11 sollte für alle Arten von Teilnehmerverzeichnissen (konventionelle und elektronische [X-500 etc.]) gelten. Dies sollte in der Regelung entsprechend klargestellt werden.

10. Art. 12 – Überwachung der Kommunikation

Das Verhältnis zwischen Art. 12 Nr. 1 und Art. 12 Nr. 2 muß klargestellt werden. Nr. 1 scheint sich auf die Lizenzierung von Abhöreinrichtungen oder anderen Einrichtungen zum Abfangen von Gesprächen auf einer gesetzlichen Basis zu beziehen. Nr. 2 scheint sich genereller auf das Abhören sowie die Weitergabe des Inhalts von Telefongesprächen zu beziehen. Beide Regelungen bedürfen der Klarstellung.

Im einzelnen sollte Nr. 2 nicht auf eine spezielle Technik („auf Band gespeichert") beschränkt werden, die bald veraltet sein könnte. Sie sollte ebenso auf das Speichern auf Mikrochips und anderen Medien anwendbar sein.

Der Verweis in Art. 12 Nr. 2 sollte auf den gesamten Art. 9 ausgedehnt werden. Anderenfalls wäre die Aufzeichnung von Notrufen bei der Feuerwehr unter der europäischen Gesetzgebung illegal.

11. Art. 13 – Unerbetene Anrufe

In Art. 13 Nr. 2 gibt es einen Unterschied zwischen der englischen Version auf der einen Seite und der französischen und der deutschen Version auf der anderen Seite. Die beiden letzteren beschränken die Anwendbarkeit dieser Ziffer auf die Übermittlung automatischer Ansagen auf „Werbung oder Verkaufsförderung/-forschung" entsprechend Art. 13 Nr. 1. Diese Beschränkung fehlt im englischen Text ohne ersichtlichen Grund. Sie sollte auch in die englische Fassung aufgenommen werden. Sonst wäre es nicht möglich, automatische Telefaxnachrichten an Teilnehmer zu schicken, die darin nicht eingewilligt haben (vgl. Art. 13 Nr. 3).

12. Art. 16 - Rechtsmittel und Ahndung

Art. 16 enthält nur eine Regelung bezüglich der Rechte des einzelnen, die in der allgemeinen Datenschutzrichtlinie enthalten ist. Dies könnte zu rechtlichen Streitigkeiten darüber führen, ob andere ähnliche Regelungen der allgemeinen Richtlinie, besonders Art. 23 über die Haftung, im Telekommunikationskontext angewandt werden kann oder nicht. Um dies zu verhindern, sollte es entweder einen allgemeineren Verweis auf die entsprechenden Artikel in der allgemeinen Richtlinie geben, oder sie sollten alle in die ISDN-Richtlinie aufgenommen werden.

13. Art. 17 - Arbeitsgruppe zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

Art. 17 Nr. 2 bestimmt, daß die Arbeitsgruppe speziell für den Zweck dieser Richtlinie konstituiert werden wird.

Unabhängig davon, welchen Zwecken diese Regelung dienen soll, sind die europäischen Datenschutzbeauftragten der Auffassung, daß es den Mitgliedstaaten überlassen werden sollte, selbst über die Zusammensetzung der Arbeitsgruppe zu entscheiden. Art. 17 Nr. 2 sollte daher gestrichen werden.

Anlage 4

Sonderbericht zur Präzisierung und Erweiterung des Informationsverarbeitungsgesetzes Berlin im Auftrag des Unterausschusses „Datenschutz" des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses von Berlin

In den Jahresberichten 1991 (Abschnitt 2.1) und 1992 (Abschnitt 6.2) hatten wir darauf hingewiesen, daß das Informationsverarbeitungsgesetz Berlin durch weitere Regelungen ergänzt werden sollte, die sich aus dem extensiven Ausbau der Informationstechnik in der Berliner Verwaltung und den damit verbundenen Risiken für die informationelle Selbstbestimmung und der Abhängigkeit der Verwaltungen von der Verfügbarkeit und Integrität der Systeme ergeben.

Diese Ausführungen aus dem Jahresbericht 1992 waren Gegenstand der Sitzung des Unterausschusses „Datenschutz" des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses von Berlin am 2. Juni 1994. Dort wurden von uns konkret folgende Punkte als regelungsbedürftig angesehen:

(1) Rechtlicher Rahmen für die berlinweiten IuK-Infrastrukturen (MAN in Verbindung mit SAZ/LAZ und das ISDN-Sprachkommunikationsnetz der Berliner Verwaltung);

(2) gesetzliche Grundlage für das LIT sowie die angestrebte neue Rechtsform;

(3) Organisation des IuK-Einsatzes und der Durchführung von IuK-Projekten in der Berliner Verwaltung;

(4) Rechtsgrundlagen für die Erhebung von Abrechnungsdaten, insbesondere bei privaten Telefongesprächen und anderer privater Nutzung der Kommunikationsinfrastrukturen;

(5) datenschutzrechtliche Einordnung und Festlegung besonderer Sicherheitsbedingungen bei der Wartung und Fernwartung von IuK-Systemen (einschließlich der ISDN-Nebenstellenanlagen);

(6) rechtliche Präzisierung der Rahmenbedingungen beim Outsourcing (insbesondere bei der Verarbeitung von Daten, die besonderen Berufsgeheimnissen oder sogar Offenbarungsverboten unterliegen);

(7) Ausweitung der Pflicht zur Risikoanalyse und der Erstellung von Sicherheitskonzepten auf alle Projekte zur Verarbeitung personenbezogener Daten;

(8) Schaffung einer Rechtsgrundlage für personenbezogene Daten, die systembedingt beim Betrieb von IuK-Technik anfallen.

