**Abgeordnetenhaus von Berlin** **Drucksache 14 / 1328**

**14. Wahlperiode**

# Vorlage – zur Kenntnisnahme –

über **Stellungnahme des Senats zum Bericht des Berliner Beauftragten für Datenschutz und Akteneinsicht zum 31. Dezember 2000**

Der Senat legt nachstehende Vorlage dem Abgeordnetenhaus zur Besprechung vor:

Gemäß § 29 Abs. 2 Satz 1 des Berliner Datenschutzgesetzes erstattet der Beauftragte für Datenschutz und Akteneinsicht dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit. Der Regierende Bürgermeister hat dazu die anliegende Stellungnahme des Senats herbeigeführt und legt sie hiermit gemäß § 29 Abs. 2 Satz 2 des Berliner Datenschutzgesetzes dem Abgeordnetenhaus vor.

Berlin, den 12. Juni 2001

Der Senat von Berlin

Diepgen
Regierender Bürgermeister

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

# Stellungnahme des Senats zum Bericht des Berliner Beauftragten für Datenschutz und Akteneinsicht zum 31. Dezember 2000

(gemäß § 29 Abs. 2 Berliner Datenschutzgesetz)

## 1. Rechtliche Rahmenbedingungen

### 1.1 Neue Herausforderungen

Die Wahrung des Grundrechts auf informationelle Selbstbestimmung oder - in der internationalen Diskussion eher verbreitet - der Schutz der Persönlichkeitsrechte (Privacy) unter den Bedingungen der Informationsgesellschaft war im vergangenen Jahr sicherlich weltweit das am meisten diskutierte Thema im Bereich des Datenschutzes. Umfrageergebnisse zeigen regelmäßig, dass E-Commerce, also das Abwickeln von Geschäftsbeziehungen über das Internet, nur dann akzeptiert wird, wenn die Kunden ein hinreichendes Vertrauen in den Schutz ihrer Persönlichkeitsrechte und die hinreichende Sicherung ihrer Daten haben[1]**.** Der dramatische Kurssturz der Aktien der Firma Doubleclick, eines der größten Unternehmen im Bereich der gezielten Bannerwerbung, nach dem Einkauf einer großen Adresshandelsfirma mit dem offenkundigen Ziel der Zusammenführung der Datenbestände hat gezeigt, dass das Problem nicht nur geistige, sondern auch handfeste ökonomische Seiten hat.

Die Regelungsbedürftigkeit des Umgangs mit personenbezogenen Daten im Netz ist global unumstritten. So wurde bei der weltweit führenden Konferenz zu Fragen der gesellschaftlichen Auswirkungen des Computereinsatzes „Computers, Freedom and Privacy“ im April 2000 an der Universität Toronto im Gegensatz zu früheren Jahren das Internet nicht mehr als rechtsfreier Raum propagiert, sondern es wurden nur noch die anzustrebenden Regelungsformen erörtert: Staatliche Regulierung, Selbstregulierung oder eine Kombination von beiden - dies ist künftig die zentrale Frage[2]. Wie diese Regulierung weltweit aussehen soll, wird in vielen Gremien diskutiert, unter anderem von der UNESCO, die in einer Tagung in Paris im November 2000 den Informationszugang, neue Formen der Sicherung des geistigen Eigentums und den Datenschutz zu einem Hauptthema globaler Anforderungen an die Informationsgesellschaft machte[3]. Auch die OECD versucht, ihre Leitlinien an diese Entwicklung anzupassen[4].

Allerdings verschaffen sich derzeit weit vehementer, als dies die Wahrer der informationellen Selbstbestimmung könnten, diejenigen Institutionen Gehör, die in den Möglichkeiten des Internet eine Gefährdung ihrer Aufgabenerfüllung oder auch ihrer Exis-

---

[1] z. B. Harris Interactive; Westin: IBM-Harris Multi-National Consumer Privacy Survey. Aramonk, NY (www.privacyexchange.org/iss/surveys/sr990714.html)

[2] www.cfp2000.org

[3] webworld.unesco.org/infoethics2000

[4] www.oecd.org/ldsti/sti/it/secur/index.htm

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

tenz sehen und zur angeblichen Vermeidung dieser Effekte die Speicherung und Verarbeitung personenbezogener Daten in einem Umfang fordern, wie dies bisher undenkbar war. Zur Bekämpfung der *Internetkriminalität („Cybercrime")* sollen Nutzungsdaten für weit über das Erforderliche hinausgehende Zeiträume aufbewahrt werden, Telekommunikations- und Teledienstеunternehmen sollen auf Anordnung der Sicherheitsbehörden weitergehende Daten speichern und zur Verfügung stellen müssen, Computerkriminalitätsbestände sollen so weit gefasst werden, dass theoretisch eine flächendeckende Überwachung möglich ist[5]. Um Rechtsstaatlichkeit in der Informationsgesellschaft zu gewährleisten, muss diesen Versuchen, die auf allen Ebenen unternommen werden (G8, Europarat, EU) mit Vorschlägen entgegengetreten werden, die das Menschenrecht auf informationelle Selbstbestimmung wahren, aber gleichwohl eine gezielte Verfolgung von Straftaten im Netz ermöglichen.

Auch die *Steuerverwaltung* fordert zunehmend die Speicherung von Nutzungsdaten, um die Versteuerung von Umsätzen, die im Netz getätigt werden, zu kontrollieren. Weltweit wird erörtert, auf welche Weise die Nutzungsentgelte für *urheberrechtlich* geschützte Werke in den Websites kassiert werden können. Auch hier gibt es Vorschläge, hierfür Nutzungsdaten zu verwenden.

Die Besteuerungsgrundsätze des § 85 Abgabenordnung - AO - machen es zur ordnungsgemäßen Besteuerung unabdingbar, dass auch personenbezogene Daten erfasst und verwertet werden. Dementsprechend wären auch Kontrollen von Nutzungsdaten zur Sicherstellung der Besteuerung des Internethandels durchaus wünschenswert, sind jedoch technisch nur sehr schwer umsetzbar.

Eine ganz andere Bedrohung rückten die Meldungen über die (angebliche) Entschlüsselung des *menschlichen Genoms* durch ein amerikanisches Genlabor im Juni 2000 ins Rampenlicht: Die nunmehr sich deutlicher abzeichnende Möglichkeit, durch Analyse der menschlichen Erbanlagen nicht nur (wie bislang praktiziert und mit Rechtsgrundlagen abgesichert) die Identität und Herkunft von Personen sowie deren Zellmaterial feststellen zu können, sondern darüber hinaus Aussagen über körperliche, ja sogar möglicherweise psychische Eigenschaften und entsprechende Prognosen machen zu können, wird die Diskussion über die Wahrung der Persönlichkeitsrechte in ganz neue Dimensionen führen. Das Recht des Nichtwissens über Informationen, die einen selbst betreffen, die Frage der Zustimmungsbedürftigkeit aller Blutsverwandten in die Verarbeitung von Daten, die Rechte von Behörden (Strafverfolgungsbehörden, Gesundheitsdienste) und Privatunternehmen (Arbeitgeber, Versicherungsunternehmen) sowie der Anspruch der Forschung, entsprechendes Material verwerten zu können, werden Themen sein, die die Datenschutzdiskussion in den nächsten Jahren intensiv beschäftigen werden.

Eine konkrete Forderung zur Speicherung von Nutzungsdaten im Netz ist dem Senat aber nicht bekannt. Die Erhebung von Nutzungsentgelten für urheberrechtlich geschützte Werke ist keine steuerrechtliche Problematik.

Die immer heftiger werdenden Forderungen, tatsächlichen oder angeblichen Bedrohungen der Sicherheit durch verstärkte oder gar flächendeckende *Video-*

Der Senat hält den polizeilichen Einsatz von Videoüberwachungstechnik an gefährdeten Orten bzw. Objekten und an Kriminalitätsbrennpunkten für ein ge-

[5] vgl. 5.1

*überwachung* zu begegnen, beherrschten in den verschiedensten Zusammenhängen die Datenschutzdiskussion in den Medien. Handlungsbedarf besteht hier in erster Linie beim Gesetzgeber, der aufgerufen ist, klare Grenzziehungen für den Einsatz der Videotechnik durch Sicherheitsbehörden, bei gefährdeten Einrichtungen von Behörden und Privatunternehmen oder im Rahmen des Hausrechts vorzunehmen. Die bisher erlassenen Gesetze weisen hier noch nicht in eine klare Richtung, der bisherige Stand einer Regelung im Bundesdatenschutzgesetz ist eher eine Nichtregelung, die zu Recht noch auf den Prüfstand gestellt werden soll.

Mit der Videotechnik hat ein ganz anderes Phänomen zu tun, das ebenfalls im vergangenen Jahr zu heftigen Kontroversen geführt hat: Das Fernsehformat „*Big Brother*“ und auf dem Fuße folgende Konkurrenzformate warfen die Frage auf, ob es, selbst unter der Bedingung der freiwilligen und voll informierten Einwilligung, Grenzen für das Eindringen in die Privatsphäre durch Videoaufnahmen gibt, die nicht nur moderiert und gebündelt über das Fernsehen, sondern rund um die Uhr über das Internet verbreitet werden. Die Diskussion hierüber ist ebenfalls noch offen. Einerseits machen diejenigen, die damit einverstanden sind, dass jegliche Verrichtung bis hin zum Sexualverkehr öffentlich beobachtet wird, von ihrer informationellen Selbstbestimmung Gebrauch. Andererseits darf denjenigen, die mit dieser Form der Selbstdarstellung konfrontiert sind, nicht der Eindruck vermittelt werden, dass es in Zeiten der Mediengesellschaft keine Privatsphäre mehr gibt. Die dadurch in der Gesellschaft provozierte Herabsenkung der Hemm- und Schamschwelle kann zu einer Desensibilisierung führen, die nicht nur dem Grundgedanken des Datenschutzes, sondern auch anderer gesellschaftlicher Werte zutiefst schaden kann.

Da die rechtlichen Möglichkeiten einzuschreiten, jedenfalls solange die medien- und strafrechtlichen Schranken nicht überschritten werden, beschränkt oder nicht vorhanden sind, wird hier der Markt selbst entscheiden müssen, ob es jedenfalls faktische Grenzen der Selbstentäußerung gibt. Der dramatische Rückgang der Einschaltquoten bei derartigen Sendungen gibt hier ein positives Signal.

eignetes Mittel, um die Wahrnehmung polizeilicher Aufgaben im Rahmen der Gefahrenabwehr und der Strafverfolgung wirksam zu unterstützen. Durch den offenen Einsatz von Videotechnik können die Prävention verstärkt, die Kriminalitätshäufigkeit reduziert, die Aufklärung von Straftaten gesteigert und das Sicherheitsgefühl verbessert werden.

Deshalb ist die Schaffung klarer Befugnisnormen für den polizeilichen Einsatz von Videotechnik dringend erforderlich.

## 1.2 Europa und Deutschland

Den zweifellos wichtigsten rechtlichen Fortschritt für den Datenschutz in Europa stellt die feierliche Proklamation der *Charta der Grundrechte der Europäischen Union* im Dezember 2000 in Nizza dar. Dieses Dokument, das Kernstück einer künftigen Europäischen Verfassung, enthält in Art. 8 die ausdrückliche Feststellung, dass es sich beim Schutz personenbezogener Daten um ein europäisches Grundrecht handelt. Der nach vielerlei Diskussionen, in die auch die Eu-

Eine Transformation der Inhalte des Art. 8 der Proklamation der Charta der Grundrechte der Europäischen Union im Dezember 2000 in Nizza in das deutsche Verfassungsrecht ist rechtlich nicht zwingend.

Die Ausführungen im Datenschutzbericht lassen den Eindruck entstehen, als ob die Grundrechtscharta bereits jetzt Bindungswirkung für die Mitgliedsstaaten entfalten würde. Dies ist jedoch nicht der Fall. Die Grundrechtscharta ist bislang nicht in die Europä-

ropäischen Datenschutzbeauftragten einbezogen waren, endgültig festgelegte Text lautet:

*(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.*

*(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Personen oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.*

*(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.*

Nicht nur die im deutschen Recht bisher verankerten Grundsätze, sondern darüber hinausgehend etwa auch die Unabhängigkeit der Datenschutzkontrollinstitutionen finden damit eine vom deutschen Recht nicht mehr einschränkbare europarechtliche Grundlage.

Nunmehr wird zu diskutieren sein, ob diese Vorgabe der Europäischen Grundrechts-Charta nicht doch in das deutsche Verfassungsrecht zu transformieren ist. Dies war in den Debatten um die Erneuerung des Grundgesetzes nach der Wiedervereinigung mit dem Argument abgelehnt worden, der Grundrechtscharakter der informationellen Selbstbestimmung ergebe sich bereits aus der Verfassungsrechtssprechung. Gleichwohl zwingt der Text der Charta dazu, zu erörtern, ob das bisher nur durch höchstrichterliche Rechtsprechung verankerte Grundrecht nicht formal in den Verfassungstext aufgenommen werden müsste.

Die Europäische Grundrechts-Charta kennt im Übrigen auch eine grundrechtliche Gewährleistung des *Zugangs zu den eigenen Daten*, die von Organen und Einrichtungen der Union bearbeitet werden (Art. 41), sowie ein allgemeines Recht auf *Zugang zu den Dokumenten* des Europäischen Parlaments, des Rates und der Kommission, wie es bisher in Art. 255 EG-Vertrag festgelegt war (Art. 42), ohne dass diese Regelungen allerdings bisher in konkrete Verfahrensvorschriften umgesetzt worden wären. Dies ist auch ein europäischer Impuls für die Schaffung von Informationsfreiheitsgesetzen in den Mitgliedsstaaten.

Selbst in Verzug geraten waren die Organe der Europäischen Union hinsichtlich der Vorgabe, für die eigenen Institutionen Datenschutzvorschriften zu schaffen. Nach einem langwierigen Prozess trat nunmehr die Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr in Kraft[6].

ischen Verträge aufgenommen und hat keinerlei rechtliche Verbindlichkeit. Ob eine Einbeziehung in die Europäischen Verträge in Zukunft erfolgen oder ob es bei der feierlichen Verkündung vom Dezember bleiben soll, ist noch völlig ungeklärt. Sie stellt daher lediglich einen ersten Schritt hin zu einer gemeinsamen europäischen Verfassung dar und kann allenfalls Signalwirkung hinsichtlich eines gemeinsamen Grundrechtsstandards in der Europäischen Union entfalten.

Darüber hinaus werden die in Art. 8 Abs.1 und 2 der Grundrechtscharta getroffenen Regelungen in der deutschen Verfassung vom Recht auf informationelle Selbstbestimmung, das Teil des allgemeinen Persönlichkeitsrechts gemäß Art 1. Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG ist, umfasst. Ihre Übernahme ins Grundgesetz hätte daher allenfalls deklaratorische Wirkung.

Lediglich die Einrichtung einer unabhängigen Kontrollinstanz gemäß Art. 8. Abs. 3 der Grundrechtscharta dürfte nicht unmittelbar aus dem Grundgesetz herzuleiten sein. Die Einrichtung von Datenschutzbeauftragten, die solch eine Kontrollinstanz darstellen, ist in Deutschland bislang einfachrechtlich in den Datenschutzgesetzen des Bundes und der Länder geregelt. Für den Fall, dass die Grundrechtscharta rechtlich verbindlich werden sollte, könnte aus Gründen der Klarstellung eine entsprechende Ergänzung des Grundgesetztes in Erwägung gezogen werden.

Darüber hinaus wird im Datenschutzbericht insbesondere auf das Recht auf Zugang zu den eigenen Daten gemäß Art. 41 sowie das Recht auf Zugang zu den Dokumenten des Europäischen Parlaments, des Rats und der Kommission in Art. 42 hingewiesen. Hierin kann durchaus ein Impuls für die Schaffung von Informationsfreiheitsgesetzen in den Mitgliedsstaaten gesehen werden. Ein entsprechendes Gesetz ist in Berlin allerdings bereits durch das Berliner Informationsfreiheitsgesetz vom Oktober 1999 geschaffen worden. Hierin sind auch die nötigen Verfahrensvorschriften zur Durchführung des Akteneinsichtsrechts enthalten, so dass es derzeit im Land Berlin auch im Hinblick auf oben genannte Artikel der Grundrechtscharta keiner weitergehender Regelungen zur Informationsfreiheit bedarf.

[6] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000, ABl. EG L 8/1

Auf der Richtlinienebene standen die Erörterungen um eine Änderung der Telekommunikationsrichtlinie im Vordergrund[7].

Auf der Vollzugsebene wurde die Diskussion monatelang beherrscht durch die Verhandlungen der Europäischen Kommission mit dem US-amerikanischen Handelsministerium über die *„Safe-Harbor-Prinzipien*“, ein Selbstregulierungsinstrument, mit dessen Hilfe auch ohne umfassende Gesetzgebung für den privaten Bereich ein angemessenes Datenschutzniveau bei Geschäftspartnern europäischer Unternehmen in den USA gewährleistet werden soll. Die Prinzipien sind nach Entscheidung und Veröffentlichung auf beiden Seiten in Kraft getreten. Die Praxis wird nunmehr zeigen müssen, ob ein derartiges Instrument geeignet ist, in gleicher Weise wie ein allgemein gültiges Gesetz (oder sogar besser?) die Wahrung der informationellen Selbstbestimmung zu gewährleisten[8].

Die deutsche Diskussion war weiterhin geprägt von der Problematik der Umsetzung der *Europäischen Datenschutzrichtlinie* in das deutsche *Bundesdatenschutzrecht*. Die Bundesregierung hat im August 2000 nunmehr endgültig einen Gesetzesentwurf beschlossen, der auf der Basis vorheriger Entwürfe die Europäische Richtlinie unter weitgehender Aufrechterhaltung des bisherigen BDSG eher formell umsetzt denn inhaltlich entscheidend weiterentwickelt. Der Entwurf enthält gleichwohl insbesondere im Hinblick auf den Systemdatenschutz deutliche Impulse in Richtung auf eine Modernisierung des Datenschutzrechtes. Mit einer Verabschiedung des Gesetzes ist im Frühjahr 2001 zu rechnen. Für die Aufsichtsbehörden für den Datenschutz wird die einschneidenste Änderung der Übergang von der Anlass- auf die Amtsaufsicht im privaten Bereich sein.

Angesichts der Unvollkommenheiten dieses Gesetzes, insbesondere im Hinblick auf die strukturelle und sprachliche Gestaltung, hat das Bundesinnenministerium ein Gutachtergremium beauftragt, weitergehende Vorstellungen über eine Vereinfachung und *Modernisierung des Datenschutzrechtes* zu entwickeln, die noch in der laufenden Legislaturperiode in eine zweite Stufe der BDSG-Novellierung überführt werden sollen[9].

Nach vielen Jahren der Diskussion ist in wesentlichen Teilen im November 2000 das *Strafverfahrensänderungsgesetz 1999*, also eine Anpassung der Strafprozessordnung an die Anforderungen des Volkszählungsurteils, in Kraft getreten. Nunmehr gibt es auch im Strafprozess Datenschutzregelungen, deren end-

[7] vgl. 5.1

[8] vgl. 4.7

[9] vgl. Gutachterausschuss Modernisierung des Datenschutzrechts: Gutachtendesign

gültige Ausgestaltung allerdings eine Reihe von Empfehlungen der Datenschutzbeauftragten außer Acht lässt. Andere Gesetze mit datenschutzrechtlichem Gehalt, wenn auch nicht von dieser Tragweite, sind das Steuersenkungsgesetz vom Oktober 2000 (Recht der *Finanzbehörden*, bei Außenprüfungen selbst in EDV-Systeme Einsicht zu nehmen), das neue *Infektionsschutzgesetz*, das alte Gesetze zu Meldepflichten von Infektionen und Maßnahmen gegen die Ausbreitung von Seuchen ersetzt und entsprechende Meldepflichten enthält, eine neues *Binnenschifffahrtsaufgabengesetz* mit Vorschriften über Daten von Bootskennzeichen, Führerscheinen und Daten zu Ordnungswidrigkeiten, eine Änderung des *Steuerberatungsgesetzes* mit Regelungen über die Erhebung und Verarbeitung personenbezogener Daten sowie eine Änderung der *Wirtschaftsprüferverordnung*, ebenfalls unter Berücksichtigung datenschutzrechtlicher Erfordernisse.

Eine Reihe weiterer spezialgesetzlicher Regelungen wird von der Bundesregierung vorbereitet oder befindet sich im parlamentarischen Prozess (z. B. *Gesetze zur Änderung des Melderechtsrahmengesetzes*, des *Bundeswahlgesetzes*, des *Bundesdisziplinarrechtes*, des *Wahlstatistikgesetzes*). Neu sind ein Untersuchungshaftgesetz, das Sozialgesetzbuch IX sowie das Zensustestgesetz im Vorgriff auf die Ablösung umfassender Volkszählungen.

Nach wie vor im Ungewissen ist, wie es mit den beiden letzten großen ausstehenden datenschutzrechtlichen Kodifizierungsvorhaben steht, nämlich der Schaffung eines *Arbeitnehmerdatenschutzgesetzes* sowie der Einführung datenschutzrechtlicher Bestimmungen in die *Abgabenordnung*. Während zu Ersterem stets auf einen angeblich vorhandenen, aber bisher nicht verfügbaren Entwurf des Bundesarbeitsministeriums verwiesen wird, hat sich erst in letzter Zeit eine Bereitschaft des Bundesfinanzministeriums gezeigt, das bereits seit Beginn der Datenschutzdiskussion angemahnte Defizit von Datenschutzregelungen im Steuerrecht nunmehr gesetzgeberisch in die Hand zu nehmen.

Einen deutlichen Rückschritt im Hinblick auf die Gewährleistung der informationellen Selbstbestimmung in der Telekommunikation stellt die Anpassung der Telekommunikationsdatenschutzverordnung (TDSV) an das Telekommunikationsgesetz von 1995 (!) und die Europäische Telekommunikationsrichtlinie dar[10].

## 1.3 Datenschutz in Berlin

Die Verpflichtung, die Europäische Datenschutzrichtlinie umzusetzen, betrifft auch das Land Berlin. Weite Verwaltungsbereiche, etwa die Gesundheits- und Sozialverwaltung, Schulen und Hochschulen, das Ar-

[10] vgl. 5.1

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

beitsrecht oder das Verkehrswesen, fallen in den Geltungsbereich der Richtlinie. Andere Bereiche wie Polizei oder Justiz werden zwar formal nicht von von der Richtlinie tangiert, sollten aber im Hinblick auf eine einheitliche Gesetzgebung für die Landesverwaltung in die Anpassung des Berliner Landesrechtes einbezogen werden.

Der Senat ist der Auffassung, dass eine Einbeziehung der Polizei in den Geltungsbereich der Richtlinie nicht erforderlich ist. Das ASOG und die Strafprozessordnung enthalten bereits umfangreiche Datenschutzregelungen. Es besteht kein Anlass, die polizeiliche Arbeit mit weiteren Datenschutzbestimmungen zu überfrachten.

Im Gegensatz zu anderen Bundesländern, die bereits vorab eigene Datenschutzgesetze verabschiedet hatten, bestand in Berlin ein Konsens darüber, bei der Konzeption des neuen Gesetzes abzuwarten, bis sich der endgültige Text des Bundesdatenschutzgesetzes abzeichnet. In der vorherigen Gesetzgebungsphase gab es erhebliche Anwendungsprobleme, die deswegen entstanden, weil zwischen Bundes- und Landesrecht etwa bei den Begriffsbestimmungen erhebliche Abweichungen bestanden. Nachdem die Bundesregierung ihren BDSG-Entwurf beschlossen hatte, begannen in der Berliner Innenverwaltung die Vorarbeiten für das Konzept eines neuen Berliner Datenschutzrechtes. Wir haben hierzu eine Vielzahl von Gegenvorstellungen entwickelt, die zu Beginn des neuen Jahres Gegenstand intensiver Beratungen zwischen der Innenverwaltung und uns waren. Es ist davon auszugehen, dass auch in Berlin im Laufe des Jahres ein an die Anforderungen der Europäischen Richtlinie angepasstes Gesetz in Kraft sein wird.

Der Senat verweist auf den Entwurf eines Gesetzes zur Änderung des Berliner Datenschutzgesetzes, der Anfang Mai ins Abgeordnetenhaus eingebracht wurde.

Ohne Berücksichtigung unserer Einwände wurde dagegen eine weitreichende Reform des Berliner Melde-, Ausweis- und Passwesens verabschiedet. Obwohl die Aufgaben dieser Verwaltungszweige auf die Bezirksämter übertragen wurden, wurden der Hauptverwaltung unmittelbare Aufgaben in diesem Bereich überlassen. Dies war aus unserer Sicht weder datenschutz- noch allgemein bundesrechtlich vertretbar. Es wird sich zeigen müssen, ob diese Regelungen Bestand haben[11].

Siehe hierzu Stellungnahme des Senats zu 4.2.1 „Meldewesen, Wahlen, Standesämter: Die „Abschichtungsdebatte“ (Seite 66)

Deutliche Verbesserungen im Hinblick auf den Datenschutz brachte dagegen die Reform des Berliner Verfassungsschutzrechtes mit sich, mit der zwar das Berliner Landesamt aufgelöst und die Aufgaben in die Senatsverwaltung für Inneres verlagert wurden (was den von uns im Jahr 1988 ausgesprochenen Empfehlungen diametral entgegenläuft), jedoch wurde im Gesetzgebungsverfahren eine Reihe von datenschutzrechtlichen Verbesserungen des Berliner Verfassungsrechtes verankert. Der Ankündigung des Senators für Inneres, dem Berliner Verfassungsschutz künftig mehr Transparenz, aber auch mehr datenschutzrechtliche Restriktionen aufzuerlegen, wurde gegen Ende des Jahres durch die Personalentscheidung Nachdruck verliehen, die bisherige Stellvertreterin des Berliner Datenschutzbeauftragten, Claudia Schmid, zur Abtei-

Der BlnBDA hatte im Jahresbericht 1989 das Fehlen einer Aufsichtsinstanz über den Verfassungsschutz als Ursache für Mängel in der Arbeit des Verfassungsschutzes angesehen. Er hatte festgestellt, dass die Einrichtung einer Fachaufsicht bei der Senatsverwaltung für Inneres und die Umwandlung des Landesamtes in eine nachgeordnete Behörde einen geeigneten Weg zur Verbesserung der Situation darstelle (Jahresbericht 1989, Seite 8).

Durch die Auflösung des Landesamtes für Verfassungsschutz und die Errichtung einer Verfasungsschutzabteilung der Senatsverwaltung für Inneres ist die Instanz der Fachaufsicht zwar entfallen.

Durch die gesetzliche Verankerung einer Innenrevision bei der Leitung der Senatsverwaltung für Inneres (§ 2 Abs.3 VSG Bln) ist jedoch eine neue unabhängige

[11] vgl. 4.2.1 sowie JB 1999, 4.2.1

lungsleiterin und damit Leiterin der Berliner Verfassungsschutzbehörde zu ernennen.

Kontrollinstanz geschaffen worden, die eine weitergehende Kontrolle als die Fachaufsicht ermöglicht. Auch durch die im neuen Verfassungsschutzgesetz geschaffene Befugnis des Ausschusses für Verfassungsschutz, zur Wahrnehmung seiner Kontrollaufgaben eine Vertrauensperson mit der Durchführung von Untersuchungen zu beauftragen, sind die Möglichkeiten zur Kontrolle des Verfassungsschutzes erheblich erweitert worden.

Wesentliches Kennzeichen der Verfassungsschutzreform ist neben der Schaffung effizienter Verwaltungsstrukturen und der damit verbundenen Erzielung von Synergieeffekten auch eine deutliche Verstärkung der gesetzlichen Kontrollmöglichkeiten.

## 2. Technische Rahmenbedingungen

### 2.1 Die Entwicklung der Informationstechnik und der Informationsgesellschaft

Die Entwicklung der Informationstechnik soll in diesem Jahr im Zusammenhang mit Beobachtungen dargestellt werden, die Tendenzen der Informationsgesellschaft beschreiben. Beides lässt sich nicht mehr voneinander trennen: Entwickelt sich die Informationsgesellschaft entlang des technischen Fortschritts, also an den Möglichkeiten, die neue technische Methoden und Anwendungsformen anbieten, oder ist es umgekehrt: Schafft die Informationsgesellschaft Bedürfnisse, für deren Befriedigung neue Informationstechnik entwickelt wird?

Es ist eigentlich überflüssig zu betonen, dass sich die seit Jahren an dieser Stelle beschriebenen Trends weiter fortgesetzt haben. Die Informationstechnik verfügt über schnellere Prozessoren, über größere Speicher, über komplexere Betriebssysteme und Anwendungsprogramme und ist - zumindest bei Berücksichtigung des Preis-/Leistungs-Verhältnisses - billiger geworden.

In quantitativer Hinsicht birgt die Entwicklung der Informationstechnik also kaum Überraschungen, die hier noch einer besonderen Erwähnung bedürften. Auch die weiter fortschreitende Vernetzung erscheint uns selbstverständlich. Bemerkenswert dürfte sein, dass man das Jahr 2000 vielleicht als jenes ansehen kann, in dem der private Anschluss an das Internet und die Erreichbarkeit über EMail endgültig zur Kulturtechnik erhoben wurden, deren Ignorieren die Gefahr gesellschaftlicher Ausgrenzung und die Abschottung von wichtigen Informationsquellen in sich birgt. Dagegen stehen Gefahren für die informationelle Selbstbestimmung, die die allseitige Beobachtbarkeit des Kommunikationsverhaltens in diesen Netzen mit sich bringen. Die durch die neuen Möglichkeiten zur Kommunikation und Information gewonnenen Chancen für die persönliche Souveränität und Unabhängigkeit werden durch die ungezielte und massenhafte Preisgabe von Lebensäußerungen gemin-

dert, die zur anonymen Manipulierbarkeit und Steuerbarkeit durch Dritte führen können.

Eine weitere Selbstverständlichkeit ist es heute, mit einem Handy ausgestattet zu sein, um so jederzeit und überall erreichbar zu sein oder selbst telefonieren zu können. Die Telekommunikation löst sich so von zeitlichen und räumlichen Restriktionen. Auch hier geschieht nichts, was nicht von dritter Seite und unbemerkt beobachtet werden kann.

Wer also die Entwicklung der Informationstechnik beobachten will, muss sich fragen, wie es weitergeht. Was fehlt noch, wo sind die Märkte der Zukunft für die neue Ökonomie? Wir beschreiben zwei Antworten, deren Bezug zum Datenschutz unverkennbar ist.

Im Sommer bezahlten Kommunikationsunternehmen fast 100 Milliarden Mark für sog. UMTS-Lizenzen an den Staatshaushalt, eine riesige Summe, die Zweifel auslöste, ob sich diese Beträge amortisieren werden und der finanzielle Aderlass dieser Unternehmen deren weitere Innovationsbereitschaft und -fähigkeit nicht beeinträchtigen würde. Bei UMTS (Universal Mobile Telecommunication System) handelt es sich um einen neuen Mobilfunkstandard, der erheblich höhere Übertragungsraten und somit eine Vielzahl neuer Dienste ermöglichen wird, die über das Telefonieren, das Versenden von Kurznachrichten (SMS) und eingeschränkte Internetnutzung (WAP) weit hinausgehen werden.

Die Investitionen werden sich wohl nur rechnen, wenn neue Formen der mobilen Kommunikation erschlossen werden. Die uns bekannt gewordenen Ansätze erschließen ein gewaltiges Spektrum neuer Anwendungsformen, deren Intentionen am besten durch ein Szenario verdeutlicht werden können, welches wichtige Beispiele für mobile informations- und kommunikationstechnologische Anwendungen erfasst.

*Der Berliner Außendienstmitarbeiter Peter M. der Haushaltsgerätefirma Q. begann seinen Tag damit, die bei seiner Firma aufgelaufenen Wartungs- und Reparaturaufträge aus dem Internet in seinen mobilen Assistenten (MobAss) einzuspielen. Dabei handelt es sich um ein spezielles Handy, welches aufgeklappt ein Display freigibt. Es verfügt über eine Spracheingabeeinheit, die eine Tastatur für die Eingabe von Steuerkommandos entbehrlich macht*

*Peter M. freute sich ausnahmsweise darüber, dass die Q-Produkte so stabil funktionieren, und dass er deshalb an diesem Tage Zeit genug haben würde, um ein paar persönliche Dinge nebenbei zu erledigen und vielleicht auch mal etwas für seine Bildung zu tun.*

*Die technischen Daten und Schaltpläne der nach Angaben der Kunden vorzufindenden Haushaltsgeräte waren mit der Einspielung der Aufträge bereits auf dem MobAss gespeichert worden. Nur wenn die Angaben der Kunden ungenau oder unrichtig sind, wür-*

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

*de es nötig sein, aktuelle Daten aus dem IT-System der Q-Vertretung in Berlin mit dem MobAss über das Internet abzurufen. Somit verfügt Peter M. beim Kunden über ein Informationssystem, welches ihm alle Informationen liefert, die eine gezielte Fehlersuche ermöglichen, u. U. sogar mit Hilfe von Simulationen, die fehlerhafte Zustände auffinden helfen und die Bauteile anzeigen, die für die gemeldeten Störungen verantwortlich sind. Selbstverständlich sind im Hintergrund auch der Rechner der Q-Vertretung in Berlin, ja sogar das weltweite Q-Netz verfügbar, um Fehler und Fehlerbehebungswege auch in außerordentlichen Konstellationen auffinden zu können.*

*Der Weg zu den Kunden war schnell gefunden. Immerhin konnte der MobAss auch Funktionen eines Verkehrsnavigationssystems erfüllen, weil das Mobilfunksystem mit Hilfe von Peilinformationen von drei und mehr erreichbaren Mobilfunk-Basisstationen den Standort genau bestimmen und an den MobAss weiterleiten konnte. Stauinformationen sowie eventuelle Umleitungen wurden orts- und zeitabhängig ebenso abgerufen wie die genauen Informationen über den einzuschlagenden Weg und auf den drahtlosen Minikopfhörer vom Peter M. übertragen*

.

*Peter M. konnte so die Kundenwünsche flott und effektiv erfüllen und hatte Zeit, einem Geburtstagswunsch seiner Frau nachzugehen. Er hatte bereits am Morgen seinem MobAss eingegeben, welches Parfum er im Laufe des Tages kaufen wollte. Beim Schlendern durch die Einkaufsstraße erhielt er über seinen MobAss sprachliche Hinweise auf seinen Miniaturkopfhörer, die ihn auf das Parfum-Angebot des Geschäfts, an dem er gerade vorbeiging, aufmerksam machten, insbesondere natürlich auf das gesuchte Produkt. Selbstverständlich wurde er auch auf andere Produkte hingewiesen, die jeweils als Sonderangebot angepriesen wurden. Auch hier war natürlich die metergenaue Standortermittlung durch den MobAss wichtig. Peter M. hätte seinen MobAss natürlich gerne befragt, welches Kaufhaus das von ihm gesuchte Produkt denn am preisgünstigsten anbot. Die Einführung eines solchen Dienstes hatten jedoch die Wettbewerbshüter verhindert, da diese Echtzeit-Preisvergleiche zur Nivellierung des Preisniveaus geführt hätten. Er musste also ein wenig durch die Einkaufsstraßen schlendern, um herauszufinden, welcher Händler ihm ein besonders günstiges Angebot machen konnte. Da er jedoch nicht mehr in den Kaufhäusern suchen musste, ging auch diese Suche noch recht schnell vonstatten*

.

*Nachdem Peter M. noch eine Geschirrspülmaschine repariert hatte, zu der er zwischenzeitlich durch Notruf gerufen wurde und die er nicht auf später verschieben konnte, da der Prioritätenmanager seines MobAss andere Aktivitäten nicht mehr unterstützen wollte, hatte er endlich Zeit, die Ausstellung historischer Telefone im Technikmuseum zu besuchen. Im*

*Museum erfuhr er über den Kopfhörer des MobAss alle Einzelheiten über die gerade betrachteten Exponate sowie Hinweise auf andere Stücke, die sein besonderes Interesse finden würden. Dann kehrte er nach Hause zurück, optimal assisiert vom Navigationssystem seines MobAss, begrüßte seine Frau und gab sich den Vergnügungen des Feierabends hin. Welche Hilfe ihm der MobAss weiter leisten konnte, bleibt der Fantasie des Lesers überlassen*

Das Szenario basiert auf veröffentlichten Konzepten, zum Beispiel dem Projekt MoVi (Mobile Visualisierung) des Fachbereichs Informatik der Universität Rostock, welches uns im Rahmen einer Sitzung des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder präsentiert[12] und in einen datenschutzrechtlichen Zusammenhang gestellt wurde[13]. Aber nicht nur die Hochschulen basteln an der künftigen Informationsgesellschaft, auch die Telekommunikationsbranche kündigt die Funktionsmerkmale der neuen UMTS-Handys an - mit einer verblüffenden Ähnlichkeit mit „*MobAss*“[14].

Es zeigt den Nutzen eines Systems, welches den zeitlichen, örtlichen und situativen Kontext kennt oder erkennt, in dem sich der Benutzer befindet, und ihm jegliche Assistenz zukommen lässt, um die jeweiligen Aufgaben zu erfüllen oder Dienstleistungen in Anspruch zu nehmen. Dabei helfen vorab gegebene Rahmendaten, im Hintergrund bereitgestellte Daten sowie Daten, die orts-, vielleicht auch zeitabhängig ohne besondere Aufforderung aufgeliefert werden. Der Benutzer bekommt alle Daten, die er gerade braucht - meist ohne eigenes Zutun. Diese fast grenzenlose Dienstleistung hat aber auch ein Gegenbild:

Jede über das mobile Assistenzsystem bereitgestellte Dienstleistung verursacht Datenspuren, die zentral aufgezeichnet und ausgewertet werden können, ohne dass der Benutzer davon etwas erfahren muss. Die Entstehung individueller Bewegungs- und Konsumentenprofile kann mit der Überwachung der Arbeitsleistung, u. U. auch mit Zahlungsgewohnheiten einhergehen. Das gesamte Verhalten des Benutzers wird transparent und damit auch von außen steuerbar. Dieses Problem leitet auf die zweite Antwort zu den Märkten in der Informationsgesellschaft über.

---

[12] Im Internet: http://wwwdb.informatik.uni-rostock.de/Forschung/movi.html

[13] Im Internet: http://wwwtec.informatik.uni-rostock.de/~buetow/lfd_akt_10_2000/vortrag_2_Lubinski/index.html

[14] z. B. MobilCom: http://www.mobilcom.de/umts_1279_1296.html?shop_id=&vp_nummer=&w_code=

T-Mobil: http://www.t-mobil.de/index/1,1064,205d,00.html

Viag Interkom: http://www.viag-interkom.de/index/indexh.html
E-Plus: http://www.eplus-online.de/NASApp/portal/eplushome

Die zweite Antwort betrifft keine neuen technische Systeme, sondern die Objekte, die der Gesellschaft der Zukunft ihren Namen gegeben haben: Informationen. Die wichtigste Ware in der Informationsgesellschaft sind die Daten, aus denen Informationen gewonnen werden, die die gesellschaftlichen Prozesse in allen Schichten steuern. Wissen ist Macht und mehr Wissen als andere ist ein Wettbewerbsvorteil. Mehr Wissen über andere schafft sogar Macht über andere.

Daher entbrennt ein Wettbewerb auf vielen Ebenen, die Daten zu erhalten, die die Wettbewerbsvorsprünge und Beeinflussungsmöglichkeiten in der Zukunft Gewinn bringend sichern sollen. Wir haben bereits im Jahresbericht 1997 über moderne Datenbanksysteme und ihre Erschließungstechniken, Data Warehouses und das sie erschließende Data Mining berichtet[15], mit denen zweckfrei gesammelte oder archivierte und in heterogenen Formaten vorliegende Datenmengen auf neue Erkenntnisse hin durchstöbert werden, in dem sie in neue Zusammenhänge gebracht werden. Damit werden aus scheinbar trivialen und meist unverfänglichen Daten wertvolle Informationen, also Grundlagen von Entscheidungsfindungen. Im Vorjahr stellten wir ein Szenario vor, welche Auswirkungen aus dem elektronischen Handel (E-Commerce) gewonnene Daten auf den Einzelnen haben können[16].

Die Quellen, aus denen der Rohstoff der Informationsgesellschaft gewonnen wird, sind sehr vielfältig:

- Daten aus Geschäftsbeziehungen (Vertragsdaten, Stammdaten);
- Daten aus Überwachungsmaßnahmen (Videoüberwachung, Überwachung der telekommunikation);
- Daten aus konkreten Beobachtungen und Recherchen (Investigative Daten);
- Nutzungsdaten von Kommunikationsdiensten (Individualkommunikation - z. B. Handy, „*MobAss*“; Massenkommunikation - z. B. Internet, Pay-TV);
- Nutzungsdaten von Verkehrsdienstleistungen (Flug, Bahn, öffentlicher Nahverkehr - Ticketing[17], Individualverkehr - Mautsysteme);
- Bewegungsdaten aus ortenden Verkehrsleit- und Kommunikationssystemen (siehe „*MobAss*“);
- Konsumverhalten (Wer kauft wann was?);
- Nutzung des elektronischen Zahlungsverkehrs .

Zu den begehrtesten Informationen gehören jene, die das Konsumverhalten einer Person beschreiben. Waren es früher z. B. Preisausschreiben in Printmedien

[15] JB 1997, 2.1

[16] JB 1999, 2.1

[17] vgl. 3.2

mit charakteristischem Leserprofil, die den Stoff für das Direktmarketing lieferten, so werden heute teils grobschlächtigere Verfahren verwendet, wie zum Beispiel Verbraucherbefragungen im scheinamtlichen Habitus und mit Gewinnversprechen, teils subtile Verfahren wie zum Beispiel Kundenkarten ohne Zahlungsfunktion und mit Rabattgewährung, um auch die Kaufspuren der Barzahler zu erfassen. Was die Unternehmen für die dabei gewonnenen personenbezogenen Daten bezahlen wollen, wird sich herausstellen, wenn die Fesseln des Rabattgesetzes gefallen sind.

## 2.2 Datenverarbeitung in der Berliner Verwaltung

### Berliner Großverfahren im schlechten Licht

Die Datenverarbeitung des Landes Berlin ist im Jahre 2000 in die öffentliche Diskussion geraten - leider meist nicht unter positiven Vorzeichen.

Der befürchtete Millenniumscrash war glücklicherweise weltweit weitgehend ausgeblieben, wobei sicher die unerhörten Anstrengungen eine entscheidende Rolle spielten, die zur Abwendung von datumsbedingten Computerirritationen erbracht worden waren. Nach Neujahr war aber dann die Berliner Feuerwehr in der öffentlichen Kritik, weil das *Einsatzleitsystem IGNIS* den besonderen Belastungen in der Silvesternacht nicht standhielt und damit die Feuerwehr nicht mit der gewohnten Zuverlässigkeit ihren in dieser Nacht erwartungsgemäß überbordenen Aufgaben gewachsen war. Auch im weiteren Verlauf des Jahres war es Gegenstand von Schlagzeilen, wenn die diversen Belastungstests des Feuerwehrleitsystems noch nicht die gewünschte Störungsresistenz aufwiesen. Nach dem derzeitigen Datenschutzrecht sind solche Verfügbarkeitseinbußen als Beeinträchigungen der Ordnungsgemäßheit zwar nur mittelbar ein Datenschutzproblem, nach der Umsetzung der Datenschutzrichtlinie (Art. 17 Abs. 1) im Berliner Datenschutzgesetz wird die Sicherstellung der Verfügbarkeit allerdings eine zentrale datenschutzrechtliche Verpflichtung.

Zu Beginn der Inbetriebnahme des Systems IGNIS mussten in der Tat verschiedene Probleme behoben werden, die zeitweise zu Funktionsstörungen geführt hatten. Das ist inzwischen in einer großen Anstrengung aller Projektbeteiligten geschehen. Der Erfolg wurde zum Jahreswechsel 2000/2001 deutlich sichtbar. Die Einsatzsteuerung durch die neue Leitstelle hat auch unter den Belastungen an diesem Tag problemlos funktioniert.

Bald darauf gelangte ein neues IT-Verfahren der Justizvollzugsanstalten in die Diskussion. Das wegen des befürchteten Ausfalls des alten Systems zum Jahrtausendwechsel überstürzt eingeführte System *BASIS 2000* (Buchhaltung und Abrechnung im Strafvollzug) konnte nicht rechtzeitig auf die Berliner Belange umgestellt werden und brachte die Insassenvertretung der Justizvollzugsanstalt Tegel auf den Plan. Die anstaltsintern erstellten Ausdrucke und Belege enthielten wesentlich mehr Daten als zuvor und so wurde die Gefahr gesehen, dass viele personenbezogene Daten unnötig im Tagesablauf der Anstalt von Unbefugten zur Kenntnis genommen werden könnten. Noch mehr Aufregung erzeugte die Entscheidung der Justizverwaltung, den Strafgefangenen statt 18 Tagen nur noch 15 Tage Urlaub zuzugestehen, weil das System „bei

Siehe hierzu Stellungnahme des Senats zu 4.3.1. “Systemumstellung im Strafvollzug” (Seite 86)

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

der Berechnung der Bezahlung der Freistellungstage nur eine Bezahlung von 15 Tagen“ zuließ. So zitiert das Inhaltsprotokoll der Sitzung des Ausschusses für Verfassungs- und Rechtsangelegenheiten, Immunität und Geschäftsordnung (Rechtsausschuss) vom 17. Februar 2000 den zuständigen Staatssekretär, der im Übrigen Verständnis für die Probleme hatte, aber auf die Abhängigkeit von technischen Programmen verwies. Man stelle sich vor, wie die Debatte stattgefunden hätte, wenn allen öffentlichen Bediensteten ab einer bestimmten Gehaltshöhe ohne Entschädigung das Einkommen gekappt worden wäre, nur weil die Zahlungsverfahren höhere Gehälter nicht hätten ausrechnen können.

Mit diesem Stichwort gelangt man zum Großverfahren *„Integrierte Personalverwaltung“* - IPV, welches nach langer Entwicklungszeit, während der sogar ein international renommiertes Beratungsunternehmen seine Beteiligung an dem Projekt aufgab[18], weil kein Konsens über eine gemeinsame Strategie zwischen Verwaltung und Unternehmen erreicht werden konnte, eingeführt wurde. Der Hersteller der zugrunde liegenden Standardsoftware übernahm die Anpassung an die Kundenbedürfnisse (Customizing) dann selbst. Der Dissens betraf die Integration der Zahlungsverfahren in das IPV-Verfahren. Offenbar hat dies jetzt auch zu dem Problem geführt, dass IPV bisher nur Daten von Beamten verarbeiten kann, nicht jedoch von Angestellten, deren komplexes Tarifsystem mit Hunderten von unterschiedlichen Zulagenarten bisher nicht abgebildet werden kann.

Der Berliner Beauftragte für Datenschutz und Akteneinsicht geht fehl in der Annahme, dass die derzeitige Einführungsstrategie noch den seinerzeitigen Dissens über die Integration der Zahlungsverfahren (ADV-Verfahren Tarif und Besoldung) in das Verfahren IPV widerspiegelt. Es liegt vielmehr in der Natur der Sache, dass ein derartiges Großverfahren nicht schlagartig einsatzfähig ist, zumal erhebliche Entwicklungs- und Anpassungsarbeiten zu leisten sind.

Maßgeblich für die sukzessive Einführung des Verfahrens IPV sind daher nicht die “Unfähigkeit“ des Systems oder die Komplexität des Tarifverfahrens, sondern die umfangreichen Vorarbeiten, die die Ablösung der ADV-Verfahren Tarif und Besoldung benötigt. Sie beinhalten im Wesentlichen ein Produktivsetzungskonzept zur Übernahme der “Altdaten“ aus den ADV-Verfahren, ein Schulungskonzept zu den verschiedenen Anwendungsbereichen für weit mehr als 1000 Einzelanwender in allen Behörden der Berliner Verwaltung und Anpassungsarbeiten an das besondere Recht des öffentlichen Dienstes im Lande Berlin (u.a. für mindestens 19 zahlungsrelevante berlinspezifische Tarifverträge). Allein dies macht einleuchtend, dass eine taggleiche Einführung der neuen Zahlungsverfahren unmöglich und nur eine schrittweise Umsetzung erfolgversprechend ist. Nachdem die entsprechenden Arbeiten – auch unter besonderer Beachtung der Aspekte “Datenschutz und Datensicherheit“ – abgeschlossen werden konnten, wird das Zahlungsverfahren Tarif seit April 2001 sukzessive eingeführt. Selbstverständlich sind zu diesem Einführungstermin alle für den Tarifbereich notwendigen Bestandteile in das Verfahren IPV eingepflegt worden. Die “alten“ Zahlungsverfahren werden parallel aufgegeben und ab 1. Januar 2002 termingerecht eingestellt, so dass sämtliche Zahlungen ausschließlich mit dem neuen SAP-System abgewickelt werden müssen.

Nach heutiger Sicht werden keine Verzögerungen in der weiteren Einführung des Verfahrens IPV auftreten, so dass in nur 24 Monaten, d.h. zum 1. Januar

[18] JB 1999, 4.4.1

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

2002, das Verfahren IPV komplett in der Berliner Verwaltung eingeführt sein wird. Der Senat sieht dies als eine außerordentliche Leistung sowohl bei den für die Entwicklung als auch bei den für den täglichen Einsatz zuständigen Mitarbeitern an.

Eigentlich sollte das IT-Verfahren der Berliner Sozialverwaltung *BASIS II* Ende 1999 in Betrieb gegangen sein. Das auch von politischer Seite vehement geforderte Nachfolgeverfahren für das alte DOS-Verfahren BASIS I auf der Grundlage des Standardprogramms PROSOZ sollte endlich die funktionalen Defizite und softwareergonomischen Mängel beheben, die die Arbeit mit dem veralteten Verfahren erschwerten. Ein Konsortium aus dem amerikanischen Softwarekonzern ORACLE, der renommierten deutschen IT-Beratungsfirma PSI und der Senatsverwaltung für Arbeit, Soziales und Frauen wollte auf der Grundlage modernster Software- und Entwicklungstechniken unter dem Namen BASIS 3000 ein umfassendes, flexibel anpassbares Verfahren entwickeln, dessen Kosten über die Vermarktung in anderen Städten und Gemeinden gemildert werden sollten.

Die Darstellung im ersten Satz des nebenstehenden Absatzes ist irreführend. Richtig ist, dass Ende 1999 das Firmenkonsortium ORACLE/PSI die Software nicht zur Abnahme bereitstellen konnte. Entsprechend dem Mitte 2000 kommunizierten Projektplan sollte die Software bis Ende 2002 erstellt werden und anschließend flächendeckend in Berlin eingeführt werden. Der Pflegevertrag für die bisher eingesetzte Software PROSOZ/DOS wurde vom Hersteller fristgerecht zum 31. Januar 2001 gekündigt mit dem Ziel, höhere Pflegegebühren zu vereinbaren. Im Dezember 2000 wurde ein neuer Pflegevertrag abgeschlossen.