Der Unterausschuß beschloß in Absprache mit der Senatsverwaltung für Inneres und uns, daß dem Jahresbericht 1994 unsere mit der Senatsverwaltung für Inneres abgestimmte Auffassung zu den noch offenen Fragestellungen in Form eines Sonderberichts als Anlage beigefügt werden solle.

Die Abstimmung erfolgte in der Weise, daß wir der Senatsverwaltung für Inneres in einem Schreiben die oben genannten Punkte dargestellt und begründet haben. Die Antwort der Senatsverwaltung war dann auf Referentenebene Gegenstand einer ausführlichen Besprechung.

1. Rechtlicher Rahmen für die berlinweiten IuK-Infrastrukturen

Das in Planung und Erprobung befindliche neue, hochleistungsfähige Verwaltungsnetz (Metropolitan Area Network - MAN) in Verbindung mit dem Konzept eines zentralen Service- und Administrationszentrums (SAZ) sowie das neue ISDN-Sprachkommunikationsnetz der Verwaltung werden die behördenübergreifende Datenkommunikation erheblich fördern und verstärken. Den damit zu erwartenden Begehrlichkeiten zur Überwindung der verfassungsrechtlich gebotenen informationellen Gewaltenteilung stehen rechtliche Schranken mit dem Berliner Datenschutzgesetz gegenüber. Die Probleme der informationstechnischen Sicherheit sind in einer sorgfältigen Bedrohungs- und Risikoanalyse in Verbindung mit einem IT-Sicherheitskonzept erfaßt worden.

Obgleich für die fachbehördenspezifische Datenkommunikation rechtliche Schranken vorliegen, ist für die Bürokommunikation (Mailing, Dokumentenaustausch, Informationsverbreitung) mit einer Intensivierung in erheblichem Umfang zu rechnen, die die Informationsbeziehungen zwischen den Stellen der Berliner Verwaltung gravierend verändern werden, ohne daß abzusehen ist, ob die rechtlichen Regelungen dafür ausreichen oder überhaupt steuernd eingreifen.

Mit den zentralen Eingriffsmöglichkeiten in die Administration und Wartung der lokalen Systeme können neue Abhängigkeiten für die Behörden und öffentlichen Stellen des Landes Berlin entstehen. Andererseits kann nicht ausgeschlossen werden, daß die wesentlich verstärkten Kommunikationsmöglichkeiten der Verwaltung

- nicht nur Entscheidungsprozesse der Verwaltung zugunsten einer erhöhten Bürgerfreundlichkeit beschleunigen und verbessern, sondern auch die Position der Verwaltung gegenüber dem Bürger durch effizientere Kontrollmöglichkeiten verstärken;
- das Verhältnis zwischen Exekutive und Legislative nicht nur durch effizientere Möglichkeiten zur Unterrichtung des Parlamentes bestimmt wird, sondern unter Umständen auch durch Störungen des Informationsgleichgewichtes zwischen Regierung und Parlament zugunsten der Exekutive. Dieses träfe dann das in § 1 Abs. 1 Nr. 2 Berliner Datenschutzgesetz (BlnDSG) definierte Schutzziel des Datenschutzes in Berlin.

Wegen dieser möglichen politischen Konsequenzen des neuen Verwaltungsnetzes halten wir es für erforderlich, die neuen Kommunikationsinfrastrukturen der Verwaltung, die Beschränkungen und Möglichkeiten ihrer Nutzung, ihre Administration, aber auch Maßnahmen zur Vorbeugung unerwünschter Nebenwirkungen auf eine gesetzliche Grundlage zu stellen. Eine wissenschaftliche Untermauerung durch eine fundierte Technologiefolgenabschätzung, die über die IT-Sicherheit hinausgeht, halten wir insoweit für sinnvoll.

Die Senatsverwaltung für Inneres vertritt dagegen die Auffassung, daß für die grundlegenden datenschutzrechtlichen Rahmenbedingungen die geltenden Bestimmungen des Berliner Datenschutzgesetzes vorerst ausreichen. Ob weitergehende einschlägige Regelungen als Gesetz oder untergesetzliche Bestimmungen erforderlich seien, könne jetzt noch nicht entschieden werden, denn die übergreifende Kommunikationsinfrastruktur Berlins sei erst im Entstehen. Es sei abzuwarten,

- wieweit während der Anfangsphase von MAN und SAZ/LAZ bei detaillierter Beachtung und Anwendung aller einschlägigen Regeln aus dem Berliner Datenschutzgesetz und dem Informationsverarbeitungsgesetz überhaupt Regelungsdefizite erkennbar würden,
- was aus Plänen für eine Änderung des Berliner Datenschutzgesetzes würde,

- wie sich die Ziele der bevorstehenden Verwaltungsreform in Richtung der Deregulierung auswirken,
- bis Regelungen gemeinsam mit den anderen beiden deutschen Stadtstaaten - falls dort überhaupt beabsichtigt - vorgenommen werden können.

Die wissenschaftliche Untermauerung durch fundierte Technologiefolgenabschätzungen wird zwar im Prinzip begrüßt. Einer für sinnvoll erachteten Kooperation des MAN-Betreibers LIT zum Beispiel mit der Technischen Universität stünde die aktuelle Haushaltssituation entgegen, denn auch diese Institutionen seien gehalten, für derartige Begleituntersuchungen Geld zu fordern.