Im Laufe der Zeit verzögerte sich der Fertigstellungstermin bis Ende 2003, ein Termin, an dem für das alte Verfahren keine Unterstützungsgarantie von dem Softwarehersteller mehr gegeben werden mochte. Der Zeitdruck führte offensichtlich auch zum Versuch, Vereinfachungen beim Testen bestimmter Programme zu finden, die mit den geltenden datenschutzrechtlichen Bestimmungen nicht in Einklang zu bringen waren und im Jahre 1999 auf Grund unserer formellen Beanstandung eingestellt wurden[19].

Hier wird Bezug genommen auf eine Beanstandung des Datenschutzbeauftragten im Jahresbericht 1999. Darin hatte er gerügt, dass zur Vorbereitung der Migration nicht ein Testdatenbestand, sondern ein Echtdatenbestand hergestellt worden war. Dieses Vorgehen hatte weder etwas mit „Zeitdruck“ noch mit „Vereinfachungen beim Testen bestimmter Programme“ zu tun. Zu diesem Vorgehen hatte sich seinerzeit das Bezirksamt Neukölln in seiner Stellungnahme geäußert.

Nunmehr wurde das Projekt aufgegeben. Aus Sicht der Firma ORACLE lag eine nicht vorhersehbare Komplexität vor, die zu finanziellem und zeitlichen Mehraufwand führte. Außerdem wurde die Unterstützung der Bezirksämter vermisst. Die Senatsverwaltung beendete das Projekt wegen des unverhältnismäßigen zeitlichen Verzuges. Die Bezirke forcieren derweil eine Übergangslösung auf der Grundlage von WINDOWS NT, die von Anfang an mit einem Problem mit der informationstechnischen Sicherheit zu kämpfen hat[20].

Das Projekt wurde bisher noch nicht aufgegeben und die Senatsverwaltung für Arbeit, Soziales und Frauen beendete bisher auch noch nicht das Projekt. Richtig ist, dass die zuständige Senatsverwaltung seit November 2000 die Rückabwicklung der bestehenden Projekt-Verträge betrieben hat. Zur Zeit besteht jedoch ein Vertragsmoratorium, um einen alternativen Vorgehensplan zur Realisierung des Projektes BASIS II zu prüfen. Der Hauptausschuss wird Ende Mai über das weitere Vorgehen beraten.

**IT-Sicherheit in der Berliner Verwaltung**

Es ist unbestritten, dass es um die informationstechnische Sicherheit in der Berliner Verwaltung nicht überall zum Besten steht. Eine solche allgemeine Aussage wird wohl überall zutreffen, wo unüberschaubar viele IT-Projekte mit unterschiedlichen Graden an Professionalität erarbeitet, eingeführt und betrieben werden.

Dem Senat ist bewusst, dass die Sicherheit des IT-Einsatzes in der Berliner Verwaltung noch weiter verbessert werden kann und muss. Die Umsetzung anforderungsgerechter Sicherheitsmaßnahmen ist ein ständiger Prozess, der durch eine entsprechende Erfolgs- und Qualitätskontrolle begleitet wird. Der Stand

[19] JB 1999, 4.4.3

[20] vgl. 4.4.3 sowie JB 1999, 4.4.3

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Und dass selbst Professionalität keine ausreichende Gewähr für erfolgreiche Projekte bringt, machten die beiden letzten Beispiele in den vorigen Absätzen deutlich. Die zentralen Koordinations- und Entscheidungsgremien für die Datenverarbeitung in Berlin haben ihre Verantwortung für die sichere Verarbeitung der personenbezogenen Daten der Bürgerinnen und Bürger einerseits sowie Mitarbeiterinnen und Mitarbeiter andererseits verstanden. Bei diesen Gremien handelt es sich um den *IT-Koordinierungs- und Beratungsausschuss Berlin* (IT-KAB) mit seinen Arbeitsgruppen, insbesondere der Arbeitsgruppe IT-Sicherheit. Wir wirken in diesen Gremien beratend mit.

Im Berichtsjahr ging es u. a. um folgende datenschutzrelevante Fragestellungen:

Mit dem *IT-Warenkorb* wurde eine Aufstellung aller Produkte unterschiedlicher IT-Produktgruppen entwickelt, deren Beschaffung in der Verwaltung empfohlen wird. Damit soll trotz der Entscheidungshoheit der einzelnen Verwaltungen auf eine gewisse Vereinheitlichung der eingesetzten Produkte hingewirkt werden, was einerseits die Anforderungen an die Qualifikation der Beschaffer begrenzt und andererseits die Beratungstiefe, z. B. durch den Landesbetrieb für Informationstechnik, verbessert. Beide Zielsetzungen dienen auch datenschutzrechtlichen Belangen, haben wir doch wiederholt unsere Sorge zum Ausdruck gebracht, dass das verwaltungsinterne Qualifikationsniveau mit der zunehmenden Komplexität der Datenverarbeitung nicht Schritt halten könnte. Die Aufnahme des Produkts *Safeguard VPN* für die Verschlüsselung von Daten im Berliner Landesnetz in den Warenkorb haben wir ausdrücklich begrüßt[21].

Der Einsatz von *Windows 2000* in der Berliner Verwaltung als Nachfolgeprodukt für Windows NT war bundesweit diskussionsbedürftig. Bestimmte in ihm enthaltene sicherheitsrelevante Teilprogramme wurden von einem amerikanischen Unternehmen zugeliefert, welches aufgrund der herausgehobenen Position des Unternehmenschefs in der Scientology Organisation den Prinzipien dieser Organisation folgt. So wurde vermutet, dass dieser Programmteil verborgene Funktionen haben könnte, die der Ausforschung der Nutzer von Windows 2000 und ihrer Arbeitgeber dienen könnten. Das Bundesministerium des Innern und Microsoft hatten sich über ein gemeinsames Vorgehen verständigt, das den Verzicht auf den problematischen Programmteil beinhaltete. Daraufhin hat das Bundesamt für Sicherheit der Informationstechnik (BSI) auf die geplante Prüfung des Windows-2000-Quellcodes verzichtet. Allerdings sind inzwischen Zweifel aufgekommen, ob Microsoft das gemeinsame Vorgehen

der Umsetzung wird u. a. durch den jährlichen IT-Sicherheitsbericht erfasst und analysiert.

Der Einsatz von Windows 2000 in der Berliner Verwaltung wird durch eine vom IT-Koordinierungsausschuss Berlin (IT-KAB) eingesetzte Arbeitsgruppe vorbereitet, die auch die im IT-Sicherheitsbericht 1999 angeführten Fragestellungen untersucht hat. Das im Bericht erwähnte Teilprogramm kann aus Windows 2000 entfernt und durch ein anderes Programm ersetzt werden.

[21] JB 1999, 4.8.1

einhält. Daher wurde Windows 2000 bisher nicht in den Berliner Warenkorb aufgenommen.

Nach der IT-Sicherheitsrichtlinie erstattet die Arbeitsgruppe IT-Sicherheit jährlich dem IT-KAB einen *IT-Sicherheitsbericht*. Der Sicherheitsbericht für 1999 konstatierte erfreuliche Fortschritte bei der Existenz und Umsetzung behördlicher Sicherheitskonzepte und bei der Absicherung der Lokalen Netze gegenüber dem Berliner Landesnetz mit Hilfe von dezentralen Firewalls. Nach wie vor wurde jedoch bemängelt, dass die Sicherheit von IT-Verfahren noch nicht befriedigend sei, weil viele Regelungen der Richtlinie in diesem Bereich noch nicht umgesetzt wurden. Als besonderes Risko wird erkannt, dass zwischen den vielen angeschlossenen Behörden im Landesnetz große Unterschiede hinsichtlich des Sicherheitsbewusstseins festzustellen seien, die sich in sehr unterschiedlichen Sicherheitsniveaus niederschlagen. Als Beispiele wurden ungenügende Virenschutzmaßnahmen und ungeschützte Übergänge in Fremdnetze genannt. Der Bericht verlangt den umfassenden Einsatz der vom Landesbetrieb für Informationstechnik bereitgestellten Verschlüsselungslösung (Safeguard VPN), die Entwicklung eines abgestimmten Konzepts zur Abwehr von Schadenssoftware und die Erarbeitung neuer und Konkretisierung vorhandener Regelungen zur Nutzung von Internet und Intranet. Es verlangt ferner, über Sanktionen gegen die Behörden nachzudenken, die wider besseren Wissens die IT-Sicherheit nur unzureichend gewährleisten und somit das Berliner Landesnetz unübersehbaren Risiken aussetzen.

Der IT-Sicherheitsbericht 1999 wurde dem IT-Koordinierungsausschuss Berlin (IT-KAB) am 30. März 2000 vorgelegt. Er bildet die Grundlage, um die weiteren erforderlichen Maßnahmen in den verschiedenen Bereichen der Berliner Verwaltung zu planen und umzusetzen.

**Die Beratung und Prüfung dezentraler IT-Verfahren**

Neben den aufwändigen Großverfahren wurden in verschiedenen Verwaltungen kleinere Verfahren eingeführt, bei denen wir in technischer und organisatorischer Hinsicht beraten haben.

Meist wird für diese Verfahren das Betriebssystem Microsoft Windows NT 4.0 eingesetzt. Dieses Betriebssystem genügt bei normalen Sicherheitsanforderungen den in § 5 Abs. 3 Ziff. 3 und 5 BlnDSB geforderten Maßnahmen hinsichtlich der Speicher- bzw. Zugriffskontrolle, wenn die Möglichkeiten zur Einrichtung von benutzerspezifischen Zugriffsrechten und zur Identifizierung und Authentifizierung der Anwender genutzt werden. Unsere Beratung kann sich in solchen Fällen darauf konzentrieren, den vom Betriebssystem angebotenen Gestaltungsspielraum optimal zu nutzen. Um die Authentifizierungsmechanismen auch ausnutzen zu können, sind an die Authentisierungsmittel, hier insbesondere an die Passwortgestaltung, Mindestanforderungen vorzugeben: Mindestlänge ($\geq$ 6 Zeichen), alphanumerischer Zeichenmix, Verhinderung der Benutzung von Trivialpasswörtern, zwangsweiser zyklischer Passwortwechsel,

Die im Bericht aufgelisteten Anforderungen an den Gebrauch von Passwörtern entsprechen den diesbezüglichen Regelungen in der für die Berliner Verwaltung geltenden IT-Sicherheitsrichtlinie und den IT-Sicherheitsstandards.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Zulassen bereits benutzter Passwörter erst nach mehreren Wechseln[22]. Regelungen zum Umgang mit Nutzerkennzeichen und Passwörtern müssen Bestandteil einer Dienstanweisung für die Nutzung des neuen Verfahrens sein.

Bei allen diesen Verfahren kommt es also zunächst darauf an, auf datenschutzgerechte Rahmenbedingungen zu achten, die bei Ansetzung mittlerer Maßstäbe (Grundschutz) von der Standardhard- und -software grundsätzlich ermöglicht werden. Wenn diese Rahmenbedingungen geschaffen sind, kommt es darauf an, deren Einhaltung bei der täglichen Routine durchzusetzen und zu kontrollieren, eine Aufgabe, die wir sporadisch erfüllen können, die die behördlichen Datenschutzbeauftragten jedoch als permanente Aufgabe sehen müssten.

Einige Beispiele mögen die Probleme verdeutlichen.

Zur Beantragung der sog. „*Roten Karte*“, einer gesundheitlichen Unbedenklichkeitsbescheinigung für Personal, welches in Lebensmittelproduktion und -handel tätig ist, und zur damit verbundenen Überwachung wird in vielen Bezirksämtern das IT-Verfahren *LEPÜK* eingesetzt. Dessen erste Version war zu Beginn der 90er Jahre entwickelt worden und konnte die bestehenden Anforderungen an den technischen Datenschutz nicht hinreichend erfüllen. Das neue Verfahren LEPÜK-2 auf der Grundlage von Windows NT wies bei unserer Kontrolle in einem Bezirksamt ebenfalls noch Schwächen bei der Benutzerkontrolle, da unter bestimmten Bedingungen Benutzer ohne Berechtigung zugreifen konnten, sowie bei der Eingabekontrolle, also der Protokollierung von Datenänderungen, auf, deren Beseitigung in Folge der Kontrolle dann zugesagt wurde.

Im Landesverwaltungsamt erfolgt die Umstellung der manuell geführten Karteikarten zur Überwachung der An- und Abwesenheitszeit der Dienstkräfte zu einer automatisierten *Abwesenheitsdatei* mit Hilfe eines Standardprogramms zur Tabellenkalkulation. Außerdem soll die Erstellung von Urlaubskarten sowie deren Ausdruck maschinell in der Büroleitung ausgeführt werden. Die uns dazu vorgelegten Sicherheits- und Netzkonzepte beschrieben in hinreichender Weise die sichere Anbindung der eingesetzten APC an das MAN für die Verwendung eines Datenbankservers im Berliner Landesnetz und die Abschottung des eigenen Netzes gegen Fremdzugriffe.

Unter dem Namen „*eLISa*“ verbirgt sich das „einheitliche Leitungs- und Informationssystem für Sachverständigenorganisationen“, welches als örtliches *Kraftfahrtsachverständigenregister* dazu dient, die für

Die Umsetzung dieser allgemeinen Anforderungen bei spezifischen Verfahren obliegt den jeweiligen Verfahrensverantwortlichen für das IT-Verfahren.

[22] BlnBDA: Ratgeber zum Datenschutz Nr. 3, Oktober 2000

Empfehlungen für die Vergabe von Passwörtern

die Anerkennung als Sachverständige relevanten Informationen zu verwalten. Die uns bereit gestellten Unterlagen zeigten, dass die verfahrensspezifischen und speziell am APC eingesetzten Sicherheitseinrichtungen nur ein geringes Schutzniveau boten. So wurde eine Speicherverschlüsselung auf der Grundlage eines Verschlüsselungsverfahrens mit einem 32 Bit langen Schlüssel vorgesehen, der nur beiläufige Kenntnisnahmen verhindern kann. Die nicht unbedingt zu verlangende Speicherverschlüsselung auf einem nicht vernetzten PC bildete in Anbetracht der geringen Schutzbedarfs zusammen mit anderen einfachen Maßnahmen jedoch ein hinreichendes Sicherheitskonzept.

Unter dem Namen *AVUS 2000* (früher AV-DAT) wird in den *Amtsvormundschaften* ein IT-Verfahren eingeführt, das in Ergänzung zu dem zentral organisierten Fachverfahren ZVK/UVK (Zentrale Vormundschaftskasse/Unterhaltsvorschusskasse) in den Bezirksämtern zur Unterstützung der Bürotätigkeiten für die Stammdatenverwaltung und zur Vordruckerstellung eingesetzt werden soll. Es soll auf den unterschiedlichen Infrastrukturen und Architekturen der Bezirksämter eingesetzt werden, so dass die verfahrensspezifischen Sicherheitskonzepte stark von den jeweiligen behördlichen Sicherheitskonzepte der Bezirke abhängen.

Ein bezirkliches *Gesundheitsamt* hat uns das Verfahren *ISGA* (Informationssystem Gesundheitsamt) vorgestellt, mit dem die Vorgangsbearbeitung im *Amts- und Vertrauensärztlichen* Dienst, also die Bewältigung der ein- und abgehenden Gutachtensaufträge und die Verwaltung der erledigten Gutachten, unterstützt werden soll. Wegen des hohen Schutzwerts der Daten im Geltungsbereich der ärztlichen Schweigepflicht sind anspruchsvolle Sicherungsmaßnahmen erforderlich. Im präsentierten Fall waren sie hinreichend konzipiert. Für den Fall jedoch, dass solche Verfahren in bezirkliche „Rathausnetze“ integriert werden, sind besondere Maßnahmen zur Abschottung solcher Daten gegenüber unbefugten Zugriffen erforderlich.

In den *Standesämtern* der Bezirke und im Standesamt I wird das schon lang eingesetzte Verfahren *AUTISTA* (Automation im Standesamt) durch das modernere Verfahren Autista NT abgelöst werden. Es wurde in Zusammenarbeit mit der bezirklichen Koordinierungs- und Beratungsstelle für Informationstechnik (KoBIT) als „dezentrales Verwaltungsverfahren ohne fachliche Durchdringung“ konzipiert, unterstützt also ausschließlich die Verwaltungsarbeit, dient jedoch nicht der Durchführung der Fachaufgabe selbst. Es handelt sich um eine Vorgangsbearbeitung zur Beurkundung von Personenstandsfällen nach § 1 Personenstandsgesetz: Heirats-, Familien-, Geburten- und Sterbebuch. Außerdem unterstützt das Programm die besonderen Beurkundungen wie z. B. Namensführung oder Vaterschaftsanerkennungen. Die personenbezogenen Daten

werden ausschließlich für diese Beurkundungen benötigt und nach Ablauf von im Programm festgelegten Fristen für die jeweiligen Dateien wieder gelöscht. Auswertemodule (Kosten und Statistik) und diverse elektronische Vordrucke sind in das Verfahren integriert. Auch dieses Verfahren arbeitet mit ausgesprochen schutzbedürftigen Daten und muss hohen Sicherheitsanforderungen entsprechen. Die uns bisher bekannt gemachten Maßnahmen konnten zufrieden stellen. Die Beratung ist jedoch weder in technischer noch rechtlicher Sicht abgeschlossen, da die bereitgestellten Herstellerunterlagen bisher keine hinreichende Transparenz aufwiesen.

In einer bezirklichen *Kindertagesstätte* wird das Verfahren *„Kita-Office“* betrieben, welches auf der Grundlage der in der Berliner Verwaltung selten zum Einsatz kommenden Standardsoftware Lotus Approach die Verwaltungsarbeit der Kita vereinfachen soll. Sein Werdegang erinnert an die frühen PC-Tage in der Berliner Landesverwaltung, als die dezentrale IT-Landschaft noch von Autodidakten geprägt war, die pioniermäßig versuchten, in ihrer Arbeitsumgebung erste Automationsschritte zu vollziehen. Benachrichtigt wurden wir über das Verfahren vom zuständigen Personalrat, der das seit langem unter der Bezeichnung „Probebetrieb“ mit Echtdaten betriebene Verfahren datenschutzrechtlich überprüfen lassen wollte. Unsere Kontrolle zeigte dann auch, dass viele Anforderungen an den sicheren IT-Einsatz nicht erfüllt wurden und man sogar einem eigenen Sicherheitskonzept nicht immer entsprach. Die Zugangskontrolle war nicht hinreichend organisiert, die eingesetzten Laufwerke für externe Speichermedien waren ungeschützt und die Protokollierung der Datenbankzugriffe entsprachen nicht den Anforderungen der Eingabekontrolle.

## 3. Schwerpunkte im Berichtsjahr

### 3.1 Videoüberwachung kein Problem?

Die Videoüberwachung war eines der dominierenden Themen in den Datenschutzdebatten des vergangenen Jahres. Die Ergebnisse von Meinungsumfragen zum Einsatz der Videoüberwachung in den unterschiedlichsten Konstellationen - zumal wenn es sich bei der Fragestellung um einen räumlich eng begrenzten Lebensbereich handelte - lassen darauf schließen, dass die Mehrheit der Befragten derartigen Überwachungsmaßnahmen durchaus positiv gegenübersteht. Die Absichten, die in aller Regel mit diesen Aktivitäten verfolgt werden, suggerieren ja auch nachgerade eine bejahende Einstellung der Befragten. Wer möchte schon gern größere Umwege in Kauf nehmen, um ungefährdet ein bestimmtes örtliches Ziel zu erreichen, wenn er doch weiß, dass er auf direktem Weg Straßen und Plätze passieren muss, die den Ruf haben, bevorzugte Aufenthaltsorte von Kriminellen zu sein.

Wer ärgert sich nicht über Vandalismusschäden in und an öffentlichen Verkehrsmitteln. Wer ängstigt sich nicht, wenn er oder insbesondere sie das eigene Fahrzeug in einem schlecht beleuchteten und unbelebten Parkhaus abstellen muss. Die Beispiele ließen sich beliebig fortsetzen, bei denen der Einsatz von Videotechnik Abhilfe versprechen könnte. Dass dies - zumindest in Berlin - schon längst gängige Praxis ist, möge das folgende Szenario veranschaulichen. Es handelt sich hierbei zwar um eine Fiktion, jedoch nur in Bezug auf den Betroffenen. Die beschriebenen Sachverhalte beruhen dagegen auf konkreten Situationen in Berlin.

*Nach dem Frühstück verlässt Herr M. seine Wohnung und fährt mit dem Lift in die Tiefgarage der Wohnanlage, um mit seinem Auto die Fahrt zu seiner Arbeitsstätte anzutreten. Im Erdgeschoss unterbricht er die Fahrstuhlfahrt, da er noch schnell die aktuelle Tageszeitung aus seinem Briefkasten holen will. Vom Hausportier, in dessen Blickfeld auch die Hausbriefkästen liegen, wird er freundlich mit der Bemerkung begrüßt, ob die Nacht wohl etwas zu kurz gewesen sei. Herr M. stutzt ein wenig, dann fällt ihm aber ein, dass er im Fahrstuhl ein paar Mal herzhaft gegähnt hatte. Er hatte ganz vergessen, dass ja sein Vermieter kürzlich eine Reihe von Maßnahmen eingeführt hatte, die der Aufwertung des Wohnumfeldes dienen sollen. Zu diesen Aktivitäten gehörte auch die Installation einer Videokamera in den Fahrstühlen, deren Bilder in der in diesem Zusammenhang ebenfalls eingerichteten Concierge-Loge auf einem Monitor auflaufen und vom Pförtner beobachtet und vorsichtshalber - man kann ja nicht ständig auf den Bildschirm starren - auf Videokassetten aufgezeichnet werden. In der Tiefgarage angekommen, stellt Herr M. bei der Suche nach dem Autoschlüssel fest, dass sich noch ein paar Zettelchen in seiner Jackentasche befinden, die er nicht mehr benötigt. Natürlich wirft er diese nicht achtlos auf den Boden, sondern entsorgt sie ordnungsgemäß in den für diese Zwecke aufgestellten Behälter. Gerade noch rechtzeitig fiel ihm nämlich ein, dass selbstverständlich ebenfalls die Tiefgarage - auch zu seiner eigenen Sicherheit versteht sich - videoüberwacht wird. Bei der vom Vermieter im Vorfeld durchgeführten Mieterbefragung hatte sich, neben der überwältigenden Mehrheit der Mitmieter, auch Herr M. zustimmend zu den geplanten Maßnahmen zur Erhöhung von Ordnung und Sicherheit in seinem Wohnquartier geäußert.*

*Mit seinem PKW erreicht Herr M. nach kurzer Fahrt ohne in einen Stau zu geraten den nächstgelegenen Bahnhof. Dabei fällt ihm ein, jüngst in der Presse gelesen zu haben, dass die große Kreuzung, die er auf dem Weg zum Bahnhof überqueren muss, seit einiger Zeit von einer Videokamera beobachtet wird, die allerdings zur Verkehrsüberwachung und -lenkung lediglich Übersichtsbilder liefert, ohne dass die KFZ-*

*Kennzeichen oder gar die Fahrzeugführer identifizierbar sind. Vielleicht kommt er auch deshalb so schnell an sein Ziel, weil seither die Ampelschaltung aufgrund der übertragenen Bilder entsprechend dem tatsächlichen Verkehrsaufkommen ferngesteuert werden kann.*

*Glücklicherweise wurde neben dem Bahnhof ein Parkhaus errichtet, in dem Herr M. eigentlich immer einen günstigen Stellplatz findet, was ihm als umweltbewusstem Bürger und Befürworter des Park-and-Ride-Prinzips natürlich entgegenkommt. Aber gerade heute findet er auf dem von ihm bevorzugten Parkdeck keinen normalen Stellplatz mehr. Lediglich einer der Plätze, die ausdrücklich den Fahrerinnen vorbehalten sein sollen, ist noch frei. Da mittlerweile die Zeit drängt, entschließt sich Herr M., ausnahmsweise diesen Stellplatz zu nutzen. Doch als er sein Auto verlassen will, weist ihn eine freundliche, aber auch keinen Widerspruch duldende Stimme aus dem Off auf sein Fehlverhalten hin, denn das Parkhausmanagement vertraut naturgemäß nicht allein auf die Einsicht der Parkhausnutzer, sondern bedient sich einer Reihe von Videokameras, um seinem Anliegen Nachdruck zu verleihen. Die Schilder, die auf die Videoüberwachung hinweisen, hatte Herr M. in der Eile übersehen.*

*Auf dem Weg zum Bahnsteig hatte Herr M. bereits vor einiger Zeit Schilder entdeckt, mit denen die Deutsche Bahn AG auf ihr 3-S-Konzept (Service Sicherheit Sauberkeit) unter dem Motto „24 Stunden alles im Blick“ auf eine permanente Videoüberwachung des Bahnhofs hinweist. Gern hätte er hierzu nähere Informationen bekommen, aber immer, wenn es ihm seine Zeit erlaubte, bei der Aufsicht nach diesen zu fragen, wurde ihm bedeutet, dass das Info-Material gerade nicht verfügbar sei. So weiß er z. B. bis heute nicht, dass die Bilder, die von den - lampenähnlichen - Domekameras erfasst und in die 3-S-Zentrale übertragen werden, nur bei besonderen Anlässen wie Straftaten, Verstößen gegen die Hausordnung und dem Betätigen der Notrufsäulen aufgezeichnet werden.*

*Am Bahnhof Zoologischer Garten angekommen, muss Herr M. in den „Keller“, denn weiter geht es mit öffentlichen Verkehrsmitteln, in diesem Fall mit einer U-Bahn der Linie 2 zum Nollendorfplatz. Auf dem Bahnsteig ertönt gerade eine Durchsage an die Fahrgäste, doch bitte das Rauchverbot zu beachten. Tatsächlich werfen einige Wartende ihre Zigaretten verstohlen auf die Gleise bzw. treten sie auf dem Bahnsteig aus. Herr M. entdeckt zwar kaum übersehbare, auf das Rauchverbot hinweisende Piktogramme und Texte. Hinweisschilder, die auf eine Videoüberwachung der Bahnsteige aufmerksam machen, sucht er jedoch vergeblich.*

*Mit einer gewissen Genugtuung stellt Herr M. fest, dass er auf dem Weg zu seinem Arbeitsplatz weder den Hardenberg- noch den Breitscheidtplatz überqueren muss, hatte er doch von Kollegen gehört, dass hier, eine Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) vorausgesetzt, ein Videoüberwachungskonzept für die Polizei bereits zur Realisierung in der Schublade liegt. So ist er schon nicht mehr überrascht, als er beim Umsteigen in die U 4 einen Wagen entdeckt, an dessen Türen auf die Videoüberwachung in diesem Fahrzeug hingewiesen wird. Da es allerdings auch einen offenbar unbewachten Wagen in diesem kurzen U-Bahn-Zug gibt, entscheidet er sich diesen zu benutzen, obwohl hier - im Gegensatz zu dem überwachten - keine Sitzplätze mehr verfügbar sind.*

*Noch ein kurzer Fußweg und Herr M. erreicht seinen Arbeitsplatz, d. h. fast, denn Herr M. ist in einem Unternehmen beschäftigt, bei dem die Sicherheit groß geschrieben ist. So muss er, ehe sich die Zugangssperre öffnet, in das Auge einer Videokamera schauen und seinen Betriebsausweis in ein Lesegerät einführen. In Sekundenschnelle hat ein Computer die von der Kamera erfassten biometrischen Daten seiner Iris mit den auf einem in den Betriebsausweis implantierten Chip gespeicherten Daten abgeglichen und gibt den Weg frei. Da die Arbeiten, mit denen Herr M. befasst ist, nicht ohne gewisse Risiken für ihn selbst sind und er aus verschiedenen Gründen diese Tätigkeit allein ausüben muss, hat sich sein Arbeitgeber entschlossen, ihn an seinem tatsächlichen Arbeitsplatz - auch zu seiner eigenen Sicherheit - mit einer Videokamera zu beobachten. In einer Betriebsvereinbarung mit der Personalvertretung wurden alle in diesem Zusammenhang stehenden Modalitäten geregelt.*

*Eigentlich wollte Herr M. nach getaner Arbeit noch ein entspannendes Bad in einem nahe gelegenen Schwimmbad der Berliner Bäder-Betriebe nehmen. Doch in der Mittagspause liest er in seiner Tageszeitung, dass in diesem Bad vor einiger Zeit Videokameras zur Eindämmung von Diebstählen in den Umkleideräumen installiert wurden. So stellt er seine Planung um und beschließt, einem seiner anderen Hobbys - mancher würde dafür den Begriff „Laster“ verwenden - zu frönen. Gelegentlich wird er nämlich von einer der zahlreichen Spielotheken magisch angezogen, obwohl er auch hier dem wachsamen Auge einer Kamera nicht entgeht.*

*Ein Blick in seine Geldbörse macht deutlich, dass die Barschaft für sein Vorhaben etwas dürftig ausfällt. Doch da ist schnell Abhilfe zu schaffen. In unmittelbarer Nachbarschaft der Spielhalle findet sich eine Bank, in deren Vorraum auch ein Geldausgabeautomat aufgestellt ist. Dass er beim „Geldziehen“ von einer Videokamera beobachtet und dieses Bildmaterial auch aufgezeichnet wird, ist für ihn sogar nach-*

*vollziehbar. Sollte ihm nämlich wider Erwarten seine ec-Karte gestohlen werden, würde ja auch der Dieb beim Versuch, diese Karte einzusetzen, „gefilmt“ werden.*

*Es muss wohl doch kein gewöhnlicher Tag in seinem Leben sein. Der Besuch in der Spielothek hat sich gelohnt und seine finanziellen Möglichkeiten beträchtlich erweitert. Was liegt da näher, als seine Frau mit einer kleinen, aber feinen Aufmerksamkeit am soeben erzielten Gewinn zu beteiligen. Er steuert also kurz entschlossen ein an seinem Heimweg gelegenes Einkaufszentrum an. Hinweisschilder machen ihn darauf aufmerksam, dass der Betreiber das Geschehen in den allgemein zugänglichen Bereichen mit Videokameras beobachtet. Dass der Juwelier, den Herr M. zum Kauf eines Armbandes für seine Frau aufsucht, zur Bewahrung seiner ausgelegten Schätze vor dem Zugriff unlauterer Zeitgenossen ebenfalls von der Videotechnik Gebrauch macht, kann ihn schon nicht mehr überraschen.*

*Nachdem Herr M. „wohl behütet“ wieder das Parkhaus an seinem Heimatbahnhof erreicht hat, sieht er schon nach kurzer Fahrt ein rotes Lämpchen am Armaturenbrett aufleuchten, das ihm signalisiert, möglichst bald eine Tankstelle aufzusuchen. Dass er sich schon daran gewöhnt hat, als potenzieller Spritdieb regelmäßig von elektronischen Augen beobachtet zu werden, bedarf eigentlich kaum der Erwähnung. Warum jedoch diese Anlage offenbar immer noch in Betrieb ist, obwohl man inzwischen ein ziemlich ausgeklügeltes Schrankensystem installiert hat, um die tatsächlichen Diebe abzuschrecken, kann er sich nicht erklären. Hier sieht Herr M. die Verhältnismäßigkeit der Mittel jedenfalls nicht mehr gewahrt.*

*Etwas erschöpft erreicht Herr M. sein Domizil. Um sich vom Tagesgeschehen noch etwas zu erholen, verwirft er den Gedanken, sich im Fernsehen die Big-Brother-Show eines privaten TV-Senders anzusehen. Auch das Surfen im Internet nach solchen Seiten, bei denen per Webcams Livebilder unterschiedlichster Couleur angeboten werden, kann ihn heute nicht reizen, obwohl er doch kürzlich auf einer solchen Seite einer Kaufhauskette seine Nachbarin erkennen konnte.*

*Herr M. erinnert sich an seine gut bestückte Bibliothek und zieht sich mit George Orwells „1984“ in seinen bequemen Sessel zurück.*

Sollte dieses zugegebenermaßen gestellte - aber eben nicht irreale - Szenario die eifrigen Befürworter des Einsatzes von Videotechnik zum Nachdenken bringen, wäre schon einiges erreicht. Scheint doch die Schwelle zur flächendeckenden Videoüberwachung bereits gefährlich nahe. Der Betrieb jeder einzelnen Überwachungsanlage für sich genommen kann sicher auf triftige Gründe gestützt werden und durchaus auch dazu beitragen, in dem jeweiligen Einsatzbereich das

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

subjektive Sicherheitsgefühl der von diesen Maßnahmen Betroffenen zu erhöhen. Aber wiegen diese Gründe die mit solchen Aktivitäten - insbesondere im öffentlich zugänglichen Raum - verbundenen erheblichen Eingriffe in die Persönlichkeitsrechte der Betroffenen auf? Zumal sich die Risiken eines Missbrauchs der personenbezogenen Bilddaten noch wesentlich erhöhen, wenn diese entgegen der bestehenden Rechtslage auch ohne Anlass aufgezeichnet und damit jederzeit verfügbar werden.

Nachdem wir im vergangenen Jahr auf die unbefriedigende Rechtslage im Hinblick auf die Videoüberwachung bereits ausführlich eingegangen waren[23] und die Diskussionen um das Für und Wider in den Medien beträchtlich zugenommen haben, hat die 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2000 eine Entschließung[24] verabschiedet, die den Gesetzgeber dazu auffordert, die Risiken und Grenzen der Videoüberwachung angemessen zu berücksichtigen. Wesentliche Forderungen dieser Entschließung richten sich auf die Sicherstellung

- einer strengen Zweckbindung,
- einer differenzierten Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen,
- der deutlichen Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- der Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten sowie
- der Löschung der Daten binnen kurzer Fristen.

Desweiteren werden sowohl eine datenschutzrechtliche Vorabkontrolle als auch eine regelmäßige Erforderlichkeitsprüfung von Überwachungsmaßnahmen gefordert. Bis auf Ausnahmen, die im Strafprozess- bzw. im Polizeirecht präzise zu regeln sind, sollten das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern grundsätzlich verboten sein; heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Bildaufnahmen sollten ebenso strafbewehrt sein wie der Missbrauch videotechnisch gewonnener - insbesondere biometrischer - Daten und deren Abgleiche. Nicht zuletzt wird darauf verwiesen, dass die Videoüberwachung nicht großflächig oder gar flächendeckend eingesetzt werden dürfe.

Der Senat hat immer betont, dass eine flächendeckende und anlassunabhängige polizeiliche Videoüberwachung öffentlicher Räume auch de lege ferenda nicht angestrebt wird.

[23] JB 1999, 3.2

[24] vgl. Anlagenband „Dokumente zum Datenschutz 2000“, S. 14

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Der Entwurf für ein Bundesdatenschutzgesetz erfüllt im Hinblick auf eine datenschutzgerechte Regelung der Videoüberwachung die Erwartungen der Datenschützer nur sehr unvollkommen. Zum Einen erfasst § 6 b des Entwurfs lediglich die „Beobachtung *öffentlich zugänglicher* Räume mit optisch-elektronischen Einrichtungen". Zum Anderen sind die Zulässigkeitsvoraussetzungen für Videoüberwachungsmaßnahmen zu weit gefasst, zumal hier auch die zur „Erfüllung eigener Geschäftszwecke erforderliche" Beobachtung als Voraussetzung zugelassen wird. Insbesondere fehlt hinsichtlich der Zulässigkeit von Bildaufzeichnungen, die einen besonders gravierenden Eingriff in das informationelle Selbstbestimmungsrecht darstellen, bisher eine signifikant höhere Schwelle gegenüber der reinen Beobachtung, da diese Speicherung von Bilddaten lediglich an die *Erforderlichkeit* zum Erreichen des mit der Beobachtung verfolgten Zweckes geknüpft ist.

Wie in anderen Ländern ist auch in Berlin von Politikern die Forderung erhoben worden, eine Rechtsgrundlage für die Videoüberwachung durch die Polizei an gefährlichen Orten im Polizeirecht zu schaffen. Im Berichtsjahr ist es jedoch noch nicht zur Vorlage eines entsprechenden Entwurfs gekommen.

In den Polizeigesetzen der Länder Baden-Württemberg, Bayern, Brandenburg, Hamburg, Niedersachsen, Nordrhein-Westfalen, Mecklenburg-Vorpommern, Sachsen, Sachsen-Anhalt, Schleswig-Holstein, Hessen und Saarland bestehen bereits Regelungen zur Videoüberwachung. Siehe hierzu auch Stellungnahme des Senats zu 1.1 „Neue Herausforderungen" (S. 3).

**3.2 Elektronisches Ticketing**

Ende April 2000 endete der erste Feldversuch der Berliner Verkehrsbetriebe (BVG) zum elektronischen Ticketing[25]. An diesem Feldversuch hatten mehr als 26.000 Testpersonen aus Berlin und Umgebung teilgenommen. Diese Testpersonen waren mit berührungslosen Chipkarten (Transponder-Chipkarten) ausgestattet worden, die sie für das Ein- und Auschecken in den Bahnhöfen bestimmter U- und S-Bahn-Linien und in bestimmten Bus- und Straßenbahnlinien benutzen konnten. Dafür waren technische Systeme aufgebaut worden, deren Funktionsfähigkeit und Robustheit mit dem Feldversuch geprüft werden sollten. Gleichzeitig wurden Akzeptanzuntersuchungen und Befragungen angestellt, um festzustellen, wie die Testpersonen mit der Technik zurechtgekommen sind und welche Wünsche sie zu einer zukünftigen Verfahrensweise äußern.

Nach den Aussagen der BVG handelte es sich bei dem Feldversuch um die weltweit erste Erprobung eines elektronischen Ticketing in einem nicht geschlossenen, d. h. ohne Zugangssperren auskommenden Verkehrssystem.

[25] JB 1999, 4.6.3

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Projektziele waren vor allem der Nachweis der Funktionsfähigkeit des offenen Check-In/Check-Out-Verfahrens, die Erprobung eines entfernungs- und zeitabhängigen Tarifmodells, welches Rabattmodelle beinhaltet, die Prüfung der Robustheit der Chipkarten und der Vordergrundsysteme, die die unmittelbare Schnittstelle zu den Fahrgästen darstellen (Check-In/-Check-Out-Terminals, Verkaufssysteme, Informationsterminals und Kontrollgeräte), die Prüfung der Fehlerresistenz der Hintergrundsysteme und die Gewinnung von Erkenntnissen zur Akzeptanz und Anwendungskompetenz der Fahrgäste.

In der Zwischenzeit liegt eine Ergebnisdokumentation des Feldversuchs vor. Zusammenfassend kommt die BVG zu dem Ergebnis, dass die Tester dem elektronischen Ticketing positiv gegenüber gestanden haben und daher eine flächendeckende Realisierung angestrebt werden soll. Im Frühjahr 2001 soll der Wirtschaftsausschuss des BVG-Aufsichtsrats darüber entscheiden, ob und wenn ja, in welcher Weise das elektronische Ticketing eingeführt werden soll.

Obwohl die BVG unsere Behörde von Anfang eingebunden hatte und eine Vielzahl datenschutzrechtlicher Fragen und Probleme in Schriftwechseln und Besprechungen zum Feldversuch behandelt wurde, spielt der Datenschutz in der Ergebnisdokumentation keine Rolle. Der beinahe 200 Seiten starke vertrauliche Bericht behandelt über 18 Zeilen nur Allgemeinplätze zum Datenschutz. Wohl bestand Einigkeit darüber, dass die für den Feldversuch spezifischen Fragestellungen des Datenschutzes keiner größeren Nachbetrachtung bedürfen, zumal durch den Einsatz freiwilliger Tester, die besondere Einwilligungen in die Verarbeitung ihrer Daten gegeben hatten, datenschutzrechtlich ganz andere Rahmenbedingungen gesetzt werden als in einem späteren Echtbetrieb. Jedoch hatten wir im Vorfeld mehrfach darauf hingewiesen, dass wir auch erwarten, dass die Erfahrungen, die sich aus dem Feldversuch für die datenschutzgerechte Gestaltung eines flächendeckenden und obligatorisch zu benutzenden elektronischen Ticketing ergeben, in einen solchen Ergebnisbericht gehören.

Der geringe Raum, der dem Datenschutz in der Ergebnisdokumentation des Feldversuchs eingeräumt wird, steht im Gegensatz zu dem Stellenwert, der ihm in den Erklärungen der Versuchsverantwortlichen vor und während des Feldversuchs zugemessen wurde. Mit der Schaffung eines Teilprojekts Datenschutz im Projekt Elektronisches Ticketing der BVG, der Einstellung einer eigenen Mitarbeiterin für diesen Bereich und der Etablierung eines „Datenschutzbeirats“ unter persönlicher Beteiligung des Berliner Beauftragten für Datenschutz und Akteneinsicht wurden Infrastrukturen geschaffen, die dem Datenschutz die gebührende Rolle in dem Projekt zuweisen sollen.

Die Stellungnahme des Senats in dieser Sache basiert auf Informationen des Vorstandes der BVG.

Von Seiten des Datenschutzbeauftragten wird kritisiert, dass der Datenschutz in der Ergebnisdokumentation „keine Rolle“ spielt. Dieses Dokument diente im Wesentlichen dazu, den derzeitigen Sachstand und die Ergebnisse einer technisch-organisatorischen Plattform eines Elektronischen Ticketing Systems, die in einem Feldversuch erprobt wurde, darzustellen. Die Konsequenzen aus den Erfahrungen des Feldversuchs werden derzeit in der Konzeption des Zielsystems im Echtbetrieb berücksichtigt. Dies gilt nicht nur für den Bereich Datenschutz, sondern auch für den Bereich der Akzeptanzforschung.

Die BVG teilt in diesem Zusammenhang auch nicht die Einschätzung, wonach die „Erklärungen der Versuchsverantwortlichen vor und während des Feldversuchs“ im Gegensatz zu dem „geringen Raum, der dem Datenschutz... eingeräumt wird“, stehen. Aus dem Umfang der Darstellung eines Problems muss nicht auf dessen zukünftige Wertigkeit geschlossen werden. Auch andere Bereiche, deren tatsächliche Bedeutung erst in der Zukunft richtig zum Tragen kommt, werden weniger umfangreich in der Ergebnisdokumentation behandelt. Dazu gehören z.B. die man-machine-interfaces.

Die BVG hat bewusst in enger Verbindung mit dem Datenschutzbeauftragten schon während des Feldversuchs ein eigenes Teilprojekt „Datenschutz“ eingerichtet. Bereits durch den im Frühjahr 2000 eingerichteten „Datenschutzbeirat“ für das Projekt wurde dafür Sorge getragen, dass der Beauftragte für Datenschutz und Akteneinsicht persönlich in das Projekt „Elektronisches Ticketing in Berlin-Brandenburg“ involviert ist. Vor dem Hintergrund dieser Tatsachen

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Im Folgenden sollen die von uns gesehenen Erfahrungen aus dem Feldversuch und die daraus zu ziehenden Konsequenzen unter folgenden Gesichtspunkten behandelt werden.

**Bahnhofsalarm durch tick.et-Start-Terminal**

Bereits im Jahresbericht des Vorjahres[26] wurde moniert, dass das *tick.et start-Terminal*, mit dem sich die Testpersonen an den Bahnhofseingängen in das Verkehrssystem einchecken konnten, bei Fehlfunktionen oder Fehlhandlungen der Tester auffällige und laute Alarmtöne abgab, die mit einer erheblichen Prangerwirkung verbunden waren. Die übrigen - meistens über den aktuellen Feldversuch weniger informierten - Passanten hätten dieses leicht als Schwarzfahrversuch werten können, obwohl dieses nicht der Fall war. Schwarzfahrer hätten bestimmt kein Tick.et über die Lesezone des Terminals geführt. Auf unsere Hinweise auf diesen Mangel reagierte die BVG sofort, in dem sie die Lautstärke herabsetzte und durch Hinweise an den Geräten über die Bedeutung der Alarmmeldungen aufklärte.

Bei der Gestaltung der zukünftig in den Einsatz kommenden *kundenorientierten Endgeräte* ist stärker auf die Interessen der Kunden zu achten, nicht durch schrille Alarme die Aufmerksamkeit der übrigen Personen auf dem Bahnhof oder in den Fahrzeugen auf sich zu lenken. Abgesehen davon, dass es selbst bei einem Schwarzfahrer eine unangemessene Reaktion wäre, wenn er vor der neugierigen Öffentlichkeit als solcher bloßgestellt werden würde, so trifft der Alarm meist jene, die bei der Nutzung des Systems unbeholfen sind (z. B. in dem sie zweimal eingecheckt haben, ohne zwischendurch ausgecheckt zu haben) oder von einem Fehler des Systems bei der Interaktion zwischen Chipkarte und Terminal betroffen sind. Die bisherige Lösung, nämlich die Kunden darüber aufzuklären, was die Alarme wirklich bedeuten und insbesondere die Betroffenen nicht diskriminieren sollen, kann nur als eine provisorische Lösung angesehen werden, die im Rahmen des Feldversuchs hinreichend gewesen sein mag. Welche Lösungen denkbar sind, hängt stark davon ab, ob die Verkehrsbetriebe weiter ohne Sperren auskommen werden oder nicht.

In der Tat sind die Geräte am Anfang des Feldversuchs (01.10.1999) in nicht genügend kalibrierter Form eingesetzt worden. Nach ersten Messungen der BVG selbst ist dies sofort im Oktober 1999 verändert worden. Vor dem Hintergrund der ein- und ausfahrenden Verkehre ist aber ein deutlich hörbares Signal als wünschenswert zu erachten. Im Übrigen hat sich bei den mit tick.et-Testern veranstalteten Diskussionsrunden herausgestellt, dass die Fahrgäste die Signale sehr wohl schätzen. Diese geben ihnen die Sicherheit, keine Fehler machen zu können. Damit ist schon im Feldversuch ein ganz wesentliches Moment von Kundenorientierung in den Vordergrund getreten: Die Fahrgäste werden bei ihren beförderungsrechtlich relevanten Handlungen vom System selbst auch noch unterstützt. Eine Prangerwirkung wurde von allen Testern nicht empfunden.

Über die konkrete akustiktechnische Ausprägung der Signale für die Anwendung im Zielsystem wird entsprechend dem jeweiligen Stand des Wissens und der Technik sicherlich noch diskutiert werden.

**PIN-Offenbarung auf dem Bahnhof**

Die Tastaturen zur Eingabe von *persönlichen Identifikationsnummern* (PIN) an den tick.et-Boxen dienten der bargeldlosen Zahlung von ausgegebenen Chipkarten oder ihrer Aufladung. Sie waren so angebracht, dass es für den Kunden im unüberschaubaren Betrieb auf einem Bahnhof unmöglich war zu verhindern, dass Dritte die PIN bei der Eingabe zur Kenntnis nehmen konnten, wenn sie dieses nur wollten. Die BVG machte geltend, dass die Terminals vom Zen-

Die zurecht geäußerte Kritik, dass das Problem der Vertraulichkeit der PIN-Eingabe für die eurocheque-Karte an den Zahlungsautomaten im Feldversuch nicht befriedigend gelöst worden ist, wurde bereits während des Feldversuchs von Seiten des Projektteams „Finanzen/Elektronisches Ticketing“ aufgenommen. In zahlreichen protokollierten Gesprächen mit Vertretern des Datenschutzes ist dieser Umstand bereits während des Feldversuchs festgehalten und

[26] JB 1999, 4.6.3

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

tralen Kreditausschuss (ZKA) freigegeben worden seien, was nur erfolgen würde, wenn die kundenorientierten Zahlungssysteme auch sicher sind. Dabei übersieht die BVG jedoch, dass die Sicherheit der Bankkunden, dass ihre PIN vertraulich bleibt, in den Verantwortungsbereich des Kunden fällt und daher beim ZKA nicht im Schwerpunkt der Sicherheitsüberlegungen steht.

Die Vertraulichkeit der PIN-Eingabe ist bei den zukünftigen kundenbedienten Geräten für die bargeldlose Zahlung besser zu schützen als beim Feldversuch. Die Tastaturen für die PIN-Eingabe müssen aus dem Gesichtsfeld normaler Passanten verschwinden. Dies kann durch Einrichtung von Diskretionszonen geschehen, durch die Änderung des Einbauwinkels der Tastaturen oder durch Blenden, die den Einblick Neugieriger verhindern.

anerkannt worden. Wie vom Beauftragten für Datenschutz und Akteneinsicht dargestellt, sind die Terminals von der deutschen Kreditwirtschaft abgenommen worden; die Kritik richtet sich somit gegen die Vorgaben der deutschen Kreditwirtschaft. Das Problem konnte während des Feldversuchs aus technischen und zeitlichen Gründen nicht mehr gelöst werden, wird aber selbstverständlich bei der Gestaltung der Endgeräte in Abstimmung mit der deutschen Kreditwirtschaft berücksichtigt werden.

**Leistungsmerkmale der Chipkarte**

Das tick.et speicherte die noch nicht verbrauchten ÖPNV-Einheiten, die eventuell aktuell im Gebrauch befindliche elektronische Fahrkarte sowie eine Historie der letzten zwanzig Fahrten mit Datum, Uhrzeit, Start- und Zielbahnhof und der letzten drei Aufladevorgänge.

Es bestand vor dem Feldversuch Einigkeit darüber, dass jeder Kunde ohne große Umstände jederzeit das auf der Karte gespeicherte Guthaben an ÖPNV-Einheiten lesen können müsste, damit er rechtzeitig weiß, wann die Karte aufgeladen werden muss, bevor er zum Schwarzfahrer wird. Er sollte dabei nicht darauf angewiesen sein, ein freies tick.et-tip-Terminal auf einem Bahnhof vorzufinden, an dem er ebenfalls die Inhalte seiner Karte auslesen konnte. Es war vorgesehen, den Kunden ein Lesegerät (Wallet) in der Größe eines Schlüsselanhängers für einen kleinen Geldbetrag anzubieten. Nach dem derzeitigen Stand der Technik funktioniert ein solches Lesegerät jedoch nur mit einer kontaktbehafteten Chipkarte, nicht jedoch mit einer Transponder-Chipkarte, die für das schnelle Ein- und Auschecken erforderlich ist. Zu Beginn des Feldversuchs wurden ausschließlich Transponder-Chipkarten eingesetzt, so dass der Einsatz von Wallets unmöglich war. Erst in der zweiten Hälfte des Feldversuchs kamen sog. Dual-Interface-Karten zum Einsatz, die beide Zugriffstechniken vereinigten.

Unabhängig von der Technologie der im späteren Echtbetrieb einzusetzenden Chipkarten ist dafür Sorge zu tragen, dass der Kunde des ÖPNV in Berlin einfache und preiswerte Geräte zur Verfügung bekommt, mit denen er den Stand seines tick.et-Kontos ablesen kann. Beim derzeitigen Stand der Technik müssten die Chipkarten mit kontaktbehafteten und kontaktlosen Schnittstellen ausgestattet werden.

Mit der Historie der letzten Fahrten und Aufladungen kann der Kunde falsche Abbuchungen von der Karte

Die BVG wird die konstruktiven Hinweise - bzgl. der Lesbarkeit der auf der Karte gespeicherten Daten durch den Kunden - prüfen und wenn möglich im Zielsystem Elektronisches Ticketing berücksichtigen.

erfolgreich reklamieren, weil sich diese aus der Karte nachvollziehen lassen. Diese Form des Reklamationsmanagements ist datenschutzfreundlicher als die Variante, bei der diese Daten in einem Hintergrundsystem gesammelt werden und somit auch für andere Zwecke verwendet werden können. Die Daten werden also nur im Interesse des Kunden auf der Karte gespeichert.

Andererseits muss der Kunde befürchten, dass die auf seiner Karte gespeicherten Daten auch Dritten zur Kenntnis gelangen, etwa bei Verlust der Karte oder bei einer Beschlagnahme durch Strafverfolgungsbehörden. Dem Prinzip der informationellen Selbstbestimmung entspräche es daher, wenn der Kunde selbst entscheiden könnte, ob er die Daten auf seiner Karte speichern möchte oder nicht. Dazu sollte er jederzeit die Möglichkeit erhalten, die Daten selbst zu löschen, entweder durch eine Zusatzfunktion des Lesegeräts oder durch Betätigung eines Kundenendgeräts auf einem Bahnhof wie z. B. das tick.et-tip-Terminal. Wenn eine solche Löschmöglichkeit gegeben wäre, wäre die Kunden darüber aufzuklären, dass dies im Reklamationsfall auf eigenes Risiko gehen würde.

**Verhinderung des gläsernen ÖPNV-Kunden**

Beim Feldversuch hatten wir im Jahresbericht 1999 konstatiert, dass ein Bezug zwischen den Personalien der Testpersonen und den von ihnen getätigten Fahrten nicht hergestellt werden konnte, so dass zumindest der „gläserne Tester“ keine Realität werden würde. Einzelne Petenten fürchteten das Gegenteil, denn sie konnten sich am tick.et-tip-Terminal über ihre letzten Fahrten informieren und bei den personalbedienten Verkaufsstellen sogar einen Ausdruck davon anfertigen lassen. Sie wussten nicht, dass diese Daten eben nur auf ihrer Karte vorhanden waren.

Leider stellte sich später heraus, dass unsere Aussage dahingehend relativiert werden musste, dass theoretisch - wenn auch wegen der unterschiedlichen Systeme mit unverhältnismäßigem Aufwand verbunden und wegen des begrenzten Personenkreises von geringem Aussagewert - eine Zusammenführung der Daten aus der Testerverwaltung und der scheinbar anonymen Erfassung der Check-in/Check-out-Prozesse möglich gewesen wäre. Beim Check-in/Check-out wurde nämlich die Chipkartennummer erfasst, die auch in der Testerverwaltung gespeichert wurde.

Beim Feldversuch hatten die freiwilligen Tester die Einwilligung zur Speicherung von Daten gegeben, die für die Auswertung des Feldversuchs von Bedeutung waren. Im späteren Echtbetrieb kann die freiwillige Einwilligung in die Datenverarbeitung als Rechtsgrundlage keine Rolle mehr spielen. Da dann fast alle in Berlin lebenden oder die Stadt nur besuchenden Personen von den Datenerhebungen betroffen sein werden, muss in erster Linie mit Datensparsamkeit und in zweiter Linie durch technische Absicherungen

Die BVG ist - angesichts der vom Unterausschusses „Datenschutz“ am 14. November 2000 formulierten Forderung an den Senat zur Unterstützung der BVG - optimistisch, in Zusammenarbeit mit dem Berliner Beauftragten für Datenschutz und Akteneinsicht und durch den gemeinsamen Datenschutzbeirat Lösungen zu finden, den Datenschutz für die Fahrgäste und die von der BVG angestrebten Verbesserungen in Einklang bringen.

gewährleistet sein, dass ein Bezug zwischen den Daten einer Person und den aus ihrem Gebrauch des ÖPNV entstehenden Daten nicht hergestellt werden kann. In seiner Sitzung vom 14. November 2000 hat der Unterausschuss „Datenschutz“ des Ausschusses für Inneres, Sicherheit und Ordnung den Senat aufgefordert, „das Projekt „elektronisches Ticketing“ der BVG darin zu unterstützen, dass ein Verfahren realisiert wird, welches die anonyme Nutzung des öffentlichen Verkehrssystems ermöglicht und die Entstehung personenbezogener Bewegungsprofile der Fahrgäste unter allen Umständen ausschließt.“

Der ersten Forderung wird sicher ohne Weiteres nachgekommen werden, denn bei vielen Produkten, z. B. den bar bezahlten Einzelfahrtausweisen, werden keine personenbezogenen Daten erhoben werden (können). Die zweite Forderung wird innerhalb der BVG nicht uneingeschränkt bejaht, weil bestimmte Qualitätsansprüche an das Marketing und die Kundenbindung dann nicht mehr erfüllt werden können. Auch Überlegungen, bestimmten Kunden, z. B. den Firmenkunden, Einzelgebührennachweise anzubieten, könnten nicht erfüllt werden, denn die dafür notwendigen Daten sind gerade jene, die für personenbezogene Bewegungsprofile notwendig wären.

Die Suche nach Lösungen, die einen optimalen Ausgleich zwischen den Datenschutz- und den Marketinginteressen erreichen könnten, könnte ein Musterbeispiel für die Entwicklung einer datenschutzfreundlichen Technologie sein. Dies bedeutet, den Gebrauch personenbezogener Daten so weit wie möglich einzuschränken und im Übrigen Wege zu finden, mit denen die Geschäftsinteressen der BVG mit anonymen, hilfsweise pseudonymen Verfahren gewahrt werden können.

Zuallererst ist zu fragen, ob die Verkehrsbetriebe ihre Kunden überhaupt namentlich kennen müssen, und wenn ja, welche und in welchem Umfang. Dies wird davon abhängen, welche Produkte in Zukunft in welcher Weise vertrieben werden sollen. Die Tarifierung soll weniger zeitabhängig als vielmehr entfernungsabhängig gestaltet werden. Rabatte sollen mehr den Vielfahrern als den regelmäßigen Fahrern zugute kommen. Soweit Produkte auch weiterhin im Abonnement vertrieben werden sollen, wird die BVG ihre Abonnenten kennen. Ferner lernt sie alle Kunden kennen, die mit kontogebundenen bargeldlosen Zahlungsverfahren ihre Fahrkarten bezahlen. Der Umfang der Daten wird durch den konkreten Zweck bestimmt, für den sie gebraucht werden.

Soweit also die Kundenidentitäten vorliegen, ist als Nächstes zu fragen, ob die personenbezogenen Angaben mit den Daten zusammengeführt werden können, die bei der Nutzung des Ticketing im ÖPNV entstehen. Zwingende Voraussetzung für diese Zusammenführung wäre ein eindeutiges Ordnungsmerkmal, wel-

ches sowohl bei den personenbezogenen Kundendaten existiert als auch beim Ein- und Auschecken erhoben wird, z. B. eine Chipkartennummer. Die Speicherung dieser Nummer ist bei den Kundenstammdaten oder den Zahlungsverkehrsdaten grundsätzlich nicht erforderlich. Eine Ausnahme könnte für jene Kunden gegeben sein, die als Abonnenten am sog. Autoload-Verfahren teilnehmen wollen. Bei diesem Verfahren wird den vertraglich entsprechend gebundenen Abonnenten ermöglicht, ihre Chipkarten, die über kein hinreichendes Guthaben mehr verfügen, beim Ein- oder Auschecken automatisch mit einem bestimmten Betrag aufzufüllen, der dann im Lastschriftverfahren beim Kunden eingezogen wird. In diesem Falle muss der Kunde über die Chipkartennummer identifizierbar sein, d. h. die Chipkartennummer muss - nur in diesem Falle! - bei den Stammdaten des Kunden gespeichert werden.

Weiter ist zu fragen, weshalb beim Ein- und Auschecken ein Identifikationsmerkmal der Chipkarte erhoben werden soll. Der elektronische Fahrschein, der beim Einchecken entsteht, ist auf der Karte gespeichert, die sich in der Hand des Kunden befindet. Sie enthält alle Angaben, die beim Auschecken für die Ermittlung des Fahrpreises benötigt werden. Es besteht also keine Notwendigkeit, diese Check-in- und Check-out-Daten in Hintergrundsystemen zusammenzuführen, wozu natürlich Identifikationsmerkmale der Chipkarte gebraucht würden. Die für die Verkehrsstrommessungen erforderlichen Daten können für jede einzelne Fahrt ohne Kartenbezug (abgebildet als Check-in/Check-out-Datenpaar) und damit anonym erfasst werden. Die einzige Einbuße wäre, dass hintereinander ausgeführte Fahrten, die einzeln ein- und ausgecheckt werden (z. B. beim Umsteigen von U-Bahn zum Bus oder umgekehrt), nicht als zusammenhängend erkannt werden können, ein Erkenntnisgewinn für das Marketing, der in keinem Verhältnis zu den Risiken für die informationelle Selbstbestimmung steht, die bei einer personenbezogenen Vorratsspeicherung entstehen.

Wenn jedoch eine Zusammenführung der Nutzungsdaten mit Chipkarten-Identitätsmerkmalen vorgesehen werden muss, die ihrerseits wieder in bestimmten Fällen die Identifizierung der Kunden zulassen, müssen komplexere Verfahren zum Schutz der Kundenidentität gefunden werden. Zu denken wäre dabei an zwei unterschiedliche Identitätsmerkmale auf einer Chipkarte, eines für die Abrechnung, z. B. bei Anwendung des Autoload-Verfahrens, und eines für die Prozesse beim Check-in/Check-out. Das erste könnte in einem kryptografisch errechneten Hashwert von kundenbezogenen Angaben (z. B. Kontoverbindungsdaten), das zweite in der herstellerseitig vergebenen Chipkartennummer bestehen. Entscheidend wäre dann, absolut sicherzustellen, dass beide Identitäts-

merkmale an keiner Stelle außerhalb der Chipkarte zusammengeführt werden können.

Zusammenfassend ist festzustellen, dass es viele Optionen gibt, mit geringen Ausnahmen alle Hoffnungen, die die Verkehrsbetriebe mit den Datenspuren aus dem Fahrverhalten ihrer Kunden, aus neuen Tarifmodellen und mit modernen Zahlungsweisen verbinden, datenschutzgerecht und unter Wahrung der Anonymität auch zu erfüllen. Wir gehen davon aus, dass das von der BVG eingerichtete „Teilprojekt Datenschutz“ diese ehrgeizigen Ziele erreichen wird.

### 3.3 Datenverarbeitung im Krankenhaus

#### Zugriffsregelungen bei medizinischen Dokumentationssystemen

Die komplexen und arbeitsteiligen Prozesse in einem modernen Krankenhausbetrieb lassen sich ohne massiven Einsatz der Informationstechnik nicht mehr bewältigen. Die Führung *elektronischer Patientendokumentationen*, („elektronische Krankenakten“), die schnelle und effiziente Informationsversorgung klinischer Sonderfunktionsbereiche, wie z. B. der für die Krankenhaushygiene zuständigen Einrichtungen, diverser Labors, der Chirurgie, der Anästhesie, der Leistungsabrechnung mit den Krankenkassen, bis zur Organisation der Krankenpflege, der Versorgungsinfrastruktur und vieles mehr machen die Speicherung und den schnellen Zugriff auf Patientendaten erforderlich. Ausnahmesituationen wie aktuelle Notfälle oder die Konsultation weiterer, gegebenenfalls externer Ärzte machen flexible Lösungen für den Datenzugriff erforderlich. Im Allgemeinen sind die Systeme für die unterschiedlichen Funktionen miteinander vernetzt. Die in einem Bereich entstandenen Daten können in anderen Bereichen direkt zur Verfügung gestellt werden, wenn sie dort gebraucht werden.

Im Berichtsjahr bestand ein Schwerpunkt unserer Prüfungen und Beratungen in der datenschutzrechtlichen Gestaltung der medizinischen Dokumentationssysteme im Krankenhaus, also derjenigen Komponenten, die unmittelbar mit der Behandlung von Patienten im Krankenhaus verknüpft sind.

Die Anforderungen an einen flexiblen und die Prozesse im Krankenhaus nicht behindernden Umgang mit und Zugang zu Daten bestehen in einem Umfeld, in denen die Regeln der ärztlichen Schweigepflicht besonders hohe Anforderungen an den vertraulichen und integeren Umgang mit den personenbezogenen Daten der Patienten stellen. Der absolute Vorrang der Lebensrettung, der Heilung von Krankheiten und der Linderung von Leiden bedeutet nicht die Aufgabe sonstiger Grundrechte, auch nicht der informationellen Selbstbestimmung der Patienten. Dies bedeutet einerseits, dass die für die Behandlung der Patienten erforderlichen Daten jederzeit und schnell im erforderlichen Umfang dort zur Verfügung gestellt werden,

wo sie gebraucht werden, andererseits aber, dass jeder dadurch oder durch andere Aufgaben im Krankenhaus nicht legitimierte Zugriff auf die personenbezogenen Daten der Patienten unterbunden wird.

Anhaltspunkte für die Umsetzung datenschutzrechtlicher Anforderungen an den Zugriffsschutz in Krankenhausinformationssystemen hat eine *Projektgruppe „Datenschutz in Krankenhausinformationssystemen"* der Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) erarbeitet und damit einen Kriterienkatalog für die Kontrolle solcher Systeme bereitgestellt, der für sich in Anspruch nehmen kann, dass er die praktischen Gesichtspunkte aus dem Krankenhausalltag einbezieht. In den „Allgemeinen Grundsätzen für den Datenschutz in Krankenhausinformationssystemen"[27] finden sich sinngemäß folgende Kernaussagen:

- Datengeheimnis und ärztliche Schweigepflicht verbieten es, das Krankenhaus als „informationelle Einheit" anzusehen. Die Weitergabe von Patientendaten innerhalb eines Krankenhauses ist eine *Offenbarung* im Sinne von § 203 Strafgesetzbuch, die einer Befugnisnorm bedarf. Die Übertragung der Zugriffsrechte obliegt der behandelnden Fachabteilung.
- Die Offenbarung von personenbezogenen Patientendaten, damit die Einräumung von *Zugriffsbefugnissen*, ist nur gestattet, wenn und soweit sie im Rahmen der Behandlung oder aufgrund rechtlicher Vorschriften erforderlich ist.
- Patientendaten sind nach dem Stand der Technik zu schützen, wobei das Prinzip der Verhältsmäßigkeit zu beachten ist und wegen der hohen Sensitivität der medizinischen Daten daher ein *hoher Sicherheitsaufwand* angemessen ist. Die Zugriffsdifferenzierungen sind technisch per Systemeinstellung zu verwirklichen. Eine Freigabe von Daten im Einzelfall muss ein bewusster Akt sein.
- Die Belastung des *medizinischen Personals* beim sachgerechten Umgang mit den Patientendaten, die durch die Sicherheitsmaßnahmen bewirkt wird, ist zu minimieren.
- Die technischen und organisatorischen Datenschutzmaßnahmen in einer Klinik erfordern die Schaffung einer entsprechenden *Infrastruktur* und eine klare Festlegung der Verantwortlichkeiten sowie die Einplanung eines angemessenen finanziellen und personellen Aufwands.

Die besonderen Anforderungen an die *Zugriffskontrolle* in medizinischen personenbezogenen Doku-

[27] Stand: 16.3.1994, http://info.imsd.uni-mainz.de/AGDatenschutz/Empfehlungen/grunds.html

mentationssystemen ergeben sich also durch strenge Zugriffsrestriktionen auf der einen Seite und bedarfsweise flexibel zu handhabende Ausnahmebefugnisse:

- Den Ärzten einer Fachabteilung kann der Zugriff auf die Daten der in der Abteilung behandelten Patienten pauschal zugestanden werden, wenn sie an der *Behandlung* der Patienten *beteiligt* sind.
- Dem *Pflegepersonal* wird der Zugriff auf die pflegerelevanten Daten der in ihrer Station befindlichen Patienten zugestanden.
- Medizinischem Personal mit *klinikübergreifenden* Querschnitts- (z. B. Krankenhaushygiene) oder Spezialaufgaben (z. B. Anästhesisten) kann der Zugriff nach Bedarf im erforderlichen Umfang durch die Fachabteilung freigeschaltet werden.
- Falls erforderlich, kann die *Notfallversorgung* von stationär behandelten Patienten durch dafür besonders autorisierte Ärzte vorgenommen werden, die in dieser Rolle mit einem speziellen Zugriffsprofil versehen werden, das den fachabteilungsübergreifenden Zugriff gestattet, aber eine strenge Protokollierung zur Missbrauchskontrolle beinhaltet, die der Fachabteilung den Einzelfall nachträglich nachvollziehbar macht.
- *Konsiliarärzten* wird im Einzelfall der Zugriff freigeschaltet.

Aus technischer Sicht spielt in Krankenhäusern neben der auch in anderen Anwendungsbereichen gängigen Zugriffsdifferenzierung nach abgeschlossenen organisatorischen Einheiten oder nach individuellen Anwenderrollen die *individuelle Freischaltung* für den Zugriff auf einzelne Datensätze oder bestimmte Datenbestände eine wichtige Rolle. Damit kann die notwendige Flexibilität erreicht werden, die den besonderen Anforderungen des Datenzugriffs in einem Krankenhaus gerecht wird. Soweit eine Beschränkung des Zugriffs nicht möglich ist und damit potenziell unbefugte Zugriffe auf die Patientendaten möglich sind, müssen die Zugriffe automatisch einschließlich der Kennung des Zugreifenden protokolliert werden und die Protokolle von der zuständigen Fachabteilung kontrolliert werden. Es muss dann auch organisatorisch sichergestellt werden, dass nicht erforderliche Zugriffe empfindliche Sanktionen nach sich ziehen.

Für die Steuerung der Zugriffe auf sensible patientenbezogene Datenbestände sowie für die Absicherung gegen Verletzungen der Vertraulichkeit und Integrität dieser Daten werden in den Krankenhausnetzen zunehmend auch Methoden der *datenschutzfreundlichen Technologien* in den Einsatz kommen. Methoden der Kryptographie werden für sichere Datenübertragung in Krankenhausnetzen, für die Pseudonymisierung der Patientendaten dort, wo die Identitäten keine Rolle

spielen, und für die Authentisierung der patientenbezogenen Daten und Mitteilungen durch elektronische Unterschrift einzusetzen sein. Zu erwarten ist, dass eine arztbezogene Authentisierungschipkarte (Health Professional Card - HPC) in Zukunft eine noch flexiblere und an den Bedürfnissen orientierte Zugriffssteuerung ermöglichen wird[28].

**Kontrolle zweier medizinischer Dokumentationssysteme in der Charité**

Auf der Grundlage dieser Anforderungen haben wir in zwei Standorten des Klinikums Charité der Humboldt-Universität zu Berlin datenschutzrechtliche Kontrollen von zwei verschiedenen medizinischen Dokumentationssystemen durchgeführt.

Im Bereich des Campus Virchow erfolgte eine Kontrolle der Zugriffsmöglichkeiten und der Zugriffskontrolle beim *Patientendokumentationssystem GUSTAV*. Dieses Dokumentationssystem wird in den chirurgischen Abteilungen und in der Anästhesie des Campus eingesetzt. Es dient der Erfassung der Diagnosen nach dem ICD-Code sowie der an einem Patienten vorgenommen medizinischen Prozeduren zur Übertragung an das Abrechnungssystem. Ferner wird es für wissenschaftliche Auswertungen herangezogen.

Dabei wurde festgestellt, dass alle Berechtigten, die sich mit einem Passwort authentifizierten, Zugriff auf drei Ebenen (Views) erhielten: Daten der eigenen Station, Daten der eigenen Abteilung, Daten aller mit GUSTAV beteiligten Abteilungen. Der Übergang von einer Ebene zur anderen erfolgte ohne weitere Legitimationsprüfungen. Dies bedeutete, dass alle auf GUSTAV zugriffsberechtigten Personen, das waren pauschal alle Ärzte der beteiligten Abteilungen sowie auf besonderen Antrag das Pflegepersonal, Studenten sowie Personen aus anderen Abteilungen, undifferenziert Zugriff auf die Daten aller beteiligten Abteilungen erhielten. Diese pauschalen Zugriffsberechtigungen machten spezielle Zugriffsberechtigungen für Vertretungen, Notfallärzte, Konsiliarärzte, Ärzte im Praktikum, Pflegepersonal und Studenten überflüssig. Wohl erfolgte eine Protokollierung der Systemanmeldungen, eine Aufzeichnung der lesenden Zugriffe erfolgte jedoch nicht. Damit konnten unbefugte Nutzungen der allzu pauschalen Zugriffsberechtigung und damit Brüche des Arztgeheimnisses auch nicht nachvollzogen werden.

Die Gewährung von umfassenden Zugriffsberechtigungen an alle Benutzer erfolgte nicht aufgrund technDie Beanstandungen des Berliner Beauftragten für Datenschutz und Akteneinsicht vom letzten Jahr wurden von der Charité zum Anlass genommen, auch die datenschutzrechtliche Prüfung anderer Software vorzunehmen. So werden erst nach Bestätigung der Datenschutzkonzepte durch den Datenschutzbeauftragten der Charité neue DV-Systeme eingeführt. Vorhandene Systeme werden ebenfalls schrittweise überprüft.

Am System GUSTAV wurde im letzten Jahr eine Reihe von Maßnahmen zur Verbesserung des Datenschutzes durchgeführt (vor dem Hintergrund einer geplanten schrittweisen Ablösung bis Ende 2000). Aufgrund neuer gesetzlicher Anforderungen im Rahmen der medizinischen Dokumentation (ICD-10 und OPS 301) zum Jahresende und deren Umsetzung in DV-Systemen hat sich die Ablösung von GUSTAV verschoben. Bis Ende April 2001 wurden mehr als die Hälfte der GUSTAV-PC durch MedVision-PC abgelöst. Der Rest soll bis Mitte des Jahres abgelöst werden. Bezüglich der Systembetreuung durch eine Fremdfirma wurden Maßnahmen eingeleitet, die eine Verbesserung des Datenschutzes darstellen (Zugriff nur noch von innerhalb des Charité-Netzes, d.h., Mitarbeiter arbeiten vor Ort an der Charité). In Kürze sollen zusätzlich diese Mitarbeiter namentlich hinsichtlich der ärztlichen Schweigepflicht verpflichtet werden.

Die pauschale Zugriffsberechtigung für ausgewählte Mitarbeiter wird in jedem Einzelfall vom ärztlichen Direktor geprüft und nur in Ausnahmefällen (Sicherung der med. Betreuung) erteilt. Sowohl bei der Weiterentwicklung der Software als auch im organisatorischen Umfeld sind zusätzliche Maßnahmen zur Verbesserung des Datenschutzes vorgesehen.

[28] Man beachte auch die differenzierteren Ausführungen der Projektgruppe „Datenschutz in Krankenhausinformationssystemen“ der GMDS zum „Zugriff auf Patientendaten im Krankenhaus“, Stand: 21.4.1999, http://info.imsd.uni-mainz.de/AGDatenschutz/Empfehlungen/zugriff.html

nischer Beschränkungen. Vielmehr erklärten die Systemverwalter, dass eine Differenzierung der Zugriffe sehr wohl möglich gewesen wäre, jedoch auf Anordnung der Klinikleitung nicht eingerichtet worden sei.

§ 26 Abs. 2 Landeskrankenhausgesetz (LKG) verlangt jedoch , dass die Krankenhausleitung zu gewährleisten hat, dass im Krankenhaus auf Patientendaten nur im erforderlichen Umfang zugegriffen werden darf. Im Rahmen der Aus-, Fort- und Weiterbildung von Ärzten und Medizinalfachpersonen ist zu gewährleisten, dass auf Patientendaten nur insoweit zugegriffen wird, als dies für die dem Berufsbild entsprechenden Funktionen erforderlich ist. Sowohl die ärztliche Schweigepflicht nach § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) als auch das Datengeheimnis nach § 8 BlnDSG gestatten die Verarbeitung von Patientendaten nur im Rahmen der Zweckbestimmung des Behandlungsvertrages oder aufgrund rechtlicher Vorschriften. Die technischen und organisatorischen Maßnahmen zum Schutz der Patientendaten vor unbefugter Kenntnisnahme, Löschung und Veränderung haben sich nach § 5 Abs. 1 BlnDSG am Stand der Technik zu orientieren. Die Maßnahmen müssen gewährleisten, dass nur der zuständige Arzt und - falls erforderlich - mitbehandelnde Ärzte und Pflegepersonal die Patientendaten lesen oder im zulässigen Rahmen weitergeben dürfen.

Wir haben beanstandet, dass die Krankenhausleitung ihrer nach § 26 Abs. 2 Landeskrankenhausgesetz (LKG) bestehenden Pflicht zur Beschränkung des Datenzugriffs auf den erforderlichen Umfang nicht nachgekommen ist, weil jeder an GUSTAV Zugriffsberechtigte die uneingeschränkte Möglichkeit hatte, alle patientenbezogenen Daten aller von GUSTAV erfassten Abteilungen zu lesen. Diese Festlegung der Nutzerprofile, die jedem Berechtigten den Zugriff auf alle Daten ermöglicht, steht im direkten Widerspruch zum Prinzip der minimalen Rechte (Need-to-Know), welches zur Gewährleistung der ärztlichen Schweigepflicht gesetzlich verlangt wird. Ferner lagen schwer wiegende Mängel der Zugriffskontrolle nach § 5 Abs. 3 Nr. 5 BlnDSG vor.

Wir empfahlen die Einführung einer technisch abgesicherten differenzierten Zugriffskontrolle, die den Zugriff auf die Individualdaten der Patienten nur in dem Umfang ermöglicht, der für die Erfüllung des Behandlungsvertrages, d. h. für die Behandlung des Patienten und die sich daraus ergebenden Folgemaßnahmen, z. B. im Rahmen der Abrechnung, erforderlich ist. Konkret forderten wir, dass nur folgende Personen die Zugriffsberechtigung auf die Daten eines Patienten erhalten sollten:

Die den Patienten behandelnden Ärzte, maximal die Ärzte der Fachabteilung, in der der Patient behandelt wird, das Pflegepersonal der Station, in der Patient behandelt wird, Ärzte und Pflegepersonal, in deren

Behandlung ein Patient zeitweise gegeben wird (z. B. Anästhesie), sofern relevant: Notfallärzte, ggf. auch aus anderen Abteilungen, aufgrund einer speziellen Zugriffsberechtigung, die eine Protokollierung auslöst, die von der behandelnden Abteilung nachträglich geprüft werden kann, sofern relevant: Konsiliarärzte aufgrund der Freischaltung eines Datensatzes, jeweils im inhaltlich und zeitlich erforderlichen Umfang.

Die Charité nahm die Beanstandungen zum Anlass, im Zusammenwirken mit dem Unternehmen, das das System GUSTAV entwickelt hatte und im Klinikum betreibt, die festgestellten Mängel durch einen externen Gutachter gegenzuprüfen. Dessen Feststellungen führten zur Einleitung von Maßnahmen organisatorischer und programmtechnischer Art, die eine signifikante Verbesserung des Schutzes der Patientendaten erreichen sollten. So sollten die geforderten Zugriffsdifferenzierungen auf Datenbankebene umgesetzt, zeitlich begrenzte Zugriffsberechtigungen ermöglicht und eine Verfahrensanweisung überarbeitet werden, die den Gesamtprozess der Zugriffsrechteverwaltung eindeutig regeln sollte. Ansonsten sollte ein vollständiges Benutzerkonzept erarbeitet werden, welches insbesondere in einem nunmehr forciert einzuführenden Nachfolgesystem zur Geltung gebracht werden sollte. Die Stellungnahme schließt mit der Ankündigung, auch weitere DV-Systeme hinsichtlich der Datenschutzanforderungen einer kritischen Prüfung zu unterziehen.

Diese Ankündigung betraf auch das medizinische Dokumentationssystem MedVision, welches wir im Campus Mitte der Charité prüften. Dort stellten wir fest, dass die Zugriffsberechtigungen der Ärzte und Pfleger auf die jeweilige Station beschränkt waren, womit den datenschutzrechtlichen Anforderungen entsprochen wurde. Jedoch mussten bestimmte Zugriffsprivilegien des Hygienedienstes und der Anästhesie bemängelt werden, deren Notwendigkeit wohl betont, aber nicht hinreichend begründet werden konnte, weil in allen Fallbeispielen, die entgegengehalten wurden, eine temporäre Individualfreigabe der benötigten Datensätze das Problem organisatorisch gelöst hätte. Solange das Verfahren selbst eine solche Datenfreigabelösung nicht ermöglicht, sind individuelle Zugriffsprotokollierungen notwendig, verbunden mit organisatorischen Regelungen zur Prüfung der Protokolle.

### 3.4 Geldwäsche

Die Bekämpfung und Verhinderung der Geldwäsche ist von großer Bedeutung bei dem Kampf gegen die organisierte Kriminalität. Im Anschluss an eine europäische Richtlinie[29] hat der Gesetzgeber 1992 die

[29] Richtlinie 91/308/EWG des Rates vom 10. Juni 1991 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche (ABl. EG Nr. L 166 S.77)

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Geldwäsche durch die Schaffung des § 261 Strafgesetzbuch (StGB) unter Strafe gestellt. Weiterhin wurde 1993 das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz (GwG)) erlassen, in dem für Kreditinstitute und Finanzinstitute, aber auch z. B. für Spielbanken gewerberechtliche Pflichten formuliert wurden, die eine erfolgreiche Bekämpfung der Geldwäsche sicherstellen sollen. Das Gesetz konstituiert insbesondere Pflichten zur Identifizierung (§§ 2 - 8 GwG), Aufzeichnungs- und Aufbewahrungspflichten (§ 9 GwG) sowie eine Pflicht zur Anzeige von Verdachtsfällen (§ 11 GwG). Zur Umsetzung des Geldwäschegesetzes gibt es verschiedene Äußerungen des Bundesaufsichtsamtes für das Kreditwesen, insbesondere die Verlautbarung über Maßnahmen der Kreditinstitute zur Bekämpfung und Verhinderung der Geldwäsche vom 30. März 1998.

Bei einer Umfrage im Jahr 1998 stellten wir fest, dass die Banken nur in geringem Umfang Strafanzeige erstattet hatten. Bedenkt man, dass nur ein einstelliger Prozentsatz der Anzeigen zur Anklage gebracht wird, ist verständlich, dass das Bundesaufsichtsamt für das Kreditwesen und der Zentrale Kreditausschuss über effektivere Maßnahmen zur Bekämpfung der Geldwäsche nachdenken. Allerdings sollten diese Maßnahmen nicht unverhältnismäßig sein und gegen das informationelle Selbstbestimmungsrecht verstoßen.

Das Bundesaufsichtsamt für das Kreditwesen fordert insbesondere von den größeren Banken die Schaffung so genannter *Research-Systeme*. Research ist die nicht auf den konkreten Anlass bezogene Recherche nach Anhaltspunkten, die auf Geldwäsche hindeuten. Die Recherche ist nicht auf eine bestimmte Person oder ein bestimmtes Konto gerichtet, sondern soll sich auf sämtliche Kontobewegungen sämtlicher Kunden beziehen. Die Implementierung von Research-Systemen stellt einen weit reichenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Bankkunden dar, ohne dass diese Art der Datenerfassung auf eine ausreichende Rechtsgrundlage gestützt werden könnte.

Aus den Daten der vom Kunden getätigten oder für ihn bestimmten Finanztransaktionen lässt sich ein facettenreiches Bild seiner wirtschaftlichen Verhältnisse zeichnen. Durch die systematische EDV-gestützte Durchleuchtung der Kundenaktivitäten kann ein weitgehendes Persönlichkeitsbild generiert werden. Durch die Verarbeitung dieser Daten in einem EDV-System tritt ein qualitativer Sprung in der Grundrechtsrelevanz dieses Eingriffs ein, denn das EDV-Research bildet die Grundlage für weitere Datenanalysen der Bank, die zu einer Verdachtsanzeige und evtl. zu Ermittlungsmaßnahmen der Strafverfolgungsbehörden führen können.

Der Beauftragte für Datenschutz und Akteneinsicht bemängelt dass sogenannte Research-System bei Banken, das zur Bekämpfung der Geldwäsche dienen soll. Es handelt sich um kein berlinspezifisches Problem, ebenso wenig ist von einem in Berlin ansässigen Kreditinstitut die Rede.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Dieses Verfahren zur Aufdeckung von Geldwäschefällen nimmt notwendigerweise überwiegend unbeteiligte Dritte in Anspruch. Somit trägt faktisch jeder Kunde, der beim EDV-Research identifiziert wird, das Risiko, nach § 11 GwG als verdächtig angezeigt und mit einem strafprozessualen Ermittlungsverfahren überzogen zu werden. Die Tätigkeit der Banken beim EDV-Research stellt eine Suche nach hinreichenden Anhaltspunkten für einen Anfangsverdacht dar. Dem Wesen nach handelt es sich also um Ermittlungen im Vorfeld eines Verdachtes.

Dieses der *Rasterfahndung* entsprechende Prinzip ist eine Umkehrung der üblichen Ermittlungstätigkeit: Es wird mit dem Ziel vorgegangen, Nicht-Verdächtige auszuschließen, bis sich aus ihrem Kreis Verdächtige ergeben haben. Dies bedeutet aber gleichzeitig, dass solange sich noch keine Verdächtigen herauskristallisiert haben, sich jeder von Rasterfahndungsmaßnahmen betroffene Bürger gleichsam im Vorfeld des Verdachtes und damit weiterer Ermittlungsmaßnahmen befindet. Es ist damit zu rechnen, dass eine große Zahl von Betroffenen lange Zeit in diesem Vorfeld verbleibt und eine Vielzahl von Informations- und Datenverarbeitungsvorgängen erfolgt, die sich im Ergebnis als strafrechtlich irrelevant erweisen. Faktisch werden damit Daten zu Zwecken der Strafverfolgung auf Vorrat gesammelt. Während bei der Rasterfahndung nach § 98 a Strafprozessordnung (StPO) zureichende tatsächliche Anhaltspunkte dafür vorliegen müssen, dass eine Straftat von erheblicher Bedeutung begangen worden ist, sollen die Banken ohne einen derartigen Verdacht Rasterfahndungen zur Kreierung von Verdachtsfällen durchführen. Problematisch ist insbesondere, dass der Kunde von der Aufzeichnung seiner Daten im Rahmen der Verdachtsabklärung durch die Bank und von der Kenntnisnahme der Daten durch die Aufsichtsbehörde nichts erfahren soll. Anderenfalls müsste die Geheimhaltungspflicht des § 11 Abs. 3 GwG im Falle der Erstattung der Verdachtsanzeige ins Leere laufen.

Der Bankenfachverband hat eingeräumt, dass es letztendlich keine verlässlichen Indikatoren für die Kennzeichnung verdächtiger Transaktionen oder Geschäftsbeziehungen gibt. Vielmehr hätten die bisherigen Erfahrungen gezeigt, dass wegen der Vielgestaltigkeit der Geschäftsbanken und zugrunde liegenden Lebenssachverhalte eine Festlegung abstrakter Verdachts- und Ungewöhnlichkeitsraster nicht möglich ist. So könne eine Geschäftsbeziehung trotz unauffälliger Zahlungsgewohnheiten dennoch zur Geldwäsche missbraucht werden, während umgekehrt Transaktionen, die zunächst ungewöhnlich erscheinen, einen vollständig legalen Hintergrund haben könnten.

Wie schnell ein unschuldiger Bankkunde in einen Geldwäscheverdacht geraten kann, lässt sich erkennen, wenn man einige vom Bundesaufsichtsamt für das Kreditwesen bzw. vom Bankenfachverband vor-

geschlagene Raster betrachtet. Danach gilt als verdächtig:

- eine unangekündigte vorzeitige Kreditrückführung,
- plötzliche rege Benutzung eines bisher nahezu inaktiven Kontos,
- Veräußerung von Wertpapieren zu einem unter Renditegesichtspunkten ungünstigen Zeitpunkt ohne ersichtlichen Grund,
- drastische Erhöhung der Anzahl der Habenumsätze,
- wiederholte Finanztransfers an denselben Empfänger usw.

Neben derartigen *„ungewöhnlichen Transaktionen“* sollen bei der Frage, ob ein Verdachtsfall vorliegt, auch - so ein Vorschlag des Bankenfachverbandes - kundenspezifische Kriterien berücksichtigt werden, wie etwa die Nationalität des Kunden, Wohnort des Kunden, Alter, Geschlecht, Branche etc. Derartige kundenspezifische Merkmale sollen im Rahmen eines Score-Systems berücksichtigt werden.

Nach § 4 Abs. 1 BDSG sind die Verarbeitung personenbezogener Daten und deren Nutzung nur zulässig, wenn das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Die Installation eines Research-Systems stellt eine Datennutzung dar, die mangels Einwilligung der Bankkunden einer Rechtsgrundlage bedarf. Eine Einwilligung des Betroffenen liegt nicht vor, da die bei der Aufnahme von Geschäftsbeziehungen erklärte Einwilligung in Datenverarbeitung und –nutzung durch die Bank nicht auch die verdachtslose Rasterfahndung nach dem Kunden unbekannten Suchkriterien im Auftrag von staatlichen Stellen mit umfasst.

§ 14 Abs. 2 Nr. 2 GwG, welcher die Kreditinstitute verpflichtet, Verfahren und Kontrollen zur Verhinderung der Geldwäsche zu entwickeln, ist nicht als Befugnisnorm anzusehen, die die Voraussetzung für eine derartige Datenerhebung und -nutzung schafft. § 14 Abs. 2 Nr. 2 GwG genügt nicht den verfassungsrechtlichen Anforderungen, die an eine Eingriffsermächtigung zur Einschränkung des Rechts auf informationelle Selbstbestimmung zu stellen sind.

Auch die genannte Verlautbarung des Bundesaufsichtsamtes für das Kreditwesen kommt nicht als Rechtsgrundlage im Sinne des § 4 Abs. 1 BDSG in Betracht, da die Verlautbarung nur die Kreditinstitute verpflichtet, nicht jedoch den Kunden, demgegenüber sie keine unmittelbare Wirkung entfaltet.

Auch § 28 Abs. 1 Nr. 2 BDSG ist keine ausreichende Rechtsgrundlage für die Einführung von Research-Systemen. § 28 Abs. 1 Nr. 2 BDSG erlaubt Privaten die Datenverarbeitung für eigene Zwecke zur Wahrung berechtigter eigener Interessen. Aus der Verlaut-

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

barung des Bundesaufsichtsamt für das Kreditwesen ergibt sich jedoch, dass Zweck des EDV-Research die Aufzeichnung der Ergebnisse zwecks Überwachung durch das Aufsichtsamt ist. Ziel ist eine bessere Erkennung von Verdachtsfällen, die dann nach § 11 GwG den Strafverfolgungsbehörden anzuzeigen sind. Somit dient das EDV-Research primär Zielen der Strafverfolgung und nicht dem eigenen Interesse der Banken. Auch wenn man in der Umsetzung des Geldwäschegesetzes einen eigenen Geschäftszweck sieht, käme das EDV-Research nicht als solcher in Betracht, da das Verfahren nach den Vorgaben des Geldwäschegesetzes so nicht vorgesehen ist.

Selbst wenn man den Begriff „Erfüllung eigener Geschäftszwecke“ weit fassen würde, würde § 28 BDSG keine Rechtsgrundlage für das Research-Verfahren darstellen. Das Research-Verfahren ist nicht im Rahmen der Zweckbestimmung des Vertragsverhältnisses mit dem Bankkunden erforderlich (§ 28 Abs. 1 Nr. 1 BDSG), und eine Nutzung des Research-Verfahrens zu Wahrung berechtigter Interessen kommt wegen der überwiegenden schutzwürdigen Belange des Betroffenen nicht in Betracht (vgl. § 28 Abs. 1 Nr. 2 BDSG). Hierzu scheitert auch § 28 Abs. 2 BDSG, der zwar eine Nutzung und Übermittlung von Daten im öffentlichen Interesse zulässt, aber nur wenn kein Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Jeder unbescholtene Bankkunde hat ein schützenswertes Interesse daran, nicht in eine Rasterfahndung und anschließend in einen falschen Verdacht zu gelangen.

Zu unterscheiden von dem Research ist das *Monitoring*. Monitoring ist die auf einen konkreten Anlass bezogene Recherche zur Verifizierung eines bereits vorhandenen oder von außen zugetragenen „Anfangsverdachts“. Die Recherche bezieht sich in diesem Fall auf bestimmte Personen bzw. Konten. Sofern tatsächlich ein Anfangsverdacht vorliegt - dies dürfte bei einigen Kriterien des Research-Systems zweifelhaft sein - bestehen gegen die Durchführung eines Monitoring keine datenschutzrechtlichen Bedenken. Bedenklich ist allerdings, dass das Bundesauftsichtsamt für das Kreditwesen auch in den Fällen, in denen sich der Verdacht nicht bestätigt, zu Kontrollzwecken eine sechsjährige Aufbewahrungsfrist fordert.

Die Arbeit der *Strafverfolgungsbehörden* nach dem Geldwäschegesetz beginnt dann, wenn ein Institut den Verdacht einer Geldwäsche nach § 11 Abs. 1 GwG den Strafverfolgungsbehörden anzeigt. An die Frage, wie die im Geldwäschegesetz geregelte Verdachtsanzeige strafprozessual zu bewerten ist, knüpfen zahlreiche datenschutzrechtliche Fragen an. Der Gesetzgeber hat sich hierzu im Geldwäschegesetz nicht geäußert. Die Strafverfolgungsbehörden bewerten die Geldwäscheverdachtsanzeige in der Regel als Strafanzeige nach § 158 Abs. 1 StPO. Die Strafanzeige ist eine

Die Aufnahme aller Geldwäscheverdachtsanzeigen in das Js-Register der Berliner Staatsanwaltschaft ist rechtlich nicht zu beanstanden.

Die Frage der Registrierung der Verdachtsanzeigen ist nach der Aktenordnung zu beantworten und darf nicht mit der streng strafprozessualen Frage eines Anfangsverdachtes im Sinne von § 152 Abs. 2 StPO vermengt werden. Die Aktenordnung legt insoweit eindeutig fest, dass eine "Anzeige" in das Js-Register und eine "Mitteilung“ in das AR-Register der Staats-

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

bloße Anregung des Verletzten oder einer anderen Person zu prüfen, ob Anlass für die Einleitung eines Strafverfahrens besteht. Diese Kriterien erfüllt die Verdachtsanzeige, da das Institut bei Feststellung von Tatsachen, die darauf schließen lassen, dass eine Finanztransaktion einer Geldwäsche (§ 261 StGB) dient oder im Fall ihrer Durchführung dienen würde, zur Anzeige verpflichtet ist (§ 11 Abs. 1 Satz 1 GwG).

Die rechtliche Einordnung der Verdachtsanzeige bei der Staatsanwaltschaft hat insbesondere Bedeutung für die registermäßige Behandlung des Vorganges und für die Frage, ob der Anzeigeerstatter über den Ausgang im Fall der Einstellung des Verfahrens zu bescheiden ist. Insbesondere an die registermäßige Behandlung knüpfen zahlreiche datenschutzrechtliche Folgen an.

Die Staatsanwaltschaft Berlin sieht nach § 47 Aktenordnung (AktenO) eine Verpflichtung, jede eingehende Geldwäscheanzeige in das Js-Register einzutragen, da sie sie als Strafanzeige nach § 158 StPO ansieht. Die Eintragung in das Js-Register erfolgt unabhängig davon, ob sich der Verdacht einer strafbaren Handlung gegen eine bestimmte Person richtet oder nicht. Die Staatsanwaltschaft prüft nicht, ob tatsächlich ein Anfangsverdacht für eine Straftat vorliegt. Für den jeweiligen Betroffenen bedeutet dies, dass er in das gleiche Register eingetragen wird, in das eröffnete Ermittlungsverfahren eingetragen werden. Als Folge dieser Eintragung gelten abhängig vom Verfahrensausgang die Aufbewahrungsvorschriften der Justiz. Dies bedeutet, dass im Fall der Einstellung des eingeleiteten Ermittlungsverfahrens eine Mindestspeicherfrist von fünf Jahren für die angezeigte Straftat folgt.

Wir halten die ungeprüfte Aufnahme aller Geldwäscheverdachtsanzeigen in das Js-Register der Staatsanwaltschaft für rechtlich höchst problematisch. Nach unserer Auffassung besteht ein Widerspruch zwischen den Regelungen der Aktenordnung und den §§ 152 Abs. 2, 160 StPO. Danach ist ein Ermittlungsverfahren erst dann einzuleiten, wenn ein Anfangsverdacht vorliegt, d. h. wenn zureichende tatsächliche Anhaltspunkte für eine Straftat gegeben sind (§ 152 Abs. 2 StPO). Dies ist durch die Staatsanwaltschaft jeweils im Einzelfall zu prüfen. Ist eine Prüfung noch nicht erfolgt, so wäre nach unserer Auffassung die Verdachtsanzeige in das Allgemeine Register für Ermittlungsverfahren (AR-Register) einzutragen bzw. müsste ein eigenes Verdachtsregister für Geldwäscheverdachtsanzeigen geschaffen werden.

Auch bei der Erstattung von Strafanzeigen ist es erforderlich, dass die Staatsanwaltschaft den jeweiligen konkreten Anfangsverdacht vor Einleitung eines Ermittlungsverfahrens prüft. Da die Polizei in der Regel vor Weiterleitung der Geldwäscheverdachtsanzeige an die Staatsanwaltschaft schon erste Ermittlungen angeanwaltschaft einzutragen ist. Auch der Gesetzgeber hat vor diesem Hintergrund in §§ 11 und 13 des Geldwäschegesetzes den Terminus "Anzeige" gewählt, und zwar jeweils im Kontext mit dem Begriff der "zuständigen Strafverfolgungsbehörde". Dementsprechend bewerten die Strafverfolgungsbehörden zu Recht auch die Geldwäscheverdachtsanzeigen als Strafanzeigen im Sinne von § 158 Abs. 1 StPO.

Die Eintragungspraxis ist auch deshalb unbedenklich, weil die Eintragung in das Js-Register einer Staatsanwaltschaft lediglich besagt, dass eine Strafanzeige vorliegt, ohne dass damit eine Aussage über deren materiellen Gehalt und insbesondere die Intensität des Tatverdachtes verbunden wäre.

.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

stellt hat, halten wir eine Prüfung eines strafrechtlichen Anfangsverdachtes für die Staatsanwaltschaft und die daran anschließende Entscheidung, in welches Register das Verfahren einzutragen ist, für zwingend. Wenn der Anfangsverdacht sich nicht als begründet erweisen sollte, vertreten wir die Auffassung, dass eine Eintragung in das Js-Register mit den sich daran anschließenden langen Aufbewahrungsfristen nicht verhältnismäßig ist. Einige andere Bundesländer haben dies ebenso gesehen und daher Eintragungen in das AR-Register oder aber in ein gesondertes Geldwäscheverdachtsregister vorgesehen.

Leider hat sich die Staatsanwaltschaft auf Nachfrage nicht noch einmal zu dem hier in Berlin durchgeführten Verfahren geäußert. Wir bedauern dies sehr, da die Diskussion dieses Themas von uns bereits 1995 angestoßen worden war. Den Presseberichten war in den vergangenen Jahr immer auch zu entnehmen, dass sich die Anzahl der angezeigten Verfahren, die tatsächlich zu einer Anklageschrift oder auch einer Einstellung oder Verurteilung geführt haben, auf höchstens vier Prozent belaufen haben soll. Dies spricht umso mehr dafür, strenge Maßstäbe bei der Beurteilung anzulegen, inwieweit bei einer Geldwäscheverdachtsanzeige tatsächlich konkrete Anhaltspunkte für eine Straftat vorliegen. Nur dann ist es gerechtfertigt, die Verdachtsanzeige als Ermittlungsverfahren in das Js-Register einzutragen und damit die Notwendigkeit zu schaffen, das Verfahren ggf. wieder einstellen zu müssen.

Entgegen den Ausführungen des Beauftragten für Datenschutz und Akteneinsicht hat sich die Berliner Staatsanwaltschaft auf dortige Nachfrage mit einem Schreiben vom 15. November 2000 erneut ausführlich zu den Grundlagen für die rechtliche Einordnung von Geldwäscheverdachtsanzeigen geäußert.

### 3.5 Informationsfreiheit: Eine erste Bilanz

Etwas mehr als ein Jahr Informationsfreiheit, des Zugangs jedes Menschen zu Unterlagen der öffentlichen Verwaltung Berlins, liegt hinter uns. War das Land zum Zeitpunkt des In-Kraft-Tretens des Berliner Informationsfreiheitsgesetzes (IFG) im Oktober 1999 das zweite nach Brandenburg, das zu Gunsten einer höheren Transparenz öffentlichen Handels ein derartiges Gesetz erlassen hat[30], so zieht diese Entwicklung nun auch im übrigen Bundesgebiet Kreise. Mittlerweile hat auch Schleswig-Holstein ein Informationsfreiheitsgesetz[31]. In den Ländern Hessen[32] und Nordrhein-Westfalen[33] wurden in der zweiten Jahreshälfte entsprechende Anträge aus der Opposition (Bündnis 90 / Die Grünen einerseits, der CDU andererseits) in den jeweiligen Landtag eingebracht. In Sachsen, Bremen und auf Bundesebene existieren Fraktions- bzw. Referentenentwürfe. Zum gegenseitigen Erfahrungsaustausch haben die Länder mit einer Informati-

[30] JB 1999, 3.1

[31] vom 9. Februar 2000, SH GVBl.;S. 166

[32] Drs. 15/1474 vom 17. August 2000

[33] Drs. 13/321 vom 31. Oktober 2000

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

onszugangsgesetzgebung, also Berlin, Brandenburg und Schleswig-Holstein, die „Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID)“ gegründet, in der nicht nur datenschutzrechtliche Fragen, sondern sämtliche Probleme des Informationszugangs behandelt werden sollen. Den Vorsitz in der AGID hatte im Berichtszeitraum der Brandenburger Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht. In ihrer ersten öffentlichen Stellungnahme hat sie - trotz bereits erzielter Fortschritte - die Weiterentwicklung der Informationsfreiheit in Bund und Ländern gefordert[34].

Erste Erfahrungen mit der Anwendung des Gesetzes in Berlin konnten die Verwaltungen inzwischen sammeln. Die Evaluierung dieser Erfahrungen ist entsprechend der damaligen Ankündigung der Senatsverwaltung für Inneres[35] zwischenzeitlich eingeleitet worden und wird durch eine an alle Verwaltungen gerichtete Fragebogenaktion umgesetzt.

Der Berliner Beauftragte für Datenschutz und Akteneinsicht erlangt entsprechend der ihm nach § 18 IFG zugewiesenen Schiedsstellenfunktion von strittigen Fällen Kenntnis. Dadurch werden wir über die in der Rechtsanwendung entstehenden Schwierigkeiten informiert. Zahlreiche Fälle haben gezeigt, dass die Anwendung des IFG sehr grundsätzliche Probleme aufwirft.