Im Ergebnis bleibt festzuhalten, daß in diesem Punkt ein Konsens mit der Senatsverwaltung für Inneres noch nicht erzielt werden konnte. Es bleibt die Frage offen, was zu geschehen hat, wenn sich die von uns erwarteten Regelungsdefizite nach Realisierung von MAN und SAZ/LAZ ergeben. Im ungünstigsten Falle liefe eine so versäumte Vorsorge auf die zeitweilige Einschränkung oder gar Stillegung des Netzes hinaus. Die vorgebrachten Einwände zeigen darüber hinaus Widersprüchlichkeiten auf:

- Einerseits steht die Inbetriebnahme des MAN einschließlich des Service- und Administrationszentrums (SAZ) konkret und unmittelbar bevor, andererseits soll die Erfüllung außerordentlich vager - zumindest, was den Zeitrahmen angeht - Bedingungen abgewartet werden. Nachfragen in den anderen Stadtstaaten haben im übrigen ergeben, daß mit dem MAN vergleichbare Verwaltungsnetze dort noch nicht geplant sind.
- Einerseits werden trotz der angespannten Haushaltslage große Investitionen für die IuK-Infrastruktur getätigt, andererseits soll die ansonsten begrüßte begleitende Technologiefolgenabschätzung an eben diesen Haushaltsrestriktionen scheitern.

2. Rechtliche Grundlage für das LIT

Es ist beabsichtigt, die Rechtsform des Landesamtes für Informationstechnik (LIT) zu verändern. Dies setzt eine Entscheidung des Gesetzgebers voraus. Damit könnten datenschutzrechtliche Probleme gelöst werden, die bisher das LIT daran hinderten, die personenbezogenen Daten seiner eigenen Mitarbeiter für Abrechnung und Kostenrechnung für seine Dienstleistung zu verarbeiten. Wir gehen davon aus, daß mit der gesetzlichen Regelung zur Änderung der LIT-Rechtsform auch Regelungen zum zukünftigen Zusammenwirken zwischen Verwaltung und LIT getroffen werden. Aus datenschutzrechtlicher Sicht bleiben die Regelungen von § 3 BlnDSG zur Auftragsdatenverarbeitung bei Beibehaltung einer öffentlich-rechtlichen Rechtsform gegenüber der alten Situation unberührt.

Die Senatsverwaltung für Inneres bestätigt, daß eine in der Diskussion befindliche neue Rechtsform des LIT, vorzugsweise als Anstalt des öffentlichen Rechts, gegebenenfalls durch ein Errichtungsgesetz die notwendige gesetzliche Grundlage erhalten würde. Dies würde aber wohl nicht mehr als den Errichtungssatz, eine kurze Aufgabenbeschreibung und die Klärung der künftigen Beziehungen zur restlichen Berliner Verwaltung enthalten.

In diesem Punkt besteht Konsens. Der von uns derzeit gesehene Regelungsbedarf für das LIT würde bei Umsetzung der Vorstellung der Senatsverwaltung für Inneres abgedeckt werden.

3. Organisation des IuK-Einsatzes und Abwicklung von IuK-Projekten

Die Organisation des IuK-Einsatzes und die Durchführung von IuK-Projekten in der Berliner Verwaltung und die Verantwortungsverteilung dabei waren in der Vergangenheit Gegenstand verwaltungsinterner Regelungen (ADV-Grundsätze) oder Regelungsversuche (IuK-Grundsätze, Entwürfe für ein IuK-Gesetz). Möglicherweise hat das Fehlen eines Organisationsgesetzes nach dem Muster einiger anderer Bundesländer auch dazu geführt, daß die verwaltungsinternen Regelungen häufigen Änderungen ausgesetzt waren. Dies hatte nach unseren Beobachtungen zur Folge, daß eine konsequente Befolgung der jeweils aktuellen Regelungen nicht überall durchgesetzt werden konnte.

Im Rahmen des Projektes BROSiA sollen Erkenntnisse zur DV-Organisation und der Organisation der Anwendungsentwicklung gewonnen werden, die dann in der Verwaltung umgesetzt werden sollen. Wir würden es begrüßen, wenn die Umsetzung in verbindlicherer Form geschähe als bisher, etwa im Rahmen gesetzlicher Bestimmungen im IVG.

Auf die erhofften Ergebnisse des Projektes BROSiA verweist auch die Senatsverwaltung für Inneres. Allerdings bezweifelt sie auch hier die Zweckmäßigkeit gesetzlicher Regelungen, weil dies dem Deregulierungsgedanken widersprechen und dem Abgeordnetenhaus die ständige Anpassung eines Gesetzes an neue technische und organisatorische Bedingungen abverlangen würde. Statt dessen sei beabsichtigt, generelle Grundsätze als Verwaltungsvorschriften und darauf aufbauend rascher zu modernisierende Richtlinien über die Organisation der Datenverarbeitung, die Anwendungsentwicklung, die technischen Mindest- und Rahmenbedingungen und die Sicherheit zu erarbeiten.

In inhaltlicher Hinsicht besteht über die Regelungsgegenstände Konsens. Wie auch die Senatsverwaltung für Inneres bedauern wir allerdings die erheblichen Verzögerungen im Projekt BROSiA, die sich aus Störungen in der Zusammenarbeit mit einer externen Beraterfirma ergeben haben. Die Konkretisierung der Inhalte steht daher noch aus.

Wir erhoffen uns jedoch, daß die BROSiA-Studie Ansätze erkennen lassen wird, auf welche Weise ein gesetzlicher Rahmen für die IuK-Entscheidungen und -Entwicklungen im Lande geschaffen werden kann, der einerseits die IuK-Politik einschließlich der IT-Sicherheitspolitik auf absehbare Zeit gegen extreme Richtungswechsel stabilisiert und andererseits selbst stabil in bezug auf die absehbare technische Entwicklung ist. Die sich durch den absehbaren technischen Fortschritt oder die Entwicklung der Einsatzorganisation dieser Technik ergebenden Anpassungen des Regelwerkes sollten in der Tat nur auf der Ebene von Verwaltungsvorschriften erfolgen.