Die Ergebnisse der von der Senatsverwaltung für Inneres durchgeführten landesweiten Umfrage zeigen, dass es erhebliche Schwierigkeiten bei der Umsetzung des Gesetzes gibt, die teilweise in der Systematik des IFG selbst begründet sind. Nach vorläufiger Auswertung der Umfrage zeichnet sich bereits in folgenden Punkten gesetzlicher Änderungsbedarf ab:

- Die Konkurrenz zwischen dem IFG und spezialgesetzlichen Regelungen, die ebenfalls Akteneinsichtsrechte vorsehen, muss geregelt werden.
- Bei den jeweiligen Regelungen wird zu untersuchen sein, wie die Wertungswidersprüche aufgelöst werden können, die sich bisher aus der unterschiedlichen Ausgestaltung der in den verschiedenen Gesetzen gewährten Akteneinsichtsrechte ergeben.
- Die Regelungen zur Entscheidungsfindung müssen praktikabler gestaltet werden.
- Es bedarf der Klarstellung, dass der Schutz des behördlichen Willensbildungsprozesses auch nach Abschluss des Vorgangs eine Ablehnung der Akteneinsicht rechtfertigen kann; es wäre die Festlegung von Schutzfristen zu erwägen, nach deren Ablauf die Akteneinsicht zu gewähren ist.

Die Senatsverwaltung für Inneres wird nach eingehender Auswertung der Umfrage einen Entwurf zur Novellierung des IFG erarbeiten.

**Anwendungsbereich**

So bereitet schon der *sachliche Anwendungsbereich* des Gesetzes Probleme. § 2 IFG normiert Informationsrechte gegenüber den Behörden und sonstigen öffentlichen Stellen des Landes Berlin. Das Gesetz unterscheidet nicht danach, ob der Staat - wie zumeist - öffentlich-rechtlich handelt oder aber privatrechtlich.

Nach den ersten Erfahrungen kann bestätigt werden, dass der Anwendungsbereich des Gesetzes teilweise nicht richtig erkannt wird. Handeln öffentliche Stellen fiskalisch oder nehmen sie am Wettbewerb teil, schließt sie das nicht vom Anwendungsbereich des IFG aus.

---

[34] „Deutschland muss für mehr Verwaltungstransparenz sorgen“; vgl. Anlagenband „Dokumente zum Datenschutz 2000“, S. 71

[35] Erste Hinweise zur Anwendung des Gesetzes zur Förderung der Informationsfreiheit im Land Berlin vom 16. November 1999, I.A 1-0201/48

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Dennoch haben Verwaltungen Anträge von Bürgern auf Akteneinsicht in Grundstücksvorgänge mit der Begründung abgelehnt, dass das Informationsfreiheitsgesetz bei fiskalischem Handeln des Staates (wie hier bei der Verwaltung und Veräußerung landeseigener Grundstücke) nicht anwendbar sei. Diese Auffassung wird weder vom Wortlaut des Gesetzes getragen, noch entspricht sie dem Sinn und Zweck des Gesetzes, der maßgeblich darin liegt, staatliches Handeln transparent zu machen. Dies gilt umso mehr, wenn bei staatlichen Transaktionen Steuergelder in nicht unerheblicher Höhe verwendet werden. Gerade in den Bereichen der Grundstücksverwaltung und der Stadtplanung ist dies der Fall.

Erstaunlicherweise bereitet neben dem sachlichen Anwendungsbereich auch der in § 3 Abs. 1 geregelte *persönliche Anwendungsbereich* Schwierigkeiten. Danach hat jeder Mensch ein Informationsrecht nach Maßgabe dieses Gesetzes. Es tauchte die Frage auf, wie es sich verhält, wenn ein parlamentarischer Ausschuss (der Bezirksverordnetenversammlung -BVV- oder des Abgeordnetenhauses) einen Antrag nach IFG stellt. Zwar sieht das IFG den Informationszugang durch Gremien der Parlamente nicht vor, es besteht aber jederzeit die Möglichkeit, dass der Antrag von einem Ausschussmitglied gestellt wird. Die Gremien vom Informationszugang auszunehmen, würde nicht nur dem Gesetzeswortlaut widersprechen, sondern hieße damit auch, ihnen weniger Rechte einzuräumen als dem „normalen“ Bürger, was gerade angesichts des Gesetzeszwecks, staatliches Handeln zu kontrollieren, nicht einsichtig wäre. Für Ausschüsse der BVV besteht unabhängig davon nach § 17 Abs. 2 Satz 2 Bezirksverwaltungsgesetz gegenüber dem Bezirksamt ein Anspruch auf Informationszugang, wenn nicht die Voraussetzungen der in Satz 2 genannten „Staatswohlklausel“ vorliegen. Diese Bestimmung stellt keinen Widerspruch zum IFG dar, sondern sieht einen eigenen Anspruch auf Informationszugang für Ausschüsse der BVV vor, der neben den Ansprüchen nach dem IFG steht und weiter geht als diese, weil er nur aus Gründen des Staatswohls nicht erfüllt werden darf.

Das im Bericht dargestellte Beispiel zeigt, dass das Verhältnis des allgemeinen Informationsanspruchs des IFG zu spezialgesetzlichen Einsichts- und Auskunftsrechten Probleme aufwerfen kann. Diese Frage bedarf aus Sicht des Senats generell einer gesetzlichen Klarstellung.

**Einschränkungen**

Das Informationsrecht muss *Einschränkungen* verschiedener Art erfahren. Die in §§ 5 ff IFG normierten Einschränkungen stellen Ausnahmen dar, die eng auszulegen sind. Insbesondere wird häufig verkannt, dass grundsätzlich ein *Anspruch* auf Informationszugang besteht, die Verwaltung also eine Entscheidung zu seinen Gunsten treffen muss, es sei denn, es greift eine der gesetzlichen Ausnahmen. Auch in diesem Fall hat die Behörde nach pflichtgemäßem Ermessen zu prüfen, ob nicht gleichwohl der begehrte Informationszugang gewährt werden kann. Dies folgt zwingend aus § 4 IFG („Akteneinsicht...ist...zu gewähren, es sei denn,...“) in Verbindung mit den Eingangsformulie-

Eine erste vorläufige Auswertung der landesweiten Umfrage zum IFG bestätigt, dass die Handhabung der Beschränkungen des Informationsrechts nach §§ 5 ff. IFG im besonderen Maße Schwierigkeiten bereitet. Diese Schwierigkeiten liegen offenbar zu einem nicht unerheblichen Teil in Wortlaut und Regelungstechnik des IFG selbst begründet und lassen sich nur zum Teil im Wege der Gesetzesauslegung sinnvoll lösen.

rungen der Ausnahmetatbestände (z. B. in §§ 6, 7, 9, 10: „Das Recht auf Akteneinsicht... besteht nicht, soweit ...“). Die Ermessensentscheidung verdichtet sich nur dann zu einem zwingenden Informationszugangsverbot, wenn gesetzliche Gründe entgegenstehen, z. B. wenn mehr personenbezogene Daten herausgegeben würden, als § 6 Abs. 2 IFG zulässt. Auch die in der „Staatswohlklausel“ (§ 11) gewählte Eingangsformulierung weicht von diesen verwaltungsgesetzestechnisch bekannten Auslegungsregeln nicht ab. Sie besagt, dass außer in den Fällen der §§ 5-10 die Akteneinsicht oder Aktenauskunft *nur versagt werden darf*, wenn das Bekanntwerden des Akteninhalts dem Wohle des Bundes oder eines deutschen Landes schwerwiegende Nachteile bereiten oder zu einer schwerwiegenden Gefährdung des Gemeinwohls führen würde. Ist dies nicht der Fall, so *muss* Informationszugang gewährt werden.

Vielfach Schwierigkeiten bereitet den Verwaltungen die Regelung, dass das Recht auf Akteneinsicht oder Aktenauskunft nicht besteht, soweit personenbezogene Daten veröffentlicht werden und tatsächliche Anhaltspunkte dafür vorhanden sind, dass überwiegend *Privatinteressen* verfolgt werden (§ 6 Abs. 1). Dieser Begriff ist erst zum Ende der Beratungen des Gesetzentwurfs in den parlamentarischen Ausschüssen aufgenommen worden, weil ausgeschlossen werden sollte, dass Anträge nach IFG missbräuchlich gestellt werden. Deshalb kommen als Ausschlussgründe nur Motive wie etwa Rache, Neugier oder Querulantentum in Betracht, die aber nach der Gesetzesformulierung überhaupt nur dann beachtlich sind, wenn personenbezogene Daten zugänglich gemacht werden sollen. Vor diesem Hintergrund ist die Auffassung, der Antrag sei abzulehnen, wenn jemand Informationszugang zur Vorbereitung eines Prozesses begehrt, nicht haltbar. Denn dabei kann durchaus auch der in § 1 genannte Gesetzeszweck verfolgt werden. Den Verwaltungen ist aber zuzugestehen, dass in Zweifelsfällen zur Ermittlung der Motive beim Antragsteller durch Rückfrage ermittelt werden muss, aus welchem Grunde er den Informationszugang begehrt, auch wenn dadurch der falsche Anschein erweckt wird, das IFG gewähre nur unter Angabe von Gründen den Informationszugang.

Eine Ermittlung der Motive für die Antragstellung beim Antragsteller ist häufig nicht zielführend, da dieser - durch einfache Bezugnahme auf den Gesetzestext (Förderung der demokratischen Meinungs- und Willensbildung, Kontrolle staatlichen Handelns) - ein überwiegendes Privatinteresse unproblematisch „verdecken“ kann.

§ 7 IFG schützt *Betriebs- und Geschäftsgeheimnisse*, ohne sie näher zu definieren. Die Verwaltungen neigen dazu, diesen Begriff sehr weit auszulegen, insbesondere dann, wenn es um Geld geht. Nicht jegliches in den Unterlagen vorhandene Zahlenwerk, aus dem ein bestimmtes Finanzgebahren hervorgeht, ist aber schützenswert und damit als geheime Information unzugänglich. Bei der Auslegung hilft die Rechtsprechung insbesondere zum Gesetz über den unlauteren Wettbewerb (§ 17) weiter. Voraussetzung ist danach die Geheimheit der Tatsache, der Geheimhaltungswille des Geheimnisinhabers sowie das berechtigte

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

wirtschaftliche Interesse an der Geheimhaltung. Das Land Berlin kann sich zwar als Adressat des IFG grundsätzlich nicht auf eigene Betriebs- und Geschäftsgeheimnisse berufen, bei fiskalischem Handeln können sie jedoch nicht von vornherein ausgeschlossen werden.

In der Anwendung problematisch erweisen sich die Ausnahmen, die den „*Schutz des behördlichen Entscheidungsprozesses*“ regeln. Nach § 10 Abs. 3 Nr. 1 IFG besteht das Recht auf Informationszugang z. B. nicht, soweit sich Akten auf die *Beratung des Senats und der Bezirksämter* sowie deren Vorbereitung beziehen. Auch dieser Ausnahmetatbestand muss eng ausgelegt werden, so dass nur Akten gemeint sein können, die sich unmittelbar auf die Beratung des Senats sowie unmittelbar auf deren Vorbereitung beziehen. Nur dann ist tatsächlich der „Kernbereich der Tätigkeit der Obersten Exekutivorgane zur Sicherung der verfassungsrechtlich geschützten exekutiven Eigenverantwortung“ berührt, um dessen Schutz es hier allein geht. Eine andere Auffassung würde bedeuten, dass der Informationszugang bei Themen, die letztlich im Senat, aber in irgendeinem Verfahrensstadium von einer Senatsverwaltung behandelt wurden, von vornherein nicht in Betracht käme, was dem Sinn und Zweck des Gesetzes zuwiderlaufen würde.

Das Recht auf Informationszugang besteht nicht, soweit durch das Bekanntwerden des Akteninhalts Angaben und *Mitteilungen öffentlicher Stellen, die nicht dem Anwendungsbereich dieses Gesetzes unterfallen*, ohne deren Zustimmung offenbart werden. Wenn die Ermessensentscheidung der Verwaltung ergibt, dass ein Informationszugang nicht in Betracht kommt, etwa weil die Information der anderen öffentlichen Stelle als geheimhaltungsbedürftig angesehen wird, muss die Verwaltung in einem nächsten Schritt bei dieser öffentlichen Stelle erfragen, ob diese aus eigener Sicht der Offenbarung der Information zustimmt. Die Verwaltung ist also *verpflichtet*, nach der eigenen „negativen“ Ermessensentscheidung die Zustimmung der anderen Stelle einzuholen. Diese Auffassung ist für die Verwaltung praktikabel, weil sie nämlich nicht von vornherein, sondern erst nach der eigentlich zu Lasten des Antragstellers ausfallenden Ermessensentscheidung die Zustimmung der anderen öffentlichen Stelle einzuholen hat.

Nach Auffassung des Senats liegt es im pflichtgemäßen Ermessen der öffentlichen Stelle, ob sie bei der anderen Stelle, die nicht dem Anwendungsbereich des IFG unterfällt, eine Anfrage auf Zustimmung stellt. Eine Verpflichtung zur Anfrage bei der anderen Stelle lässt sich aus dem Wortlaut des § 10 Abs. 3 Nr. 2 IFG nicht ableiten.

Der Informationszugang soll versagt werden, wenn sich der Inhalt der Akten auf den *Prozess der Willensbildung* innerhalb von und zwischen Behörden bezieht (§ 10 Abs. 4 IFG). Dieser Ausschlussgrund gilt nicht mehr nach Abschluss des Verfahrens, was sich aus der Wortwahl und der Überschrift zu § 10 IFG ergibt, denn ab diesem Zeitpunkt ist ein behördlicher Entscheidungsprozess nicht mehr zu schützen. Unterlagen auch nach Abschluss des Willensbildungsprozesses zwischen den Verwaltungen auszunehmen ist vor dem Hintergrund der gesetzgeberi-

Der Anwendungsbereich des § 10 Abs. 4 IFG wurde nach ersten Erfahrungen besonders kontrovers diskutiert. Hier besteht Klarstellungsbedarf. Entgegen der Auffassung des Berliner Beauftragten für Datenschutz und Akteneinsicht gilt der Schutz des Prozesses der Willensbildung nach Ansicht des Senats auch nach Abschluss des Verfahrens. Hierfür spricht bereits der unterschiedliche Wortlaut des § 10 Abs. 4 IFG im Vergleich zu § 10 Abs. 1 IFG, wo das Recht auf Akteneinsicht oder Aktenauskunft ausdrücklich nur „bis zum Abschluss eines Verwaltungsverfahrens“ in be-

schen Intention nicht einsichtig, weil gerade auch die Kooperation zwischen den Berliner Behörden förderlich für die demokratische Meinungs- und Willensbildung des Einzelnen sein kann.

stimmten Fällen beschränkt wird. Auch die Zielrichtung der Norm, innerhalb der Behörden und zwischen den Behörden im Vorfeld von Entscheidungen einen offenen Meinungsaustausch zu gewährleisten, spricht gegen eine Auslegung, nach der nach Abschluss des Verfahrens der Ausschlussgrund des § 10 Abs. 4 nicht mehr gilt.

**Sonderproblem: Auftragsvergabe**

Mehrfach wurde die Frage gestellt, ob das Informationsfreiheitsgesetz (IFG) auch bei der Auftragsvergabe durch öffentliche Verwaltungen gilt, oder ob dieses Gesetz zum Schutz eventueller Konkurrenten oder aus Geheimhaltungsinteressen des Staates in diesem Bereich keine Anwendung findet.

Es gibt keine haushaltsrechtlichen Regelungen, die das öffentliche Vergabeverfahren vom Anwendungsbereich des Informationsfreiheitsgesetzes ausschließen.

Bei einem Akteneinsichtsbegehren für die behördliche *Planungs- und Projektionsphase* enthalten weder das Gesetz gegen Wettbewerbsbeschränkungen noch die Verdingungsverordnungen Regelungen für Akteneinsichtsrechte. Hier gilt also das Informationsfreiheitsgesetz. In der Regel dürfte allerdings das Recht auf Akteneinsicht an dem in § 10 IFG geregelten Schutz des behördlichen Entscheidungsprozesses scheitern.

Auch *nach Abschluss des Auftragsvergabeverfahrens* gelten keine Spezialregelungen, so dass das Informationsfreiheitsgesetz uneingeschränkt gilt. Bei der Frage, ob Akteneinsicht gewährt werden kann, ist insbesondere zu prüfen, ob durch die Akteneinsicht ein Betriebs- oder Geschäftsgeheimnis offenbart wird (vgl. § 7 IFG). Grundsätzlich kann davon ausgegangen werden, dass die Entscheidungsgründe, die zu einer Auftragsvergabe durch die Verwaltung geführt haben, keine *Geschäftsgeheimnisse* i.S.d. § 7 IFG enthalten. Problematischer sind demgegenüber die Unterlagen, die die Unternehmen eingereicht haben, aus denen wirtschaftliche Strukturen ersichtlich sind sowie die Kalkulationen, die dem Angebot zugrunde gelegt werden. Hier ist eine Einzelabwägung durchzuführen, bei der auch zu klären ist, ob das Informationsinteresse das schutzwürdige Interesse des Betroffenen an der Geheimhaltung überwiegt.

*Während des Vergabeverfahrens* ist das Informationsfreiheitsgesetz auch anzuwenden, soweit es um Bauleistungen unter 5 Millionen Euro, Dienstleistung unter 200 Tausend Euro und freiberufliche Leistungen unter 200 Tausend Euro geht. Bezüglich des Betriebsgeheimnisses gilt das oben Gesagte entsprechend. Zusätzlich ist noch zu prüfen, ob der konkrete Akteneinsichtswunsch die ordnungsgemäße Durchführung des Bieterverfahrens behindert.

Bei öffentlichen Aufträgen, die den o. g. Schwellenwert übertreffen, gelten die §§ 97 ff. Gesetz gegen

Der Senat teilt die Auffassung des Berliner Beauftragten für Datenschutz und Akteneinsicht, dass das IFG grundsätzlich auch im Vergabeverfahren gilt. Die Schranken dieses Gesetzes, insbesondere die §§ 7 und 10 IFG, sind jedoch bei der Vergabe von Aufträgen oberhalb der Schwellenwerte gemäß § 2 Vergabeverordnung (VgV) in Übereinstimmung mit höherrangigen vergaberechtlichen Bestimmungen anzuwenden.

Dabei findet das IFG in der Projektierungs- und Planungsphase uneingeschränkt Anwendung. Die Möglichkeit einer Kollision besteht hier nicht. Während des Vergabeverfahrens – also zwischen Bekanntmachung und Zuschlag – ist ein Informationsanspruch nach § 3 Abs. 1 unter Hinweis auf § 10 Abs. 1 IFG auf jeden Fall zu versagen. Dies folgt aus entsprechenden oberhalb der Schwellenwerte höherrangigen Vorschriften der Verdingungsordnungen. Nach Abschluß des Vergabeverfahrens kommt ein Anspruch aus § 3 Abs. 1 IFG in Betracht. Allerdings sind die Geheimhaltungsinteressen der Bieter und Bewerber streng zu beachten. Dies gilt insbesondere im Hinblick auf ein mögliches Nachprüfungsverfahren, da § 111 Abs. 2 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) bestimmt, dass die Vergabekammer die Einsicht in die Unterlagen zu versagen hat, soweit dies aus wichtigen Gründen, insbesondere des Geheimnisschutzes oder zur Wahrung von Fabrikations-, Betriebs- oder Geschäftsgeheimnissen geboten ist. Insofern ist die Einschränkung in § 7 IFG zwingend in Übereinstimmung mit § 111 Abs. 1 GWB auszulegen, damit § 111 Abs. 2 GWB nicht leerläuft. Dabei ist auch zu beachten, dass § 111 Abs. 1 GWB lediglich den am Nachprüfungsverfahren Beteiligten einen Anspruch auf Akteneinsicht einräumt.

In der Projektierungs- und Planungsphase bei der Vergabe von Aufträgen unterhalb der Schwellenwerte gelten die vorgemachten Aussagen ebenfalls. Bei der Vergabe von Aufträgen unterhalb der in § 2 VgV genannten Schwellenwerte kommt eine Kollision mit höherrangigem Bundesrecht nicht in Betracht.

Jedoch ist eine Auskunft in Bezug auf ein laufendes Vergabeverfahren unter Berufung auf § 10 Abs. 1 IFG auch unterhalb der Schwellenwerte zu versagen. Nach Abschluß des Vergabeverfahrens gelten die allgemeinen Vorschriften, wobei insbesondere die Geheimhaltungsinteressen von Bieter und Bewerbern im Rahmen von § 7 IFG zu berücksichtigen sind.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Wettbewerbsbeschränkungen (GWB). Das Vergabeverfahren selbst enthält keine Einsichtsregelungen, wohl aber das Nachprüfungsverfahren, nämlich § 111 GWB. Da das Gesetz gegen Wettbewerbsbeschränkungen insgesamt verschiedene Einsichtsrechte regelt, ist davon auszugehen, dass der Gesetzgeber hier eine abschließende Regelung getroffen hat. Außerhalb des in § 111 GWB geregelten Einsichtsrechts im Verfahren vor der Vergabekammer soll den Beteiligten keine Einsicht gewährt werden, damit sich diese hierdurch keine Vorteile verschaffen können. Da Beteiligte ohne Probleme mit Hilfe von Dritten (Freunde etc.) die Vorgaben des Gesetzes gegen Wettbewerbsbeschränkungen unterlaufen könnten, sollte das Informationsfreiheitsgesetz im Rahmen des §§ 97 ff. GWB angewandt werden.

Auch hier wird deutlich, wie schwierig im Einzelfall die Bestimmung des Verhältnisses zwischen dem IFG und spezialgesetzlichen Einsichts- und Auskunftsrechten sein kann. Insoweit ist zu überdenken, inwieweit die Regelung eines weitreichenden allgemeinen Akteneinsichts- und Aktenauskunftsrechts nicht notwendigerweise Wertungswidersprüche im Verhältnis zu spezialgesetzlichen Akteneinsichts- und Aktenauskunftsrechten provozieren muss, und wie dieses Problem gelöst werden kann.

**Verfahren**

Die notwendige Folge eines auf § 10 gestützten Ablehnungsgesuchs wird häufig übersehen. Die Behörde hat nämlich mitzuteilen, *zu welchem Zeitpunkt eine Einsichtnahme voraussichtlich erfolgen kann* (§ 15 Abs. 4 IFG). Ist der Anknüpfungstatbestand der Abschluss des Verwaltungsverfahrens, so bedeutet dies, dass diese Verpflichtung der Verwaltung nur dann gelten kann, wenn der Informationszugang wegen eines noch laufenden Verwaltungsverfahrens abgelehnt worden ist, also der Antrag zum „falschen Zeitpunkt" gestellt worden ist. Die uns (häufig erst nach Erlass) zur Kenntnis gegebenen ablehnenden Bescheide der Verwaltung treffen meistens keine Aussage zu der Bestimmung des § 15 Abs. 4, so dass sie unvollständig und damit rechtswidrig sind, weil sich ihnen eine für den Bürger wichtige Information über den Zeitpunkt einer späteren möglichen Einsichtnahme nicht entnehmen lässt.

Häufig falsch ausgelegt wird auch die Frist des § 15 Abs. 5 IFG. Danach ist der Antragsteller innerhalb zwei Wochen nach Antragstellung zu bescheiden, wenn die öffentliche Stelle den Antrag zurückweisen will. Umgekehrt ausgedrückt, bedeutet dies, dass bei Nichtreaktion der Verwaltung innerhalb zwei Wochen der Antrag - wenigstens teilweise - positiv beschieden werden muss. Angesichts dieser Fristenregelung empfiehlt es sich jedenfalls, innerhalb von zwei Wochen mitzuteilen, dass der Antrag noch geprüft wird, aber möglicherweise mit der Ablehnung gerechnet werden müsse.

Die Nichtreaktion der Verwaltung innerhalb der Frist von zwei Wochen bedeutet keinesfalls, dass der Antrag ganz oder teilweise positiv beschieden werden muss. Diese Auffassung des Berliner Beauftragten für Datenschutz und Akteneinsicht ist rechtlich nicht haltbar und findet keinerlei Stütze im Gesetz. Bei § 15 Abs. 5 IFG handelt es sich offensichtlich um eine bloße Ordnungsvorschrift.

Besondere Schwierigkeiten bereitet den Verwaltungen die bei positiven Bescheiden zu treffende *Gebührenentscheidung* (§ 16 IFG). Die erforderliche Änderung der Verwaltungsgebührenordnung ist nach etwa einem halben Jahr nach In-Kraft-Treten des Gesetzes vorgenommen worden[36]. Danach wird für die Gewährung

Die Gebührenentscheidung richtet sich nach den Vorgaben der Verwaltungsgebührenordnung. Bei der Ausfüllung des Gebührenrahmens ist der Verwaltungsaufwand zu berücksichtigen. Dieser ist eine Frage des Einzelfalles und lässt sich nicht allein aus der letztlich vorgelegten Seitenzahl erschließen. Zu be-

[36] 22. Verordnung zur Änderung der Verwaltungsgebührenordnung vom 30. Mai 2000, GVBl. S. 349, GVBl. 1997, S. 525

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

von Akteneinsicht oder Aktenauskunft eine Gebühr zwischen 20 und 1.000 DM erhoben. Für Fotokopien wird pro Seite 1,00 DM verlangt. Mehrere Verwaltungen haben zwischenzeitlich Gebührenentscheidungen getroffen, die entweder vor dem Hintergrund von § 5 Verwaltungsgebührenordnung[37], der ein Beurteilungsermessen einräumt, nicht nachvollziehbar waren, oder aber der Höhe nach, verglichen mit dem Bürger tatsächlich zugänglich gemachten Aktenmaterial, unverhältnismäßig wirkten. So erschienen 150,-- DM für 17 vorgelegte Seiten genauso unangemessen wie die 600,-- DM, die eine Verwaltung maßgeblich anhand der Stundenzahl bemessen hat, die ein Beamter des höheren Dienstes mit der (Vorbereitung der) Akteneinsichtsgewährung in 2 Vorgänge verbracht hat, ohne dass dessen eigentlicher Arbeitsaufwand näher beschrieben worden wäre. Dass die Gebühr eine angemessene Höhe nicht überschreiten darf, hat schon der Europäische Gerichtshof zum Umweltinformationsgesetz entschieden[38]. Danach ist der Begriff „angemessener Betrag“ nicht derart zu verstehen, dass „die gesamten den öffentlichen Haushalten durch eine Zusammenstellung von Unterlagen tatsächlich entstandenen, namentlich mittelbaren, Kosten auf Einzelne abgewälzt werden, die einen Antrag auf Information gestellt haben“. Insbesondere darf die Gebühr Einzelne, „die Informationen erhalten möchten, hiervon nicht abhalten und ihr Recht auf Zugang zu diesen Informationen nicht beschränken.“ Wir haben empfohlen, zur besseren Handhabbarkeit des mit der Verwaltungsgebührenordnung vorgegebenen Gebührenrahmens Gebührenkategorien zu entwickeln, etwa in Anlehnung an die zum Umweltinformationsgesetz ergangene Gebührenordnung. Sie sieht eine Staffelung vor, je nachdem, welche Fallgruppe im Einzelfall betroffen ist (einfacher Verwaltungsaufwand, umfangreiche bzw. außergewöhnliche Maßnahmen zur Zusammenstellung der Unterlagen). Leider ist die Senatsverwaltung für Inneres dieser Empfehlung nicht gefolgt. Die zum schleswig-holsteinischen Informationsfreiheitsgesetz ergangene Gebührenordnung hat dagegen diesen Ansatz aus dem Umweltinformationsbereich aufgegriffen[39].

achten ist freilich das so genannte Äquivalenzprinzip, welches eine gebührenrechtliche Ausprägung des Verfassungsgrundsatzes der Verhältnismäßigkeit darstellt und auch ohne einfachrechtliche Normierung zu beachten ist. Aus dem Urteil des Europäischen Gerichtshofs zum Umweltinformationsgesetz ergeben sich allerdings keine zusätzlichen gebührenrechtlichen Vorgaben, da bei der Gebührenerhebung für Amtshandlungen nach dem IFG keine richtlinienkonforme Umsetzung europarechtlicher Vorgaben in nationales Recht zu beachten ist. Die Entwicklung von Gebührenkategorien in Anlehnung an die Anlage zum Gebührenverzeichnis zur Umweltinformationsgebührenverordnung (UIGGebV) wurde abgelehnt, da der tatsächliche Verwaltungsaufwand eine Frage des Einzelfalls ist und sich mit Blick auf das IFG nur schwerlich sinnvoll kategorisieren lässt. Insbesondere würde eine Kategorisierung wie in der Anlage zum Gebührenverzeichnis zur Umweltinformationsgebührenverordnung (UIGGebV) nur eine Verschiebung des allgemeinen Problems der Gebührenberechnung bewirken, da die entscheidende Frage, wann im Einzelfall ein einfacher, ein umfangreicherer oder ein außergewöhnlich aufwendiger Fall vorliegt, auch durch die Bildung dieser drei Gruppen nicht beantwortet wird. Das Problem wäre lediglich verlagert auf die Frage der Zuordnung zu einer der Gruppen.

Insgesamt betrachtet sind dies die typischen anfänglichen Schwierigkeiten, die sich bei der Umsetzung eines neuen Gesetzes ergeben, die jedoch nach einer Eingewöhnungsphase in jeder Verwaltung in den Griff zu bekommen sind. Die eigentlichen Schwierigkeiten sind aus unserer Sicht in der grundsätzlich ablehnenden Haltung gegenüber diesem Gesetz zu sehen, das sich von dem althergebrachten Prinzip der grundsätzlichen Wahrung des Amtsgeheimnisses ab-

Der Senat sieht keine Anhaltspunkte dafür, dass die Anwendungsschwierigkeiten auf eine „grundsätzlich ablehnende Haltung gegenüber dem Gesetz“ zurückzuführen sind. Er weist vielmehr auf die bestehenden strukturellen Mängel des Gesetzes hin, die die Auslegung des Gesetzes und die Umsetzung im Einzelfall erschweren.

---

[37] in der Fassung vom 13. November 1978, GVBl. S. 2410

[38] Urteil vom 9. September 1999, in: NVwZ 1999, S. 1209,1211

[39] VO vom 4. Juli 2000, SH GVBl. 2000, S. 546

wendet und deshalb ein Umdenken in den Amtsstuben erforderlich macht.

## 4. Aus den Arbeitsgebieten

### 4.1 Sicherheit

#### 4.1.1 Verfassungsschutz

Für den Verfassungsschutz haben sich im Berichtsjahr gravierende Änderungen ergeben. Nachdem das Amt wiederholt in den negativen Schlagzeilen war, hat sich die Senatsverwaltung für Inneres entschlossen, das Landesamt für Verfassungsschutz aufzulösen. Die Verfassungsschutzaufgaben im Land Berlin werden seit Anfang Januar 2001 in einer neu eingerichteten Abteilung der Senatsverwaltung für Inneres wahrgenommen. Das *Gesetz zur Reform des Verfassungsschutzes* im Land Berlin ist am 9. Dezember 2000 in Kraft getreten[40].

Der Senat beabsichtigt, dass der Berliner Verfassungsschutz nach den öffentlichen Diskussionen der letzten Jahre die Akzeptanz, die einer wichtigen Institution der wehrhaften Demokratie zukommt, wiedergewinnt und den gestiegenen Anforderungen in Zukunft gerecht wird. Deshalb soll unter der Zielsetzung „Verfassungsschutz durch Aufklärung“ die Transparenz und die bürgerbezogene Aufklärung über die gewonnenen Erkenntnisse intensiviert werden. Der Schwerpunkt des Verfassungsschutzes soll verstärkt auf der Analyse von Bestrebungen extremistischer Organisationen sowie der Einschätzung sicherheitsgefährdender, vorrangig gewaltgeneigter Bestrebungen liegen. Es ist beabsichtigt, die Zusammenarbeit mit anderen Verfassungsschutzbehörden zu intensiveren und insbesondere in den Aufgabenbereichen Spionageabwehr und Geheimschutz die zentrale Auswertungszuständigkeit des Bundesamtes für Verfassungsschutz zu berücksichtigen. Auch die neue Verfassungsschutzabteilung soll nachrichtendienstliche Mittel zur Aufklärung einsetzen, um Informationen über im Verborgenen sich entwickelnde und wirkende verfassungsschutzfeindliche Bestrebungen zu erhalten. Der Einsatz nachrichtendienstlicher Mittel soll nach dem Grundsatz der Verhältnismäßigkeit einer strengen Prüfung unterzogen werden[41].

Zu begrüßen ist, dass wir bereits bei der Erarbeitung der Vorentwürfe zu dem Gesetzentwurf von der Senatsverwaltung für Inneres einbezogen wurden und Gelegenheit hatten, Empfehlungen zu den datenschutzrechtlich relevanten Teilen abzugeben. In den

Ziel der Verfassungsschutzreform im Land Berlin ist die Schaffung eines modernen, effektiven, transparenten und bürgernahen Verfassungsschutzes, der den Anforderungen der Bundeshauptstadt gerecht wird.

Hand in Hand mit der Strukturreform geht auch eine personelle Erneuerung der Behörde. Der Berliner Verfassungsschutz soll noch stärker für wissenschaftlich ausgebildete Fachkräfte geöffnet werden.

[40] GVBl. S. 495

[41] Landespressedienst (LPD) vom 5. September 2000, S. 1

Gesetzesberatungen wurden die meisten unserer Empfehlungen aufgegriffen.

So ist eine klare datenschutzrechtliche Abgrenzung bei der Datenweitergabe von der neuen Verfassungsschutzabteilung an andere Stellen innerhalb der Senatsverwaltung für Inneres vorgesehen (§ 2 Abs. 2). Eine gesetzliche Verankerung einer weisungsfreien Revision, wie wir sie schon 1989 anlässlich unserer Grundsatzprüfung beim Verfassungsschutz gefordert hatten, ist erfolgt (§ 2 Abs. 3). Gestrichen wurde die 1993 aufgenommene Aufgabe der Beobachtung früher fortwirkender Strukturen und Tätigkeiten durch Mitarbeiter des ehemaligen Staatssicherheitsdienstes der DDR. Die Beteiligung des Verfassungsschutzes bei „sonstigen Überprüfungen“ (§ 5 Abs. 3 Satz 1 Ziff. 4) wurde konkretisiert.

Für so genannte „Prüffälle“ wurde eine eindeutige Rechtsgrundlage geschaffen (§ 7 Abs. 2). Das sind Fälle, in denen erst - und nur mit öffentlich zugänglichen Quellen - zu klären ist, ob tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen vorliegen. Unserer ursprünglichen Empfehlung, diese personenbezogenen Daten in Dateien und zur Person geführten Akten erst zu speichern, wenn sich tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen bestätigt haben, wurde zwar nicht gefolgt; angesichts der technischen Entwicklung haben wir jedoch gegen die nunmehr vorgesehene Speicherung in Dateien keine Bedenken, da entsprechend unserer Empfehlung klargestellt wurde, dass eine Speicherung dieser Daten nur in internen Dateien und nicht im Nachrichtendienstlichen Informationssystem NADIS oder anderen Verbunddateien erfolgen darf. Wenn innerhalb eines Jahres keine relevanten Erkenntnisse angefallen sind, sind die Daten zu löschen.

Die nachrichtendienstlichen Mittel sind nunmehr im Gesetz aufgeführt (§ 8 Abs. 2). In den Gesetzesberatungen haben sich die Koalitionsfraktionen auf weitergehende Einschränkungen des Einsatzes nachrichtendienstlicher Mittel geeinigt. Dem Einsatz nicht konkret aufgeführter, aber vergleichbarer nachrichtendienstlicher Mittel, insbesondere dem sonstigen Eindringen in technische Kommunikationsbeziehungen durch Bild-, Ton- und Datenaufzeichnungen, hat der Verfassungsschutzausschuss vorab zuzustimmen. Zudem dürfen zeugnisverweigerungsberechtigte Personen wie Geistliche, Strafverteidiger, Rechtsanwälte und Ärzte (vgl. §§ 53 und 53 a StPO) nicht von sich aus zur Beschaffung von Informationen in Anspruch genommen werden, auf die sich ihr Zeugnisverweigerungsrecht bezieht.

Für die Beobachtung gewalttätiger Bestrebungen oder geheimdienstlicher Tätigkeit wurde klargestellt, dass personenbezogene Daten von Kontakt- und Begleitpersonen nur mit nachrichtendienstlichen Mitteln

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

erhoben werden dürfen, wenn dies für die Gewinnung von Erkenntnissen unerlässlich ist (§ 8 Abs. 3 Satz 2).

Die Kompetenzen der G 10-Kommission werden erweitert, indem sie auch die Anordnung nachrichtendienstlicher Mittel, die in ihrer Art und Schwere dem Brief-, Post- und Fernmeldegeheimnis gleichkommen, sowie die Unterrichtung der Betroffenen kontrollieren soll (§ 9 a Abs. 2). Unserer Anregung, wegen unserer bestrittenen Kontrollkompetenz im G 10-Bereich[42] im Gesetz klarzustellen, dass hierdurch unsere Kontrollbefugnis für den weiteren Umgang mit den erlangten personenbezogenen Daten nicht berührt wird, wurde nicht nachgekommen. Allerdings wurde dies in der abschließenden Ausschussberatung von der Senatsverwaltung für Inneres klargestellt.

Nicht berücksichtigt wurde unsere Empfehlung, den vollständigen Ausschluss des Informationsfreiheitsgesetzes für die bei der Verfassungsschutzabteilung geführten Akten durch eine differenzierte Regelung zu ersetzen. Den besonderen Bedingungen des Verfassungsschutzes hätte dadurch Rechnung getragen werden können, dass der bislang nur untergesetzliche Schutz von Verschlusssachen ausdrücklich gesetzlich geregelt wird (z. B. durch eine entsprechende Ergänzung des IFG selbst, was den Vorteil hätte, dass auch Verschlusssachen außerhalb der Verfassungsschutzbehörde eingeschlossen wären). Die Ansprüche nach dem IFG würden sich dann nur noch auf die offenen Vorgänge beziehen, soweit nicht andere Beschränkungen greifen. Eine derartige Regelung hätte auch die Zielsetzung, der Behörde mehr Transparenz zu verschaffen, mehr entsprochen als ein pauschaler Ausschluss des IFG.

Das Berliner Informationsfreiheitsgesetz (IFG) trifft bis auf wenige Ausnahmen keine Aussagen über die Konkurrenz zu anderen gesetzlichen Regelungen. Der Ausschluss der Anwendbarkeit des Gesetzes auf die Unterlagen der Verfassungsschutzabteilung soll verhindern, dass die detaillierten Spezialregelungen des Verfassungsschutzgesetzes über die Informationsübermittlung (dritter Abschnitt) und die Gewährung von Auskunft und Akteneinsicht (vierter Abschnitt), die nicht den Schutz von Verschlusssachen betreffen, unterlaufen werden. Die Regelung wird bei der Ende 2002 im Lichte der Erfahrungen der Berliner Verwaltung mit dem Berliner Informationsfreiheitsgesetz durchzuführenden Bestandsaufnahme überprüft.

### 4.1.2 Polizei

**Großer Lauschangriff**

In seiner Entscheidung zum sog. Großen Lauschangriff hat das *Landesverfassungsgericht Mecklenburg-Vorpommern*[43] festgestellt, dass der im Landespolizeigesetz festgeschriebene Katalog von Straftaten, aufgrund derer in Wohnungen gelauscht werden darf - etwa bei einfachen Umweltstraftaten -, viel zu weit gefasst ist und damit gegen das in Art. 13 Abs. 1 GG gewährleistete Grundrecht auf Unverletzlichkeit der Wohnung verstößt. Es darf nur dann abgehört werden, wenn die Gefahr, der begegnet werden soll, eine Wertigkeit hat, die einer gemeinen Gefahr oder einer Lebensgefahr vergleichbar ist.

Die Polizei darf außerhalb von Wohnungen Gespräche, die durch Amts- oder Berufsgeheimnis geschützt sind - wie beispielsweise bei Ärzten und Rechtsan-

[42] JB 1995, 5.1

[43] Urteil vom 18. Mai 2000, Az.: LVerfG 5/98

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

wälten -, nur noch in Fällen dringender Gefahr oder bei polizeilichem Notstand zur Verhinderung schwerer Schäden für Rechtsgüter besonders hohen Ranges abhören.

Im Übrigen begrüßen wir auch die Klarstellung im Urteil, dass grundsätzlich jeder, über den die Polizei durch die Überwachung personenbezogene Daten erlangt hat, zu benachrichtigen ist, ebenso wie die Aussage des Gerichtes, dass der Landesbeauftragte für den Datenschutz frühzeitig und nicht erst - wie im Gesetz vorgesehen - nach fünf Jahren zu informieren ist, wenn eine Unterrichtung des Betroffenen vorher nicht möglich ist. Des Weiteren ist die Verwendung der Daten für Zwecke der Strafverfolgung durch das Urteil eingeschränkt worden.

Die vom Verfassungsgericht für seine Entscheidung angeführten Gründe enthalten wichtige Fingerzeige. Wir erwarten, dass sie auch bei der Rechtsentwicklung in Berlin berücksichtigt werden.

Nach einer Änderung des ASOG vom 11. Mai 1999 hat der Senat das Abgeordnetenhaus jährlich über die durchgeführten - auch präventiven - Lauschangriffe zu unterrichten (Art. 13 Abs. 6 GG; § 25 Abs. 10 ASOG). Das hat der Senat - wenn auch verspätet - getan und dabei unsere Empfehlungen, die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. Juni 2000 zu dem *Bericht* der Bundesregierung zum Einsatz technischer Mittel zur akustischen Überwachung von Wohnraum für Zwecke der Strafverfolgung im Jahr 1998[44] berücksichtigt. Im Berichtszeitraum wurde eine Maßnahme durchgeführt, die nicht der richterlichen Überprüfung bedurfte, weil die aufgezeichneten Daten unverzüglich nach Beendigung des Einsatzes gelöscht wurden. Die Maßnahme diente ausschließlich dem Schutz einer bei einem polizeilichen Einsatz tätigen Person. In den Bericht wurde der Umfang der Maßnahme einbezogen. Unsere weiteren Empfehlungen - wie in den Wire-tap-Reports der USA -, die Anzahl der Gespräche, die Art der betroffenen Räume, die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahmen und die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen anzugeben, konnten nicht berücksichtigt werden, weil das Verfahren noch nicht abgeschlossen ist.

Der Senat ist um eine möglichst umfassende Berichterstattung gegenüber dem Parlament bemüht. Diese darf allerdings nicht soweit gehen, daß daraus Hinweise zu entnehmen sind, durch welche Gegenvorkehrungen polizeiliche Maßnahmen unterlaufen werden können.

**Schleierfahndung**

Die Einführung *einer verdachts- und anlassunabhängigen Kontrolle* war umstritten und wurde im Gesetzgebungsvorhaben kontrovers diskutiert[45]. Die ersten Erfahrungen mit dem neuen Instrument sind nicht sehr

Vorab ist darauf hinzuweisen, daß der Gesetzgeber in § 18 Abs. 7 des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) gerade keine verdachtsunabhängigen, sondern **lageabhängige** Kontrollen geregelt

[44] vgl. Anlagenband „Dokumente zum Datenschutz 2000“, S. 17

[45] vgl. JB 1999, 4.1.2

[46] § 18 Abs. 7 ASOG

beeindruckend. Die Senatsverwaltung für Inneres hält die bisherigen Ergebnisse sogar für ernüchternd. Die Maßnahmen haben bisher in keinem Fall ihrem eigentlichen Zweck - der Bekämpfung der grenzüberschreitenden Kriminalität - gedient. Die bis Redaktionsschluss angeordneten vier Maßnahmen reichen aber noch nicht aus, um ein abschließendes Urteil über die Tauglichkeit des Instruments zu fällen. Feststellen lässt sich bereits jetzt Folgendes:

Das Landeskriminalamt und die Direktionen sind angewiesen, Anträge zur Durchführung einer verdachts- und anlassunabhängigen Kontrolle[46] freitextlich so abzufassen, dass folgende Angaben enthalten sind:

- Erläuterung der Delikte der grenzüberschreitenden Kriminalität,
- Aufführung der Lageerkenntnisse,
- gewünschter Zeitraum für die Kontrollmaßnahme,
- möglichst differenzierte Beschreibung des Bereichs der Kontrollmaßnahmen und
- Darlegung des Umfangs der Maßnahme und der eingebundenen Dienstkräfte.

Die Überprüfung der vorgelegten Unterlagen für die Anordnung einer Schleierfahndung hat ergeben, dass diesen Anforderungen nur in einem Fall fast vollständig Rechnung getragen wurde. Insbesondere sind die Lageerkenntnisse sehr diffus. Das korrespondiert mit den von der Senatsverwaltung für Inneres beschriebenen - statistisch nicht belegbaren - Folgen der Kontrollmaßnahmen, der Stärkung des Sicherheitsgefühls (Kontrollen vermitteln Polizeipräsenz) und der Verunsicherung potenzieller Straftäter (präventive Wirkung durch die Gefahr, kontrolliert zu werden). Hier stellt sich allerdings die Frage, ob die abseits des eigentlichen Zwecks erreichten Erfolge einen so tiefen Eingriff in das informationelle Selbstbestimmungsrecht rechtfertigen.

Die Maßnahmen sind ausnahmslos in vollem Umfang beantragt und angeordnet worden (Anhalten, selektive Überprüfung der Fahrzeugführer und -insassen, selektive Befragung der Fahrzeugführer und -insassen, selektive Überprüfung der mitgeführten Ausweispapiere und selektives Öffnen und die Inaugenscheinnahme mitgeführter Sachen und Behältnisse). Bei den vier angeordneten Maßnahmen sind insgesamt etwa 3.700 Personen und etwa 1.650 Fahrzeuge kontrolliert worden. In erster Linie waren verkehrsrechtliche Verstöße zu ahnden. In 36 Fällen wurden auch Strafanzeigen gefertigt (z. B. Verstoß gegen das Ausländergesetz), die aber in keinem Fall Delikte betrafen, deren Bekämpfung Anlass für die Anordnung der Kontrollen war. Festnahmen gab es nicht.

Abgesehen von den Fällen, in denen strafrechtliche Ermittlungs- oder Ordnungswidrigkeitenverfahren eingeleitet wurden, sind keine personenbezogenen

hat. Der Begriff „Schleierfahndung“ ist in diesem Zusammenhang also zumindest irreführend und sollte deshalb vermieden werden.

Der Senat teilt die Auffassung des Berliner Beauftragten für Datenschutz und Akteneinsicht, daß nachvollziehbar sein muß, aufgrund welcher Erkenntnisse die den Kontrollen zugrundeliegende Lageeinschätzung getroffen wurde. Dafür ist auch Vorsorge getroffen. Anträge an den Polizeipräsidenten oder seinen Vertreter im Amt zur Durchführung von Maßnahmen nach § 18 Abs. 7 ASOG sind freitextlich so abzufassen, dass die folgenden Angaben enthalten sind:

- Die für eine Anordnung als Voraussetzung geforderten Delikte der grenzüberschreitenden Kriminalität sind zu erläutern.
- Die erforderlichen Lageerkenntnisse, aufgrund derer anzunehmen ist, dass Straftaten von erheblicher Bedeutung begangen werden sollen, sind im Antrag aufzuführen.
- Der für die Kontrollmaßnahmen gewünschte Zeitraum ist anzugeben. (Von Einzelterminen sollte Abstand genommen werden, da bei erforderlichen Terminverschiebungen sonst ein neuer Antrag erforderlich würde).
- Der für die Kontrollmaßnahmen vorgesehene Bereich ist möglichst differenziert zu beschreiben.
- Der Umfang der beabsichtigten Maßnahmen und die eingebundenen Kräfte (Dienststellen, nicht Anzahl) sind darzulegen.

Die Senatsverwaltung für Inneres hat die Polizei noch einmal gebeten, diese Vorgaben in jedem Fall zu beachten.

Die Ergebnisse der ersten Maßnahmen waren in der Tat eher ernüchternd. Allerdings gibt die neue Befugnis der Polizei jedenfalls mehr Rechtssicherheit bei der Durchführung von Kontrollen im öffentlichen Verkehrsraum, die vorher nur in eingeschränktem Umfang zur Verkehrsüberwachung durchgeführt werden durften.

Außerdem lassen sich zwei Folgen der Kontrollen nicht durch statistische Angaben belegen:

- Die Stärkung des Sicherheitsgefühls - Die Kontrollen finden in kriminalitätsbelasteten Bereichen statt und vermitteln Polizeipräsenz.
- Die Verunsicherung potentieller Straftäter – Die gesteigerte Gefahr, kontrolliert zu werden, übt für sich genommen schon eine präventive Wirkung aus.

Schließlich ist auch noch zu berücksichtigen, daß mit der neuen Befugnis erst praktische Erfahrungen gesammelt werden müssen. Auf einige wenige Einsätze lassen sich noch keine Aussagen über die Geeignet-

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Daten der kontrollierten Personen gespeichert worden. Die Betroffenen wurden lediglich nach ihren Personalien befragt und gebeten, die Personalpapiere vorzuzeigen. Dabei wurden die Papiere auf Echtheit und Authentizität geprüft. Weiterhin wurden keine Aufzeichnungen darüber geführt, wie oft mitgeführte Sachen in Augenschein genommen wurden. Die Polizei hat aber mitgeteilt, dass bei Kontrollen am Busbahnhof die Gepäckstücke aus den Bussen herausgeholt, in einer Reihe aufgestellt und Rauschgiftspürhunde entlanggeführt wurden. Insoweit wurden die mitgeführten Sachen in Augenschein genommen. In wenigen Fällen, wo die Hunde anschlugen, wurden diese Gepäckstücke genauer kontrolliert. Alle Untersuchungen verliefen negativ.

heit stützen. Kontrollmaßnahmen zur Bekämpfung der Schleusungskriminalität im Dezember 2000 haben immerhin zu zwölf vorläufigen Festnahmen geführt.

**Alle Jahre wieder - das leidige Thema Errichtungsanordnungen**

In den vergangenen Jahren[47] haben wir wiederholt über unsere unzulängliche Beteiligung beim Erlass von Errichtungsanordnungen für neue, beim Bundeskriminalamt betriebene Dateien berichtet. Zunächst wurden wir von der Senatsverwaltung für Inneres überhaupt nicht darüber informiert, dass ein Zustimmungsverfahren[48] für die Einrichtung einer neuen Datei läuft, in die auch die Daten der Landespolizeien eingestellt werden. Wenn wir davon Kenntnis erhalten haben, war das immer von dritter Seite. Dieser unbefriedigende Zustand konnte erst nach längeren Verhandlungen zwischen dem Bundesbeauftragten für den Datenschutz und dem Bundesministerium des Innern (BMI) beseitigt werden. Das BMI hat sich bereit erklärt, zeitgleich mit der Versendung der Errichtungsanordnungen an die Innenverwaltungen der Länder diese auch den Landesbeauftragten für den Datenschutz zur Verfügung zu stellen. Auf diesem Wege erhalten wir seit etwa Mitte 2000 parallel die Entwürfe, denen die Innenverwaltungen der Länder zustimmen sollen.

Die Darstellung des Berliner Beauftragten für Datenschutz und Akteneinsicht hinsichtlich der Übersendung von Errichtungsanordnungen von Dateien in der Vergangenheit ist so nicht zutreffend. Es kann in diesem Zusammenhang auf diverse Schreiben verwiesen werden, in denen er sich für die Übersendung von Errichtungsanordnungen explizit bedankt. Als Beispiele hierfür seien u.a. die Errichtungsanordnungen für die Dateien „Geldwäsche“, „Schleusung/Menschenhandel“ und „ESEK“ genannt. Da aber nunmehr – wie zutreffend dargestellt wird – das Bundesministerium des Innern zeitgleich den Datenschutzbeauftragten der Länder die Errichtungsanordnungen zur Verfügung stellt, dürfte sich dieser Kritikpunkt erledigt haben.

Wir haben allerdings nach wie vor nicht den Eindruck, dass sich die Senatsverwaltung für Inneres ernsthaft mit unseren Stellungnahmen auseinandersetzt und unsere Empfehlungen und Anregungen - anders als in anderen Bundesländern - bei der Entscheidung berücksichtigt. Es wurde vielmehr regelmäßig in einem Satz mitgeteilt, dass der Errichtungsanordnung zugestimmt wurde. Lediglich für unsere Stellungnahme zur Datei „Gewalttäter Sport“ wurde uns gedankt und mitgeteilt, dass die Überlegungen bei einer später in Aussicht genommenen Änderung eingebracht werden können. Das geschah dann in der Form, dass dem BMI unsere Stellungnahme zur Kenntnis gegeben wurde. Zuletzt wurde bei der Datei „FUSION“ der

Auch diese Kritik kann nicht unwidersprochen hingenommen werden, da sie nicht den Tatsachen entspricht.

Beispielhaft verweist die Senatsverwaltung für Inneres unter anderem auf das Zustimmungsverfahren bei der Errichtungsanordnung für die Verbunddatei „FDR“ (Falldatei Rauschgift). Die Fachabteilung der Senatsverwaltung hat sich zeitnah und ausführlich mit den Einwendungen des Berliner Beauftragten für Datenschutz und Akteneinsicht auseinander gesetzt. Dasselbe gilt für die „Geldwäscheverbunddatei“, die Datei „Kinderporno“ (hier hatte die Senatsverwaltung der Datei zwar bereits zugestimmt, konnte die Bedenken aber nicht teilen) und die Datei „ESEK“. In den

[47] JB 1998, 4.1.1, JB 1999, 4.1.2

[48] § 34 Abs. 2 BKAG

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Standpunkt der Polizei erfragt und uns zur Kenntnis gegeben. Wir haben leider weitestgehend einen Dissens feststellen müssen.

meisten Fällen holt die Senatsverwaltung für Inneres zu den vom Berliner Beauftragten für Datenschutz und Akteneinsicht geäußerten Bedenken eine fachliche Stellungnahme der Polizei ein, so wie im Fall der Errichtungsanordnung zu der Datei „FUSION".

Diese Stellungnahme hat die Senatsverwaltung für Inneres an den Berliner Beauftragten für Datenschutz und Akteneinsicht weitergeleitet, jedoch nicht unbesehen, sondern nach deren eingehender Prüfung, die die Senatsverwaltung von den Argumenten der Polizei überzeugte. Soweit die Bedenken hinsichtlich der Errichtungsanordnung zu dieser Datei von Seiten der Senatsverwaltung für Inneres geteilt wurden, wurden sie in das Zustimmungsverfahren eingebracht (hier: Präzisierung der Zweckbestimmung der Datei).

Was das Zustimmungsverfahren bezüglich der Errichtungsanordnung der Datei „Gewalttäter Sport" betrifft, ist festzustellen, dass die Senatsverwaltung für Inneres der Errichtungsanordnung bereits zugestimmt hatte, als der Berliner Beauftragte für Datenschutz und Akteneinsicht hierzu Bedenken mitteilte. Die spätere Änderung der Datei war rein redaktionell, so dass für die Senatsverwaltung kein Anlass bestand, an dieser Stelle des Verfahrens Bedenken zu äußern, nachdem die Senatsverwaltung inhaltlich bereits zugestimmt hatte. Allerdings hat die Senatsverwaltung für Inneres dem Wunsch des Berliner Beauftragten für Datenschutz und Akteneinsicht entsprochen und seine Bedenken durch Übersendung der von ihm gefertigten Stellungnahme an das BMI in das Verfahren eingebracht.

Wir würden es sehr begrüßen, wenn die Senatsverwaltung für Inneres erkennen ließe, dass sie sich mit unseren Stellungnahmen auseinandergesetzt hat und dann, wenn sie unseren Anregungen und Empfehlungen nicht folgen will oder kann, die Gründe dafür erläutert.

Die Senatsverwaltung für Inneres bedauert, dass ein falscher Eindruck von ihrer Kooperationsbereitschaft entstanden ist, und versichert, dass sie an einer guten Zusammenarbeit interessiert ist und weiter bemüht sein wird, das ihrerseits hierzu Erforderliche zu leisten.

**Auftragsdatenverarbeitung durch das Bundeskriminalamt**

Im Rahmen der *Neukonzeption von INPOL-neu* wollen die Polizeien mehrerer Bundesländer ihre Landesdaten dauerhaft beim Bundeskriminalamt im Rahmen der auftragsweisen Datenverarbeitung verarbeiten lassen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder[49] hat in einer Entschließung dagegen erhebliche Einwände erhoben und an die Innenminister/-senatoren appelliert, die Landespolizeien aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Das Bundesministerium des Innern vertritt dagegen die Auffassung, dass eine dauerhafte Auftragsdatenverarbeitung beim BKA

[49] Entschließung zur Auftragsdatenverarbeitung durch das Bundeskriminalamt,

Anlagenband „Dokumente zum Datenschutz 2000", S. 17

mit dem Bundeskriminalamtsgesetz vereinbar ist. Dem hat sich die Innenministerkonferenz angeschlossen[50]. Zumindest die Berliner Polizei hat sich gegen eine Auftragsdatenhaltung beim BKA und für eine eigene Datenhaltung innerhalb Berlins beim Landesbetrieb für Informationstechnik entschieden.

**DNA-Analyse: Statt richterlicher Anordnung fragwürdige Einwilligungen**

Die Datenschutzbeauftragten des Bundes und der Länder halten die Praxis, *DNA-Analysen* systematisch auf der Grundlage von *Einwilligungen* durchzuführen, für eine Umgehung der gesetzlichen Regelungen und damit für unzulässig[51]. Die Datenschutzbeauftragten haben daher gefordert, DNA-Analysen zum Zweck der Identitätsfeststellungen für künftige Strafverfahren nur noch auf der Grundlage von richterlichen Anordnungen durchzuführen.

Die Gerichte in Berlin[52] haben dagegen entschieden, dass bei Vorliegen einer Einwilligung des Betroffenen eine *richterliche Anordnung* der Maßnahmen nicht mehr ergehen könne. Das haben wir zur Kenntnis genommen - auch wenn wir die rechtliche Bewertung nicht teilen können. Umso wichtiger ist es daher, die Betroffenen in jeder Hinsicht entsprechend den datenschutzrechtlichen Vorschriften über die Einwilligung im Hinblick auf den tiefen Eingriff umfassend aufzuklären.

Bei der Einholung der Einwilligung ist auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen (§ 6 Abs. 3 BlnDSG). Die Polizei hat sich einen *Vordruck* geschaffen, ohne die Senatsverwaltung für Justiz oder uns im Vorfeld zu beteiligen. Dieses Formular wird vor dem Hintergrund der Intensität der mit der Folge der Einwilligung verbundenen Grundrechtseingriffe den gesetzlichen Anforderungen ebenso wenig gerecht wie denen an eine informierte Einwilligung. Es wird nicht zwischen den von einer DNA-Analyse betroffenen Gruppen (Beschuldigte, Inhaftierte, ehemalige Inhaftierte, Zeugen bzw. sonstige Dritte) differenziert, die sich erheblich voneinander unterscheiden. So ist beispielsweise die Situation eines Zeugen nicht mit der eines Strafgefangenen, der sich in einem besonderen Gewaltverhältnis befindet, oder mit einem Beschuldigten in einem Ermittlungsverfahren vergleichbar. Die Schaffung *eines*

---

[50] Beschlussniederschrift über die 165. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder am 24. November 2000 in Bonn

[51] vgl. Entschließung zur DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen, Anlagenband „Dokumente zum Datenschutz 1999“, S. 18 f.

[52] vgl. LG Berlin, Beschluss vom 5. November 1999, Az.: 522 Qs 118/99

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Vordruckes für alle Fallgruppen halten wir für nicht sachgerecht.

So wird in den „Hinweisen zu der Einverständniserklärung“ lediglich der Gesetzestext wiedergegeben. Erläuterungen zur besseren Verständlichkeit werden nicht gegeben. Es wird weiterhin nicht darauf hingewiesen, dass die Möglichkeit besteht, nur teilweise - also z. B. in die Entnahme von Körperzellen - einzuwilligen. Auch ein Hinweis auf die Widerrufsmöglichkeit der Einwilligung fehlt. Informationen über die weiteren Rechtsvorschriften zum Zweck der Datenverarbeitung bei dem Bundeskriminalamt sind unvollständig. Ohne Hilfe eines Mitarbeiters der Polizei dürfte der Betroffene nicht in der Lage sein, das Formular auszufüllen.

Die Freie und Hansestadt Hamburg hat in ihren Einwilligungsvordrucken diese Kritikpunkte berücksichtigt. Einvernehmlich mit der Senatsverwaltung für Justiz halten wir diese Vordrucke für eine geeignete Grundlage und haben dem Polizeipräsidenten in Berlin empfohlen, diese - mit erforderlichen berlinspezifischen Ergänzungen - zu übernehmen. Bei einer Beratung im Unterausschuss Datenschutz hat die Justizverwaltung eine Änderung des Vordrucks in diesem Sinne zugesagt.

Es ist darauf hinzuweisen, dass die Senatsverwaltungen für Inneres und Justiz dahingehend übereingekommen sind, dass alle Verfahrensschritte im Rahmen der retrograden Erfassung von DNA-Daten bis zum Vorliegen des DNA-Analyse-Ergebnisses grundsätzlich in den Zuständigkeitsbereich der Staatsanwaltschaft fallen. Die Polizei ist erst für das weitere Verfahren nach Vorliegen der DNA-Profile (z.B. Fragen betreffend die Datenspeicherung) zuständig. Daraus folgt, dass auch die Frage, ob DNA-Analysen auf der Basis von Einwilligungserklärungen durchgeführt werden dürfen und wie die Erklärungsvordrucke ausgestaltet werden müssen, abschließend von den Senatsverwaltungen für Justiz und Inneres geprüft und festgelegt werden müssen.

Die Senatsverwaltung für Inneres hat aber keine Bedenken dagegen, die Formulare entsprechend dem Hamburger Muster zu gestalten. Dies ist dem Berliner Beauftragten für Datenschutz und Akteineinsicht bekannt, er hat Entwürfe hierfür erhalten.

**Im Rotlichtmilieu angetroffen**

*Verzweifelt teilte uns eine polnische Staatsangehörige mit, dass sie im Zusammenhang mit einem Polizeieinsatz in den Räumen ihres Arbeitgebers kontrolliert wurde. In ihrem Pass wurde ein Datumsstempel angebracht. Den Stempelaufdruck ergänzte der Polizeibeamte mit dem handschriftlichen Vermerk „Im Rotlichtmilieu angetroffen“.*

Mit In-Kraft-Treten des Schengener Abkommens sind an den Binnengrenzen der Mitgliedstaaten des Abkommens die Grenzkontrollen weggefallen. Die Stempel und Einträge sollen als Ausgleichsmaßnahme für den Wegfall der Schengen-Binnengrenzkontrollen und die verminderten Außenkontrollen den Behörden die Feststellung ermöglichen, ob ein ausländischer Staatsbürger seine Aufenthaltsfristen einhält. Sie dienen als *Ersatz für einen Einreisevermerk an der Grenze* dazu, anlässlich der Inlandskontrolle einen nach der Einreise liegenden Aufenthaltszeitpunkt zu dokumentieren. Art und Inhalt des Eintrages sollen sich dabei an den Vorgaben des Bundesministeriums des Innern orientieren. Danach ist der Vermerk in Form eines Kontrollstempels, der handschriftlich zu ergänzen ist („angetroffen am ... in ...“, Abkürzung der Dienststelle, Unterschrift), oder in Form eines entsprechenden gänzlich handschriftlichen Kontrolleintrages vorzunehmen.

Die Feststellung der Anwesenheit eines Ausländers an einem bestimmten Ort durch Mitarbeiter des Polizeipräsidenten in Berlin ist als Erhebung (§ 4 Abs. 2

Der dargestellte Sachverhalt, insbesondere die handschriftliche Eintragung in dem Pass „im Rotlichtmilieu angetroffen“, trifft zu. Diese Maßnahme war rechts-

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Nr. 1 BlnDSG), die Anfertigung des Vermerkes im Ausweispapier (Stempel oder Eintrag) als Speicherung (§ 4 Abs. 2 Nr. 2 BlnDSG) von personenbezogenen Daten des Betroffenen anzusehen. Eine Übermittlung dieser Angaben (§ 4 Abs. 2 Nr. 4 BlnDSG) liegt vor, wenn gespeicherte Daten Dritten bekannt gegeben werden. Das ist hier der Fall, da die Petentin regelmäßig zur Identifikation ihr Reisedokument auch anderen Behörden oder nicht-öffentlichen Stellen zur Einsichtnahme auszuhändigen hat (beispielsweise bei Bankgeschäften).

Weil keine Einwilligung vorlag, ist die Datenverarbeitung nur zulässig, wenn eine Rechtsvorschrift dies erlaubt (§ 6 Abs. 1 BlnDSG). Die Bestimmungen des Ausländergesetzes enthalten keine ausreichenden Rechtsgrundlagen, auf die die Maßnahme gestützt werden kann. Bei einem Rückgriff auf die Bestimmungen des Polizeigesetzes (§§ 42 Abs. 1, 44 Abs. 1, 45 Abs. 1 ASOG) wäre in jedem Fall der Erforderlichkeitsgrundsatz zu beachten. Nach den Empfehlungen des Bundesministeriums des Innern dienen diese Vermerke als Hilfsmittel, um die Aufenthaltsdauer von Drittausländern im Bundes- und Schengen-Gebiet zu überprüfen, um ggf. aufenthaltsbeendende Maßnahmen einleiten zu können. Zur Erfüllung dieser Aufgabe ist lediglich ein - der erste - Kontrollvermerk erforderlich. Dieser Kontrollvermerk kann als Ersatz für die nicht erfolgte Grenzkontrolle angesehen werden, in deren Verlauf schon bisher das Einreisedatum im Pass oder Passersatz festgehalten werden konnte. Anlässlich des Antreffens des Ausländers im Inlandsbereich wird nunmehr zwar nicht das Einreisedatum, dafür aber das Datum, zu dem sich der Ausländer spätestens auf deutschem Hoheitsgebiet befunden hat und der als Ausgangspunkt für die Berechnung eines Datums dienen kann, zu dem die Aufenthaltsdauer spätestens abläuft, im Pass oder Passersatz vermerkt. Der Kontrollvermerk im Inland erfüllt damit einen dem Grenzkontrollvermerk vergleichbaren Zweck.

Für den handschriftlichen Vermerk „Im Rotlichtmilieu angetroffen“ hat es sowohl an der Geeignetheit als auch an der Erforderlichkeit und der Angemessenheit gemangelt. Der Zweck, einen Anhaltspunkt für die Berechnung der zulässigen Aufenthaltsdauer zu geben, ist bereits mit dem Stempelaufdruck und dem Datum erfüllt. Nach alledem war der handschriftliche Zusatz neben dem Stempelaufdruck unzulässig. Wir haben das gegenüber der Senatsverwaltung für Inneres beanstandet. Die Polizei hat sich bei der Petentin entschuldigt und sich gegenüber der Außenstelle der Botschaft der Republik Polen bereit erklärt, eventuell anfallende Kosten bei der Neuausstellung eines Reisepasses zu übernehmen.

widrig, soweit sie den handschriftlichen Eintrag betraf, und erfolgte aufgrund einer bedauerlichen Fehlinterpretation der Vorschriftenlage. Danach hätte nur Folgendes vermerkt werden dürfen:

**„Angetroffen am 25. März 2000 in D-Berlin“**,

abgekürzte Dienststellenbezeichnung und Unterschrift des Kontrollbeamten.

Die zuständige Direktion der Polizei hat sich für den Fehler in aller Form bei der Betroffenen schriftlich entschuldigt und den Vorgang im Rahmen der Dienstaufsicht mit den betroffenen Mitarbeitern ausgewertet.

Um einer Wiederholung derartiger Fehler entgegen zu wirken, hat die Polizei unmittelbar nach Bekanntwerden des Vorfalls folgende Maßnahmen eingeleitet:

- Die für Kontrollmaßnahmen eingeteilten Beamten werden eingehend über die ausländerrechtlichen Bestimmungen und Verfahrensweisen informiert. Insbesondere bezüglich der Verwendung von Kontrollstempeln und –einträgen bei Überprüfungen des Personenverkehrs erfolgt eine intensive Belehrung und Beschulung.
- Es werden konzeptionell Kräfte des Arbeitsgebiets Ausländer (AGA) bei geplanten Kontrollmaßnahmen begleitend eingesetzt, da diese fachlich kompetent die durchzuführenden Maßnahmen anleiten bzw. kontrollieren können.

Darüber hinaus wurde die zuständige Dienststelle durch einen Beamten mit AGA-Ausbildung verstärkt.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

**Der fotografierte Jugendliche**

*Ein aufgebrachter Vater beschwerte sich darüber, dass zwei Polizisten in ziviler Kleidung seinen minderjährigen Sohn angehalten, seine Personalpapiere überprüft und anschließend Polaroid-Fotos angefertigt haben, obgleich nichts gegen ihn vorlag.*

Dem lag Folgendes zugrunde: In der näheren Umgebung des Ortes ist es zu Straftaten gekommen, die von oder aus Gruppen Jugendlicher begangen wurden. Die Polizei hatte den Auftrag, durch Ermittlungen im Tatortbereich Tatverdächtige namhaft zu machen, die aufgrund der nach Zeugenvernehmungen erlangten Personenbeschreibungen als Täter in Betracht kommen könnten. Die vorhandene Täterbeschreibung war sehr allgemein gehalten. Mit einem der Geschädigten wurde in Tatortnähe Streife gefahren. Dabei wurde der Sohn des Petenten angetroffen, der nach den Erklärungen des Geschädigten einer der Täter hätte sein können, sicher sei er sich jedoch nicht gewesen. So erklärt sich die Personalienfeststellung. Die angefertigten *Polaroid-Foto*s wurden später anderen Geschädigten und Zeugen vorgelegt, um eine Tatbeteiligung beweisen bzw. die Teilnahme an den angezeigten Straftaten ausschließen zu können. Die Anfertigung der Fotos hielt der Polizeipräsident in Berlin zum Zweck der Durchführung eines Strafverfahrens für erforderlich (§ 81 b 1. Alternative StPO); im Übrigen würden in vergleichbaren Fällen regelmäßig Personenfeststellungen vorgenommen und Polaroid-Fotos angefertigt.

Die Zeugen und andere Geschädigte haben den Sohn des Petenten als Täter ausgeschlossen. Deshalb wurde das Foto in keine Kartei oder Datei eingestellt und ist inzwischen vernichtet worden.

Wir haben den Vorgang beanstandet. Trotz des insoweit bestehenden Beurteilungsspielraumes lassen die Gesamtumstände nicht hinreichend deutlich erkennen, dass hier ein ausreichender *Anfangsverdacht* bestand. Die gesamte Behandlung des Vorganges ließ nicht auf einen Beschuldigten-Status des Sohnes schließen. Die Täterbeschreibungen waren so allgemein gehalten, dass sie auf eine Vielzahl Jugendlicher zutreffen. Die Aussagen zur Tatbeteiligung waren eher vage, so dass lediglich die Nähe des Betroffenen zum Tatortbereich übrig blieb.

Sofern jemand einer Straftat verdächtig ist, können die Beamten des Polizeidienstes die zur Identitätsfeststellung notwendigen Maßnahmen treffen (§ 163 b StPO). Dabei ist der Person auch zu eröffnen, welche Tat ihr zur Last gelegt wird. Dies ist hier ebenso wenig erfolgt wie eine Aufklärung über die Rechte als Beschuldigter. Dass die Polizei ebenfalls von einem fehlenden Anfangsverdacht ausging, zeigt die Tatsache, dass der Sohn zu keinem Zeitpunkt aktenmäßig oder im ISVB als Beschuldigter geführt wurde. Einen Aktenvorgang zur Person des Sohnes gibt es nicht.

Die Darstellung ist grundsätzlich zutreffend. Die Polizei ist in dem konkreten Fall jedoch von einem „Anfangsverdacht“ gegen den betreffenden Jugendlichen ausgegangen, wie sie in einem umfangreichen Schriftverkehr dargelegt hat. Allerdings ergaben Nachprüfungen der Senatsverwaltung für Inneres, dass sie hinsichtlich der Anforderungen an den Anfangsverdacht ihren Beurteilungsspielraum überzogen hat und bereits „irgendeinen Verdacht“ für die getroffenen Maßnahmen für ausreichend hielt, ohne den Betroffenen notwendigerweise als Beschuldigten zu qualifizieren.

Die Senatsverwaltung für Inneres hat daraufhin der Polizei ihre mit der Senatsverwaltung für Justiz abgestimmte Rechtsauffassung mitgeteilt, wonach eine erkennungsdienstliche Maßnahme nach § 81 b 1. Alt. StPO nur dann rechtmäßig vorgenommen werden kann, wenn der Betroffene infolge der Einleitung eines gegen ihn geführten Ermittlungsverfahrens förmlich Beschuldigter ist, oder aber zumindest zureichende tatsächliche Anhaltspunkte den konkreten Verdacht einer Straftat gegen ihn begründen und ein Verfol-

Dem hat sich die Senatsverwaltung für Inneres angeschlossen und die Polizei gebeten, in geeigneter Weise sicherzustellen, dass Lichtbilder auf der Grundlage des § 81 b StPO nur noch dann angefertigt werden, wenn der Betroffene Beschuldigter ist, und ferner Lichtbildaufnahmen nach § 163 b StPO nur zum gesetzlich vorgesehenen Zweck der Identitätsfeststellung anzufertigen.

**Aufbewahrung der Protokolle über Melderegisterabfragen**

*Empört berichtete eine Bürgerin von ihrem Nachbarschaftsstreit. Es ging um den Vorwurf der Erschleichung von Sozialleistungen. Ihr Nachbar, der bei dem Landeskriminalamt tätig ist, habe seine dienstliche Stellung ausgenutzt, um außerhalb seiner dienstlichen Obliegenheiten die Meldeverhältnisse der Betroffenen zu überprüfen. Erst danach habe er sich mit einer anonymen Anzeige an den Polizeipräsidenten in Berlin gewandt und später auch zu erkennen gegeben.*

Die Bürgerin hatte sich erst mehr als ein Jahr nach dem Vorgang an uns gewandt. Eine strafrechtliche Verfolgung schied damit wegen Ablauf der Antragsfrist aus. Eine Auswertung der Protokolldaten für die automatisierten Zugriffe auf das Melderegister ist negativ verlaufen, weil die *Protokolldaten* bereits *gelöscht* waren. Die Sicherheitsbehörden (§ 25 Abs. 4 MeldeG) haben bei Datenübermittlungen aus dem Melderegister den Namen und die Anschrift der Betroffenen unter Hinweis auf den Anlass der Übermittlungen aufzuzeichnen. Diese Aufzeichnungen sind gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Aufzeichnung folgt, zu vernichten. Die erfolgte Verkürzung der Aufbewahrungsfrist auf ein Jahr hat die vom Gesetzgeber vorgesehene Überprüfbarkeit der Zulässigkeit der Datenübermittlungen hier unmöglich gemacht. Der Polizeipräsident in Berlin wird künftig sicherstellen, dass die Protokolldaten erst am Ende des Kalenderjahres, das der Aufzeichnung folgt, gelöscht werden.

**Der abgehörte Anwalt - das Ende einer Fortsetzungsgeschichte**

Wir hatten darüber berichtet, dass die Polizei ohne Kenntnis der Staatsanwaltschaft das Lichtbild eines Strafverteidigers aus dem Personalausweisantrag unzulässigerweise in eine Wahllichtbildvorlage aufgenommen hatte[53]. Den Vorgang hatten wir beanstandet. Die Senatsverwaltung für Inneres fühlte sich wegen der Sachleitungsbefugnis der Staatsanwaltschaft nicht als richtiger Adressat und hat sich inhaltlich nicht geäußert. Erst nach einem klarstellenden Beschluss des Abgeordnetenhauses[54] hat uns die Senatsverwaltung gungswille der ermittelnden Behörde besteht, und um künftige Beachtung gebeten.

[53] JB 1997, 4.1.1

[54] JB 1999, Anlage 2

für Inneres den Sachverhalt bestätigt und sich unserer Bewertung angeschlossen, die bereits zuvor von der Staatsanwaltschaft geteilt wurde.

Sie hat darüber hinaus eingeräumt, dass - unabhängig von der Verfahrensposition des Verteidigers - dessen Lichtbild nicht schon allein aufgrund der Tatsache, dass er in einem ganz anderen Verfahren telefonischen Kontakt mit dem Beschuldigten hatte, in dem Parallelverfahren Zeugen im Rahmen einer Wahllichtbildvorlage als Abbild eines möglichen Tatverdächtigen vorgelegt werden darf. Hierfür findet sich in der Strafprozessordnung nicht die erforderliche Rechtsgrundlage. Die Senatsverwaltungen für Inneres und Justiz sind einvernehmlich der Auffassung, dass die Verwendung von Lichtbildern von Personen, die im konkreten Ermittlungsverfahren unverdächtig sind, rechtswidrig ist. Dem tragen auch die bundeseinheitlichen „Richtlinien für die Führung der Lichtbildvorzeigekartei (LVK)“ Rechnung, auf die die für die Polizeibehörde geltende Geschäftsanweisung über erkennungsdienstliche Maßnahmen ausdrücklich Bezug nimmt. Danach können in die LVK nur Lichtbilder von Personen aufgenommen werden, die verurteilt oder einer rechtswidrigen Tat dringend verdächtigt sind und bei denen nach Beurteilung ihres bisherigen Verhaltens Wiederholungsgefahr besteht. Diese Voraussetzungen lagen hier nicht vor.

Die Senatsverwaltung für Inneres hat den Polizeipräsidenten aufgefordert, künftig die Einhaltung der einschlägigen Vorschriften sicherzustellen.

### 4.2 Ordnungsverwaltung

#### 4.2.1 Meldewesen, Wahlen, Standesämter

**Die „Abschichtungsdebatte“**

Die zähe Debatte um die *Abschichtung der Aufgaben der Meldestellen des Landeseinwohneramtes auf die Bezirksämter* ist nach mehr als zwei Jahren abgeschlossen. Das Abgeordnetenhaus hat den noch einmal marginal überarbeiteten Entwurf als Gesetz beschlossen. Durch die Neuregelung werden den Bezirksämtern vor allem Aufgaben des Melde-, Pass- und Personalausweiswesens zugewiesen. Allerdings bleiben die Zuständigkeiten für die Führung des zentralen Melde-, Pass- und Personalausweisregisters sowie die Durchführung weiterer spezifischer melde-, pass- und ausweisrechtlicher Aufgaben aus gesamtstädtischen Gründen beim Landeseinwohneramt.

Unsere schon früh[55] geäußerte Kritik, dass die Aufspaltung einerseits in die materielle Aufgabenwahrnehmung und andererseits die Registerführung daten-

Die Einbringung des Gesetzentwurfs zur Neuregelung der Zuständigkeiten des Landeseinwohneramtes Berlin geht auf einen Beschluss zurück, den das Abgeordnetenhaus am 28. Mai 1998 aus Anlass der Verabschiedung des Zweiten Verwaltungsreformgesetzes und der damit verbundenen weitreichenden Aufgabenverlagerung aus der Hauptverwaltung in die Bezirke getroffen hat. Mit Blick auf die Meldestellen war der Senat zur Vorlage eines Gesetzentwurfes aufgefordert worden, der einen Übergang aller bisher dezentralen von den Meldestellen wahrgenommenen Aufgaben des Landeseinwohneramtes auf die Bezirke regelt. Beim Landeseinwohneramt sollten nur noch die notwendigen zentralen Aufgaben verbleiben. Gleichzeitig sollte das Landeseinwohneramt als „Kopfstelle“ für die bezirklichen Meldestellen ausgestaltet werden.

[55] JB 1999, 4.2.1

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

schutzrechtlich unzulässig ist, wurde lediglich zur Kenntnis genommen. Auch der Hinweis darauf, dass die bundesrechtlichen Regelungen (Melderechtsrahmengesetz, Passgesetz und Personalausweisausgesetz), die vom Landesgesetzgeber nicht geändert werden können, von dem Grundsatz ausgehen, dass nur die Melde-, Pass- und Ausweisbehörde - denen die jeweiligen materiellen Aufgaben und Befugnisse zugewiesen sind - die hierfür erforderlichen Register führen dürfen, das Bundesrecht also nur jeweils ein Register zulässt und ausweislich der Gesetzesmaterialien eine zusätzliche zentrale Registerführung ausgeschlossen ist, fand keine Beachtung. Das ist insofern bedauerlich, weil das Land Berlin im Zusammenhang mit der Entscheidung des Kammergerichtes[56] zur Rückübertragung der Durchführung der Verkehrsordnungswidrigkeiten zum Polizeipräsidenten in der Vergangenheit seine - auch teuren - Erfahrungen mit Zuständigkeitsregelungen gemacht hat.

Wir sehen nun den technischen und organisatorischen Konzepten zur Umsetzung dieses Gesetzes entgegen.

Mit der Einbringung des Gesetzentwurfes zur Neuregelung der Zuständigkeiten des Landeseinwohneramtes Berlin ist der Senat dem ihm erteilten Auftrag des Abgeordnetenhauses nachgekommen.

Der Berliner Beauftragte für Datenschutz und Akteneinsicht hat während des gesamten Gesetzgebungsverfahrens hinreichend und wiederholt Gelegenheit zur Darlegung seiner vom Senat abweichenden Rechtsauffassung bezüglich der rechtlichen Zulässigkeit der mit dem Gesetzentwurf verbundenen Zuständigkeitsverteilung im Melde-, Pass- und Ausweisbereich zwischen Bezirksämtern und Landeseinwohneramt erhalten. Das Abgeordnetenhaus ist bei der Verabschiedung des Gesetzes den Bedenken des Berliner Beauftragten für Datenschutz und Akteneinsicht nicht gefolgt; der Senat erachtet die damit verbundene Diskussion nunmehr als für beendet. Der Senat ist der Auffassung, dass mit dem Gesetz zur Neuregelung der Zuständigkeiten des Landeseinwohneramtes eine sinnvolle Aufgabenverteilung zwischen Bezirksämtern und Landeseinwohneramt getroffen wurde, die die Integration von Meldestellenaufgaben in die Bürgerämter unter gleichzeitiger Beibehaltung der Zuständigkeiten des Landeseinwohneramtes für die Durchführung notwendiger zentraler Aufgaben ermöglicht.

**Meldegesetz**

Auch in diesem Berichtszeitraum hat die Senatsverwaltung für Inneres entgegen einem Beschluss des Abgeordnetenhauses zum Jahresbericht 1997[57] den immer wieder angekündigten Entwurf zur *Novellierung des Meldegesetzes*[58] nicht vorgelegt. Auch ein weiterer Beschluss des Unterausschusses „Datenschutz“ hat die Senatsverwaltung für Inneres offensichtlich wenig beeindruckt. Inzwischen hat der Deutsche Bundestag zwei Änderungsgesetze zum Melderechtsrahmengesetz verabschiedet. Darüber hinaus wurde schon ein Arbeitsentwurf des Bundesministeriums des Innern eines *Dritten Änderungsgesetzes des Melderechtsrahmengesetzes* auf der Expertenebene beraten. Wir sind sehr gespannt darauf, wann die Änderungsgesetze von 1994 und 2000 in Landesrecht umgesetzt werden. Schon jetzt muss festgestellt werden, dass Berlin im Melderecht bundesweit das Schlusslicht bildet.

Es trifft zu, dass der angekündigte Entwurf zur Novellierung des Berliner Meldegesetzes noch aussteht. Grund hierfür war das sich hinziehende Gesetzgebungsverfahren zur Abschichtung der Meldestellenaufgaben auf die Bezirksämter, das sich nicht zuletzt auch deshalb so schwierig gestaltete, weil der Berliner Beauftragte für Datenschutz und Akteneinsicht dagegen immer wieder rechtliche Einwände vortrug, deren Prüfung zu einer Verzögerung bei der Erarbeitung des Gesetzentwurfes führte. Um ein politisch gewolltes zeitgleiches Inkrafttreten der mit dem Gesetzentwurf verbundenen Zuständigkeitsverlagerungen mit der Bildung der neuen Bezirke nicht zu gefährden, erschien aus Sicht des Senats eine Belastung des Gesetzentwurfes mit einer weitergehenden Novellierung des Landesmelderechtes untunlich zu sein. Es ist jedoch verwaltungsmäßig sichergestellt, dass durch die noch ausstehende Novellierung des Berliner Meldegesetzes in der meldebehördlichen Vollzugspraxis keine melderechtlichen Vollzugsdefizite entstehen.

Wenn gleich die seitens des Senats bereits wiederholt angekündigte und vom Berliner Beauftragten für Da-

---

[56] 2 Ss 292/86-3 Ws (B) 396/86 vom 26. März 1987

[57] Abghs.-Drs. 13/3840, Anlage 2 zum JB 1999

[58] zuletzt JB 1999, 4.2.2

[59] Beschluss vom 26. März 1987, Az.: 2Ss 292/86-3 Ws (B) 396/86

Gegen diesen Ersten Arbeitsentwurf des Bundesministeriums des Innern haben wir erhebliche Bedenken und Einwände gegenüber der Senatsverwaltung für Inneres geäußert. So soll beispielsweise danach durch Landesrecht bestimmt werden können, dass der *elektronische Abruf* eine Form der Melderegisterauskunft an Private darstellt. Dagegen hat sich auch die 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder Sitzung am 12./13. Oktober 2000 gewandt[59]. Das Bundesministerium des Innern will den Arbeitsentwurf vor der Hausabstimmung in wesentlichen Punkten nochmal überarbeiten. Bei Redaktionsschluss war der Entwurf noch nicht in den Deutschen Bundestag eingebracht. Wir erwarten von der Senatsverwaltung für Inneres, dass sie unsere Bedenken in die Länderabstimmung einbringt, und werden im nächsten Jahr über den Fortgang berichten.

**Die Bundestagsabgeordneten und die Meldepflicht**

*Für viel Aufregung sorgte eine „Panorama"-Sendung: Das Fernsehmagazin berichtete darüber, dass sich mehrere Bundestagsabgeordnete nach dem Umzug des Deutschen Bundestages nicht ordnungsgemäß in Berlin angemeldet haben. Die Betroffenen haben sich nicht nur darüber beschwert, dass das Landeseinwohneramt der Redaktion Auskünfte aus dem Melderegister erteilt hat, sondern auch darüber, dass eine Mitarbeiterin aus einer Liste Namen von Abgeordneten verlesen hat, die ihrer Anmeldepflicht offensichtlich nicht nachgekommen sind.*

Im Vorfeld der Sendung hatte die Redaktion einen Antrag auf einfache Melderegisterauskünfte zu 65 Amts- und Mandatsträgern gestellt. Daraufhin wurde ihr zu 29 Personen schriftlich mitgeteilt, dass diese mit den aufgelieferten Informationen im aktuellen Melderegister nicht als „gemeldet" oder „gemeldet gewesen" verzeichnet sind. Die Beschwerdeführer gehörten zu diesem Personenkreis. Zu den übrigen 36 Personen war eine Auskunftssperre gespeichert. Für diesen Personenkreis hat das Landeseinwohneramt die Auskunftserteilung abgelehnt. Auf Wunsch der Redaktion hat der Behördenleiter eine Mitarbeiterin gebeten, für die Aufnahmen zur Verfügung zu stehen, die dann aus der der Redaktion erteilten Melderegisterauskunft zitiert hat.

Die ganze Aufregung hätte vermieden werden können, wenn die Bundestagsabgeordneten ihrer gesetzlichen

tenschutz und Akteneinsicht bereits wiederholt angemahnte Novellierung des Berliner Melderechts auch noch aussteht, so gibt die nunmehr durch die zeitliche Verzögerung eingetretene Situation doch Gelegenheit für eine gründliche und umfassende Überarbeitung des Berliner Meldegesetzes. Mit Blick auf die Einführung der digitalen Signatur im Meldewesen können so voraussichtlich auch bereits die Voraussetzungen für die Nutzung moderner Informations- und Kommunikationstechnologien geschaffen werden.

Der vom Bundesministerium des Innern erarbeitete Entwurf eines Dritten Gesetzes zur Änderung des Melderechtsrahmengesetzes (MRRG) und anderer Gesetze, den der Berliner Beauftragte für Datenschutz und Akteneinsicht in seinem Jahresbericht anspricht, wird von der Bundesregierung voraussichtlich in Kürze in den Deutschen Bundestag eingebracht werden. Die Senatsverwaltung für Inneres hat den vorliegenden Referentenentwurf aus dem Hause des Bundesministeriums des Innern dem Berliner Beauftragten für Datenschutz und Akteneinsicht zur Stellungnahme zugeleitet. Die zu dem Entwurf vorliegenden Stellungnahmen der Datenschutzbeauftragten des Bundes und der Länder werden in den weiteren Meinungsbildungsprozess einfließen.

Meldepflicht nachgekommen wären. Das Meldegesetz schreibt vor, dass derjenige, der eine Wohnung bezieht, sich innerhalb einer Woche bei der Meldebehörde anzumelden hat (§ 12 MeldeG). Im Rahmen einer einfachen Melderegisterauskunft darf die Meldebehörde über einzelne bestimmte Einwohner Auskunft erteilen über

- Familiennamen,
- Vornamen,
- akademische Grade,
- gegenwärtige Anschriften und
- die Tatsache, dass der Einwohner verstorben ist.

Dazu zählt auch die Tatsache, dass eine gesuchte Person nicht im Einzugsgebiet der Meldebehörde gemeldet ist oder war (§ 28 Abs. 1 MeldeG).

Auch wenn die Voraussetzungen für eine einfache Melderegisterauskunft vorliegen, dürfen schutzwürdige Belange durch die Verarbeitung oder sonstige Nutzung personenbezogener Daten nicht beeinträchtigt werden (§ 6 MeldeG). Dies ist dann der Fall, wenn die Verarbeitung oder sonstige Nutzung, gemessen an ihrer Eignung und ihrer Erforderlichkeit zu dem vorgesehen Zweck, den Betroffenen unverhältnismäßig belastet. Somit ist eine Abwägung des Interesses an der Auskunftserteilung und des Betroffenen an der Geheimhaltung seiner Daten vorzunehmen. Diese Prüfung ist auch in den Fällen vorzunehmen, in denen keine Auskunftssperre besteht oder die Betroffenen keine Wohnung angemeldet haben.

Das Landeseinwohneramt ist zu dem Ergebnis gekommen, dass das Interesse der Betroffenen an der Geheimhaltung das Interesse an der Auskunft an die Redaktion nicht überwiegt. Zwar besteht die Möglichkeit, dass das Bekanntwerden der Adresse eines Politikers diesen Gefährdungen aussetzt, insbesondere wenn er in exponierter Stellung tätig ist; dem kann nach der Anmeldung durch die Melderegistersperre jedoch entgegengewirkt werden, die zwar nicht pauschal für alle Abgeordneten eingerichtet werden kann, wir aber davon ausgehen, dass die Meldebehörde Einzelanträgen stattgeben wird.

Sofern keine Wohnung gemeldet ist, scheidet logischerweise eine Gefährdung aufgrund der Negativ-Auskunft aus. Stattdessen kann allerdings der Verdacht einer Ordnungswidrigkeit (Unterlassen der Anmeldung) oder gar einer Straftat (Hinterziehung der Zweitwohnungssteuer) entstehen. Dem Interesse der Betroffenen, dass aus diesem Grund die Auskunft unterbleibt, steht das Interesse der Auskunftsuchenden gegenüber. Im vorliegenden Fall ist zu berücksichtigen, dass Behörden gegenüber der Presse erhöhte Auskunftspflichten haben, damit diese ihren Aufgaben im demokratischen Willensbildungsprozess nachgehen kann. Ob und in welchem Umfang Politiker den

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

rechtlichen Verpflichtungen nachgehen, die alle Bürger haben, gehört sicherlich zu den Fragestellungen, die in diesem Rahmen relevant sind. Vor diesem Hintergrund ist nicht zu beanstanden, dass die fraglichen Melderegisterauskünfte an die Redaktion erteilt wurden.

Problematischer erscheint, dass eine Mitarbeiterin des Landeseinwohneramtes einen Teil der Namen vor der Kamera vorgelesen hat. Auf diese Weise haben alle Zuschauer der Sendung gleichsam eine Melderegisterauskunft erhalten, ohne diese im einzelnen beantragt zu haben. Zudem entstand der Eindruck, dass es zulässig sei, dass das Landeseinwohneramt in einer Fernsehsendung personenbezogene Daten offenbaren darf. Allerdings hätten aufgrund der zulässigen Auskunft die Namen von der Redaktion selbst z. B. durch das Vorzeigen des Auskunftsschreibens des Landeseinwohneramtes offenbart werden dürfen. Das hätte datenschutzrechtlich nicht überprüft werden können, weil das Bundesdatenschutzgesetz die materiellen Bestimmungen für die journalistische Arbeit ausschließt (§ 41 BDSG). Im Ergebnis war damit auch hinsichtlich der Fernsehsendung selbst eine Beanstandung nicht angezeigt. Die Beantwortung von Fragen der Presse, insbesondere vor Fernsehkameras, hat sich - nicht zuletzt aufgrund unserer Empfehlungen - künftig die Behördenleitung vorbehalten.

**Was bei der Bearbeitung eines Personalausweisantrages alles passieren kann**

*Verwundert legte uns eine Bürgerin die Aufforderung des Landeseinwohneramtes vor, sie möge sich innerhalb einer festgelegten Frist ihren Personalausweis abholen. Da sie keinen Ausweis beantragt hatte, war sie gespannt, was man ihr bei ihrem Besuch in der Meldestelle zeigen wird. Das war dann ein neuer Personalausweis mit ihren personenbezogenen Daten, aber dem Bild und der Unterschrift einer anderen Person.*

Wir haben festgestellt, dass eine andere Person mit einem ähnlichen Namen, gleichem Geburtstag und annähernd gleichem Geburtsjahr einen Personalausweis beantragt hat. Dabei unterliefen der Mitarbeiterin der Meldestelle bei dem Aufruf des Datensatzes des Personalausweisregisters zwei Eingabefehler, die zur Ausgabe des Datensatzes der Bürgerin, die sich bei uns beschwert hat, führten. Dieser Fehler wurde von der Mitarbeiterin nicht bemerkt. Der Ausdruck des Ausweisantrages erfolgte daher ebenfalls mit ihren Personalien. Gleichfalls erfolgten die automatische Vergabe der Seriennummer und der Aufbau einer entsprechenden Ausweisgruppe in ihrem Datensatz.

Auch bei der weiteren Bearbeitung (Vorlage des Antrages zur Unterschrift, Einkleben des Lichtbildes) wurde der Fehler von der Mitarbeiterin nicht bemerkt. Dies war dem Landeseinwohneramt Berlin schon deshalb unverständlich und nur mit einer sehr wenig

Es handelt sich bei dem dargestellten Sachverhalt um einen abgeschlossenen Einzelfall, bei dem durch die Mitarbeiterin einer Meldestelle bedauerlicherweise eine fehlerhafte Bearbeitung eines Personalausweisantrages erfolgte. Der Berliner Beauftragte für Datenschutz und Akteneinsicht hat zutreffend darauf hingewiesen, dass die fehlerhaft im Ausweisregister gespeicherten Daten gelöscht und der fehlerhafte Ausweis vernichtet wurde. Die Mitarbeiterinnen und Mitarbeiter der Meldestellen wurden in diesem Zusammenhang auch erneut auf äußerste Sorgfalt bei der Bearbeitung personenbezogener Daten aufmerksam gemacht.

sorgfältigen Arbeitsweise zu erklären, weil die Mitarbeiterinnen und Mitarbeiter selbstverständlich gehalten sind, sich von der Richtigkeit der ausgedruckten Einträge zu überzeugen und außerdem die Antragsteller anzuhalten, sich den Antrag vor Unterschrift auch auf die Richtigkeit der Angaben zur Person hin anzusehen. Zudem hätten allein die Unterschiede im Familiennamen - zumindest aber die unterschiedlichen Vornamen - bei auch nur oberflächlicher Betrachtung des fertigen Antrages auffallen müssen. Das war nicht der Fall. Auch die Antragstellerin bemerkte bei der Unterschrift nicht, dass der Antrag mit fremden Personalien ausgefertigt war. Bei der weiteren Prüfung des Antrages zur Weiterleitung an die Bundesdruckerei und bei der Prüfung des gelieferten Ausweises konnte dieser Fehler nicht mehr festgestellt werden, weil weder die richtige Antragstellerin noch die Beschwerdeführerin anwesend waren.

Erst aufgrund der Eingabe und unserer Nachforschungen wurden die Zusammenhänge klar. Die zur Beschwerdeführerin fehlerhaft im Ausweisregister gespeicherten Daten wurden gelöscht; der fehlerhafte Ausweis wurde vernichtet.

**Privatadresse von Wahlbewerbern**

*Wegen unliebsamer Äußerungen wurde ein Mitglied des Abgeordnetenhauses an einem Sonntagnachmittag, vor dem Privathaus, von einer Gruppe Politclowns heimgesucht, die u. a. die Hauswand mit Parolen besprühten. Auch hier tauchte das Problem auf, dass die Privatanschrift offenbart wurde.*

Die melderechtliche *Auskunftssperre* (§ 28 Abs. 5 MeldeG), wonach jede Melderegisterauskunft an Private unzulässig ist, wenn der Betroffene der Meldebehörde Tatsachen glaubhaft gemacht hat, die die Annahme rechtfertigen, dass hieraus ihm oder einer anderen Person eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen kann, hat bei Abgeordneten keine Wirkung. Der Landeswahlleiter hat die zugelassenen *Wahlvorschläge* (§ 40 LWahlO) und die gewählten und nachrückenden Bewerberinnen und Bewerber (§ 74 LWahlO) nicht nur mit erlerntem und ausgeübtem Beruf, sondern auch mit der Anschrift im Amtsblatt zu veröffentlichen. Hinzu kommt, dass der Kulturbuchverlag die Amtsblätter von Berlin in das Internet eingestellt hat. Damit ist auch auf diesem Weg die Privatanschrift dieses Personenkreises allgemein zugänglich.

Diese Veröffentlichungspflicht ist im Hinblick auf die Transparenz der Wahl und der Kandidaten ohne Zweifel sinnvoll; dabei ist aber offen, wie weit die Pflicht zur Offenbarung personenbezogener Daten für die Wahlvorschläge und Bewerberinnen und Bewerber gehen muss. Die Pflicht zur Veröffentlichung personenbezogener Daten findet nämlich dort ihre Grenzen, wo schutzwürdige Belange beeinträchtigt werden

können. Die Grenzen sehen wir bei der Veröffentlichung der Privatanschrift überschritten. Durch die Bekanntgabe der vollständigen Wohnanschrift wird weder die Wahl noch der Kandidat transparenter.

Unsere Anregung, noch vor den nächsten Wahlen zum Abgeordnetenhaus und zu den Bezirksverordnetenversammlungen die Landeswahlordnung zu ändern und die Veröffentlichungspflicht zu reduzieren, will die Senatsverwaltung für Inneres nicht umsetzen. Personen, die sich für ein Mandat bewerben oder bereits Mandatsträger sind, wollen Interessen der Wahlberechtigten in den Vertretungskörperschaften öffentlichkeitswirksam wahrnehmen. Sie müssen nach Auffassung der Senatsverwaltung für Inneres daher grundsätzlich persönlich erreichbar sein. Hierauf habe die Wahlbevölkerung ein Anrecht. Dieser Grundsatz der Öffentlichkeit des Wahlvorbereitungs- und Parlamentsgeschehens ist nach Auffassung der Senatsverwaltung für Inneres ein unverzichtbares verfassungsrechtliches Gut. Im Übrigen trage der Landeswahlleiter stets dafür Sorge, dass die Betroffenen vor der Veröffentlichung gefragt werden, ob anstelle ihrer melderechtlich gesperrten Wohnanschrift eine andere, für die Bevölkerung zugängliche Adresse (Partei oder Arbeitsstätte) im Amtsblatt veröffentlicht werden soll. Dem können wir uns nicht verschließen. Dessen ungeachtet ist der Landeswahlleiter aufgefordert, das Verwaltungshandeln in geeigneter Weise bekannt zu geben.

Der Senat bekräftigt, dass die Regelung der Landeswahlordnung, neben Namen, Geburtsjahr und -ort sowie Beruf auch die Anschrift von Wahlbewerbern, Gewählten und Nachrückern im Amtsblatt für Berlin zu veröffentlichen, vom wahlrechtlichen und wahlpolitischen Ansatz her richtig und sinnvoll ist. Personen, die sich zur Mandatsträgerschaft bewerben oder Mandatsträger sind, wollen Interessen der Wahlberechtigten öffentlichkeitswirksam wahrnehmen. Sie müssen daher wegen des unverzichtbaren verfassungsrechtlichen Guts der Öffentlichkeit des Wahlvorbereitungs- und Parlamentsgeschehens grundsätzlich persönlich erreichbar sein.

In den Fällen der im Melderegister aus Gefährdungsgründen eingetragenen Auskunftssperren wird die Veröffentlichungspflicht der Anschrift durch ein individuell abgestimmtes Verwaltungshandeln begleitet. Der Landeswahlleiter trägt in jedem dieser Einzelfälle stets dafür Sorge, dass die Betroffenen vor der Veröffentlichung gefragt werden, ob anstelle ihrer melderechtlich gesperrten Wohnanschrift eine andere für die Bevölkerung zugängliche Anschrift im Amtsblatt veröffentlicht werden soll. Der Senat wird darüber hinaus in diesen Fällen beim Landeswahlleiter anregen, in den schriftlichen Informationen an die Wahlbewerber einen Hinweis aufzunehmen, dass die Betroffenen von sich aus die Veröffentlichung einer solchen geeigneten Ersatzanschrift im Amtsblatt beantragen können.

**Personenstandsgesetz**

Im vergangenen Jahr[60] haben wir über die Anfragen von Familienforschern berichtet, die wenig Verständnis dafür aufbringen, dass ihnen der Zugang zu den *Personenstandsbüchern* verwehrt ist und sie somit bei den Bemühungen, die Ahnengalerien gerade auch hinsichtlich längst - z. T. mehr als 100 Jahre - verstorbener Angehöriger zu vervollständigen, nicht vorankommen. Der Senat hat in seiner Stellungnahme[61] zugesagt, unsere Anregungen aufzunehmen und zu unterstützen. Im Berichtszeitraum hat das Bundesministerium des Innern bisher noch keinen neuen Entwurf vorgelegt. Das soll im kommenden Jahr geschehen.