4. Abrechnung von Kommunikationskosten

Die Erhebung und Verarbeitung personenbezogener Daten zur Abrechnung der privaten Nutzung von Telekommunikationsdiensten - speziell von privaten Telefonaten - bedarf nach § 6 Abs. 1 BlnDSG einer gesetzlichen Grundlage. Hierzu liegen uns bereits Denkansätze aus der Senatsverwaltung für Inneres vor, wonach dies im Rahmen des IVG geregelt werden sollte.

Die Senatsverwaltung für Inneres geht davon aus, daß die Einführung einer automatisierten Erhebung von Gebührendaten für die private Nutzung gem. § 34 Abs. 2 BlnDSG i. V. m. § 28 BDSG auch nach der gegenwärtigen Rechtslage ohne bereichsspezifische Regelung möglich ist.

Für den Fall, daß man hier § 6 BlnDSG für anwendbar hielte, verweist die Senatsverwaltung für Inneres darauf, daß § 6 BlnDSG nach dem augenblicklichen Erkenntnisstand noch in der laufenden Legislaturperiode geändert werden soll.

Es besteht insoweit Konsens, daß die automatische Erfassung von personenbezogenen Gebührendaten zur Abrechnung der privaten Nutzung von Telekommunikationsdiensten von dienstlichen Geräten derzeit noch keine bereichsspezifische Rechtsgrundlage hat.

Wir halten jedoch § 34 Abs. 2 BlnDSG in diesem Falle nicht für anwendbar, weil die Abrechnung der privaten Nutzung von Telekommunikationsdiensten nicht frühere, bestehende oder künftige dienst- oder arbeitsrechtliche Rechtsverhältnisse betrifft.

Ansätze zur Ergänzung des Informationsverarbeitungsgesetzes um eine entsprechende Regelung, die uns aus der Senatsverwaltung für Inneres bereits bekanntgeworden sind, halten wir für angemessener als eine pauschale Abkehr vom im Volkszählungsurteil des Bundesverfassungsgerichts verlangten und mit § 6 BlnDSG konsequent umgesetzten Prinzip, daß Eingriffe in das informationelle Selbstbestimmungsrecht einer expliziten und normenklaren Rechtsgrundlage bedürfen, wenn die Einwilligung des Betroffenen nicht vorliegt.

5. Wartung und Fernwartung

Bei der Wartung und Fernwartung von IuK-Systemen handelt es sich um Vorgänge, bei denen personenbezogene Daten an Dritte offenbart werden können, ohne daß die Einordnung als Datenübermittlung oder Auftragsdatenverarbeitung eindeutig möglich ist. Zwar wird gemeinhin davon ausgegangen, daß Wartung und Fernwartung als Auftragsdatenverarbeitung anzusehen sind; dies läßt aber außer acht, daß der Auftrag zur Wartung oder Fernwartung nicht die Verarbeitung personenbezogener Daten umfaßt. Die Offenbarung solcher Daten ist in gewissen Grenzen oft unvermeidlich, jedoch wenn möglich zu begrenzen. Es liegt jedenfalls kein expliziter Auftrag zur Verarbeitung solcher Daten vor, vielmehr muß der Auftrag u. a. regeln, daß die Verwendung personenbezogener Daten so weit wie möglich zu vermeiden ist, insbesondere bei der Fernwartung.

In Ermangelung eindeutiger Regelungen betrachten auch wir Wartung und Fernwartung als Datenverarbeitung im Auftrag. Dies hat zur Folge, daß bei Wartung und Fernwartung durch private Unternehmen die Regelungen von § 3 Abs. 4 BlnDSG Anwendung finden. Dies bedeutet, daß die mit der Wartung betrauten Firmen vertraglich zusichern müssen, daß sie sich dabei nach dem Berliner Datenschutzgesetz richten und der Kontrolle des Berliner Datenschutzbeauftragten unterwerfen.

Besondere Schwierigkeiten ergeben sich bei der Frage der Rechtmäßigkeit der Fernwartung und Wartung medizinischer IuK-Systeme, wenn dabei personenbezogene Daten offenbart werden, die der ärztlichen Schweigepflicht unterliegen. Dabei spielt die rechtliche Einordnung der Wartung oder Fernwartung keine Rolle, da der Offenbarungstatbestand auch bei der Bereitstellung von personenbezogenen Daten für die Auftragsdatenverarbeitung erfüllt ist.

Die Senatsverwaltung für Inneres sieht die beschriebenen Einordnungsprobleme und erkennt an, daß es für Fernwartung und Wartung von IT-Systemen mit Bezug zu personenbezogenen Daten bisher keine eindeutige Regelung gibt.

Wir stimmen mit der Senatsverwaltung für Inneres darin überein, daß bei der gegenwärtigen Rechtslage grundsätzlich die gesetzlichen Regelungen zur Datenverarbeitung im Auftrag analog angewendet werden sollten. Wir würden es allerdings nach wie vor bevorzugen, wenn durch eine Sonderregelung im Informationsverarbeitungsgesetz Wartung und Fernwartung einen besonderen Status erhielten. Dadurch ergäbe sich die Möglichkeit, die besonderen datenschutzrechtlichen Fragestellungen dabei klar zu regeln und der Inflationierung von Auftragsverhältnissen entgegenzuwirken, bei denen sich private Unternehmen dem Berliner Datenschutzgesetz und der Kontrolle durch den Berliner Datenschutzbeauftragten unterwerfen müssen.