**Versteckte Kamera im Standesamt**

*Ein Paar, das im Schöneberger Standesamt sein Aufgebot bestellen wollte, wurde in den Amtsstuben Opfer einer Fernsehproduktion mit versteckter Kamera. Ein vermeintlicher Standesbeamter hat den Verlobten allein in das Zimmer gebeten und dann nicht nur ge-*

[60] JB 1999, 4.2.2

[61] BT-Drs. 14/423

*fragt, wie er seine Zukünftige kennengelernt hat, sondern darüber hinaus auch, wie er es mit der Treue halte. Schließlich hat sich eine dem Verlobten völlig unbekannte Frau neben ihn gesetzt. Nachdem nun der vermeintliche Standesbeamte eine Trauungszeremonie eingeleitet hatte, verließ der Verlobte empört den Raum.*

Die Produktionsfirma hatte sich zunächst bei dem Standesamt nach der Möglichkeit erkundigt, das Trauzimmer für einen *Dreh mit versteckter Kamera* anzumieten, um Paare „anlässlich einer gespielten Anmeldung zur Eheschließung zu befragen“, und wurde von dort an die für Raumvermietungen zuständige Stelle im Bezirk verwiesen. Dort hatte man sich zwar über die Rahmenbedingungen und Inhalte der Sendung informieren lassen, ist aber bei Abschluss des Mietvertrages davon ausgegangen, dass die Entscheidung, ob eine Drehgenehmigung erteilt wird, von dem Standesamt getroffen wird. Das Standesamt hingegen hat angenommen, dass diese Entscheidung von der für Raumvermietungen zuständigen Stelle als Vertragspartner der Produktionsfirma getroffen wird. Die Verwaltung hat es versäumt, Vorgesetzte oder Dezernenten zu informieren und die Drehabsicht bekannt zu geben. Das Bezirksamt selbst hat erst nach Abschluss der Dreharbeiten Kenntnis von den Vorgängen erhalten.

Das Standesamt hat allerdings versichert, dass keine personenbezogenen Daten an die Produktionsfirma weitergegeben wurden. Auf die Intervention der Betroffenen unterblieb die geplante Sendung. Die Bezirksbürgermeisterin hat sich von dem Fernsehsender bestätigen lassen, dass die Aufnahmen auch nicht anderweitig verwertet werden, und sich bei dem Brautpaar entschuldigt. Als Konsequenz wird das Bezirksamt schriftlich festlegen, wer künftig die Entscheidungen über *Drehgenehmigungen* trifft.

### 4.2.2 Ausländische Bürger und Gäste

**Ehefähigkeitszeugnis**

*In mehreren Eingaben wurden wir gefragt, ob die Präsidentin des Kammergerichts Berlin im Verfahren zur Befreiung von der Beibringung eines Ehefähigkeitszeugnisses nach § 1309 Abs. 2 Bürgerliches Gesetzbuch (BGB) berechtigt ist, die gesamte Ausländer- oder Asylakte zur Einsichtnahme bei der Ausländerbehörde bzw. dem Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) anzufordern.*

Im Verfahren zur Befreiung von der Beibringung des Ehefähigkeitszeugnisses nach § 1309 Abs. 2 BGB hat die Präsidentin des Kammergerichts zu prüfen, ob nach dem Heimatrecht des ausländischen Verlobten der beabsichtigten Eheschließung ein Ehehindernis

Es ist eine Frage des Einzelfalles, welches Gewicht Verdachtsmomenten in Bezug auf eine Scheinehe zukommt. Deshalb ist die Aussage unzutreffend, es müssten stets mehrere Anhaltspunkte vorliegen, um Ermittlungen zu rechtfertigen. Ebensowenig ist die

[62] BGBl. I S. 833

entgegensteht. Eine solche Prüfung setzt die sichere Feststellung der Identität, der Staatsangehörigkeit und des Familienstandes voraus. Da die beantragte Bescheinigung dann nicht ausgestellt werden kann, wenn ein Rechtsschutzbedürfnis fehlt, ist auch dieser Umstand zu prüfen.

Rechtsgrundlage für die Datenerhebung des Kammergerichts Berlin in diesem Verfahren ist § 13 Bundesdatenschutzgesetz (BDSG), der auch für die Berliner Verwaltung Anwendung findet, wenn aufgrund einer Rechtsvorschrift des Bundes personenbezogene Daten verarbeitet werden, ohne dass die Verarbeitung im Einzelnen geregelt ist (§ 6 Abs. 2 BlnDSG). Nach § 13 Abs. 2 Satz 1 BDSG sind die für das Verfahren erforderlichen Daten grundsätzlich bei dem Betroffenen zu erheben. Bei Dritten (hier: die Ausländerbehörde bzw. das BAFl) ist eine Erhebung von personenbezogenen Daten nur unter den restriktiven Voraussetzungen des § 13 Abs. 2 Satz 2 BDSG zulässig, der die überwiegenden schutzwürdigen Interessen der Betroffenen in den Vordergrund stellt. Dabei ist in jedem Fall der Erforderlichkeitsgrundsatz (vgl. § 9 Abs. 1 BlnDSG) zu berücksichtigen.

Zweifel in Bezug auf das Rechtsschutzbedürfnis der Betroffenen können sich u. a. daraus ergeben, dass der Verdacht besteht, der Antragsteller beabsichtige, eine *Scheinehe* zu schließen.

Dies entspricht auch den Vorgaben des am 1. Juli 1998 in Kraft getretenen *Gesetzes zur Neuordnung des Eheschließungsrechtes*[62]. Nach dem neugefassten § 1314 BGB kann eine Ehe aufgehoben werden, wenn beide Ehegatten sich bei der Eheschließung darüber einig waren, dass sie keine eheliche Lebensgemeinschaft begründen wollen. Wenn konkrete Anhaltspunkte für das Eingehen einer derartigen Scheinehe bestehen, hat der Standesbeamte das Recht, die Verlobten zu befragen (§ 5 Abs. 4 Personenstandsgesetz (PStG)). Er kann die Beibringung geeigneter Nachweise und notfalls eine eidesstattliche Versicherung über Tatsachen verlangen, die für die Feststellung, ob eine „Scheinehe“ vorliegt, von Bedeutung sind. Diese Neuregelungen zielen u. a. darauf ab, Scheinehen von ausländischen Staatsangehörigen zu verhindern, die zum Erwerb eines Aufenthaltsrechtes geschlossen werden sollen.

Die Befragungen des Standesbeamten bzw. die Ermittlungen der Präsidentin des Kammergerichts sind jedoch nur zulässig, wenn Tatsachen vorliegen, die konkret den Verdacht einer Scheinehe begründen. Dabei sind unterschiedliche Lebensformen zu berücksichtigen. Die Erkenntnis, dass bei Ausländern aus bestimmten Herkunftsländern gehäuft die Absicht besteht, eine Scheinehe einzugehen, um ein Bleiberecht

Ansicht zu teilen, eine Beiziehung der Ausländerakten sei nicht erforderlich und damit unzulässig. Bei der Fülle der für jeden Einzelfall in unterschiedlicher Weise zu erhebenden Daten läßt sich die Einsichtnahme in die Ausländerakte nicht durch eine gezielte Anfrage bei der Ausländerbehörde ersetzen. Von Amts wegen zu überprüfen sind die dort angegebenen Daten hinsichtlich Familiennamen, Vornamen, Geburtsdatum, Geburtsort, Familienstand und Staatsangehörigkeit. Die Einsichtnahme dient auch der Feststellung, mit welchen Unterlagen, Personenstandsurkunden, Personalausweisen etc. sich der Antragsteller gegenüber der Ausländerbehörde zur Person und Staatsangehörigkeit ausgewiesen hat. Ferner dient sie der Ermittlung von Kriterien, die darauf hindeuten, dass es sich bei der beabsichtigten Eheschließung um die Eingehung einer Scheinehe handelt, insbesondere weil der Antragsteller gemäß Feststellung der Ausländerbehörde bereits früher Scheinehen eingegangen ist oder sich unbefugt in der Bundesrepublik Deutschland aufhält, weil er Eheschließungsabsichten mehrmals zeitgleich mit Ausreiseaufforderungen der Ausländerbehörde geäußert hat bzw. weil der angegebene Zeitpunkt der erstmaligen persönlichen Begegnung der Verlobten nach dem aus der Ausländerakte ersichtlichen Einreisedatum nicht möglich ist oder weil bereits Urkunden für eine beabsichtigte Eheschließung zu einem Zeitpunkt beschafft wurden, zu dem die Verlobten sich nachweislich noch nicht kennen konnten.

Die Präsidentin des Kammergerichts ist zur Einsichtnahme in die Ausländerakte gemäß 6 Abs. 1 Satz 1 Nr. 3 BlnDSG ferner schon dann berechtigt, wenn der ausländische Antragsteller in die Einsichtnahme in die Ausländerakte eingewilligt hat. In diesem Zusammenhang ist darauf hin zu weisen, dass die Standesbeamten gehalten sind, die Einwilligung bereits in der Niederschrift über die Anmeldung zur Eheschließung schriftlich einzuholen und ein Merkblatt aushändigen, in dem angeführt wird, dass sich die Dauer des Verfahrens im Einzelfall durch die Beiziehung von Ausländerakten, auch der Ausländerakten in anderen Bundesländern, verzögern kann.

Im Übrigen ist fest zu stellen, dass die Beiziehung der Ausländerakten gemäß der Auswertung der veröffentlichten Entscheidungen weder von den Zivilsenaten des Kammergerichts noch von den übrigen Oberlandesgerichten beanstandet worden ist.

---

[63] JB 1998, 4.2.2

zu sichern, begründet für sich allein nicht einen derartigen Verdacht. Auch das Fehlen einer häuslichen Gemeinschaft oder einer Aufenthaltsgenehmigung für sich allein begründet keine Ermittlungsbefugnisse[63]. Es müssen weitere Umstände - z. B. Unstimmigkeiten in den von den Verlobten vorgelegten Unterlagen - hinzukommen.

Auch wenn der konkrete Verdacht besteht, dass eine Scheinehe eingegangen werden soll, ist es jedoch nicht erforderlich, die gesamte Ausländer- bzw. Asylakte anzufordern und einzusehen. Diese Unterlagen enthalten eine Vielzahl von zum Teil sehr sensiblen personenbezogenen Daten der Antragsteller, die für die Aufgabenerfüllung des Kammergerichts nicht erforderlich sind. Im Zusammenhang mit den vom Kammergericht zu führenden Ermittlungen sind daher nur konkrete Fragenstellungen zulässig, die an die Ausländerbehörde zur Klärung des Sachverhaltes zu stellen sind.

**Ausschreibung im Schengener Informationssystem**

*Als Ersatz für die abgeschafften Binnengrenzkontrollen zwischen den Ländern haben die Schengen-Staaten auf der Grundlage des Schengener Durchführungsübereinkommens (SDÜ) Maßnahmen zur Sicherung bei Einreisen über die Außengrenzen getroffen. Beantragt ein Ausländer, der nicht Staatsangehöriger eines Schengen-Staates ist (Drittausländer), bei der zuständigen Ausländerbehörde ein Aufenthaltsrecht, hat diese zu prüfen, ob in einem der Mitgliedstaaten ein Einreisehindernis besteht. Ausländer, bei denen ein Einreisehindernis gegeben ist, werden zu diesem Zweck im Schengener Informationssystem (SIS) ausgeschrieben.*

Die Voraussetzungen, unter denen eine Auschreibung im SIS zulässig ist, scheinen vielen Ausländerbehörden nicht bekannt zu sein. Jedenfalls hat das Bundesministerium des Innern die Innenministerien der Länder - angesichts der festgestellten hohen Zahl unzulässiger Ausschreibungen - gebeten, eine *SDÜ-konforme Ausschreibungspraxis* sicherzustellen und dabei auch auf denkbare Schadensersatz- und Regressansprüche im Zusammenhang mit der Ablehnung bzw. verzögerten Erteilung von Visa nach einer unzulässigen schengenweiten Ausschreibung hingewiesen.

Eine Ausschreibung im SIS zur Einreiseverweigerung ist nur bei der Ausweisung, Zurückweisung oder Abschiebung zulässig (Art. 96 Abs. 3 SDÜ). Daraus ergibt sich, dass eine Ausschreibung von anderen vollziehbar ausreisepflichtigen Ausländern, bei denen die Voraussetzungen für eine Abschiebung vorliegen, deren Aufenthalt jedoch unbekannt ist, zum Zweck der Aufenthaltsermittlung und Festnahme nicht im SIS erfolgen darf. Aus Art. 112 SDÜ ergibt sich eine regelmäßige Löschungsfrist von drei Jahren für die Ausschreibung nach Art. 96 SDÜ. Erhält die Ausländerbehörde die Mitteilung über den Fristablauf, hat sie

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

im Einzelfall die Erforderlichkeit einer Verlängerung der Ausschreibung zu prüfen und gegebenenfalls die Gründe für eine Verlängerung der Ausschreibung in der Ausländerakte des Betroffenen zu vermerken.

Die Senatsverwaltung für Inneres teilt unsere Auffassung zu den Voraussetzungen für die Ausschreibung nach Art. 96 SDÜ. Unserer Empfehlung, die Ausschreibungsvoraussetzungen und -praxis, der Bitte des BMI und dem Beispiel anderer Länder (z. B. Nordrhein-Westfalen, Hessen) folgend, in einer verbindlichen Arbeitsanweisung gegenüber der Ausländerbehörde zu regeln, ist die Senatsverwaltung jedoch nicht gefolgt.

Wie in dem Bericht zutreffend ausgeführt wird, teilt der Senat die Auffassung des BlnBDA, dass eine Ausschreibung im SIS zur Einreiseverweigerung gemäß Art. 96 Abs. 3 SDÜ nur bei Ausweisung, Abschiebung oder Zurückschiebung zulässig ist. Die Ausländerbehörde verfährt seit Aufnahme des Wirkbetriebes des SIS im Frühjahr 1995 auf der Grundlage von Arbeitsanweisungen der Senatsverwaltung für Inneres dementsprechend.

**Dokumentation von Ausschreibungen**

*Im vergangenen Jahr[64] haben wir über einen Einzelfall berichtet, in dem wir eine Speicherung zur Einreiseverweigerung im SIS überprüft haben. In der Ausländerakte des Betroffenen befand sich lediglich ein Hinweis auf eine INPOL-, nicht jedoch auf eine SIS-Ausschreibung. Die Ausländerbehörde teilte dazu mit, dass mit Aufnahme des Wirkbetriebes des SIS eine Vielzahl von Ausschreibungsvorgängen, die bis dahin im INPOL-Verfahren erfassten waren, retrograd in den Datenbestand des SIS übernommen wurden, ohne dass im Einzelfall die Ausschreibungsvoraussetzungen überprüft wurden. Wir hatten empfohlen, diese Fälle - angesichts der Vielzahl - „anlassbezogen" (z. B. bei einem Antrag auf Auskunft bzw. Löschung) einer Einzelfallprüfung hinsichtlich der Ausschreibungsvoraussetzungen und -fristen zu unterziehen und das Ergebnis nachvollziehbar in der Akte zu dokumentieren.*

Die Senatsverwaltung für Inneres sah keine rechtliche Verpflichtung zu dieser Vorgehensweise und bat, die Empfehlung näher zu begründen.

„Der Sinn der Aktenaufbewahrung ist, dass man Verwaltungsvorgänge und Regierungsentscheidungen nachvollziehen kann - und zwar nicht nur das Ergebnis der Entscheidungen, sondern auch den Entscheidungsprozess. Man muss alle Elemente verifizieren können, die dazu beigetragen haben, eine solche Entscheidung zu Stande zu bringen."[65]. Diese Aussage des Präsidenten des Bundesarchivs gilt in besonderem Maße bei Entscheidungen, die den betroffenen Bürger belasten. Die Ausschreibung zur Einreiseverweigerung nach Art. 96 SDÜ bedeutet für den Betroffenen einen erheblichen Eingriff, der nicht nur sein informationelles Selbstbestimmungsrecht berührt.

Hinsichtlich Neuausschreibungen ergibt sich das von der Ausländerbehörde einzuhaltende Verfahren aus den Ziffern 45.0.10.1.1 und 49.3.1.1 der bundeseinheitlichen Verwaltungsvorschriften zum Ausländergesetz (VwV AuslG). Hiernach hat die Ausländerbehörde im Falle von Ausweisung oder Abschiebung die „für die Dateneingabe zuständige Polizeidienststelle zum Zweck der Ausschreibung in INPOL und im SIS (Einreiseverweigerung nach Artikel 96 Abs. 3 SDÜ)" zu unterrichten. Eine darüber hinausgehende Dokumentationspflicht sehen die Verwaltungsvorschriften nicht vor. Diese Regelung ist nicht zu beanstanden, gehen doch die Voraussetzungen für Ausweisung und

[64] JB 1999, 4.2.3

[65] Hartmut Weber, Präsident des Bundesarchivs, „Die Welt" vom 29. Juni 2000, S. 2

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Eingriffe in das informationelle Selbstbestimmungsrecht sind nur zulässig, wenn sie auf eine normenklare Regelung gestützt werden können. Artikel 96 SDÜ lässt die Speicherung von Einreiseverweigerungen im SIS zu. Daran anknüpfende Individualrechte (z. B. Auskunfts-, Löschungsansprüche) kann der Betroffene jedoch nur dann geltend machen bzw. durchsetzen, wenn die entscheidungserheblichen Umstände ausreichend dokumentiert sind. Nur so ist nachvollziehbar, dass und auf welcher Rechtsgrundlage die Entscheidung für eine Weiterspeicherung getroffen wurde, welchen Inhalt sie hat und in welchem Ausmaß und für welchen Zeitraum sie Wirkung entfaltet.

Die *Aktenführung und -verwaltung öffentlicher Stellen* und Behörden hat sich an den Prinzipien der Klarheit und Wahrheit zu orientieren. Dies ergibt sich aus dem Gebot der Transparenz von Verwaltung in einem demokratischen Rechtsstaat. Nur so ist das Handeln der Verwaltung durch parlamentarische und andere Kontrollen, z. B. im Rahmen der Dienst-, Fachaufsicht, durch den Rechnungshof, den behördlichen Datenschutzbeauftragten oder durch den Beauftragten für Datenschutz und Akteneinsicht, überprüfbar.

Durch die umfassende Dokumentation von Verwaltungsvorgängen und -entscheidungen werden auch Zwecke des Mitarbeiterschutzes erfüllt. Eine interne Rechenschaftslegung hat den Effekt der Selbstkontrolle. Sie nötigt dem handelnden Verwaltungsmitarbeiter eine Reflektion über die Gründe und das Ausmaß seiner Entscheidung ab. Des Weiteren schützen Transparenz und Nachprüfbarkeit seines Vorgehens den Mitarbeiter vor unberechtigten disziplinar-, schadensersatz- oder strafrechtlichen Konsequenzen.

Unabhängig davon ist eine Aktenführung, in der die Entscheidungsprozesse ausreichend belegt sind, zur Fehlerkorrektur notwendig. So kann es bei der Führung von umfangreichen Personendateien wie INPOL und SIS zu Personenverwechslungen kommen. Derartige Fehler lassen sich nur korrigieren, wenn nachprüfbar ist, wessen Daten zu welchem Zweck aus welchen Gründen und für welchen Zeitraum in die Datei eingespeichert wurden.

Die Senatsverwaltung für Inneres sieht die Ausländerbehörde im Fall von Ausweisung oder Abschiebung lediglich in der Pflicht, die für die Dateneingabe zuständige Polizeidienststelle zum Zweck der Ausschreibung in INPOL und im SIS (Einreiseverweigerung nach Art. 96 Abs. 3 SDÜ) zu unterrichten. Eine darüber hinausgehende Dokumentationspflicht sei nicht gegeben. Die Voraussetzungen für die Ausweisung und Abschiebung würden sich aus den entsprechenden Verwaltungsakten ergeben. Die Überwachung der Prüffristen würde nicht der Ausländerbehörde, sondern der Deutschen Kontaktstelle (SIRENE) obliegen.

Abschiebung aus entsprechenden schriftlichen Verwaltungsakten, insbesondere Ausweisung und Abschiebungsandrohung hervor.

Ungeachtet dessen wird die Ausländerbehörde im Juni diesen Jahres damit beginnen, bei jedem Ausschreibungsersuchen eine Verfügung zur Ausländerakte zu nehmen, die inhaltlich dem vollständig ausgefüllten, an die für die Dateneingabe zuständige Polizeidienststelle gesandten Vordruck für das Ausschreibungsersuchen entspricht.

Hinsichtlich der zwischen dem 01.01.1994 und dem 26.03.1995 retrograd aus dem INPOL-System in das SIS übernommenen Daten ist zunächst festzustellen, dass das SIS seit Anfang 1997 im Rahmen mehrerer einmaliger Aktionen bereinigt worden ist.

Bei den ausnahmsweise noch nicht gelöschten Ausschreibungen findet eine „anlassbezogene“ Prüfung statt. Dies betrifft insbesondere Fälle, in denen die von Ausweisung oder Abschiebung herrührende Sperrwirkung auf Antrag des Betroffenen aufgehoben oder befristet wird. Bei Aufhebung oder Befristung der Sperrwirkung ist die Ausschreibung nämlich gemäß Ziffer 2.2.2.2 der Anwendungshinweise des BMI zum SDÜ (AAH-SDÜ) zu löschen. Die Veranlassung der Löschung wird in diesen Fällen wie bei anderen „anlassbezogenen“ Prüfungen aktenkundig gemacht.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Der von uns im vergangenen Jahr überprüfte Einzelfall belegt, dass diese Maßnahmen nicht geeignet sind, den Schutzinteressen der Betroffenen in der Verwaltungspraxis ausreichend Rechnung zu tragen. Die Unterrichtung der für die Dateneingabe zuständigen Stellen erfolgt mit einem Formblatt, auf dem die entsprechende Maßnahme anzukreuzen ist. Die Verwaltungsakten benennen in der Regel nur die Rechtsgrundlagen. Die SIRENE Deutschland ist nur für die Überwachung der Prüffristen, nicht jedoch für deren Festsetzung, Verlängerung, Berichtigung, Löschung zuständig. Diese Entscheidungen sind von der einspeichernden Stelle zu treffen. Wir halten daher an unserer Auffassung fest, dass die Ausländerbehörde bei der Ausschreibung nach Art. 96 SDÜ in jedem Einzelfall eine ausreichende Dokumentation der Entscheidungsvoraussetzungen, -gründe für die Speicherung und der Ausschreibungsdauer in der Ausländerakte des Betroffenen vorzunehmen hat. Für die in den Jahren 1994 und 1995 retrograd aus dem INPOL-System in das SIS übernommenen Daten ist die erforderliche Einzelfallprüfung „anlassbezogen“ nachzuholen und das Ergebnis aktenkundig zu machen.

### 4.2.3 Verkehr

**Identitätsausweis in Taxen**

*Von der Senatsverwaltung für Stadtentwicklung wurden wir darüber infomiert, dass in die nächste Neufassung der Berliner Taxenordnung eine Regelung zur Mitführung eines Identitätsausweises durch die Taxifahrer aufgenommen werden soll. Diese Pläne würden unabhängig davon bestehen, dass auf Bundesebene beabsichtigt sei, eine entsprechende Vorschrift in der Verordnung über den Betrieb von Kraftfahrunternehmen im Personenverkehr (BOKraft) zu schaffen.*

Die Verpflichtung der Taxifahrer, während der Berufsausübung ständig einen Ausweis mit Namen und Lichtbild bei sich zu tragen und für Dritte gut sichtbar im Innenraum der Taxen anzubringen, schränkt das informationelle Selbstbestimmungsrecht der Fahrer erheblich ein. Die Verordnungsermächtigung für den Landesgesetzgeber in § 47 Abs. 3 Satz 3 Nr. 3 Personenbeförderungsgesetz (PBefG) bietet für einen derartigen Eingriff keine ausreichende Rechtsgrundlage.

Bereits der Wortlaut steht einer derartig weiten Auslegung des § 47 PBefG entgegen. Die Vorschrift ermächtigt den Verordnungsgeber lediglich zur Regelung „der Einzelheiten des Dienstbetriebs“. Dazu zählt nach § 47 Abs. 3 Satz 2 Nr. 3 PBefG insbesondere der „Fahr- und Funkbetrieb“. Zum Fahrbetrieb zählt aber nicht die Einführung einer *Ausweispflicht für* den *Fahrer*. Dies folgt auch aus dem Regelungszweck des § 47 PBefG. Dieser besteht allein in der Organisation des technischen Ablaufes des Taxenbetriebes.

Die Darstellung des Berliner Beauftragten für Datenschutz und Akteneinsicht ist zutreffend. Es war ursprünglich beabsichtigt, u.a. die Pflicht zur Mitführung eines Identitätsausweises in Taxen an gut sichtbarer Stelle vorzuschreiben, da nach bundesweiten Erkenntnissen wiederholt Beförderungen ohne den erforderlichen Personenbeförderungsschein durchgeführt werden. Nachdem der Berliner Beauftragte für Datenschutz und Akteneinsicht auf Anfrage der zuständigen Senatsverwaltung erhebliche Bedenken aus datenschutzrechtlicher Sicht gegenüber einer solchen Regelung geäußert hatte, wurde von der Aufnahme einer entsprechenden Regelung im Entwurf für eine Neufassung der Berliner Taxenordnung Abstand genommen.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Auch eine Konkretisierung bzw. Ergänzung der bestehenden Regelungen in der BOKraft auf Bundesebene stößt auf Bedenken. Der Bundesgesetzgeber hat bereits detaillierte Regelungen darüber, welche Fahrzeugpapiere bei Taxifahrten mitzuführen und wem sie auszuhändigen sind, geschaffen. In § 27 BOKraft ist geregelt, dass die Ordnungsnummer des Taxis sowie Name und Betriebssitz des Unternehmes gut sichtbar im Taxi anzubringen sind. Nach § 17 Abs. 4 PBefG ist die erforderliche personenbeförderungsrechtliche Genehmigung auf Verlangen den zuständigen Personen zur Kontrolle auszuhändigen. Mit diesen Angaben und der Kenntnis des Unternehmers, wer zum konkreten Beschwerdezeitpunkt gefahren ist, sind die Fahrer identifizierbar. Die Beschwerdemöglichkeit von Fahrgästen ist daher schon nach der bisherigen Rechtslage ausreichend sichergestellt.

Weitergehende Eingriffe in das Persönlichkeitsrecht der Taxifahrer - z. B. durch die Einführung einer Ausweispflicht - stellen einen Verstoß gegen den Verhältnismäßigkeitsgrundsatz dar. Wir haben daher empfohlen, von der Einführung eines Identitätsausweises für Taxifahrer abzusehen.

**Bereinigung der Fahrerlaubnisakten**

*Seit dem 1. Januar 1999 gelten hinsichtlich der Führung der Fahrerlaubnisakten einige neue Regelungen[66]. In § 29 Abs. 9 StVG ist z. B. bestimmt, dass eine unbefristete Aufbewahrung von Unterlagen in den Fahrerlaubnisakten nicht mehr zulässig ist. Registerauskünfte, Gutachten, Führungs- und Gesundheitszeugnisse sowie andere Unterlagen in der Fahrerlaubnisakte sind grundsätzlich nach zehn Jahren zu vernichten. Die vorhandenen Fahrerlaubnisakten sind nach § 65 Abs. 1 StVG anlassbezogen zu bereinigen.*

Zur Umsetzung der genannten Bestimmungen und Einhaltung der Vernichtungsfrist hat das Landeseinwohneramt Berlin im Jahr 1999 eine Arbeitsanweisung erlassen[67]. Um das Verfahren insgesamt und insbesondere den jeweiligen Bearbeitungsstand bei der *Altaktenbereinigung* auch nach außen transparent zu gestalten, haben wir - mit Unterstützung des Unterausschusses „Datenschutz“ - weitere Maßnahmen gefordert. Das Landeseinwohneramt Berlin ist dem durch eine Ergänzung der Arbeitsanweisung gefolgt. Im Teil IV Statistik und Transparenz wurde u. a. festgelegt, dass über den Stand der bereinigten Fahrerlaubnisakten eine Statistik zu führen, vierteljährlich die Gesamtzahl der bereinigten und noch zu bereinigenden Akten zu ermitteln und zu gewährleisten ist,

Die auf Anregung des Berliner Beauftragten für Datenschutz und Akteneinsicht vorgenommene Ergänzung der Arbeitsanweisung des Landeseinwohneramtes Berlin über die Bereinigung der Fahrerlaubnisakten sieht u.a. die jährliche Unterrichtung des Berliner Beauftragten für Datenschutz und Akteneinsicht über den aktuellen Bearbeitungsstand der Aktenbereinigung vor. Es ist beabsichtigt, den Bericht jeweils mit dem Stand 30. Juni abzuschließen, ihn mit dem Berliner Datenschutzbeauftragten unverzüglich abzustimmen und ihn dem Unterausschuß Datenschutz zuzuleiten.

---

[66] Gesetzes zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze vom 24. April 1998, BGBl. I S. 747

[67] JB 1999, 4.2.4

dass jederzeit festgestellt werden kann, welche Fahrerlaubnisakten (Personen) noch zu überprüfen sind. Die bereinigten Fahrerlaubnisakten sind äußerlich zu markieren. Wir sind jährlich über den aktuellen Bearbeitungsstand bei der Bereinigung der Fahrerlaubnisakten schriftlich zu unterrichten.

**Wahllichtbildvorlage im Verkehrsordnungswidrigkeitenverfahren**

*In einem Verkehrsordnungswidrigkeitenverfahren, das vom Polizeipräsidenten in Berlin wegen eines Rotlicht-Verstoßes im Straßenverkehr gegen den Beschuldigten geführt wurde, wurden einer Zeugin neben dem Lichtbild des Beschuldigten im Rahmen einer Wahllichtbildvorlage fünf weitere Lichtbilder aus der Lichtbildvorzeigekartei/ -datei des Polizeipräsidenten in Berlin vorgelegt. Die Auswahl der Lichtbilder erfolgte aufgrund einer typenähnlichen Personenbeschreibung der Betroffenen mit dem Beschuldigten.*

Die erkennungsdienstlichen Unterlagen (z. B. Lichtbilder) werden vom Erkennungsdienst nach § 81 b 2. Alternative Strafprozessordnung (StPO) i.V.m. § 42 Abs. 1 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) zum Zweck der vorbeugenden Straftatenbekämpfung gespeichert. Die Nutzung dieser personenbezogenen Daten zu einem anderen polizeilichen Zweck ist danach zulässig, soweit die Polizei die Daten auch zu diesem Zweck hätte erheben und nutzen dürfen (§ 42 Abs. 2 Satz 2 ASOG).

Wird die Polizei als Verfolgungsbehörde in einem Verkehrsordnungswidrigkeitenverfahren tätig, hat sie die Rechte und Pflichten (vgl. § 53 OWiG), die der Staatsanwaltschaft bei der Verfolgung von Straftaten eingeräumt werden. Insofern finden - soweit das OWiG nichts anderes bestimmt - die Vorschriften des Strafverfahrens (z. B. die der StPO) nach § 46 Abs. 1 OWiG auch im Bußgeldverfahren Anwendung.

Bei der Übertragung von Eingriffsrechten für die Verfolgungsbehörde aus dem Straf- in das Bußgeldverfahren ist nach dem Grundsatz der Verhältnismäßigkeit näher zu prüfen, ob und in welchem Umfang sie gerechtfertigt sind. Die Maßnahme muss zur Erreichung des angestrebten Zweckes geeignet und erforderlich sein. Ferner darf der mit ihr verbundene Eingriff nicht außer Verhältnis zur Sache und dem bestehenden Tatverdacht stehen. Da der Vorwurf einer Straftat grundsätzlich schwerer wiegt als der einer Ordnungswidrigkeit, können Maßnahmen, die im Strafverfahren in der Regel erlaubt sind, im Bußgeldverfahren nicht oder nur bei Vorliegen besonderer Umstände gerechtfertigt sein.

Die Nutzung erkennungsdienstlicher Unterlagen ist bei der Verfolgung von Ordnungswidrigkeiten zwar nicht ausdrücklich ausgeschlossen. Ihre Notwendigkeit ist jedoch unter Berücksichtigung des Grundsat-

zes der Verhältnismäßigkeit in der Regel zu verneinen.

Durch einen Rotlicht-Verstoß im Straßenverkehr können im Einzelfall erhebliche Folgeschäden verursacht werden. Dennoch ist zweifelhaft, ob diese Verfehlung (die nach dem Bußgeldkatalog mit einer Geldbuße von weit unter DM 1.000,- bewehrt ist) unter der Berücksichtigung des Grundsatzes der Verhältnismäßigkeit die Nutzung erkennungsdienstlicher Unterlagen rechtfertigt.

Durch die Vorlage der Bilder aus der Lichtbildvorzeigekartei/-datei an einen Dritten wurde erheblich in die Persönlichkeitsrechte der Betroffenen eingegriffen. Ein derartiger Eingriff ist nur bei der Durchführung von Strafermittlungsverfahren zulässig. Anhaltspunkte für eine Beteiligung der fünf anderen Personen an der dem Beschuldigten zur Last gelegten Tat lagen nicht vor. Die Wahllichtbildvorlage erfolgte zur Identifizierung/Wiedererkennung des (bekannten) Beschuldigten durch eine Zeugin. Die Durchführung einer Wahllichtbildvorlage war zu diesem Zweck nicht erforderlich.

Der Polizeipräsident in Berlin hat sich unserer Auffassung, dass die Verwendung von Lichtbildern aus der Lichtbildvorzeigedatei bei Wahllichtbildvorlagen in Ordnungswidrigkeitenverfahren unzulässig ist, angeschlossen und alle Dienststellen auf diesen Sachverhalt hingewiesen.

**Auskunft über abgeschlossene Ordnungswidrigkeiten**

*In einem Strafverfahren wurden dem Beschuldigten Ordnungswidrigkeitenverfahren aus der Vergangenheit vorgehalten. Die Verfahren lagen ein Jahr zurück und waren rechtskräftig abgeschlossen. Der Beschuldigte erhielt jeweils vom Polizeipräsidenten in Berlin den Hinweis: „Ihre zur Durchführung des Verfahrens gespeicherten persönlichen Daten werden zum Monatsende gelöscht." Um sich Klarheit zu verschaffen, welche Daten zu seiner Person gespeichert sind, stellte er einen Auskunftsantrag. Das Antwortschreiben des Polizeipräsidenten in Berlin enthielt nur Angaben über aktuelle Verfahren. Die Ordnungswidrigkeitenverfahren aus der Vergangenheit, die u. a. Gegenstand des Strafverfahrens waren, wurden nicht erwähnt.*

Nach Auskunft des Polizeipräsidenten in Berlin bezog sich der Hinweis an den Petenten über die Datenlöschung zum Monatsende nur auf die persönlichen Daten, die zur Durchführung der Verfahren in der automatisierten *Datei BOWI I* gespeicherten sind. Auch die Angaben im Auskunftsbescheid gaben nur die in der Computerdatei erfassten Vorgänge wieder. Unabhängig davon werden die abgeschlossenen Verkehrsordnungswidrigkeiten- und Bußgeldvorgänge bzw. Akten zeitlich begrenzt gesondert aufbewahrt.

Insofern ist der Hinweis zur Datenlöschung am Monatsende in den Einstellungsnachrichten irreführend, weil ein Betroffener davon ausgehen muss, dass nach diesem Zeitpunkt über ihn keine weiteren Daten mehr vorhanden sind. Hier ist klarzustellen, dass sich die Mitteilung nur auf die in der automatisierten Datei befindlichen Daten erstreckt, die Aufbewahrung von Verfahrensakten unabhängig davon nach eigenständig geregelten Fristen erfolgt.

Nach § 50 Abs. 1 ASOG hat der Antragsteller einen Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten. Der Begriff des „Speicherns“ meint das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger[68]. Dazu zählen auch Akten. Der Auskunftsanspruch ist daher nicht auf Daten in elektronischen Systemen und Dateien beschränkt. Der Polizeipräsident in Berlin hat angekündigt, seine Auskunftspraxis entsprechend zu korrigieren.

**Kundendaten in einem Taxiunternehmen**

*Ein Bürger beschwerte sich bei uns darüber, dass ein Taxiunternehmen personenbezogene Daten von Kunden speichert. Bei einer telefonisch - über seinen ISDN-Anschluss - aufgegebenen Bestellung sei er nicht dazu gekommen, seinen Namen sowie die Adresse zu nennen. Der Mitarbeiter des Unternehmens hatte diese und weitere Angaben (z. B. über Fahrziele) über die Rufnummernanzeige bereits aus einer Datenbank, in der Angaben über frühere Bestellungen des Kunden gespeichert sind, abgerufen.*

Die Tatsache, dass der Betroffene die Rufnummernanzeige nicht unterdrückt, kann nicht als wirksame (aktive) Einwilligung nach § 4 Abs. 1 und 2 BDSG für eine Speicherung sämtlicher im Telefonat preisgegebener Daten (Anschrift, Ziel der Fahrt) angesehen werden. Liegt eine Einwilligung des Betroffenen nicht vor, kann die Datenspeicherung nur auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG gestützt werden. Danach ist die Speicherung personenbezogener Daten nur im Rahmen einer Zweckbestimmung eines Vertragsverhältnisses zulässig, also nur in dem Umfang, in dem die Datenverarbeitung zur Erfüllung des Vertrages erforderlich ist. Die Daten von Taxikunden dürfen also nicht über die Erfüllung des jeweiligen Fahrauftrages hinaus gespeichert werden. Eine derartige Speicherung von personenbezogenen Daten „auf Vorrat“, also für den Fall, dass erneut ein Vertrag geschlossen wird, ohne Einwilligung des Betroffenen ist unzulässig. Wir haben das Taxiunternehmen aufgefordert, das rechtswidrige Verfahren künftig zu unterlassen.

[68] vgl. § 4 Abs. 2 Satz 2 Nr. 2 BlnDSG

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

**Taxifahrt im Internet**

*Ein Taxiunternehmen bietet an, während der Fahrt Bilder aus dem Innern des Wagens über das Internet zu verbreiten.*

Eine derartige Weitergabe von Bildern stellt einen Eingriff in das Recht des Betroffenen am eigenen Bild dar. Dieser Eingriff ist nur zulässig, wenn die Voraussetzungen des Kunsturhebergesetzes (KunstUrhG), insbesondere der §§ 22, 23, erfüllt sind. Nach § 22 Satz 1 KunstUrhG dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet werden. Das Bild des Fahrgastes darf also nur mit dessen vorheriger Zustimmung aus der Taxe in das Internet übertragen werden. Sofern die Kamera auf das Geschehen außerhalb des Taxis gerichtet ist und dabei Personen erfasst werden, ist die Weitergabe dieser Bilder in das Internet nur unter den Voraussetzungen des § 23 Abs. 1 Nr. 2 KunstUrhG zulässig. Danach dürfen ohne die nach § 22 erforderliche Einwilligung Bilder verbreitet werden, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen.

**Auskunft über Taxiunternehmer**

*Eine Berliner Interessenvertretung von Taxiunternehmen trug vor, dass sie die Beschwerden von Fahrgästen nur dann abschließend bearbeiten können, wenn das betroffene Unternehmen zu ihren Mitgliedern zählt. Sie würden jedoch auch gern in den Fällen vermittelnd eingreifen, wenn es sich um einen Betrieb handelt, der keinem Verband angeschlossen ist. Zur Identifizierung des betroffenen Unternehmens könne die Konzessionsnummer - die vielfach von den Beschwerdeführern benannt werde - herangezogen werden. Ist das Landeseinwohneramt Berlin berechtigt, in diesen Fällen Namen und Anschrift eines Unternehmens mitzuteilen?*

Ordnungsbehörden (hier: das Landeseinwohneramt Berlin) dürfen personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, wenn der Auskunftsbegehrende ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und die schutzwürdigen Interessen der betroffenen Person (hier: des Taxiunternehmers) nicht überwiegen (§ 45 Abs. 1 Nr. 4 ASOG). Ein rechtliches Interesse an der Datenübermittlung kann hier jedoch - wenn überhaupt - nur der Fahrgast und Beschwerdeführer geltend machen. Die Vermittlerrolle, die die Interessenvertretung der Taxiunternehmer bei Beschwerden zwischen dem Fahrgast und dem Taxiunternehmer einzunehmen beabsichtigt, begründet kein derartiges rechtliches Interesse.

Da auch im Personenbeförderungsgesetz und in der Taxenordnung keine Befugnisnormen für eine Datenübermittlung geregelt sind, ist das Landeseinwohneramt Berlin an eine Interessenvertretung von Taxiunternehmen im vorgetragenen Fall keine Befugnisnorm existiert. Entsprechend werden seitens des Landeseinwohneramtes Berlin keine personenbezogenen Daten an Berliner Interessenvertretungen von Taxiunternehmen übermittelt. Im übrigen liegt die Zuständigkeit zur Bearbeitung von Beschwerden von Fahrgästen nicht bei den Interessenvertretungen von Taxiunternehmen, sondern beim Landeseinwohneramt Berlin, zu dessen Ordnungsaufgaben nach Nr. 33 der Anlage zum Allgemeinen Sicherheits- und Ordnungsgesetz u. a. die Aufgaben der Genehmigungsbehörde für Taxen- und Mietwagen nach dem Personenbeförderungsgesetz gehören. Es liegt in der Verantwortung der Interessenvertretungen der Taxiunternehmen, Beschwerden, die an sie von Seiten der Fahrgäste in Un-

neramt Berlin nicht berechtigt, den Namen und die Anschrift eines Taxiunternehmens mitzuteilen.

kenntnis dieser Rechtslage herangetragen werden, an das zuständige Landeseinwohneramt zur weiteren Veranlassung weiterzuleiten.

### 4.3 Justiz und Finanzen

#### 4.3.1 Justiz

**StVÄG - Das Strafverfahrensänderungsgesetz**

Nach schwierigen Verhandlungen im Vermittlungsausschuss hat der Deutsche Bundestag endlich das Gesetz zur Änderung und Ergänzung des *Strafverfahrensrechtes* - Strafverfahrensänderungsgesetz 1999 (StVÄG 1999) - beschlossen. Am 1. November 2000 ist es in Kraft getreten[69].

Damit hat der Gesetzgeber nun auch im Strafverfahrensrecht der Rechtsprechung des Bundesverfassungsgerichtes Rechnung getragen und datenschutzrechtliche Vorschriften für die Durchführung des Strafverfahrens geschaffen. Dabei sind Regelungen zur

- Öffentlichkeitsfahndung,
- polizeilichen Ermittlungstätigkeit,
- längerfristigen Observation,
- Erteilung von Auskünften und Akteneinsicht,
- Errichtung von Dateien bei den Strafverfolgungsbehörden,
- Übermittlungsbefugnis für Strafverfolgungsdaten an die Polizei zum Zweck der Gefahrenabwehr.

In den §§ 131 bis 131 c Strafprozessordnung (StPO) finden sich nun differenzierte Regelungen für die *Öffentlichkeitsfahndung* zum Zweck der Aufenthaltsermittlung bei mit Haft- oder Unterbringungsbefehl Gesuchten, aber auch bei Zeugen. Im Vermittlungsausschuss wurden die Veröffentlichungsmöglichkeiten durch die Aufnahme des Zusatzes in § 131 c Abs. 2 Satz 1 StPO „in Fällen andauernder Veröffentlichung in elektronischen Medien“ im letzten Moment noch auf Veröffentlichungen im Internet erweitert. Damit wurde nun klargestellt, dass eine Öffentlichkeitsfahndung auch im Internet zulässig sein soll. Allerdings hat der Gesetzgeber den Besonderheiten einer Veröffentlichung im Internet nicht Rechnung getragen. Regelungen zur Datensicherheit bei der Nutzung des Mediums Internet fehlen völlig. Wir hoffen, dass dieser Schnellschuss noch eine Nachbesserung erfahren wird.

[69] BGBl. I S. 1253, JB 1999, 4.3.1

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Durch die Einfügung des § 163 f StPO wurde eine Rechtsgrundlage für *längerfristige Observationen* geschaffen. Im Gesetzgebungsverfahren hatte der Rechtsausschuss des Deutschen Bundestages für Eilanordnungsmaßnahmen der Polizei vorgeschlagen, dass diese nach 24 Stunden außer Kraft treten, wenn die Anordnung nicht von der Staatsanwaltschaft bestätigt wird. Im Vermittlungsausschuss wurde diese Frist von 24 Stunden auf drei Tage heraufgesetzt. Darin sehen wir eine erhebliche Verschlechterung. Aus Gründen der Verhältnismäßigkeit halten wir nach wie vor auch eine Anordnungsbefugnis des Richters für erforderlich, da bei Observationen die Eingriffsintensität vergleichbar ist mit der Eingriffsintensität bei Telefonüberwachungsmaßnahmen.

Durch das StVÄG wurden erstmals ausführliche *Auskunfts- und Akteneinsichtsregelungen* in die StPO eingefügt. Der verteidigerlose Beschuldigte hat in § 147 Abs. 7 StPO ein Auskunftsrecht und einen Ermessensanspruch auf Abschriften erhalten. Das von uns geforderte Akteneinsichtsrecht - und damit eine Gleichstellung des verteidigerlosen Beschuldigten mit dem Beschuldigten, der einen Verteidiger hat - ist nicht aufgegriffen worden. Ansonsten regeln die §§ 474 ff. StPO Auskunfts- und Akteneinsichtsrechte für Gerichte, Staatsanwaltschaften und andere Justizbehörden, für sonstige öffentliche Stellen, Privatpersonen und sonstige nicht-öffentliche Stellen sowie für wissenschaftliche Forschungseinrichtungen. Eine Regelung für Auskünfte aus Dateien findet sich darüber hinaus in § 491 StPO. Neu in die StPO eingefügt worden sind *Dateiregelungen*, die bundeseinheitlich auch die Vorgangsverwaltungssysteme der Staatsanwaltschaften auf eine gesetzliche Grundlage stellen. Darüber hinaus ist die Möglichkeit, die Dateien auch für Zwecke künftiger Strafverfahren zu nutzen, jetzt ausdrücklich eröffnet. Ebenfalls in die StPO eingefügt wurde eine Rechtsgrundlage für *automatisierte Abrufverfahren*.

Viele Forderungen der Datenschutzbeauftragten haben in der verabschiedeten Änderung der StPO keinen Eingang gefunden und es wurden Eingriffe in das Persönlichkeitsrecht geregelt, deren Eingriffstiefe durchaus problematisch ist. Trotzdem ist das StVÄG 1999 als ein datenschutzrechtlicher Meilenstein im Bereich der Strafjustiz zu sehen, da er nach vielen Jahren der Diskussion endlich Rechte festschreibt und damit Rechtssicherheit, aber auch Rechtseinheitlichkeit schafft. Die Praxis wird zeigen, ob sich das StVÄG 17 Jahre nach dem Volkszählungsurteil bewährt.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

**Systemumstellung im Strafvollzug**

Ende des Jahres 1999 erhielten wir von der Gesamtinsassenvertretung einer Berliner Justizvollzugsanstalt zahlreiche datenschutzrechtliche Beschwerden. Hintergrund war eine Umstellung von einem alten Datenverarbeitungssystem auf das neue System BASIS 2000. Befürchtungen, dass das alte System den Wechsel in das Jahr 2000 nicht fehlerfrei mitmachen würde, hatten zu einer schnelleren Systemumstellung geführt, als geplant war. Die für die Gefangenen spürbaren Änderungen ließen bei ihnen Zweifel an der Einhaltung der datenschutzrechtlichen Vorschriften aufkommen. Die in den Justizvollzugsanstalten verwandten Mitteilungsbögen enthielten plötzlich - im Vergleich zu den alten Ausdrucken - mehr personenbezogene Daten der Gefangenen.

Bei dem Datenverarbeitungssystem BASIS 2000 handelt es sich um ein gemeinsam mit neun weiteren Bundesländern betriebenes Datenverarbeitungssystem, das ursprünglich für das Land Nordrhein-Westfalen entwickelt worden war. Die Beschwerden der Gefangenen waren Anlass für uns, eine datenschutzrechtliche Prüfung des Datenverarbeitungssystems in Berlin durchzuführen, um einen möglichst umfassenden Überblick über das neue System zu erhalten und der Senatsverwaltung für Justiz unsere Änderungsvorschläge vorlegen zu können. Unsere Prüfung hat sich in eine rechtliche und eine technische Prüfung unterteilt.

Zur Vorbereitung der rechtlichen Prüfung wurden uns alle zur Zeit produzierbaren Ausdrucke vorgelegt mit Hinweisen, für welche Stellen die Ausdrucke vorgesehen sind, d. h. auch, an welche Stellen die Ausdrucke übermittelt werden. Momentan können Ausdrucke (Druckausgaben) für die Vollzugsgeschäftsstelle, die Zahlstelle sowie den Bereich der Arbeitsverwaltung erstellt werden.

Bei der datenschutzrechtlichen Bewertung stellten sich die sog. *A-Bögen* auch sechs Jahre nach unserer Grundsatzprüfung im Strafvollzug[70] als ein Schwerpunktproblem dar. Der A-Bogen setzt sich bei BASIS 2000 aus dem Personalblatt, dem Vollstreckungsblatt und der Aufnahmeverfügung zusammen. Daneben gibt es den Wahrnehmungsbogen, der dem Personalblatt und dem Vollstreckungsblatt des A-Bogens entspricht. Der A-Bogen gibt in komprimierter Form Informationen über den einzelnen Gefangenen. Er enthält beispielsweise Personalien, Ausbildungsdaten, Adressdaten, Daten über Familienangehörige, Daten über die Festnahme, das Strafverfahren, das Urteil und den Vollstreckungsverlauf. Bei unserer Prüfung mussten wir feststellen, dass der Datenumfang des A-Bogens heute mehr Daten enthält als zur Zeit unserer Das IT-Verfahren BASIS wurde nach Einführung im Jahre 2000 durch den Berliner Beauftragten für Datenschutz und Akteneinsicht einer datenschutzrechtlichen Prüfung unterzogen.

Zur Überprüfung des Umfangs der erhobenen Daten wurden dem Datenschutzbeauftragten mit Schreiben vom 26. April 2000 zunächst Muster aller Ausdrucke übergeben, deren Erstellung im Verfahren möglich ist. Unter Einbeziehung der Justizvollzugsanstalten und nach einer mündlichen Erörterung am 7. März 2001 mit Vertretern des Datenschutzbeauftragten wurde diesem mit Schreiben vom 2. April 2001 ein Bericht übersandt, in welchem neben der Darstellung der Erforderlichkeit der erhobenen Daten auch insbesondere auf die Weiterleitung des so genannten A-Bogens an verschiedene Dienststellen einer Justizvollzugsanstalt eingegangen wurde.

Zwischenzeitlich ist eine Äußerung des Beauftragten für Datenschutz und Akteneinsicht hinsichtlich der Erforderlichkeit von Daten erfolgt. Mit Schreiben vom 20. April 2001 hat er eine abschließende rechtliche Bewertung des Verfahrens vorgenommen. Darin wurde festgestellt, dass an das Briefamt, die Hauskammer, die Zahlstelle (Kontoauszug) und die Arbeitsverwaltung (Lohnschein) z.T. Daten übermittelt werden, die zur Aufgabenerfüllung nicht erforderlich sind. Ferner wurde als Mangel im Sinne des § 26 Abs. 2 BlnDSG gerügt, dass aus technischer Sicht eine Änderung des Verfahrens zur Unterdrückung der nicht erforderlichen Daten nicht möglich ist.

Der im Unterausschuss „Datenschutz“ des Ausschusses für Inneres, Sicherheit und Ordnung behandelte Antrag der Fraktion Bündnis 90/Die Grünen über „Computerprobleme im Justizvollzug kurzfristig beseitigen“ wurde auf der Sitzung des Unterausschusses am 8. Mai 2001 mit folgender Empfehlung verabschiedet:

*Der Senat wird aufgefordert, bei der technischen Weiterentwicklung des Verfahrens BASIS den Zugriff auf personenbezogene Daten der Strafgefangenen auf das erforderliche Maß zu beschränken.*

Dem wird der Senat schnellstmöglich durch Schaffung der hierfür erforderlichen technischen Voraussetzungen entsprechen.

In der Erörterung am 7. März 2001 und in dem Bericht vom 2. April 2001 wurde auf die Problematik hingewiesen, die eine Programmänderung zur Unterdrückung bestimmter Daten auf den Ausdrucken für das Land Berlin mit sich bringen würde. Da das Verfahren BASIS in einem Länderverbund mit 11 Bundesländern genutzt und weiterentwickelt wird, würde eine Pro-

[70] JB 1995, 3.4

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Prüfung 1994. So enthält das Personalblatt jetzt auch noch die Felder „Kinderzahl“ und „Angaben zu den Geburtsjahren der Kinder“ sowie Hinweis- und Bemerkungsfelder (zuvor gab es das Feld „Vermerke“). Bereits bei unserer Prüfung 1994 hatten wir Zweifel an der Erforderlichkeit folgender noch immer vorhandener Daten geäußert: Geburtsort/-kreis, Bekenntnis, Anschrift nächster Angehöriger, Namen der Tatbeteiligten mit Geburtsdatum, Daten über getilgte Vorstrafen, Verteidiger sowie Hinweise und Bemerkungen. Auch für die neu hinzugekommenen Daten ist nicht erkennbar, welchem Zweck sie dienen, d. h., warum sie erforderlich sind. Besonders problematisch ist die Datenvielfalt des Personalblattes durch die Übermittlung an eine nicht näher bezeichnete Anzahl von Stellen innerhalb der Anstalt sowie an die Einweisungsbehörde als Stelle außerhalb der Anstalt. Es ist nicht ersichtlich, dass bei Datenübermittlungen nur einzelne Teile des A-Bogens übermittelt werden. Jede Übermittlung von Daten ist an ihrer Erforderlichkeit für die Vollstreckung der Freiheitsstrafe zu messen. Ein Teil der Daten dient aber diesem Zweck nicht. Eine Reduzierung des Datensatzes und eine Differenzierung zwischen den unterschiedlichen Erfordernissen der Stellen, an die die Daten übermittelt werden, halten wir für zwingend.

Ein weiteres Problem, auf das die Gefangenen uns aufmerksam gemacht haben, betrifft den *Transport von Ausdrucken*, die für den Gefangenen selbst bestimmt sind, innerhalb der Anstalt. Der Kopfbogen dieser Ausdrucke enthält nach der Systemumstellung auf BASIS 2000 nun auch die Daten „Geburtsname“, „Geburtsdatum“ und „Geburtsort/-kreis“. Da die Transportwege in großen Anstalten sehr lang sind und die Bögen von Hand zu Hand unverschlossen weitergereicht werden, befürchten die Gefangenen, dass Unbefugte auf dem langen Transportweg Einsicht in die Bögen nehmen und die Daten dann missbräuchlich genutzt werden könnten. Hinter diesen Befürchtungen steht datenschutzrechtlich das Problem des sicheren

grammänderung auf alleinige Initiative des Landes Berlin auch die alleinige Kostentragungspflicht dieser Änderung für Berlin bedeuten. Hinzu kämen laufende Kosten für geänderte Up-Date-Versionen.

Seit der Einführung des Verfahrens BASIS wurde den Gefangenen für 15 Tage Freistellung von der Arbeitspflicht gemäß § 42 StVollzG Freistellungsentgelt gewährt. Mit Beschluss des Kammergerichts vom 19. Juli 2000 wurde eine Entscheidung der Strafvollstreckungskammer bestätigt, die den Antrag eines Gefangenen als unbegründet zurückwies, die Anstalt zu verpflichten, ihm gemäß § 42 Abs. 1 StVollzG für die 18 Werktage dauernde Freistellung von der Arbeitspflicht nicht nur 15 Arbeitstage (Montag bis Freitag), sondern 18 Werktage (Montag bis Sonnabend) Freistellungsentgelt zu zahlen. In der Begründung bestätigte das Kammergericht, dass die jetzige Praxis keineswegs „nur von einem Computerprogramm vorgegeben ist“, sondern allein den gesetzlichen Grundlagen entspricht. Gemäß der Ausführungsvorschrift zu § 42 StVollzG bemisst sich der Umfang der Freistellung auf 18 Werktage, zu denen auch die arbeitsfreien Sonnabende gezählt werden. Entsprechend erfolgt die Zahlung der Bezüge ebenfalls für 18 Werktage. Damit ist jedoch nicht gemeint, dass der 18-fache durchschnittliche Tagesverdienst gezahlt wird, sondern dasjenige Entgelt, welches der Gefangene für 18 Tage erhalten hätte, wenn er gearbeitet hätte. Eine Vergütung für die in den Freistellungszeitraum fallenden arbeitsfreien Sonnabende kann nicht verlangt werden.

Die zum Zeitpunkt der technischen Überprüfung des Verfahrens noch fehlenden Sicherheitskonzepte wurden vom LIT erarbeitet und liegen derzeit im Entwurf vor. Nach Prüfung und Abnahme der Konzepte wird in den Justizvollzugsanstalten die entsprechende Sicherheitstechnik (Firewall) zum Einsatz kommen. Mit dem Einsatz der Firewall ist ein unverschlüsselter und undokumentierter Zugriff der IT-Leitstelle mit ihren Administratorenrechten nicht mehr möglich. Der Zugriff der Mitarbeiter der IT-Leitstelle im Rahmen ihrer Adminstrationstätigkeit erfolgt dann verschlüsselt und wird durch die Log-Datei der Firewall nachgewiesen werden.

Transportweges und der datenschutzrechtliche Grundsatz der Datensparsamkeit. Ideal wäre ein verschlossener Transport der Ausdrucke innerhalb der Anstalt. Auch andere Lösungen sind - zumindest zur Verbesserung - denkbar. Hier sollten die Befürchtungen der Gefangenen ernst genommen werden.

Das überstützt eingeführte Verfahren BASIS 2000 wurde zwar kostenlos zur Verfügung gestellt, doch es galten Rahmenbedingungen, die den Einsatz des Verfahrens in Berlin sehr problematisch machten. Die Anwenderländer bilden Koordinierungsgremien zur Entscheidung über Änderungswünsche, die dann bei der Herstellerfirma umgesetzt werden. Dies erfolgt gegen Mittel, die über Umlagen bereitgestellt werden. Landesspezifische Einzelwünsche, die von den übrigen Ländern nicht mitgetragen werden, können auch Berücksichtigung finden, müssen jedoch von dem jeweiligen Bundesland allein bezahlt werden.

Aus diesem Sachverhalt ergibt sich die mangelnde Flexibilität des Verfahrens, die dazu führte, dass eine notwendige Anpassung an Berliner Rahmenbedingungen nicht erfolgte. Deshalb - und nicht aus rechtlichen Gründen - konnte die unangemessene Datenflut auf den Ausdrucken nicht unterbunden werden. Datenschutzrechtlich weniger relevant, dennoch aber spektakulärer, war die Kürzung des den Gefangenen gewährten Urlaubs von 18 auf 15 Tage, weil BASIS 2000 auf diese Berliner Besonderheit nicht angepasst werden konnte. Im Ergebnis ist festzustellen, dass auf Grund dieser Inflexibilität des schon bei der Beschaffung veralteten Programms eine ordnungsgemäße Anwendung des Programms nicht nach § 19 Abs. 1 Satz 2 BlnDSG gewährleistet ist, denn Ordnungsmäßigkeit heißt auch die Beachtung rechtlicher Vorgaben des Anwendungsbereichs, hier des Strafvollzugs.

Das BASIS 2000-Verfahren für die Justizvollzugsanstalten ist im Wesentlichen eine auf dem Betriebssystem UNIX basierende Client-Server-Anwendung, auf die mit IBM-kompatiblen Arbeitsplatzrechnern zugegriffen werden kann. Die Haltung und Verarbeitung der Verfahrensdaten findet ausschließlich auf dem UNIX-Server statt. BASIS 2000 ist dezentral strukturiert, d. h. jede JVA verfügt über einen eigenen Verfahrensserver. Das eigentliche Verfahren besteht aus diversen Unterprogrammen, die der Nutzer über ein Menü aufruft. Die Menüs und die Zugriffsberechtigungen auf die Unterprogramme können separat von der Systemverwaltung gestaltet werden.

Die örtlichen Systemadministratoren verfügen über die privilegierte Kennung „root“, um ihren Aufgaben nachzugehen. Erfolgte zunächst auch die produktbezogene Unterstützung (Second-Level Support), die von der IT-Leitstelle in der JVA Charlottenburg allen anderen JVAs gewährt wird, über diese privilegierte Kennung, so wurde in der Zwischenzeit dazu übergegangen, eine spezielle Nutzerkennung zu verwenden,

die es ermöglicht, die Aktivitäten während des Supports, die immerhin Eingriffe von außen darstellen, gesondert zu protokollieren und von den Aktivitäten der Systemverwalter vor Ort unterscheidbar zu machen. Allerdings gab es zum Zeitpunkt der Kontrolle in der JVA Tegel noch Probleme im Praxisbetrieb, die dazu führten, dass hier noch „root“ von der IT-Leitstelle zur Administration verwendet werden musste. Wir haben empfohlen, diese Schwachstelle schnellstmöglich zu unterbinden. Wir haben ferner empfohlen, die bisher mittels TELNET unverschlüsselt stattfindende Interaktionen der Fernadministration, die auch das Systemverwalterpasswort enthalten, durch das Secure-Shell-Verfahren (SSH) abzulösen, mit dem die gleichen Funktionen in gesicherter Form ausgeführt werden können.

Positiv hervorzuheben war die Lösung der örtlichen Systemverwaltung für das Problem, den Zugriff von normalen Benutzern auf die Betriebssystemebene einzuschränken. Die Eingriffsmöglichkeiten am Klienten wurden mit Hilfe eines Profileditors stark eingeschränkt. Beim Systemstart ist weder die Menüoption „Ausführen“ (Ausführen von Programmen) noch der „Windows Explorer“ verfügbar. Auch sind keine Programme zur möglichen Datei- oder Programmveränderung installiert. Für das Verfassen von Texten wurde die Textverarbeitung „WordPad“ installiert, bei der die Ausführung von Skripten bzw. Makros, mit deren Hilfe ein Zugriff auf die Betriebssystemebene erlangt werden könnte, ausgeschlossen ist. Allerdings ist eine solche Lösung nur möglich, wenn sich die Textverarbeitung auf einfache Funktionen, wie sie WordPad eben bietet, beschränken lässt.

Es musste allerdings bemängelt werden, dass eine Firewall fehlte, die das lokale Netz vor Angriffen aus dem MAN schützt.

Die Senatsverwaltung für Justiz hat die Beseitigung der Mängel zugesagt.

**Der Große Lauschangriff - Umfang der Berichtspflicht**

Die Bundesregierung unterrichtet den Deutschen Bundestag jährlich über den nach Art. 13 Abs. 3 GG erfolgten Einsatz technischer Mittel. Nach § 100 e Abs. 2 i.V.m. Abs. 1 Strafprozessordnung (StPO) soll der Bericht auf der Grundlage der Ländermitteilungen über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen nach § 100 c Abs. 1 Nr. 3 StPO, d. h. der akustischen Wohnraumüberwachung, erfolgen. Die Berichte sollen den Gesetzgeber in die Lage versetzen, die Normeffizienz des Großen Lauschangriffes zu prüfen.

Mittlerweile liegen für die Jahre 1998 und 1999 Berichte der Bundesregierung vor[71]. Danach wurde 1998

Wie in der zwischenzeitlich ergangenen Antwort an den Berliner Beauftragten für Datenschutz und Akteneinsicht ausgeführt, beruht der Umfang der Mitteilungen zur Vorbereitung des jährlichen Berichts der Bundesregierung an den Bundestag auf einem ländereinheitlich abgestimmten Verfahren, das das Ergebnis eines eingehenden Abstimmungsprozesses zwischen den Beteiligten darstellt.

Es wird nicht in Abrede gestellt, dass insoweit die eine oder andere Konkretisierung in der Sache sinnvoll sein könnte; die Diskussion ist nicht abgeschlossen und wird nach hiesiger Kenntnis durch das Gremium nach Art. 13 Abs. 6 Grundgesetz des

[71] Drs. 14/2452 und Drs. 14/3998

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

in Berlin keine einzige Maßnahme der akustischen Wohnraumüberwachung durchgeführt. 1999 waren es im Land Berlin erstmals drei durchgeführte Überwachungen. Diese Berichte entsprechen jedoch nicht dem gesetzlichen Auftrag, über den Umfang der Maßnahmen zu berichten. Die Datenschutzbeauftragten haben sich deshalb in ihrer Entschließung vom 26. Juni 2000 für eine effektive parlamentarische Kontrolle von Lauschangriffen durch *aussagekräftigere jährliche Berichte der Bundesregierung* ausgesprochen[72]. Insbesondere die tatsächliche Anzahl der von der akustischen Wohnraumüberwachung betroffenen Personen wird bei der derzeitigen Berichtsform nicht deutlich. Bei jeder Wohnraumüberwachungsmaßnahme gibt es immer auch Dritte wie Besucher und Familienangehörige, deren gesprochenes Wort mit abgehört wird. Eine bloße Nennung der Zahl der betroffenen Beschuldigten und Wohnungsinhaber gibt die Eingriffsintensität nicht ausreichend wieder. Darüber hinaus spielt es auch eine Rolle, wie viele Gespräche insgesamt abgehört wurden. Die Datenschutzbeauftragten bemühen sich, noch eine Differenzierung bei der Berichtspflicht - und damit eine Erweiterung - zu erreichen.

Der Bundesbeauftragte hatte sich auf der Grundlage der gemeinsamen Entschließung mit der Bitte um Unterstützung an die Bundesministerin für Justiz sowie an das Parlamentarische Kontrollgremium gewandt, das zur Kontrolle der akustischen Wohnraumüberwachung einberufen worden ist. Da die Bundesjustizministerin die Zuständigkeit für das Datenerhebungsverfahren für die Berichtspflicht bei den Bundesländern sieht, hat sie die Datenschutzbeauftragten an die jeweiligen Bundesländer verwiesen. Wir haben uns daraufhin auch an unsere Senatsverwaltung für Justiz gewandt. Eine Antwort steht jedoch leider noch aus.

Deutschen Bundestages fortgeführt. Jedenfalls bestünde im Hinblick auf konkrete Änderungsvorschläge ein Koordinierungsbedarf zwischen den Landesjustizverwaltungen, bei dem auch die zusätzliche Belastung der Staatsanwaltschaften in Rechnung zu stellen wäre.

Selbstverständlich werden die Vorschläge der Datenschutzbeauftragten der Länder und des Bundes in die künftige Diskussion einbezogen werden. Ein einseitiges Abgehen von der vereinbarten Berichtspraxis durch Berlin kommt aus Gründen der Einheitlichkeit der Berichtsvorlagen aber nicht in Betracht.

**Mitteilungen der Staatsanwaltschaft an die Polizei über den Verfahrensausgang**

Nach Inkrafttreten des Strafverfahrensänderungsgesetzes 1999 (StVÄG 1999) regelt § 482 Strafprozessordnung (StPO) nun die Unterrichtung der Polizei über den Verfahrensausgang durch die Staatsanwaltschaft. § 482 StPO ist wortgleich aus dem Justizmitteilungsgesetz (JuMiG) in die StPO übernommen worden.

Nachdem wegen technischer Probleme mit einer automatisierten Datenübermittlung zwischen dem AStA-System der Staatsanwaltschaft und dem ISVB-System der Polizei eine Datenübermittlung nur in bestimmten Fällen durch Übersendung eines Mitteilungsblattes auch knapp anderthalb Jahre nach Inkrafttreten des JuMiG möglich war, hatten wir dies gegenüber der

Der Senat strebt bereits seit 1986 die Einführung eines automatisierten Rückmeldeverfahrens an. Er hat dies in einer Mitteilung zur Kenntnisnahme über automatisierte Datenverarbeitung bei der Polizei vom 01.12.1986 gegenüber dem Abgeordnetenhaus von Berlin erklärt. Allerdings wurde bereits 1986 auch darauf hingewiesen, daß es bei einer seinerzeit erwarteten Zahl von etwa 180.000 Verfahrensrückmeldungen pro Jahr unmöglich sei, diese in Papierform entgegenzunehmen und manuell in das ISVB einzustellen. Deshalb käme nur ein ADV-gestütztes Rückmeldeverfahren in Betracht.

In der Folgezeit scheiterte die praktische Umsetzung an rechtlichen und auch technischen Problemen.

[72] Anlagenband „Dokumente zum Datenschutz 2000“, S. 17

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Senatsverwaltung für Justiz beanstandet. Da die technischen Probleme Anfang des Jahres noch immer nicht gelöst waren, hat die Staatsanwaltschaft im April 2000 damit begonnen, die Mitteilungen an die Polizei im Formularverfahren durchzuführen. Damit hatte die Justiz ihre gesetzlich geregelte Pflicht zur Übermittlung der Daten erfüllt. Seit August des Jahres 2000 ist sogar ein technischer Datenaustausch zwischen dem AStA- und dem ISVB-System möglich. Streit herrscht jedoch in der Diskussion mit der Polizei darüber, welche Konsequenzen die Polizei aus der Übermittlung der Daten über den Verfahrensausgang von der Staatsanwaltschaft zu ziehen hat.

Die rechtlichen Probleme sind durch das Inkrafttreten des Justizmitteilungsgesetzes am 1. Juni 1998 und das zeitgleiche Inkrafttreten der Anordnung über Mitteilungen in Strafsachen (MiStra) gelöst.

Leider trifft es aber zu, daß die technischen Voraussetzungen für einen automatisierten Datenaustausch auf Seiten der Polizei erst Mitte 2000 geschaffen werden konnten.

Nach bisherigen Erfahrungen übermittelt die Justiz aus dem ASTA-Verfahren täglich ca. 500 Verfahrensrückmeldungen an das ISVB. Diese Rückmeldungen werden im ISVB als Freitext (etwa „Einstellung nach § 170 II StPO“) erfaßt.

Eine manuelle Prüfung der weiteren Speicherungsnotwendigkeit aus Anlaß der Verfahrensrückmeldung scheidet bei der großen Zahl der Rückmeldungen wegen fehlender Personalkapazitäten aus.

Die Polizei prüft derzeit noch, ob es möglich ist, aufgrund bestimmter Einstellungsgründe „Warnlisten“ zur Wiedervorlage solcher Vorgänge automatisch zu erzeugen, die nach Verfahrenseinstellung gelöscht werden **müssen**, z.B. wenn es sich um keine Straftat handelte, eine Tat nicht rechtswidrig begangen wurde oder der Betroffene nicht der Täter war. Ob so etwas möglich ist, hängt aber von dem Informationsgehalt der Rückmeldungen ab. Die bloße Mitteilung einer Verfahrenseinstellung nach § 170 II StPO (das macht ca. 50 % der Rückmeldungen aus) läßt keine derartigen Schlüsse zu. Gespräche zwischen Polizei und Staatsanwaltschaft über die Frage, ob in bestimmten Fallkonstellationen auch weitergehende Informationen (z.B. Einstellungsbegründungen oder Urteilsbegründungen) von der Staatsanwaltschaft übermittelt werden können, haben noch zu keinem Ergebnis geführt.

**Löschung im AStA-Verfahren nach Ablauf der Aufbewahrungsfrist**

Im Jahresbericht 1999[73] hatten wir darüber berichtet, dass die Staatsanwaltschaft die Daten in ihrem AStA-System in der Regel nach Ablauf der Aufbewahrungsfrist nicht fristgerecht löscht und auch die Vernichtung der dazugehörigen Akten nicht zeitnah erfolgt. In dem von uns geschilderten Fall war es dadurch zu einem Vorhalt durch die Staatsanwaltschaft in der Hauptverhandlung gekommen, obwohl die Daten schon längst hätten gelöscht sein müssen.

Aufgrund unserer Beanstandung in diesem Fall hat die Senatsverwaltung für Justiz uns mitgeteilt, dass die Staatsanwaltschaft sich künftig um eine zeitnahe Löschung der Daten nach Ablauf der Aufbewahrungsfristen bemühen werde. Bei der Neukonzeptionierung des elektronischen Registriersystems sollen die technischen Voraussetzungen für eine fristgerechte Lö-

Die Senatsverwaltung für Justiz hat dem Unterausschuss „Datenschutz“ fristgemäß über den Sachstand der Neukonzeptionierung des AStA-Systems berichtet und dabei u.a. ausgeführt, dass das IT-Verfahren AStA noch in diesem Jahr ein Datenlöschungssystem erhält, das es entsprechend der Forderung des Berliner Beauftragten für Datenschutz und Akteneinsicht ermöglicht, in jedem Fall auf den einzelnen Beschuldigten abzustellen und belastende Informationen nach Ablauf der für ihn speziell geltenden Löschungsfrist aus dem Registersystem zu tilgen.

[73] JB 1999, 4.3.1

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

schung geschaffen werden. Wir werden uns hierzu erneut berichten lassen, um möglichst bald eine endgültige Lösung dieses alten Problems zu erreichen. Selbstverständlich ist auch die fristgerechte Vernichtung der Akten von der Staatsanwaltschaft sicherzustellen.

Der Unterausschuss „Datenschutz“ des Ausschusses für Inneres, Sicherheit und Ordnung hat das Problem in einer seiner Sitzungen ebenfalls erörtert und die Senatsverwaltung für Justiz aufgefordert, bis zum 31. März 2001 über den Sachstand der Neukonzeptionierung des AStA-Systems zu berichten.

### 4.3.2 Finanzen

**Der Betriebsprüfer und die Firmen-EDV**

Im Sommer 2000 hat der Bundestag das Gesetz zur Senkung der Steuersätze und zur Reform der Unternehmensbesteuerung (*Steuersenkungsgesetz* - StSenkG) verabschiedet[74]. In diesem Gesetz wurde u. a. eine Regelung verankert, die gerade aus datenschutzrechtlicher Sicht heftig diskutiert wurde. § 146 Abs. 6 AO sieht jetzt vor, dass die Finanzbehörde im Rahmen ihrer Außenprüfung das Recht hat, Einsicht in die gespeicherten Daten (des geprüften Unternehmens) zu nehmen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen. Sie kann im Rahmen einer Außenprüfung auch verlangen, dass die Daten nach ihren Vorgaben maschinell ausgewertet oder ihr die gespeicherten Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden. Aufgrund massiver Proteste aus der Wirtschaft und von den Datenschutzbeauftragten wurde im Gesetzgebungsverfahren die Frist für die Anwendung dieser neuen Vorschrift lediglich um ein Jahr auf den 1. Januar 2002 verschoben.

§ 146 Abs. 6 AO eröffnet dem Mitarbeiter des Finanzamtes grundsätzlich den Zugriff auf alle Unternehmensdaten. Insbesondere Daten aus dem Personalbereich könnten bei diesen Einsichtnahmen von unbefugten Zugriffen betroffen sein. Wenn der Betriebsprüfer z. B. Lohnabrechnungen prüfen will, so stößt er zurzeit auch auf die anderen Personaldaten wie Abwesenheitszeiten, Leistungsdaten. Die Unternehmen sind nach einer Befragung durch die Gesellschaft für Datenschutz und Datensicherung bisher im Personalbereich nicht in der Lage, die steuerlich relevanten Daten für Zwecke der Außenprüfung von den anderen hierfür nicht relevanten Daten zu trennen. Die Wirtschaft und die Datenschutzbeauftragten haben deshalb eine Übergangsfrist gefordert, um eine Anpassung der Datenverarbeitungssysteme in den Unternehmen zu ermöglichen. Die Verlängerung der Frist

Die vom Berliner Beauftragten für Datenschutz und Akteneinsicht gemachten Ausführungen betreffen den § 147 Abs. 6 AO.

Mit der durch diese Vorschrift geschaffenen Möglichkeit der Einsichtnahme und Nutzung des DV-Systems im Rahmen einer Außenprüfung wird die erforderliche Überprüfbarkeit der zunehmend papierlosen Buchführung durch die Finanzbehörden sichergestellt.

[74] BGBl. I S. 1433

im Gesetzgebungsverfahren für die unbegrenzten Zugriffsbefugnisse für Steuerprüfer um nur ein Jahr erscheint jedoch zu knapp, um in dieser Zeit Lösungen zu finden.

**Die Grenzen der Rasterfahndung**

Der VII. Senat des Bundesfinanzhofs hat sich in einem Beschluss[75] zu den Grenzen der *Rasterfahndung bei Banken* geäußert. Folgenden Sachverhalt hatte der BFH zu bewerten:

Die *Steuerfahndung* hatte im Rahmen eines von ihr eingeleiteten Ermittlungsverfahrens gegen unbekannte Mitarbeiter einer Bank wegen des Verdachts der Beihilfe zur Steuerhinterziehung durch namentlich ebenfalls noch unbekannte Anleger ermittelt. Aufgrund eines Beschlusses des Amtsgerichtes durchsuchte die Steuerfahndung alle Grundstücke und Gebäude der betroffenen Bank. Das Amtsgericht hatte in dem Durchsuchungsbeschluss auch die Beschlagnahme aller Unterlagen angeordnet, die seit 1992 entstanden waren im Zusammenhang mit einem nicht ordnungsgemäß bekundeten Geld- und/oder Wertpapiertransfer (einschließlich Depotübertragung) zu und von einer luxemburgischen Bank und zur Identifizierung der Personen, die den nicht ordnungsgemäß bekundeten Transfer nutzen und im Verdacht der Steuerhinterziehung und der Beihilfe standen.

Die Steuerfahnder ließen sich bei der Durchsuchung auch Unterlagen über sämtliche Tafelgeschäfte der Kalenderjahre 1992 und 1993 vorlegen. Sie sichteten außerdem die zum Wertpapiergeschäft angelegten Ordner mit Belegen, aus denen sich die Einlieferung von effektiven Stücken, die der Kunde über die Tafel oder anderweitig erworben hatte, in ein Kundendepot ergab. Unter Zuhilfenahme von Übersendungsschreiben an die Lagerstelle der Wertpapiere ermittelten die Steuerfahnder weitere Betroffene. Eine Betroffene beantragte daraufhin, dem Finanzamt im Wege der einstweiligen Anordnung bis zum Abschluss des Hauptverfahrens zu untersagen, die ihre Person betreffenden Daten, d. h. die anlässlich der Durchsuchung in Beschlagnahme genommenen Unterlagen, gefertigten Aufzeichnungen und gewonnenen Erkenntnisse, zu verwerten.

Die Steuerfahndung hat die Aufgabe, unbekannte Steuerfälle aufzudecken und zu ermitteln (§ 208 Abs. 1 Satz 1 Nr. 3 AO 1977). Voraussetzung hierfür sind jedoch konkrete Anhaltspunkte oder die allgemeine Erfahrung, dass die Möglichkeit einer Steuerverkürzung in Betracht kommt. Unzulässig sind nach der Rechtsprechung Ermittlungen „ins Blaue hinein", Rasterfahndungen und Ausforschungsdurchsuchungen. Den vorliegenden Fall hat der Senat als unzulässige Rasterfahndung angesehen, da die Steuerfahn-

Der vom Berliner Beauftragten für Datenschutz und Akteneinsicht dargelegte und zitierte Beschluss des Bundesfinanzhofs vom 25.07.2000 - VII B 28/99 - wird von der Finanzverwaltung über den entschiedenen Einzelfall hinaus nicht allgemein angewendet (BMF-Schreiben vom 12.12.2000 - IV A 4 - S 0130a - 9/00 -), da die Grundsätze dieses Beschlusses weder mit der Rechtsauffassung der Finanzverwaltung noch mit dem BFH-Beschluss vom 04.09.2000 - I B 17/00 - im Einklang stehen.

Nach letztgenannter Entscheidung ist die Steuerfahndungsprüfung nach § 208 Abs. 1 Abgabenordnung - AO keine Außenprüfung i.S. des § 30a Abs. 3 AO, sodass ein Verwertungsverbot nach § 30a Abs. 3 Satz 2 AO nicht in Betracht kommen kann. Des Weiteren seien die Ermittlungen dann nicht „ins Blaue hinein", wenn aufgrund konkreter Momente oder der allgemeinen Erfahrung die Möglichkeit einer objektiven Steuerverkürzung besteht.

Die Finanzverwaltung hält somit weiterhin an der Auffassung fest, dass nach der allgemeinen und begründeten Erfahrung Tafelgeschäfte steuerlich und auch steuerstrafrechtlich zumindest erheblich sein können, weil solche Geschäfte mit der korrespondierenden Abwicklung über CpD- und vergleichbare Zwischenkonten der Kreditinstitute in der Vergangenheit zur Verbergung von Schwarzgeldern geeignet waren und auch entsprechend genutzt wurden. Dadurch können flächendeckende Ermittlungen gerechtfertigt sein bzw. sind entsprechende Auskunftsersuchen zulässig.

Die genannten BFH-Entscheidungen ergingen im Eilverfahren zum vorläufigen Rechtsschutz, die Hauptsacheverfahren stehen noch aus.

[75] Beschluss vom 25. Juli 2000, Az.: VII B 28/99

dung ein steuerstrafrechtliches Ermittlungsverfahren in einem Kreditinstitut dazu benutzt hat, ohne Rücksicht auf einen etwaigen Zusammenhang mit diesem Auftrag bestimmte Verhaltensweisen von Kunden dieses Kreditinstitutes in ihrer Totalität oder jedenfalls möglichst vollständig mit dem Ziel zu erfassen, in allen Fällen undifferenziert, d. h. unabhängig von der Höhe der festgestellten Beträge oder von sonstigen Besonderheiten der Vorgänge, auf ihre steuerlich korrekte Erfassung einer Überprüfung zu unterziehen.

Die Vorgehensweise der Steuerfahndung war auch unvereinbar mit § 30 a Abs. 3 AO 1977. Diese Spezialvorschrift begrenzt im Bankenbereich die Ermittlungsbefugnisse der Steuerfahndung hinsichtlich der Feststellung der Verhältnisse anderer als der von der Prüfung unmittelbar betroffenen Personen. Die Inhaberschaft von Tafelpapieren, jedenfalls verbunden mit der Einlieferung solcher Papiere in die (legitimationsgeprüfte) Sammeldepotverwahrung, begründet keinen steuerstrafrechtlichen Anfangsverdacht.

Der Senat hat mit seinem Beschluss die Grenzen für die Zulässigkeit einer Rasterfahndung deutlich gezogen.

**Private Nutzung von dienstlichen Telefon- und Internetanschlüssen**

Das Bundesministerium für Finanzen hatte mit Rundschreiben[76] vom 24. Mai 2000 die steuerliche Behandlung der Aufwendungen für einen Telefonanschluss des Arbeitnehmers sowie die Nutzung von betrieblichen Telefonen und Internet-Verbindungen durch Arbeitnehmer ab dem 1. Januar 2001 neu geregelt. Für Zwecke der Besteuerung sollte die Mitbenutzung des Telefonanschlusses und von Internet- und sonstigen Online-Zugängen des Arbeitgebers zu privaten Zwecken des Arbeitnehmers vollständig protokolliert werden. Außerdem sollten Aufwendungen für die betrieblich veranlasste Nutzung des Telefonanschlusses in der Wohnung und die private Mitbenutzung arbeitgebereigener Telefone durch den Arbeitnehmer gegenüber den Finanzämtern durch *Einzelverbindungsnachweise* der Telefongesellschaften nachgewiesen werden. Mit diesem Rundschreiben sollte die bislang mögliche pauschale Ermittlung eines steuerfreien Auslagenersatzes ersetzt werden.

Nicht nur die Datenschutzbeauftragten und die Betroffenen haben sich gegen die geplanten Datenerhebungen gewandt. Auch die Finanzbehörden hatten damit - wenn auch aus anderen Gründen - ihre Schwierigkeiten. Die detaillierte Dokumentation der Internetnutzung und der geführten Telefonate ist auch dazu geeignet, das Verhalten des Arbeitnehmers und seine Leistung am Arbeitsplatz zu kontrollieren, und stellt

Zwischenzeitlich ist durch das Gesetz zur Änderung des Investitionszulagengesetzes 1999 vom 20.12.2000, BStBl.I 2001 S. 28, unter § 3 Nr. 45 EStG die private Nutzung betrieblicher Personalcomputer und Telekommunikationsgeräte steuerfrei gestellt worden, sodass sich Berührungspunkte mit dem Datenschutz insoweit nicht mehr ergeben.

[76] BStBl. I S. 613

einen unverhältnismäßigen Eintriff in die auch für Arbeitnehmer geltende Telekommunikationsfreiheit dar.

Mittlerweile hat das BMF das Rundschreiben aufgehoben[77]. Auch wenn es nicht bessere Einsicht gewesen sein sollte, begrüßen wir diesen Schritt.

**Kontenwahrheit oder: Speicherung von Adressänderungen auch noch nach Auflösung des Girokontos**

*Eine Berliner Bank hatte uns mitgeteilt, dass sie nach dem Anwendungserlass zu § 154 AO verpflichtet sei, nach Beendigung einer Geschäftsbeziehung (Kontoauflösung) innerhalb der sechsjährigen Aufbewahrungsfrist jede ihr irgendwie bekannt werdende Änderung der Kundendaten zu berichtigen. Hierüber hatte sich ein Kunde bei uns beschwert.*

Nach Ziff. 6 zu § 154 des Anwendungserlasses zur AO (AEAO) ist ein Kreditinstitut verpflichtet, ein besonderes, alphabetisch geführtes *Namensverzeichnis* der Verfügungsberechtigten zu führen, um jederzeit Auskunft über die Konten und Schließfächer geben zu können. § 154 Abs. 2 AO regelt die Pflicht der kontoführenden Stelle, den Verfügungsberechtigten zu identifizieren, d. h. Namen und Anschrift zu speichern und dem Finanzamt Auskunft hierüber zu erteilen. Beide Regelungen betreffen vom Wortlaut her nur bestehende Konten. Der Anwendungserlass zu § 154 Abs. 2 Satz 2 AO regelt lediglich, dass eine Namensliste mit den verfügungsberechtigten Personen zu führen ist.

Eine Aktualisierungspflicht für die Bank nach Beendigung der Geschäftsbeziehung ergibt sich hieraus nicht. Die Aufbewahrungsvorschrift des § 147 AO, die eine sechsjährige Aufbewahrung der Unterlagen vorsieht, lässt sogar eine Speicherung auf Bildträgern zu, was eine Aktualisierung ausschließt. Im Übrigen hängt die Möglichkeit einer Aktualisierung der Daten vom Zufall ab, denn nicht jeder ehemalige Kunde nimmt erneut Geschäftsbeziehungen mit der Bank auf.

Die Senatsverwaltung für Finanzen sieht auch nach längerer Diskussion eine *Verpflichtung der Bank zur Aktualisierung der Kundendaten* nach Abschluss der Geschäftsbeziehung. Sie schließt sich damit der Meinung der AO-Referenten der Bundesländer an, die sich mit Auslegungsfragen in steuerlichen Angelegenheiten befassen. Nach ihrer Auffassung konkretisiert § 154 Abs. 2 Satz 2 AO § 93 Abs. 1 Satz 3 AO, der Dritte bei steuerlichen Sachverhalten zur Auskunft verpflichtet.

Diese Begründung der AO-Referenten hat uns nicht überzeugt. Die Mitwirkungspflicht des § 93 AO ist eine von § 154 AO unabhängige Pflicht. Sie enthält

Der Berliner Beauftragte für Datenschutz und Akteneinsicht hat den Stand der Rechtslage und die dazu vertretenen Rechtsauffassungen zutreffend dargestellt: Im Wesentlichen besteht ein Dissens hinsichtlich der Frage der Aktualisierung von Kundendaten auch nach Beendigung der Geschäftsbeziehungen.

§ 154 AO soll verhindern, dass die Nachprüfung der steuerlichen Verhältnisse durch die Verwendung falscher oder erdichteter Namen erschwert oder unmöglich gemacht wird. Dieses Verbot der Identitätstäuschung normiert § 154 Abs. 1 AO. Damit korrespondierend sieht § 154 Abs. 2 AO eine Legitimationsprüfung vor. Dabei muss die kontoführende Person jederzeit in der Lage sein, über den Kontoinhaber Auskunft geben zu können. Diese Auskunftsverpflichtung besteht noch 6 Jahre nach Beendigung der Geschäftsbeziehung fort (Nr.6 des AOAE zu § 154). Da die Veranlagung zur Einkommensteuer frühestens im Jahr nach Ablauf des Jahres der Entstehung der Einkommensteuer erfolgt (§§ 25 Abs. 1, 36 Abs. 1 EStG), kann das Erfordernis, die Daten über das Jahr der Beendigung der Geschäftsbeziehung hinaus vorzuhalten, dem Grunde nach nicht streitig sein.

Dabei impliziert das Sicherstellen dieser notwendigen Auskunftsbereitschaft auch eine Aktualisierung. Würde eine solche Aktualisierung unterbleiben, wäre die Auskunftsverpflichtung für Jahre nach Beendigung der Geschäftsbeziehung ad absurdum geführt, denn es würden im Bedarfsfall „wissentlich“ veraltete Daten weitergegeben, die Legitimationsprüfung ginge ins Leere. Erfolgt die Aufbewahrung mittels Speicherung auf Bildträgern, soll eine Aktualisierung mittels separater Aufbewahrung der Unterlage bzw. Ergänzung - nicht durch Abänderung - des Datensatzes erfolgen.

Eine Aktualisierung kommt nur in Betracht, wenn der kontoführenden Person geänderte Identifikati-

[77] BMF-Schreiben vom 16. Oktober 2000 - IV C 5 - S 2336-13/00 VI

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

darüber hinaus auch keine Verpflichtung, Daten zu speichern, um sie im Auskunftsfall beauskunften zu können. Leider hat sich die Senatsverwaltung für Finanzen mit unseren rechtlichen Argumenten nicht auseinander gesetzt. Sie hat uns vielmehr darauf hingewiesen, dass die Anwendung und Auslegung der Steuergesetze den Finanzverwaltungen der Länder obliegen und die Länder in analoger Anwendung des Artikel 59 Abs. 2 Satz 2 Grundgesetz (GG) 1970 ein Verwaltungsabkommen geschlossen hätten, wonach das Bundesministerium für Finanzen u. a. berechtigt sei, bei Auslegungsfragen im Steuerrecht ein Schreiben herauszugeben, wenn die Mehrzahl der Länder dagegen keine Einwendungen erhoben habe. Dies steht einer anderen Auffassung grundsätzlich nicht entgegen.

onsmerkmale bekannt werden, Ermittlungen zur Aktualisierung sind ausdrücklich nicht vorgesehen.

**Akteneinsicht nach Berliner Informationsfreiheitsgesetz**

*Ein Bürger beantragte bei der Senatsverwaltung für Finanzen Akteneinsicht auf der Grundlage des Berliner Informationsfreiheitsgesetzes (IFG) in einen Verwaltungsvorgang, der die Kaufvertragsverhandlungen zwischen der GmbH, die er vertrat, und dem Land Berlin über mehrere Grundstücke enthielt. Er wollte insbesondere ein Verkehrswertgutachten einsehen, das sich in dem Vorgang befindet. Da dieses Verkehrswertgutachten auch in dem bezirklichen Verwaltungsvorgang zu den Kaufvertragsverhandlungen sein musste sowie in dem Vorgang der Senatsverwaltung für Stadtentwicklung, die das Gutachten erstellt hatte, stellte er auch bei diesen Verwaltungen Anträge auf Akteneinsicht nach dem Berliner Informationsfreiheitsgesetz.*

Alle drei Verwaltungen hatten dem Petenten zunächst die Akteneinsicht verweigert. Ihm wurde entgegengehalten, dass das Berliner Informationsfreiheitsgesetz bei fiskalischem Handeln des Staates gar nicht anwendbar sei und dass die begehrten Unterlagen Betriebs- und Geschäftsgeheimnisse enthalten würden, so dass eine Akteneinsicht nicht in Betracht käme. Wir haben daraufhin alle Akten, auf die sich die Anträge auf Akteneinsicht bezogen haben, selbst eingesehen und sind zu dem Schluss gekommen, dass der Petent einen Anspruch auf die Einsichtnahme in alle Akten hat. Die Grundsatzfragen dieses Falles - Anwendbarkeit des Informationsfreiheitsgesetzes bei fiskalischem Handeln, wann liegen Betriebs- und Geschäftsgeheimnisse vor und inwieweit stellen Verkehrswertgutachten abgeschlossene Verwaltungshandlungen dar, die auch innerhalb eines noch nicht abgeschlossenen Verfahrens zu offenbaren sind[78] - haben auch für andere Fälle Bedeutung.

Im vorliegenden Fall wurde dem Antragsteller zwischenzeitlich bei einer der betroffenen Verwaltungen Akteneinsicht nach dem IFG gewährt.

Siehe hierzu auch Stellungnahme des Senats zu 3.5 „Informationsfreiheit: Eine erste Bilanz“ (ab S. 46).

[78] vgl. 3.5

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

## 4.4 Sozialordnung

### 4.4.1 Arbeitnehmer und öffentliche Bedienstete

**Das Landesschulamt - Hüter der Lehrerpersonaldaten ?**

*Von einer Schulleiterin erhielten wir den Hinweis auf ein offensichtlich übliches Verfahren beim Landesschulamt, persönliche Schreiben an Lehrpersonal als Kopie der jeweiligen Schulleitung zu übersenden. Es handelt sich z. B. um Schreiben zum Mutterschaftsurlaub, zur Stundenreduzierung/-erhöhung, zur stufenweisen Wiedereingliederung in den Dienstbetrieb nach dem „Hamburger Modell", zur Beendigung der Probezeit oder zur Berufung in das Beamtenverhältnis.*

Die Versendung von Kopien der Originalschreiben für die Lehrkräfte an die Schulleitungen ist datenschutzrechtlich unzulässig. Überwiegend enthalten solche Personalschreiben wichtige Hinweise bzw. Daten für die Lehrkraft, in geringem Umfang auch Informationen für den jeweiligen Schulleiter. Das Versenden der kopierten Originalschreiben bedeutet somit eine unnötige Datenvorhaltung bei der jeweiligen Schulleitung, die ihrerseits gezwungen wird, quasi Personalnebenakten in den Schulen anzulegen. Da sich das Führen von Personalnebenakten an der Erforderlichkeit zu orientieren hat (§ 56 Abs. 2 2. Halbsatz Landesbeamtengesetz (LBG)), bedeutet das derzeit praktizierte Verfahren einen Verstoß gegen das LBG und gleichzeitig gegen Datenschutzrecht.

Da der überwiegende Inhalt dieser Schreiben für die Schulleitung nicht von Bedeutung ist, wurde das Landesschulamt gebeten, spezielle Formschreiben für Schulleitungen zu formulieren bzw. zu entwickeln und den Inhalt auf die wirklich für die Schulleitung relevanten Informationen zu beschränken.

Die vom BlnBDA erbetenen speziellen Formschreiben für die Schulleitungen werden zur Zeit in Abstimmung mit dem behördlichen Datenschutzbeauftragten erarbeitet.

*Ein Lehrer beschwerte sich darüber, in seinem persönlichen Postfach ein Schreiben des Landesschulamtes bezüglich seiner Teilnahme an einer Streikmaßnahme unverschlossen - und damit für andere Kollegen zugänglich - vorgefunden zu haben. Das Landesschulamt teilte auf unser Befragen mit, diese Schreiben seien für jede Schule gesammelt in verschließbaren Umlaufmappen an die Schulleitungen verschickt worden. Dieses Verfahren ermögliche ihnen noch einmal eine Kontrolle der von den Schulleitungen stammenden Daten durch sie selbst. Im Übrigen sei dies seit 25 Jahren so praktiziert worden.*

Bei den in dem Schreiben enthaltenen Daten handelt es sich um sensible Personaldaten, die im Ergebnis zu arbeitsrechtlichen bzw. dienstrechtlichen Maßnahmen führen können. Sie unterliegen daher einer gesteigerten Geheimhaltungspflicht durch den Arbeitgeber und sind auch gegenüber Kollegen vertraulich zu behandeln.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Zwar ist die bündelweise Versendung der Schreiben an die Schulen für Kontrollzwecke noch hinnehmbar. Sie sind jedoch nach Einsichtnahme durch die Schulleitung in Umschlägen zu verschließen und erst dann in das persönliche Fach der Lehrkraft zu legen.

Die Schulleitungen werden nach Kenntnisnahme künftig entsprechende Schreiben in verschlossenen Umschlägen den Lehrern in die Postfächer legen.

**Zuständigkeitswechsel als Begründung für Datenschutzverstoß**

*Ein Mitarbeiter einer Senatsverwaltung stellte eine ausdrücklich als „Vertraulich" ausgezeichnete schriftliche Anfrage in Personalangelegenheiten an eine andere Verwaltungsstelle, in der er hervorhob, keinesfalls seine Dienst-/Personalstelle von der Anfrage in Kenntnis zu setzen. Zwischenzeitlich hatte sich jedoch die Zuständigkeit für die Beantwortung dieser Anfrage dahingehend geändert, dass nunmehr doch seine Dienst-/Personalstelle mit der Bearbeitung des Vorganges betraut war. Zwar wurde dieser Zuständigkeitswechsel durch verwaltungsinterne Bekanntmachung den Beschäftigten zur Kenntnis gegeben, tatsächlich aber war dem betreffenden Mitarbeiter diese Veränderung unbekannt. Dies führte dazu, dass im Ergebnis - entgegen dem ausdrücklichen Wunsch - die Anfrage genau zu der Stelle gelangte, deren Kenntnisnahme er verhindern wollte.*

Da erfahrungsgemäß entsprechende Umläufe innerhalb der Verwaltung erhebliche Zeit benötigen, bis sie jeden einzelnen Beschäftigten erreicht haben, haben wir das betreffende Amt gebeten, für eine Übergangszeit von mindestens drei Monaten Post, die mit „Vertraulich" ausgewiesen ist, zunächst bei dem vom Betroffenen genannten Adressaten zu belassen, bis eine Klärung über die Weiterleitung (ggf. nach Rücksprache mit dem Absender) herbeigeführt ist.

**Missbräuliche Verwendung der Personalnummer**

*Die Berliner Polizei plant derzeit den Aufbau einer Datei, die in allen Polizeiabschnitten des sog. „Berliner Modells" die Vorgangsfertigung und -bearbeitung erleichtern und effizienter gestalten soll (BMo-Office/Formular-Bearbeitungsprogramm). Die Datei besteht aus den bisher von den Polizeibeamten verwendeten papierenen Formularen, die dann elektronisch ausgefüllt werden. Der Vorteil der Datei besteht u. a. darin, dass Vorgänge mit dieser Datenverarbeitungsunterstützung direkt am Einsatzort gefertigt und ggf. zu einem späteren Zeitpunkt weiter- bzw. abschließend bearbeitet werden können. Dabei sollten jedoch personenbezogene Daten der Benutzer - u. a. deren Personalnummer und vereinzelt deren Amtsbezeichnung - gespeichert werden*[79].

Die Speicherung dieser Daten ist unzulässig. Bei der *Personalnummer* handelt es sich um ein Personaldatum (§ 56 Abs. 1 LBG). Danach dürfen Personalak-

Bei der Personalnummer eines Mitarbeiters handelt es sich nach Auffassung der Senatsverwaltung für Inneres nicht um ein Personalaktendatum im Sinne des

[79] JB 1999, 4.1.2

tendaten nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verwendet werden - es sei denn, der Beschäftigte willigt in eine andere Verwendung ein.

Nach der Rechtsprechung des Bundesverwaltungsgerichtes gehören zur *Personalakte* alle schriftlichen Aufzeichnungen, die sich mit der Person des Beamten und dem Inhalt und Verlauf seines Beschäftigungsverhältnisses befassen. Dabei ist nicht entscheidend, wo, in welcher Form und unter welcher Bezeichnung die Daten gespeichert sind. Erforderlich ist nur, dass die Vorgänge in einem inneren Zusammenhang mit dem Dienstverhältnis stehen, also nicht einem Zweck dienen, der außerhalb des durch das Beschäftigungsverhältnis begründeten Rechts- und Pflichtenkreises liegt. Diese Voraussetzungen liegen hier vor.

Selbst wenn es sich um ein sog. „einfaches Personaldatum“ handeln sollte, wäre die Verarbeitung nach dem *Informationsverarbeitungsgesetz* (IVG) unzulässig. Nach § 2 Abs. 1 IVG dürfen die öffentlichen Stellen des Landes Berlin bei der Wahrnehmung ihrer Aufgaben personenbezogene Daten ohne Einwilligung des Betroffenen verarbeiten, soweit das für die allgemeine Verwaltungstätigkeit erforderlich ist und schutzwürdige Belange dem nicht entgegenstehen. Die Speicherung der Personalnummer und der anderen o.g. Personaldaten ist zur Erreichung des Zieles - Verwaltung der Benutzer - nicht erforderlich. Darüber hinaus birgt die Personalnummer als „Schlüssel“ zum Zugriff auf Personalakten[80] ein erhöhtes Risiko, den besonderen Schutzbereich der Personalaktendaten zu durchbrechen. Damit liegt ein überwiegendes schutzwürdiges Interesse der Betroffenen an dem Ausschluss der Verarbeitung ihrer Daten vor.

Die Speicherung der Amtsbezeichnung ist darüber hinaus nicht nur nicht erforderlich, sondern im Hinblick auf die Zahl der Berechtigten und den zu erwartenden Änderungsdienst auch nicht zweckmäßig. Vielmehr genügt die Vergabe einer gesonderten Identifikationsnummer.

Die Verwendung der Personalnummer als Mittel der Benutzer-, Speicher- und Zugriffskontrolle bei Datenverarbeitungssystemen ist weder durch eine Rechtsgrundlage gedeckt noch erforderlich. Die Begründung der Verwaltung, durch die Verwendung der Personalnummer werde eine „unkomplizierte Benutzungsverwaltung“ geschaffen und gleichzeitig die Pflege eines „aufwendigen zusätzlichen Datenbestandes“ vermieden, konnte deshalb nicht überzeugen.

Die Senatsverwaltung für Inneres hat dennoch der Errichtung der Datei wegen der angeblichen besonderen Eilbedürftigkeit zugestimmt, weshalb wir das Verfahren nach § 26 Abs. 1 BlnDSG beanstandet haben.

§ 56 Abs. 1 Satz 2 LBG. Die Personalnummer ist lediglich ein formelles Personalaktendatum. Ein Verstoß gegen § 56 Abs. 1 Satz 3 LBG liegt deshalb bei der Verwendung der Personalnummer von Polizeibeamten zur Protokollierung von Zugriffen auf automatisierte Dateien nicht vor.

Personalaktendaten sind gemäß § 56 Abs. 1 Satz 2 LBG alle Unterlagen einschließlich der in Dateien gespeicherten, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen.

Diese Voraussetzungen liegen bei der Personalnummer nicht vor.