6. Outsourcing

Ähnliche Probleme treten bei der Auftragsdatenverarbeitung von Daten auf, die besonderen Berufsgeheimnissen unterliegen (ärztliche Schweigepflicht, Steuergeheimnis usw.). Da der Trend zum „Outsourcing" auch in der öffentlichen Verwaltung Berlins verstärkt zu beobachten ist, besteht nach unserer Auffassung ein zusätzlicher Regelungsbedarf über § 3 BlnDSG hinaus, damit zur Zulässigkeit bzw. zu den Voraussetzungen solcher Outsourcing-Projekte bei Daten, die dabei nicht offenbart werden dürfen, verbindliche Regelungen geschaffen werden.

Die Senatsverwaltung für Inneres betont, daß das IT-Outsourcing auf dem Weg zur „schlanken Verwaltung" noch an Bedeutung gewinnen wird, wenn sich die Verwaltung auf ihre „Kernaufgaben" konzentrieren will, indem sie Teil-, Unterstützungs- bzw. Assistenzfunktionen an prädestinierte Dienstleister überträgt. Sie erkennt gesetzlichen Regelungsbedarf an und befaßt sich daher sehr ausführlich mit diesem Punkt.

Sie trifft zunächst die Unterscheidung zwischen dem Outsourcing durch Funktionsübertragung und der Auftragsdatenverarbeitung i. S. von § 3 BlnDSG. Im ersten Falle werden Aufgaben und Geschäftszwecke der Verwaltung ganz oder teilweise an Outsourcingnehmer übertragen. Dabei durchzuführende Datenverarbeitung dient dem Zweck der Aufgabenerfüllung, stellt aber selbst keinen eigenständigen Zweck dar. In diesem Falle wird der Outsourcingnehmer nicht als Auftragnehmer der Datenverarbeitung i. S. von § 3 BlnDSG tätig, sondern ist selbst datenverarbeitende bzw. speichernde Stelle. Die Senatsverwaltung für Inneres ist sich einerseits der Tatsache bewußt, daß eine Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs gemäß § 13 BlnDSG in der Regel ausgeschlossen ist, sieht aber andererseits durch § 2 Abs. 1 a. E. BlnDSG ausdrücklich sichergestellt, daß auch Personen des privaten Rechts dem Berliner Datenschutzgesetz unterworfen sind.

Anders ist die Situation bei der Auftragsdatenverarbeitung. Durch die damit verbundene zusätzliche Offenbarung von Daten an weitere Personen und Organisationen und durch die geringere Transparenz des Verbleibs der Daten, insbesondere, wenn der Auftragnehmer weitere Unterauftragnehmer einschaltet, entstehen datenschutzrechtliche Risiken, die mit der rein zivilrechtlichen Absicherung durch vertragliche Garantien und Vereinbarungen zur Unterwerfung unter das Berliner Datenschutzgesetz vor allem dann nicht ausreichend abgedeckt werden, wenn die Daten besonderen Amts- oder Berufsgeheimnissen unterliegen. Der Umfang des Datenschutzes hängt dann von der rechtlichen Ausgestaltung des Outsourcingvertrages ab. Eine Ausnahme besteht dabei für Sozialdaten, für die in § 80 SGB X spezielle Regelungen getroffen wurden.

Die Senatsverwaltung für Inneres verneint die Möglichkeit, Outsourcing für besonders sensible Daten generell zu verbieten, weil dies die betroffenen Behörden in Ausnahmesituationen unflexibel macht und ihnen zum Beispiel die Teilnahme an Netzdiensten versagen würde. Sie sieht theoretisch zwei Lösungswege:

- Schaffung einer Soll-Vorschrift, nach der bei besonders schutzbedürftigen Daten die Datenverarbeitung im Auftrag durch private Auftragnehmer grundsätzlich unterbleiben soll (vergleichbar mit Ziff. 3.3 der Vollzugsbekanntmachung zu Art. 3 Bayerisches Datenschutzgesetz oder § 4 Landesdatenschutzgesetz Rheinland-Pfalz).

- Einbeziehung privater Outsourcingnehmer in den Adressatenkreis der für den öffentlichen Bereich geltenden Datenschutzgesetze, so daß der Verwaltung größere Spielräume bei der Ausgestaltung der Outsourcingverträge belassen blieben. Dieser Ansatz könne allerdings wegen der Gesetzgebungskompetenzen nur durch den Bund verfolgt werden.

Die „Soll-Vorschrift" wäre zwar leicht umsetzbar, würde aber die Betätigungsfreiheit im Rahmen der Umstrukturierung der Verwaltung einschränken und die Teilnahme von Dienststellen mit besonders schutzbedürfigen Daten an Netzdiensten „grundsätzlich" verhindern, die von privaten Anbietern betrieben werden.

Die Senatsverwaltung für Inneres sieht ebenso das Problem der Amts- und Berufspflichten, verweist aber zusätzlich darauf, daß Berlin nicht den Ergebnissen der zur Zeit bundesweit laufenden Diskussion dieser Frage unter den Aufsichtsbehörden für den privaten Bereich vorgreifen sollte.

In diesem Punkt besteht insoweit Konsens mit der Senatsverwaltung für Inneres, daß ein Regelungsbedarf existiert.

Im Unterschied zur Senatsverwaltung für Inneres gehen wir jedoch davon aus, daß eine Funktionsübertragung nur dann mit § 2 Abs. 1 a. E. BlnDSG erfaßt wird, wenn hoheitliche Aufgaben von Privaten, etwa durch Beleihung, wahrgenommen werden. Dies würde bedeuten, daß nicht jede Aufgabenübertragung, z. B. die Organisation von Veranstaltungen oder der Versand von Broschüren, unter § 2 Abs. 1 a. E. BlnDSG fällt.

Klärungsbedarf bestünde bei dieser Lösung auch für die Frage, welche Rechtsgrundlage für die Übermittlung personenbezogener Daten heranzuziehen wäre, wenn die übertragende Verwaltung personenbezogene Daten an das private Unternehmen übermitteln muß, damit der Auftragnehmer seinen Auftrag erfüllen kann. Wir stimmen der Senatsverwaltung für Inneres zu, wenn sie feststellt, daß § 13 BlnDSG, der die Übermittlung an Stellen außerhalb des öffentlichen Bereiches regelt, die Übermittlung im Normalfall ausschließt.

Dieses Problem müßte auch geklärt werden, wenn mit dem zweiten Lösungsvorschlag für die rechtliche Ausgestaltung der Auftragsdatenverarbeitung bei besonders sensiblen Daten auch Auftragsdatenverarbeiter zum Beispiel in den Geltungsbereich des Berliner Datenschutzgesetzes aufgenommen werden würden.

Der erste Lösungsvorschlag, die Soll-Vorschrift zum grundsätzlichen Verbot des Outsourcing bei besonders schutzbedürftigen Daten, hätte zum Beispiel zur Folge, daß unter den in Abschnitt 5 dargestellten Argumenten die fast immer erforderliche Wartung durch private Unternehmen entweder grundsätzlich verboten oder bereits eine verwässernde Routineausnahme vom grundsätzlichen Verbot wäre. Damit ergäbe sich ein weiteres Argument dafür, Wartung/Fernwartung gesetzlich gesondert zu behandeln.

Inwieweit die Diskussion im „Düsseldorfer Kreis", dem Koordinationsgremium der Aufsichtsbehörden für den Datenschutz im privaten Bereich, Ergebnisse zur Auftragsdatenverarbeitung unter Beachtung der Amts- und Berufspflichten erbringt, die auch im öffentlichen Sektor umsetzbar sind, bleibt abzuwarten.

Das Landeskrankenhausgesetz (LKG) regelt jedenfalls abschließend die Fälle, in denen Daten, die der ärztlichen Schweigepflicht unterliegen, außerhalb des Krankenhauses offenbart werden dürfen. Auftragsdatenverarbeitung, auch Wartung/Fernwartung, gehört nicht dazu. Auch für den Fall, daß einem der Vorschläge der Senatsverwaltung für Inneres gefolgt würde, müßte eine Änderung des LKG erfolgen, die die Offenbarung zu Zwecken der Auftragsdatenverarbeitung - unter besonderen Anforderungen an die Sicherung der Vertraulichkeit - an Dritte ermöglicht. Erste Erfahrungen mit einem innovationsbereiten Outsourcingnehmer im Krankenhausbereich zeigten, daß es Konzepte geben kann, bei denen Mitarbeiter des Auftragnehmers personenbezogene Daten nicht zur Kenntnis erhalten können. Denkbar wäre es also, die Umsetzung solcher Zielsetzungen gesetzlich vorzugeben.

7. Risikoanalyse

Im Informationsverarbeitungsgesetz Berlin (IVG) wird eine Risikoanalyse für alle automatisierten Verfahren verlangt, die dem IVG unterfallen. In der Regel sind dies jedoch Verfahren (Textverarbeitung, Bürokommunikation), deren Schutzbedürftigkeit aus datenschutzrechtlicher Sicht nicht über diejenige der Verfahren herausgeht, für die bereichsspezifische Regelungen gelten oder erforderlich wären und bei denen mehr personenbezogene Daten stärker detailliert und strukturiert verarbeitet werden. Für solche Verfahren existiert keine gesetzliche Forderung nach einer Risikoanalyse und - damit verbunden - nach der Erarbeitung von Datenschutz- und IT-Sicherheitskonzepten.

Wir haben daher angeregt, die gesetzliche Forderung nach einer Risikoanalyse auf alle personenbezogenen Anwendungen und Systeme zu erweitern und zusätzlich die Erstellung von Datenschutz- und IT-Sicherheitskonzepten zu verlangen.

Eine solche Forderung hält die Senatsverwaltung für Inneres für verfrüht. Es gäbe jedenfalls für komplexe Systeme noch keine ausreichenden Erfahrungen mit der Umsetzung von § 4 IVG, der Risikoanalysen für Verfahren der allgemeinen Verwaltungstätigkeit vorschreibt. Sie erhofft sich mehr vom Fortgang des BRO-SiA-Projektes und der einschlägigen Arbeiten des Bundesamtes für die Sicherheit in der Informationstechnik (BSI). Das Fazit der Senatsverwaltung für Inneres:

> „Statt anzunehmen, daß komplexe Systeme und Netze durch ein vorher zu erstellendes umfassendes Sicherheitskonzept vollständig sicher realisiert werden und alle Sicherheitsmechanismen gewissermaßen vorbeugend eingebaut werden können, nehmen wir jetzt eher an, daß die Risikoanalyse auch eine kontinuierliche Aufgabe in Abhängigkeit von der verfügbaren Technik darstellt, daß also ein besonderer Schwerpunkt auf die fortlaufende Beobachtung der IT-Systeme und insbesondere der Netze, ihrer Filter-Server sowie der Störungsvorkommnisse - auch im Umfeld - gelegt werden muß."

Wir stimmen der Senatsverwaltung zu, daß Bedrohungs- und Risikoanalysen sowie Sicherheitskonzepte der ständigen Revision und Anpassung an neue Situationen und technische Rahmenbedingungen unterliegen müssen. Auch im IT-Sicherheitshandbuch des BSI wird die Umsetzung des IT-Sicherheitskonzepts einschließlich der Risikoanalysen als Daueraufgabe gesehen.

Es muß aber selbstverständlich sein, daß ein fundiertes anfängliches IT-Sicherheitskonzept umgesetzt sein muß, wenn mit dem sicherheitsbedürftigen IT-Einsatz begonnen wird. Dieses anfängliche IT-Sicherheitskonzept kann dann Ausgangspunkt weiterer Verbesserungen sein. Das IT-Sicherheitshandbuch des BSI stellt eindeutig klar, daß sein Verfahren auch durchgeführt werden kann, wenn der IT-Einsatz erst geplant wird.

Das IT-Sicherheitshandbuch des BSI bzw. daraus abgeleitete einfachere Verfahren wurden bereits in verschiedenen IT-Projekten der Berliner Verwaltung (z. B. MAN, AHW, BASIS, Dialogisierung des Wohngeldverfahrens) vollständig oder partiell, stets aber nutzbringend angewendet. Hier liegen mittlerweile ausreichende und in der Summe positive Erfahrungen vor, insbesondere, wenn die Analysen von externen Dritten vorgenommen wurden, die auch bei drohendem Finanzbedarf für ihre Bewältigung Risiken offen benannten.

Die fehlenden Erfahrungen mit Risikoanalysen bei Verfahren der allgemeinen Verwaltungstätigkeit können kein Argument dafür sein, entsprechende Methoden bei sicherheitsempfindlichen Infrastruktur- und Großanwendungsverfahren nicht gesetzlich abzusichern - zumal dort mittlerweile Erfahrungen vorliegen.

8. Systembedingt anfallende personenbezogene Daten

Beim Einsatz von IuK-Technik fallen systembedingt personenbezogene Daten an - vor allem Daten von Benutzern. So werden z. B. Dateien in Dateiverzeichnissen Besitzerkürzel zugeordnet, Benutzer sind in Benutzerdateien mit ihren Berechtigungen und Authentifikationsdaten gespeichert, es entstehen benutzerbezogene Protokolle - und zwar nicht nur aus datenschutzrechtlichen Gründen, sondern auch im Rahmen des Accounting oder für die Datensicherung. Für solche personenbezogenen Daten muß es nach § 6 Abs. 1 BlnDSG eine Rechtsgrundlage geben. Wir haben bisher § 1 Abs. 2 IVG so ausgelegt, daß die systembedingt erzwungenen personenbezogenen Daten in dieser Vorschrift einbezogen sind, halten es jedoch für unbefriedigend, daß dies erst durch eine Auslegung ermittelt werden kann.

Wir haben daher empfohlen, im IVG eine Rechtsgrundlage für derartige Daten zu schaffen.

Die Senatsverwaltung hält es dagegen nicht für unbefriedigend, daß solche Daten durch Auslegung von § 2 Abs. 1 IVG unter das IVG fallen. Sie verweist darauf, daß in der Begründung des IVG Daten zum Zwecke der Systemverwaltung beim Einsatz von IT-Systemen, wie z. B. Daten der Bearbeiter in sogenannten Benutzerdateien mit ihren individuellen Benutzerberechtigungen, als unter das IVG fallend benannt werden.

Wir akzeptieren, daß mit der Klarstellung der Innenverwaltung ein zwingender Bedarf für eine besondere Rechtsgrundlage nicht mehr besteht. Falls jedoch eine Novellierung des IVG erfolgen sollte, würden wir es im Sinne der Normenklarheit begrüßen, wenn eine explizite Berücksichtigung solcher Daten nicht nur in der Begründung einer Vorschrift erfolgt.

Anlage 5

Abkürzungsverzeichnis

ADV	– Automatisierte Datenverarbeitung
ÄROV	– Ämter für offene Vermögensfragen
AGGVG	– Gesetz zur Ausführung des Gerichtsverfassungsgesetzes
AHW	– Automatisiertes Haushaltswesen (Projekt)
ALK	– Automatisierte Liegenschaftskarte
AO	– Abgabenordnung
AOÄG	– Abgabenordnungsänderungsgesetz
AOAnwG	– Abgabenordnungsanwendungsgesetz
APC	– Arbeitsplatzcomputer
Art.	– Artikel
ASOG	– Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin (Allgemeines Sicherheits- und Ordnungsgesetz)
AV-Schüler-Unterlagen	– Ausführungsvorschriften über die Führung schriftlicher Unterlagen über Schüler
AZRG	– Ausländerzentralregister
BASIS	– Berliner Automatisiertes Sozialhilfe Interaktions-System (Projekt)
BauGB	– Baugesetzbuch
BBG	– Bundesbeamtengesetz
BBesG	– Bundesbesoldungsgesetz
BDSG	– Bundesdatenschutzgesetz
BGB	– Bürgerliches Gesetzbuch
BGBl.	– Bundesgesetzblatt
BGSNeuRegG	– Bundesgrenzschutz-Neuregelungsgesetz
BImschG	– Bundesimmissionsschutzgesetz
BKA	– Bundeskriminalamt
BlnDSG	– Berliner Datenschutzgesetz
BND	– Bundesnachrichtendienst
BOWI	– ADV-Verfahren Bußgeld und Verkehrsordnungswidrigkeiten
BR-Drs	– Bundesrats-Drucksache
BROSiA	– Berliner Rahmenkonzept 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
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)
DV	– Datenverarbeitung
DVO-MeldeG	– Durchführungsverordnung zum Meldegesetz
EALG	– Entschädigungs- und Ausgleichsleistungsgesetz
EU	– Europäische Union
EUROPOL	– Europäisches Polizeiamt
EWW	– ADV-Verfahren Einwohnerwesen
f.	– folgende Seite
ff.	– folgende Seiten
FIS	– Fachübergreifendes Informationssystem (Projekt)
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 (Infrastruktur-Projekt)
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-Gerätebestand
IPV	– Integrierte Personalverwaltung (Projekt)
ISDN	– Integrated Services Digital Network (Dienste-integrierendes digitales Netz)
ISVB	– Informationssystem Verbrechensbekämpfung
IT	– Informationstechnik
IuK-...	– Informations- und Kommunikations-...
IVG	– Informationsverarbeitungsgesetz Berlin
I. v. m.	– In Verbindung mit
KPMD-S	– Richtlinien für den kriminalpolizeilichen Meldedienst in Staatsschutzsachen
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
LIT	– Landesamt für Informationstechnik
LPD	– Landespressedienst
LVwA	– Landesverwaltungsamt
MAN	– Metropolitan Area Network – stadtweites Netz
MBA	– Modellbezirksamt (Infrastrukturprojekt)
MiZi	– Mitteilungen in Zivilsachen

MfS	– Ministerium für Staatssicherheit der ehemaligen DDR
MOD	– Magneto-Optical Disk
MS-DOS	– Microsoft-Disk Operating System (PC-Betriebssystem)
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
RDV	– Recht der Datenverarbeitung
SAZ	– Service- und Administrationszentrum (Infrastruktur-Projekt)
SDÜ	– Durchführungsübereinkommen zum Schengener Abkommen
SGB	– Sozialgesetzbuch
SIS	– Schengener Informations-System
SMD	– Sozialmedizinischer Dienst
StaLa	– Statistisches Landesamt
StGB	– Strafgesetzbuch
StPO	– Strafprozeßordnung
StudDatVO	– Studentendatenverordnung
StUG	– Stasi-Unterlagen-Gesetz
SISY	– Staatsanwaltschaftliches Informationssystem
TDSV	– Telekommunikations-Datenschutzverordnung
UVollzO	– Untersuchungshaftvollzugsordnung
VermG	– Vermögensgesetz
VwVfG	– Verwaltungsverfahrensgesetz
WAN	– Wide Area Network (Weitbereichsnetz)
WBS	– Wohnberechtigungsschein-Verfahren
WoBindG	– Wohnungsbindungsgesetz
WORM	– Write Once Read Multiple (einmal beschreibbarer Speicher)
WWW	– World Wide Web (Mehrwertdienst auf dem Internet)

Anlage 6

Auszug aus dem Geschäftsverteilungsplan des Berliner Datenschutzbeauftragten
Stand: 31. Dezember 1994

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;
GB: Abgeordnetenhaus, Senatskanzlei, Bundes- und Europaangelegenheiten, Rechnungshof
Dr. Alexander Dix

GB: Gesundheit; Jugend und Familie; Kulturelle Angelegenheiten; Soziales
QB: Schutz von Gesundheits- und Sozialdaten
Dr. Ulrich von Petersdorff

GB: Schule, Berufsbildung und Sport; Wissenschaft und Forschung; Umweltschutz
QB: Forschung und Statistik
Dr. Rainer Metschke

GB: Arbeit und Frauen; Betriebe
QB: Personaldaten; Beratung von Personalräten
Birgit Saager

GB: Medien und Telekommunikation
Diplominformatiker Sven Mörs

Allgemeine Verwaltung; Büroorganisation, Haushaltsplanung und -bewirtschaftung, Beauftragte des Haushalts
Diplomverwaltungswirtin Doris Werth

Allgemeine Verwaltung, Personalsachbearbeitung
Dagmar Klossek

Rechnungsstelle, Sekretariat
Monika Klössing

Sekretariat
Marion Werth

Bereich Bürger und Öffentlichkeit
Bereichsleiterin; Vertreterin des DSB für den Bereich; Konzeption und Durchführung der Öffentlichkeitsarbeit
GB: Landesamt für Verfassungsschutz
Claudia Schmid

Redaktion von Veröffentlichungen
GB: Bau- und Wohnungswesen; Inneres; Stadtentwicklung
Volker Brozio

GB: Finanzen; Justiz; Wirtschaft und Technologie; Verkehr
QB: Rechtspflege
Dagmar Hartge

Bürgerberatung und -betreuung
GB: Landeseinwohneramt, Bezirksämter
QB: Geschäftsordnung
Detlef Schmidt

Sekretariat
Sabine Krissel

Bereich Technik und Organisation
Bereichsleiter; Vertreter des DSB als Dienststellenleiter und für den Bereich;
QB: Grundsatzfragen der ADV-Organisation und -Technik und ihrer Entwicklung
Diplominformatiker Hanns-Wilhelm Heibey

SG: Großrechner mit proprietären Betriebssystemen
Diplomphysiker Joachim Laß

SG: Systeme unter UNIX und seinen Derivaten; Rechner- und Kommunikationsnetze
Diplominformatikerin Ursula Meyer zu Natrup

Koordination der technisch-organisatorischen Beratung; Beratung der behördlichen Datenschutzbeauftragten; Dateien- und Geräteregister
Jürgen Horn

SG: PCs, lokale Netze, nicht automatisierte Datenverarbeitung
Diplominformatiker (FH) Ralf Hauser

Systemverwaltung
André Drescher

Sekretariat
Nicole Müller

GB: Geschäftsbereiche
QB: Querschnittsbereiche
SG: Sachgebiete
DSB: Datenschutzbeauftragter

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.