In diesem Sinne können Personalaktendaten nur Informationen sein. Die Personalnummer eines Mitarbeiters enthält als solche gerade keine Information. Ihr selbst können unmittelbar keine personenbezogenen Daten entnommen werden. Die Zuordnung einer Personalnummer zu einer Person ist unter dem Gesichtspunkt der Personenbezogenheit rein zufällig. Es erfolgt dabei allein eine Zuteilung der einzelnen Beschäftigungsarten zu bestimmten Personalnummerngruppen (Ziff. 14 Abs.2 der Richtlinien über die Erteilung von Berechnungs- und Anweisungsaufträgen für Personalbezüge sowie Berechnung, Zahlbarmachung, Auszahlung und Abrechnung von Personalbezügen mit zentraler Datenverarbeitung vom 29. Juli 1996, DBl. I 1997, S. 3).

Die Personalnummer ist vielmehr nur ein „Schlüssel“, um auf Personalaktendaten zugreifen zu können. Somit besteht lediglich ein mittelbarer Zusammenhang mit dem Dienstverhältnis und nicht der gemäß § 56 Abs. 1 Satz 2 LBG geforderte unmittelbare Zusammenhang.

Die Personalnummer eines Mitarbeiters ist folglich bloß ein Personalaktendatum im formellen Sinne.

Der formelle Personalaktenbegriff betrifft die Art der Registrierung und Aufbewahrung der schriftlichen Vorgänge, er bezeichnet die von der personalverwaltenden Behörde als „Personalakte“ gekennzeichneten Ordner, Hefter oder sonstigen Blattsammlungen. Der materielle Personalaktenbegriff betrifft dagegen den Inhalt des jeweiligen schriftlichen Vorgangs unabhängig von der Art der Registrierung und Aufbewahrung.

Die Personalnummer ist in diesem Sinne als eine Art „Ordner“ zu verstehen, unter der bestimmte Personalaktendaten im materiellen Sinne registriert sind. Deshalb befindet sich die Personalnummer auch „auf“ und nicht „in“ der Akte. Unter dieser Personalnummer werden lediglich bestimmte Informationen aufbewahrt. Sie dient damit der bloßen Zuordnung und Unterscheidbarkeit bestimmter Informationen zu einer

[80] JB 1997, 4.4.1

bestimmten Person, hat aber selbst keinen Dateninhalt.

Der Gesetzgeber hat sich mit der Regelung in § 56 Abs. 1 Satz 2 LBG für den materiellen Personalaktenbegriff entschieden und damit einem Abstellen auf formelle Gesichtspunkte wie die Art der Aufbewahrung eine Absage erteilt.

Der Wortlaut des Gesetzes spricht in § 56 Abs. 1 Satz 2 LBG auch wörtlich von „Unterlagen“. Damit setzt der materielle Personalaktenbegriff voraus, dass überhaupt ein Schriftstück angefallen und zur Aufbewahrung vorgesehen ist. Geschützt sind nach dem Gesetz somit nur die Unterlagen selbst, nicht jedoch der Zugang bzw. der Schlüssel zu diesen Unterlagen.

Diese Sichtweise ergibt sich auch aus dem Sinn und Zweck einer Personalakte und der darin enthaltenen Personalaktendaten. Die Personalakte hat die Funktion, ein möglichst vollständiges Bild über den beruflichen Werdegang und insoweit über die Persönlichkeit des Beamten zu geben, um daraus Erkenntnisse über den sachgemäßen Personaleinsatz und eine effektive Personalplanung zu gewinnen. Da die Personalnummer allein jedoch, wie oben dargestellt, keine Informationen über die Person des Beamten enthält, kann sie diese Funktion auch nicht erfüllen.

Aus diesen Gründen sieht die Senatsverwaltung für Inneres keine Veranlassung, die Verwendung der Personalnummer von Polizeibeamten in der Datei „BMo-Office“ als Mittel der Zugangskontrolle zum Datenverarbeitungssystem durch ein anderes System zu ersetzen.

**Öffentliche Erfolgsstatistik als Leistungsansporn**

*Der Betriebsrat eines Berliner Unternehmens informierte uns über die Existenz einer „Verkäuferleistungstafel“, die detailliert und personenbezogen über Verkaufserfolge der einzelnen Verkäufer Aufschluss gab. Diese Leistungstafel war in einem durch Glaswände abgetrennten Büro angebracht und daher auch von Kunden einzusehen.*

Bei den auf der Tafel ausgewiesenen Merkmalen handelt es sich um leistungsbezogene Personaldaten von Mitarbeitern, die wegen ihrer Sensibilität einen besonders sorgfältigen Umgang erfordern. Nach § 28 Abs. 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) ist das Speichern und Übermitteln personenbezogener Daten zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen.

Die sowohl personen- als auch leistungsbezogenen Daten eines jeden Mitarbeiters wurden an der in Rede stehenden Tafel gespeichert und an Kollegen und Kunden übermittelt. Dabei war der Personenbezug zur Wahrung berechtigter Interessen des Arbeitgebers nicht erforderlich. Ziel einer Dokumentation der Verkaufsleistungen ist regelmäßig, Leistungsanreize bzw.

Vergleichsmöglichkeiten für den einzelnen Beschäftigten zu eröffnen. Ausreichend wäre hier gewesen, dem jeweiligen Mitarbeiter den eigenen Leistungsstand regelmäßig schriftlich oder im Rahmen eines vertraulichen Gespräches mitzuteilen und ansonsten die Leistungsstatistik anonymisiert zu führen bzw. Verkäufernummern zu vergeben, damit eine Personenbeziehbarkeit auch für Kollegen nicht möglich ist, andererseits der Mitarbeiter aber seine eigene Verkaufsleistung auf der Tafel im Vergleich zu den übrigen erkennen kann.

**Schwangerschaft als Entmündigungsgrund**

*Die Beschäftigte eines Zeitarbeitsunternehmens beschwerte sich darüber, dass die Geschäftsführerin nach einem Telefongespräch mit ihr ihre Mutter über ihre bestehende Schwangerschaft informierte. Als Begründung für diese Vorgehensweise gab die Geschäftsführerin an, die Petentin habe sich bei dem zuvor geführten Telefongespräch in einer psychologischen Ausnahmesituation befunden und des Beistandes Dritter bedurft. In dieser Situation habe sie sich menschlich verpflichtet gefühlt, die Mutter auf die Hilfsbedürftigkeit der Tochter aufmerksam zu machen. Bei der Erörterung der psychischen Situation sei das Gespräch ganz natürlich auf deren Schwangerschaft gekommen, die Auslöser der Depressionen sei. Die Mutter hatte bis zu diesem Zeitpunkt keine Kenntnis über die bestehende Schwangerschaft ihrer Tochter.*

Bei der Schwangerschaft der Petentin handelt es sich - jedenfalls solange die Schwangerschaft nicht offenkundig ist - um ein besonders sensibles Personalaktendatum. Dieses unterliegt einer gesteigerten Geheimhaltungspflicht des Arbeitgebers und darf Dritten gegenüber nur in Ausnahmefällen (z. B. zur Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder zum Schutz berechtigter, höherrangiger Interessen des Dritten) offenbart werden.

Die Offenbarung durch den Arbeitgeber ist nur zulässig, wenn sie zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Da im vorliegenden Fall ein überwiegendes schutzwürdiges Interesse der Petentin an der Geheimhaltung ihres Personaldatums bestand, war die Übermittlung bzw. die Mitteilung über das Bestehen einer Schwangerschaft unzulässig und stellt einen Verstoß gegen geltendes Datenschutzrecht dar.

Ob sich die Betroffene dabei in einer psychischen Ausnahmesituation befunden hat, kann dahingestellt bleiben, da sie volljährig war und selbst bestimmen konnte, wem sie die Tatsache einer bestehenden Schwangerschaft oder eine psychischen Ausnahmesituation offenbaren will und wem nicht. Keinesfalls

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

kann der Arbeitgeber aus sog. fürsorgerischen Gründen selbst eine ihm geeignet erscheinende Person auswählen, um höchstpersönliche Angelegenheiten seiner Arbeitnehmerin zu besprechen.

Das Zeitarbeitsunternehmen wurde aufgefordert, künftig einen der Sensibilität von Personalakten Rechnung tragenden Umgang mit Personalangelegenheiten sicherzustellen.

### 4.4.2 Gesundheit

**Datenschutz für Hundehalter?**

Der Senat hat ein Gesetz über das Halten und Führen von Hunden in Berlin in das Abgeordnetenhaus eingebracht[81], das im Gegensatz zu der Hundeverordnung[82] Regelungen zur Verarbeitung personenbezogener Daten der Hundehalter enthält.

Der Senat verweist auf das bereits laufende Gesetzgebungsverfahren, in dessen Rahmen die Bedenken des Berliner Beauftragten für Datenschutz und Akteneinsicht ggf. berücksichtigt werden können.

Zu der - auch in der geltenden Verordnung enthaltenen - Regelung, dass Hunde ein Halsband mit Namen und Anschrift des Halters tragen müssen, liegen uns Beschwerden von Hundehaltern vor, die befürchten, dass Dritte unbefugt ihre Personalien in Erfahrung bringen können und diese z. B. für telefonische Belästigungen oder einen Einbruch in die während des Spazierganges möglicherweise leer stehende Wohnung nutzen könnten. Da ohnehin ein Datenaustausch mit dem Finanzamt wegen der Hundesteuer geplant ist, für den das Hundesteuergesetz geändert werden muss, sollte dort auch eine Offenbarungsbefugnis für die Personalien von Hundehaltern vorgesehen werden, wenn dies für konkret zu benennende Zwecke (z. B. ordnungsbehördliche oder polizeiliche Zwecke, Geltendmachung von Schadensersatzansprüchen) erforderlich ist.

Die Zuverlässigkeit von Haltern gefährlicher Hunde soll durch die Vorlage von Behördenführungszeugnissen festgestellt werden. Als unzuverlässig gelten nach dem Gesetzentwurf Personen, die wegen bestimmter Straftaten rechtskräftig verurteilt wurden (§ 8 Abs. 1). Diese Norm ist nicht hinreichend bestimmt. Die Formulierung erlaubt eine Ausdehnung der Überprüfung auf jede Straftat und hebt damit die durch den Straftatenkatalog vorgesehene Konkretisierung wieder auf. Die Kriterien für die Zuverlässigkeitsprüfung orientieren sich nach der Begründung im Wesentlichen an den Anforderungen an die Zuverlässigkeitsprüfung des Waffengesetzes. Dann sollte auch - wie im Waffengesetz - eine Einschränkung der in Frage kommenden Straftaten erfolgen. Ungeachtet dessen haben wir Zweifel, ob alle aufgeführten Straftaten für die Zuverlässigkeitsprüfung geeignet und verhältnismäßig im engeren Sinne sind. Dies gilt insbesondere für die Eigentumsdelikte.

---

[81] Abghs.-Drs. 14/618

[82] JB 1999, 4.4.5

Es sollte klargestellt werden, auf welche Weise Feststellungen wie „alkoholkrank“ oder „rauschmittelsüchtig“ festgestellt werden sollen (Anfrage bei Dritten? Gutachten über Suchtverhalten?). Eine Offenbarungsbefugnis öffentlicher Stellen über derartige Krankheitsdaten besteht nicht.

Es fehlen, wie auch in der Verordnung, Regelungen zur Löschung der gespeicherten personenbezogenen Daten. Die Formulierung des Gesetzentwurfes macht es vom Zufall abhängig, wann nicht mehr erforderliche Daten gelöscht werden. Das ist mit dem Verhältnismäßigkeitsgrundsatz nicht zu vereinbaren. Unserer Empfehlung, konkrete Prüffristen festzulegen, wurde nicht gefolgt.

**Rechtsprechung stärkt ärztliche Schweigepflicht**

Die *ärztliche Schweigepflicht* hat im vergangenen Berichtsjahr eine erneute Stärkung und Bestätigung erfahren. Der Bundesgerichtshof für Strafsachen[83] hat das Schweigerecht von Angeklagten und von Ärzten gestärkt. Wenn ein Angeklagter im Strafprozess einen Arzt nicht von dessen Schweigepflicht entbindet, dürfe das nicht als belastendes Indiz im Strafprozess verwertet werden, entschied der Bundesgerichtshof. Anderenfalls sei weder das Abwehrrecht des Beschuldigten gewährleistet, noch werde die Vertrauensbeziehung zwischen Arzt und Patient ausreichend geschützt. Ein Arzt habe im Streitfall nämlich ein Zeugnisverweigerungsrecht über die Identität eines Beschuldigten unabhängig davon, ob er diesen behandelt habe oder nicht. Auch der Angeklagte ist im Strafverfahren grundsätzlich nicht verpflichtet, aktiv zur Sachaufklärung beizutragen. Es steht ihm frei, sich zu den Beschuldigungen zu äußern oder nicht zur Sache auszusagen. Dementsprechend muss auch das Zeugnisverweigerungsrecht eines Arztes nach § 53 Abs. 1 Ziff. 3 StPO gewürdigt werden. Steht in Frage, ob ein Angeklagter bei einem bestimmten Arzt in Behandlung war, hat der Arzt, der nicht von seiner Schweigepflicht entbunden worden ist, dieses Zeugnisverweigerungsrecht, gleich ob er den Patienten tatsächlich behandelt hat oder nicht.

Diese sorgsame Wahrung des Instituts der ärztlichen Schweigepflicht auch im Strafprozess durch die höchstrichterliche Rechtsprechung steht zumindest in einigen Fällen in einem befremdlichen Kontrast zur Handhabung der Schweigepflicht durch betroffene Garanten selbst. Während von der Rechtsprechung die Schweigepflicht immer wieder erneut ausgefeilt und bestätigt wird, nimmt im alltäglichen Betrieb, wie der folgende Vorfall zeigt, eher eine sorglose Unbekümmertheit überhand. Es wäre zu wünschen, dass wenigstens im praktischen Betrieb die Maßstäbe ange-

[83] Urteil vom 22. Dezember 1999, Az.: 3 StR 401/99

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

legt werden, die von der Rechtsprechung vorgegeben worden sind.

**Die gefundenen Zytologiebefunde**

*Ein Berliner Bürger brachte uns an einem Freitag einen prall gefüllten Leitz-Ordner mit etwa 1000 Laborberichten und anderen dazugehörigen Unterlagen des ehemaligen Klinikums Charlottenburg der Freien Universität Berlin aus der Abteilung für Neurologie „Liquorlabor". Der Aktenordner enthielt überwiegend formularmäßige Patientenberichte über Diagnose und Befunde mit dazugehörigen Angaben wie Namen, Geburtsdatum, Station, Datum der Entnahme und Einzelbefunde. Vom Überbringer wurde berichtet, dass diese von seinen spielenden Kindern außerhalb der östlichen Stadtgrenze Berlins am südlichen Ortsausgang der kleinen Gemeinde Eiche, am Rande einer dortigen Straßengabelung gefunden worden seien. Dort würden noch große Mengen weiterer solcher Leitz-Ordner vorzufinden sein.*

Die von uns verständigte Senatsverwaltung für Wissenschaft, Forschung und Kultur wurde unverzüglich tätig, um eine sofortige Sicherung der Fundstelle durchzuführen. Dazu beauftragte die Senatsverwaltung einen Wachschutz, um über das Wochenende die Akten zu überwachen. Der Bericht des Unbekannten erwies sich als richtig. Es wurde dort eine Lastwagenladung voll von Ordnern und Akten des Krankenhauses mit Patientendaten gefunden. Die Senatsverwaltung beauftragte eine weitere Firma, diese Akten aufzunehmen und zu sichern, um sie anschließend ordnungsgemäß unter Aufsicht zu vernichten. Dies erwies sich als besonders aufwendig, da die Akten mittlerweile mit Bauschutt und anderen Abraummaterialien vermischt waren. Die Ermittlung der Senatsverwaltung ergab, dass die für die Aktenvernichtung beauftragte Firma ihre vertraglichen Pflichten nicht erfüllt hatte und statt für die Vernichtung sich für die Entsorgung auf der Abraumhalde entschieden hatte.

Der Vorfall war wieder einmal geeignet, über die Probleme der Auftragsdatenverarbeitung nachzudenken. Die Patientenunterlagen stammten überwiegend aus dem Jahre 1987. Nach Ablauf der Aufbewahrungsfristen und nach Schließung des Krankenhauses durften sie zwar vernichtet werden, es wurde jedoch nicht sichergestellt und kontrolliert, ob die vertraglich vereinbarte Vernichtungsaktion auch tatsächlich durchgeführt wurde.

Gerade die Dokumentation, die Datenverarbeitung, die Datennutzung und auch die Datenvernichtung sind Tätigkeiten, die im Zentrum der ärztlichen Tätigkeit stehen. Das Beispiel zeigt, dass Auftragsdatenverarbeitung bei nachlässiger Umgangsweise nicht immer einen positiven ökonomischen Effekt erzeugt und zu sehr viel höheren Folgekosten führen kann.

Die Verfahren und die Kontrolle der Entsorgung datenschutzrelevanter Unterlagen wurden in Abstimmung mit dem Berliner Beauftragten für Datenschutz und Akteneinsicht verändert. Die Entsorgung wird jeweils durch einen Mitarbeiter des Hauses beaufsichtigt. Die Kosten für den seinerzeit erforderlichen zusätzlichen Aufwand wurden der Firma auferlegt, die die vertraglichen Vereinbarungen nicht eingehalten hatte.

**Case-Management der Krankenkassen**

*Unter dem Begriff Case-Management werden Gesundheitsberater, die auch als Versicherungsberater bezeichnet werden, von den Betriebskrankenkassen eingesetzt. Es handelt sich bei dem Projekt „Versicherungsberatung im Krankenhaus“ um eine Vereinbarung verschiedener Betriebskrankenkassen, die ein „BKK ServiceCenter“ in Form einer BGB-Gesellschaft gegründet haben, welches für die Betriebskrankenkassen eine Versichertenberatung im Krankenhaus durchführen soll. Im BKK ServiceCenter sind zwei bei einer BKK fest angestellte Krankenschwestern und im Übrigen freiberufliche Mitarbeiterinnen tätig. Daneben gibt es Fallmanager/Gesundheitsberater, die bei Stellung von Anträgen und der Unterrichtung von Angehörigen helfen sollen. Die Berater sollen die Patienten im Krankenhaus aufsuchen, sind von der Krankenkasse über die notwendigen Einzelheiten des Falles informiert und sollen möglichst auch Ärzte oder Pflegepersonal des Krankenhauses über die Behandlung befragen.*

Bei der Tätigkeit des BKK ServiceCenters handelt es sich nicht um eine Datenverarbeitung im Auftrag; § 284 Abs. 3 SGB V sowie § 69 Abs. 1 Nr. 1 SGB X rechtfertigen nicht eine vollständige Übermittlung aller der Krankenkasse bekannten Behandlungsdaten an das BKK ServiceCenter. An die Zulässigkeit der Datenübermittlung sind folgende Anforderungen zu stellen:

- Den Patienten sind schriftlich konkrete Informationen über den Zweck und die Vorgehensweise bei der Patientenberatung sowie über den Umgang mit ihren Daten (z. B. in einem Merkblatt) zu geben. Die Information muss insbesondere Aussagen zur Speicherung (auch die Dauer der Datenspeicherung), der Nutzung und der Weitergabe der beim Patienten und bei dem Pflegepersonal oder bei Ärzten erhobenen Daten enthalten.
- Der Patient muss der Versichertenberatung im Krankenhaus zuvor zustimmen.
- In der Einverständniserklärung müssen die Patienten darauf hingewiesen werden, dass die Einwilligung freiwillig ist, dass ihnen aus der Verweigerung der Einwilligung keine Nachteile entstehen und ein Widerruf der Einwilligung mit Wirkung für die Zukunft jederzeit möglich ist.
- Der Name des zuständigen Versichertenberaters ist anzugeben.
- Die Einwilligung muss unterscheiden zwischen der Datenerhebung über das häusliche und soziale Umfeld - diese Daten dürfen nur beim Patienten selbst erhoben werden - und der Datenerhebung bei Ärzten und Pflegepersonal. Hinsichtlich der medizinischen Daten, die von Ärzten und Pflegepersonal offenbart werden, ist vorab zu klären, welche Angaben im

Einzelfall für die Patientenberatung erforderlich sind. Diese Daten sind in der Einwilligungserklärung aufzuführen.

- Die Einwilligung muss auch die Übermittlung evtl. erforderlicher Daten vom BKK ServiceCenter an die jeweilige BKK umfassen.
- Bei den Modalitäten der Versichertenberatung soll darauf geachtet werden, dass vor dem Besuch eines Patientenberaters die schriftliche Einwilligung des Patienten vorliegen muss. Bei der Durchführung der Beratung soll die Befragung von Ärzten und Pflegepersonal stets in Anwesenheit des Patienten erfolgen. Der MDK sollte eingeschaltet werden, wenn im Einzelfall Zweifel an der Notwendigkeit und der Dauer der Krankenhausbehandlung bestehen (vgl. § 112 Abs. 2 Nr. 2 SGB V und § 275 Abs. 1 Nr. 1 SGB V) oder wenn Datenerhebungen notwendig werden, die nur der MDK durchführen darf (z. B. Durchsicht von OP-Berichten).
- Die Sozialdaten der Versicherten der einzelnen Betriebskrankenkassen dürfen nicht anderen Betriebskrankenkassen zur Kenntnis gelangen. Es ist deshalb eine personelle, organisatorische und räumliche Trennung der Funktion des Versichertenberaters und Fallmanagers von der beauftragten BKK erforderlich.

**Auskunft aus dem Gemeinsamen Krebsregister (GKR)**

Aufgrund des Staatsvertrages der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen vom 20./24. November 1997[84] werden die Daten des nationalen Krebsregisters der DDR vom GKR gespeichert, weiter gepflegt und die weiteren Krebsregistermeldungen eingestellt. Es unterscheidet zwischen der Vertrauensstelle und der Registerstelle. In der Vertrauensstelle befinden sich die Namen der dorthin gemeldeten Patienten und der Codierungsschlüssel, während in der Registerstelle die wissenschaftlich bedeutsamen epidemiologischen Basisdaten zum Krankheitsverlauf und zur Krankheitsart pseudonym verwaltet werden.

Das Bundeskrebsregistergesetz[85], das nach seinem § 14 Abs. 1 am 31. Dezember 1999 außer Kraft getreten ist, gilt aufgrund des Staatsvertrages landesrechtlich fort, soweit der Staatsvertrag nicht andere Regelungen getroffen hat. Im Bundeskrebsregistergesetz darf eine Entschlüsselung oder Übermittlung identifizierender Daten nur für Maßnahmen des Gesundheitsschutzes und für ein im öffentlichen Interesse stehendes Forschungsvorhaben stattfinden. Zuvor

[84] GVBl. 1998 S. 174 - 176

[85] BGBl. 1994 I S. 3351

ist die schriftliche Einwilligung des Patienten einzuholen. Ist er verstorben, so sollen seine nächsten Angehörigen einwilligen. In § 9 Abs. 1 BKRG ist geregelt, dass der Patient, der Auskunft über seine Erkrankung haben will, weder eine schriftliche Auskunft noch eine Ablichtung oder eine Abschrift der schriftlichen Auskunft des Krebsregisters erhalten darf. Der behandelnde Arzt, der befugt ist, für solche Zwecke an das Krebsregister heranzutreten, darf die erhaltene Auskunft nicht an den Patienten schriftlich weiterleiten. Die Regelung soll verhindern, dass das Krebsregister zu einem allgemeinen bevölkerungsbezogenen Gesundheitsregister degeneriert und dem Patienten im Wege faktischer Zwänge ein Auskunftsanspruch durch Dritte aufgenötigt wird.

*Durch eine Beweisanordnung vom Sommer 2000 gab das Sozialgericht Düsseldorf dem GKR auf, Zweitschriften derjenigen Unterlagen dem Gericht zu übermitteln, die über einen 1952 geborenen und 1983 verstorbenen Patienten vorliegen. Das GKR hat die Frage an uns weitergeleitet.*

Nach Art. 6 Abs. 5 Staatsvertrag zum GKR ist auf die *Aufbewahrung und Nutzung von Meldebögen* aus den Jahren 1953 bis 1960 das Berliner Archivgesetz entsprechend anzuwenden. Dies gilt ab 1. Januar 2000 auch für die in Abs. 3 genannten Meldebögen. Das gemeinsame Krebsregister darf zur Vervollständigung seines auf elektronischen Datenträgern vorhandenen Datenbestandes des Nationalen Krebsregisters der Deutschen Demokratischen Republik bis zum 31. Dezember 1999 die auf Meldebögen vorhandenen Daten aus den Jahren 1961 bis 1989 verarbeiten. Die Meldebögen sind räumlich getrennt zu verwahren und dürfen nur hierfür besonders befugten Mitarbeitern der Registerstelle zugänglich sein. Sie dürfen nicht für andere Zwecke genutzt werden. Die enge Nutzungsbeschränkung des Krebsregistergesetzes nach § 8 Bundeskrebsregistergesetz, wonach nur für Maßnahmen des Gesundheitsschutzes und der Forschung eine Entschlüsselung der medizinischen Daten erlaubt ist, steht in dem hier zu entscheidenen Fall nicht entgegen. Das Bundeskrebsregister geht zwar davon aus, dass das GKR ausschließlich epidemiologische Aufgaben wahrnehmen soll, es sind jedoch auch Aufgaben nach dem Archivgesetz von Berlin wahrzunehmen, wenn personenbezogene Unterlagen nicht mehr dem informationellen Selbstbestimmungsrecht unterliegen. Nach dem Landesarchivgesetz von Berlin darf Archivgut, das sich nach seinem wesentlichen Inhalt auf natürliche Personen bezieht (personenbezogenes Archivgut), nur mit Einwilligung des Betroffenen zugänglich gemacht werden. Nach dem Tod des Betroffenen bedarf die Nutzung des Archivgutes bis zum Ablauf von 10 Jahren der Einwilligung der Angehörigen. Diese archivrechtliche Regelung unterscheidet nicht zwischen besonders schutzwürdigen und weniger schutzwürdigen personenbezogenen Daten im

Sinne der ärztlichen Schweigepflicht. Da das Bundesverfassungsgericht im Mephisto-Urteil festgestellt hat, dass der Persönlichkeitsschutz als Grundrecht mit dem Ableben einer Person endet und über den Tod hinaus nur noch eine abnehmende Schutzwirkung entfaltet, die unter Umständen auch von Angehörigen treuhänderisch wahrgenommen werden kann, bestehen gegen die Regelungen im Staatsvertrag keine verfassungsrechtlichen Bedenken.

Es bestanden daher aus unserer Sicht keine Bedenken dagegen, in Anwendung der Regelungen des Staatsvertrages in Verbindung mit dem § 8 Abs. 3 ArchG der Beweisanordnung des Sozialgerichts Düsseldorf Folge zu leisten. Auch die Versagungsgründe des § 8 Abs. 9 Ziff. 5 ArchG konnten hier die Übermittlung nicht verhindern. Zwar heißt es dort, dass die Nutzung des Archivgutes zu versagen und einzuschränken ist, soweit Berufs- oder besondere Amtsgeheimnisse im Sinne des § 203 Abs. 1-3 StGB verletzt würden. Jedoch bezieht sich diese Vorschrift auf Sachbereiche, bei denen noch geltende Schutzfristen zu berücksichtigen wären. Hier ist jedoch die nach § 8 Abs. 3 ArchG zu bemessene Schutzfrist in Bezug auf den Patienten abgelaufen.

**Krankenheimcontrolling**

In Berlin beträgt der Anteil älterer Menschen über 65 Jahre ca. 14 % der Gesamtbevölkerung. Im Zuge der weiteren Verschiebung der demografischen Struktur in Deutschland wird dieser Anteil an der Gesamtbevölkerung spürbar wachsen. Die Gesellschaft wird immer älter und der Anteil von Bürgern mit multimorbidem Krankheitsbild und chronischen Leiden nimmt zu. Meist handelt es sich dabei um ältere Menschen. Durch die gesetzliche Trennung von Pflege und medizinischer Versorgung entstehen an der Schnittstelle im Pflegeheim Reibungsverluste durch Probleme in der Abgrenzung von Zuständigkeiten. Dies macht neue Behandlungsansätze und Kostenübernahmestrukturen notwendig.

*Neben Pflegeheimen gibt es in dieser Stadt als eine Berliner Besonderheit den Einrichtungstyp „Krankenheim“ und als weitere Besonderheit den Einrichtungstyp „Krankenhäuser und Abteilungen für chronisch Kranke“. Mit dem Ziel, eine qualitätsgesicherte Versorgung der chronisch Kranken, multimorbiden und psychisch erkrankten Patienten in stationären Pflegeeinrichtungen zu ermöglichen, werden zur Erhöhung der Wirtschaftlichkeit im Zuge einer Rahmenvereinbarung ambulante und stationäre Leistungsbereiche gestaltet. Im Zuge einer Wirtschaftlichkeitsüberprüfung sollte ein Controlling im Rahmen des „Berliner Modellprojekts vollstationärer Versorgung für multimorbide und chronisch Kranke durchgeführt werden.*

Hierzu wurde eine private Datenverarbeitungsfirma zur Entwicklung eines Konzepts beauftragt. Für die

Durchführung des Projektes war es erforderlich, Patientendaten aus den unterschiedlichen Einrichtungen zusammenzuführen und auszuwerten. Unsere Beratungstätigkeit setzte in einem sehr frühen Stadium ein, so dass ohne Schaden für die Patienten die erforderlichen Maßnahmen rechtzeitig entwickelt und eingesetzt werden konnten. Wir haben empfohlen und im Zuge unserer Beratungstätigkeit auch durchsetzen können, dass ein *Pseudonymisierungsmodell* nicht nur eine komfortable Auswertung und Nutzung der Daten zuließ, sondern auch die Sicherheit der Patientendaten gewährleistet blieb. Darüber hinaus können auf der entwickelten Informationsstruktur weitere Konzepte für Wirtschaftlichkeitsprüfungen entwickelt werden. Das Gesamtprojekt wurde von einem Lenkungsausschuss gesteuert, an dem sowohl die Senatsverwaltung für Gesundheit und Soziales als auch eine gesetzliche Krankenkasse beteiligt waren.

### 4.4.3 Sozial- und Jugendverwaltung

**Behandlungs- und Rehabilitationsplan**

Nach § 93 Abs. 2 Bundessozialhilfegesetz (BSHG) muss durch den Träger der Sozialhilfe eine leistungsorientierte und auf Effizienz bedachte *Vergütung von sozialen Einrichtungen* sichergestellt werden. Um den Umfang der Bedürftigkeit und damit die Höhe der zu erstattenden Kosten für einen Hilfeempfänger festzustellen (personenzentrierte Hilfe) werden die Träger aufgefordert, einen *Formbogen „Behandlungs- und Rehabilitationsplan“* auszufüllen. Der Formbogen wurde vom Landesbeauftragten für Psychiatrie entwickelt, mit dem die weitere Gestaltung auch erörtert wurde.

*Gegen die Erforderlichkeit der zu erhebenden Daten wurden Zweifel laut. So werden Angaben zu bedeutsamen sozialen Kontakten verlangt und nach der Religionszugehörigkeit gefragt. Weiterhin werden Auskünfte über „Selbstwertgefühl, Körpererleben, störendes Verhalten im sexuellen Bereich, Sinnorientierung des Lebens und Gestaltung frei verfügbarer Zeit“ verlangt. Dies seien höchst sensible Daten, die einen Rückschluss auf Charaktereigenschaften zulassen, die man ungern computervernetzt der Datenverarbeitung überlassen möchte.*

Der *Behandlungs- und Rehabilitationsplan* soll der Ermittlung und Abstimmung des spezifischen Hilfebedarfs des seelisch behinderten Menschen im Einzelfall dienen und in eine Zuordnung zu einer Gruppe mit vergleichbarem Hilfebedarf (Hilfebedarfsbemessung) münden.

Ausgehend von den Wünschen und Bedürfnissen des Klienten soll gemeinsam mit ihm eine Zielvorstellung zur angestrebten Lebensform erarbeitet werden. Bei dieser Art Bedarfsplanung kann neben dem Hilfeempfänger der Leistungserbringer, der Sozialpsychiatrische Dienst und das Sozialamt beteiligt sein. Die be-

teiligten Stellen sollen nicht gegeneinander, sondern miteinander die für den seelisch behinderten Menschen geeignete Hilfe ermitteln. Im Behandlungs- und Rehabilitationsplan sind - bezogen auf dieses Ziel - Angaben zur aktuellen Problemlage sowie zur vorhandenen Fähigkeit bzw. Beeinträchtigungen zu machen, da sich hieraus unmittelbar der Ansatzpunkt für die erforderlichen Betreuungsmaßnahmen ableitet. Die Beantwortung der Fragen zum religiösen Bekenntnis und zu sexuellen Bereichen ist freiwillig und im Übrigen sollen auch die anderen Angaben immer von dem Grundsatz der Verhältnismäßigkeit geleitet bzw. qualifiziert und quantifiziert werden. Die Seite 3, auf der die wesentlichen medizinischen Daten enthalten sind, ist grundsätzlich nur beim Sozialpsychiatrischen Dienst abzulegen.

Als Ergebnis der Beratung hat die Senatsverwaltung für Arbeit, Soziales und Frauen ein mit uns abgestimmtes Informationsschreiben zur Anwendung und zu den Rechtsgrundlagen des Behandlungs- und Rehabilitationsplanes an die Leistungserbringer verschickt, um Probleme beim Ausfüllen des Formbogens auszuräumen.

**Im Ausland unverschlossen**

*Eine Deutsche, die im sonnigen Ausland lebte, sollte von der Landesversicherungsanstalt (LVA) in Anspruch genommen werden, um eine überbezahlte Rente eines verstorbenen Rentenempfängers zu erstatten, die sie als Erbin verbraucht haben sollte. Abgesehen davon, dass der Vorwurf sachlich unzutreffend war, hat die Landesversicherungsanstalt den Rentenrückerstattungsbescheid an die Deutsche Botschaft des Wohnsitzlandes der Petentin geschickt, wo diese ihn sich nach der Benachrichtigung durch die Botschaft unverschlossen abholen konnte. Sie spürte, dass der Rückerstattungsbescheid von den dortigen Mitarbeitern wohl gelesen worden sei. Für sie bedeutete das Ganze eine peinliche Angelegenheit, umso mehr als der Vorwurf ungerechtfertigt war.*

Die Landesversicherungsanstalt bestand zunächst darauf, dass eine Zustellung in anderer Weise nicht möglich sei. Sie berief sich auf § 14 *Verwaltungszustellungsgesetz*. Die von uns eingeholten Erkundigungen beim Post- und Kurierdienst des Auswärtigen Amtes der Bundesrepublik Deutschland erbrachten die Information, dass selbstverständlich auch bei Auslandszustellung nach § 14 Verwaltungszustellungsgesetz eine *verschlossene Zustellung* erfolgen kann. Ja man wunderte sich sogar, dass in diesem Fall die Zustellung offen betrieben worden war. Zur Sicherstellung des Zugangs kann an das Auswärtige Amt auch ein eingeschriebener Brief gerichtet werden, in dem in einem doppelten Außenumschlag das zuzustellende Schriftstück enthalten ist. Das Auswärtige Amt übernimmt dann die Übersendung des zustellungsbedürftigen Briefes an die jeweilige ausländische Botschaft

der Bundesrepublik Deutschland, von wo aus dann die Zustellung im Wege der Abholung des verschlossenen und registrierten Dokumentes bewerkstelligt werden kann. Erfreulich, dass zumindest in diesem Bereich der Datenschutz auch im Ausland durch deutsche Behörden gewährleistet werden kann.

**Post als Bermuda-Dreieck**

*Eine Petentin führte einen Sozialrechtsstreit wegen der Höhe der Rentenansprüche gegen die Landesversicherungsanstalt. Für die Anfertigung eines Gutachtens übersandte das Gericht die Prozessakte an einen Gutachter, der jedoch die Begutachtung ablehnte und die Akte unfrankiert an das Gericht zurücksenden wollte. Am Sozialgericht galt die dienstliche Anweisung, dass die Annahme unfrankierter Post zu verweigern sei. Die Post wollte daraufhin die Sendung dem Gutachter als Absender aushändigen, der nunmehr jedoch seinerseits auch die Rücknahme der Sendung verweigerte. Seitdem sind die Spuren des Verbleibs der Akte vollkommen verloren gegangen. Der Petentin obliegt die mühselige Aufgabe der Rekonstruktion der Prozessakte, was nicht nur einen erheblichen materiellen Aufwand erfordert, sondern auch eine schwere Allgemeinbelastung darstellt.*

Der Bundesbeauftragte für den Datenschutz, den wir zur Überprüfung des Falles eingeschaltet hatten, teilte uns mit, dass das Verhalten der Post ohne Fehl war. Die Post hat sich zu jedem Zeitpunkt datenschutzgerecht verhalten. Wegen der Auswirkungen des Zusammentreffens von rigiden Dienstanweisungen mit der Gleichgültigkeit eines *Gerichtsgutachters* soll der Ablauf hier dargestellt werden.

Der Versand von Paketen durch die Deutsche Post AG ist in den Allgemeinen Geschäftsbedingungen der Deutschen Post AG für den Frachtdienstinland (AGBFrDinL) geregelt. Im vorliegenden Fall ist die Sendung durch die doppelte Annahmeverweigerung nach § 4 Abs. 7 AGB FrDinL unzustellbar und durch die Annahmeverweigerung des Absenders als „preisgegeben“ zu behandeln. Es habe daher für die Deutsche Post AG nicht das Recht bestanden, die Sendung zu öffnen, da Absender und Empfänger bekannt waren und eine Öffnung keine Fortschritte bezüglich der Zustellbarkeit der Sendung gebracht hätte. Sendungen, deren Annahme durch Absender und Empfänger verweigert wurde, werden von der Zustellbasis an die Nachverpackungsstelle des Frachtzentrums gesandt und von hier an die Ermittlungsstelle für unanbringliche Paketsendungen mit Sitz in Bamberg weitergeleitet. Dort werden unzustellbare Sendungen nach einer Lagerfrist von 6 Wochen an eine Verwertungsfirma verkauft. Unverwertbares Gut, zu dem auch z. B. eine Gerichtsakte zählen würde, die schon aus datenschutzrechtlichen Gesichtspunkten nicht an Dritte veräußert werden dürfte, kann und muss die Deutsche Post AG

nach § 4 Abs. 7 AGBFrDinL sogar vor Ablauf dieser Frist vernichten, wenn dies erkennbar gewesen wäre.

Da die Deutsche Post AG hier nicht das Recht auf eine Öffnung der Sendung hatte, weil Absender und Empfänger bekannt waren, ist davon auszugehen, dass die Sendung an einen Verwerter veräußert worden ist. Aber auch in diesem Fall ist die Einhaltung des Datenschutzes gewährleistet, da der Käufer in § 2 Ziff. 2.2 des Verwertungsvertrages ebenfalls zur Vernichtung von Inhalten mit personenbezogenen Daten verpflichtet wird. Nach Ziff. 2.4 des Verwertervertrages ist auch der Verkauf der Inhalte an den ursprünglichen Absender oder Empfänger ausdrücklich verboten. Eine Verletzung datenschutzrechtlicher Vorschriften durch die Deutsche Post AG war daher nach den Feststellungen des Bundesbeauftragten verfahrenstechnisch ausgeschlossen.

Ein wirksamer Nachforschungsauftrag hätte im vorliegenden Fall nur durch den Absender der Sendung, also durch den Gutachter unter der Angabe des Ident-Codes gestellt werden können. Ist der Ident-Code bekannt, lassen sich Postpakete bis zu zwei Jahren nach der Auslieferung nachweisen. Ein *Nachforschungsauftrag* ohne Angabe des Ident-Codes kann nicht bearbeitet werden. Die Deutsche Post AG weist darauf hin, dass unter Berücksichtigung des Massenverkehrs im Frachtbereich sie nicht in der Lage ist, den Inhalt unzustellbarer Sendungen zu selektieren und zu bewerten und nach irgendwelchen noch zu erstellenden Bewertungskriterien dem Absender oder dem Empfänger ein zweites Mal zur Auslieferung gegen Zahlung der Gebühr anzubieten oder evtl. andere im Inhalt genannte dritte Personen zu fragen, ob bei ihnen das Interesse besteht, die Sendung für sich zu erwerben. Diese Möglichkeiten verbieten sich auch schon aus datenschutzrechtlicher Sicht.

Die Deutsche Post AG weist deshalb ausdrücklich darauf hin, dass sich das Landessozialgericht Berlin überlegen müsse, ob das Verfahren, generell die Annahme unfreier Paketsendungen zu verweigern, als zweckmäßig angesehen werden kann oder ob die Vertragsgestaltung und die Verfahrensweise bei der Beauftragung und Auswahl von externen Gutachtern nachgebessert werden sollte.

Das Annahmeverbot für unfreie Sendungen wurde inzwischen vom Gericht aufgehoben.

**Kindlicher Opferschutz**

*In einer Kindertagesstätte war ein Kind aufgenommen worden, dessen Vater wegen Kindesmissbrauchs rechtskräftig verurteilt war. Das Urteil war dem Jugendamt bekannt und es wurde befürchtet, dass der Vater sich an anderen Kindern der Kita „vergreifen" würde. Nach einer geraumen Zeit wurde das Kind aus der Kita genommen und in eine andere Kita in einem benachbarten Bezirk eingegliedert.*

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

*Die interdisziplinären Arbeitsgruppe „Kindlicher Opferschutz", die aus Mitarbeiterinnen und Mitarbeitern der Jugendverwaltung, von Schulen, der Polizei und der Staatsanwaltschaft besteht, bat um eine rechtliche Beurteilung. Die beim Jugendamt durch die Entscheidungsgründe des Gerichts (Mitteilungspflicht nach Nr. 35 MiStra) bekannt gewordene Straftat hatte dazu geführt, dass dem Vater des Kindes durch die Kita-Leitung aufgegeben worden war, keine anderen Kinder zu sich einzuladen. Dies war eine vertragliche Aufnahmebedingung, um die anderen Kinder der Kita-Gruppe nicht in Gefahr zu bringen.*

Die Frage war, ob andere Eltern über die Straftat hätten informiert werden dürfen, wenn gegen diese Auflage vom Vater verstoßen worden wäre. Eine weitere Frage betraf die Befugnis, das Wissen um die Straftat von der abgebenden Kita an die neue Kita dieser Familie zu übermitteln.

Da mit der Zustimmung des Betroffenen zur Datenübermittlung wohl nicht gerechnet werden kann, wäre zu fragen, ob auch ohne dessen Mitwirkung eine Übermittlung möglich ist. Für die Datenübermittlung ohne Mitwirkung ist auf § 64 Abs. 1 Kinder- und Jugendhilfegesetz (KJHG) abzustellen, der zugleich auch eine Nutzungsbefugnis enthält. Sozialdaten dürfen nach § 64 Abs. 1 KJHG zu dem Zweck übermittelt und genutzt werden, zu dem sie erhoben worden sind. Also ist auf die Datenerhebungsvorschrift in § 62 KJHG zurückzugreifen. Die Voraussetzungen der Datenerhebung sind also mit denjenigen für die Datenübermittlung identisch. Die Datenerhebung gemäß § 62 Abs. 2 SGB VIII (KJHG) ist zwar primär beim Betroffenen durchzuführen. Jedoch kann sie auch ohne den Betroffenen erfolgen, wenn die „Aufgabe ihrer Art nach eine Erhebung bei anderen erfordert" (§ 62 Abs. 3 Nr. 2 SGB VIII (KJHG)). Es ist also auch bei der Datenübermittlung darauf abzustellen, ob die „Aufgabe ihrer Art nach" eine Übermittlung erfordert.

Bei der krisenbezogenen Arbeit der Jugendhilfe ist diese Beurteilung ausschließlich auf das „Kindeswohl" zu beziehen. Der Verhältnismäßigkeitsgrundsatz fordert bei der Anwendung dieser Rechtsvorschriften, dass dabei täterbezogene Daten immer nur zur Abwehr konkreter Gefährdungslagen erhoben, übermittelt und genutzt und nicht unabsehbar auf Vorrat erhoben und gespeichert bzw. übermittelt werden dürfen. Der Umfang der zu übermittelnden Daten muss auf das unabdingbar Erforderliche begrenzt werden.

Im Ergebnis war hier die Weitergabe von Daten grundsätzlich zulässig. Jedoch ist es keineswegs erforderlich, den ganzen Tatkomplex in allen Einzelheiten und Gründen zu übermitteln oder gar den Eltern in einer Kita bekannt zu geben. In der Regel

Die Ausführungen des Berliner Beauftragten für Datenschutz und Akteneinsicht stellen die rechtlichen Erwägungen zur Vereinbarkeit des individuellen Datenschutzes mit der krisenbezogenen Arbeit der Jugendhilfe dar. Der Senat teilt die Auffassung des BlnBDA, wonach bei der Abwägung , ob Daten übermittelt werden dürfen, „ausschließlich auf das Kindeswohl" abzustellen ist.

dürfte ein Hinweis auf eine allgemeine Gefährdungslage für einen bestimmten Personenkreis ausreichen.

Dies gilt erst recht, wenn die Verdachtsmomente gegen eine Person zwar stark sein mögen, jedoch kein Strafurteil vorliegt. Oft erhalten die Jugendämter lange vor der Verurteilung Hinweise von Nachbarn oder der Polizei (z. B. nach § 44 ASOG oder § 18 Abs. 1 letzter Satz AG KJHG oder nach § 38 JGG i. V. m. § 50 AG KJHG).

**Datensicherheit beim Berliner Sozialhilfe-System BASIS**

Für die Verarbeitung personenbezogener Daten bei der Gewährung von Sozial- und Jugendhilfe wird seit Mitte der neunziger Jahre das Berliner Automatisierte Sozialhilfe-Interaktions-System (BASIS I) auf der Grundlage des Standardprogramms PROSOZ eingesetzt. Das Verfahren besteht aus unterschiedlichen Modulen für verschiedene Formen bei der Gewährung sozialer Unterstützung durch den Staat.

BASIS I wurde ursprünglich für die Verwendung unter dem Betriebssystem MS-DOS oder einem dazu kompatiblen Betriebssystem konzipiert. Diese inzwischen längst veralteten Betriebssysteme können den parallelen Ablauf von mehreren Programmen nicht unterstützen, wie es z. B. bei Betriebssystemen wie UNIX oder Windows NT der Fall wäre. Das Sicherheitskonzept wurde daher auch speziell für den Betrieb in einer DOS-Umgebung entwickelt. Mit der teilweisen Einführung von Windows 3.11 bzw. Windows NT in den Sozialämtern, mit der die Arbeitsbedingungen am BASIS-I-System verbessert werden sollten, entstanden neue Probleme hinsichtlich der informationstechnischen Sicherheit bei der Anwendung, wie bereits 1999 eine Reihe von Kontrollen in verschiedenen Bezirksämtern ergab[86].

Die alte DOS-Version von BASIS I speichert alle Verfahrensdaten in einem bestimmten Verzeichnis. Der Zugriffsschutz wird durch das Anwendungsprogramm realisiert. Wenn ein Zugriff unter Umgehung des Anwendungsprogramms möglich ist, so kann der vorhandene Zugriffsschutz unterlaufen werden, so dass die BASIS-Daten unbefugt gelesen werden können. Ein Zugriffsschutz, der über die vom modernisierten Serverbetriebssystem zu erteilenden Dateirechte realisiert wird, ist nur sehr eingeschränkt möglich, da alle BASIS-Nutzer pauschale Schreibrechte für die BASIS-Daten benötigen und damit auch pauschale Leserechte erhalten. Eine Differenzierung auf bestimmte Fälle oder Datenbereiche ist auf dieser Ebene nicht möglich. Sie ist aber erforderlich, denn den Sachbearbeitern ist die Kenntnisnahme von Daten, die nicht in ihrem Zuständigkeitsbereich liegen, zu verwehren. Trotz anzuerkennender Bemühungen

[86] JB 1999, 4.4.3

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

konnte die BASIS-Geschäftstelle im Bezirksamt Schöneberg eine Lösung zu diesem Problem bisher nicht vorgelegen.

Microsoft hatte für das Ende der 90er Jahre die Einstellung der Unterstützung für seine Betriebssysteme MS-DOS und Windows 3.x angekündigt. Auch aus diesem Grunde wurde es notwendig, ein Nachfolgesystem für BASIS I zu entwickeln, welches auf einer modernen Client-Server-Architektur beruhen sollte.

Das neue Projekt BASIS II sollte auf einer Software mit der anspruchheischenden Bezeichnung „Bundesweiter allgemeiner Softwarestandard für integrierte Sozialleistungen - BASIS 3000“ aufsetzen, die von der Senatsverwaltung für Arbeit, Soziales und Frauen in Zusammenwirken mit den Firmen ORACLE und PSI erwickelt werden sollte. Dieses Verfahren hätte bei einer erfolgreichen Einführung die angesprochene Sicherheitslücke beseitigt. In der Zwischenzeit hat sich einer der Projektpartner zurückgezogen, nachdem bereits bekannt war, dass mit jahrelangen Verzögerungen gerechnet werden müsste. Die weitere Zukunft des Projekts ist ungewiss.

In dem auch politisch geführten Streit um eine Übergangslösung wurde von den Bezirken die Standardsoftware PROSOZ/S für Windows favorisiert (Projekt Modernisierung von PROSOZ -MOPS). Die wesentlichen Änderungen betreffen dabei die Benutzeroberfläche und fachliche Belange. Aus Sicht des technischen Datenschutzes besteht das oben beschriebene Sicherheitsproblem allerdings weiterhin.

Wegen der Umstellung des Betriebssystems auf den Clients sind die bezirklichen Sicherheitskonzepte anzupassen. Schon für BASIS I war die Erstellung von Sicherheitskonzepten bei den Verfahrensbetreibern vorgesehen. In der Praxis wurden leider nur in den wenigsten Fällen Sicherheitskonzepte erstellt, teilweise deswegen, weil man auf zentrale Vorgaben wartete, die aber zu Recht nicht eintrafen, denn jeder Bezirk hat eine unterschiedliche, individuelle Infrastruktur und eigene organisatorische Vorgaben, die in ein Sicherheitskonzept einfließen müssen. Jede für die Erstellung eines Sicherheitskonzepts erforderliche Risikoanalyse ist auf die jeweils vorhandene Situation abzustimmen. Betrachtet man den Vernetzungsgrad in den Bezirken, so ist umso wichtiger, dass die Sicherheitsanforderungen an BASIS in das bezirkliche Sicherheitskonzept einbezogen werden.

Im Zusammenhang mit der Verschmelzung verschiedener lokaler Netze zu einem bezirklichen Gesamtnetz und im Hinblick auf die Bezirksfusionen, die die Sozialämter der Bezirke auf unterschiedliche Standorte verteilen, tritt das Problem der Sicherheit der Daten bei der Übertragung auf solchen Netzen verstärkt auf.

Die Verfahrenssicherheit hat nach wie vor eine vorrangige Stellung bei der Konzeption der Betriebsumstellung des Verfahrens.

Die BASIS-Geschäftsstelle im Bezirksamt Schöneberg wurde gebeten, bei den Bezirksämtern als den Verfahrensbetreibern erneut darauf hinzuwirken, dass nunmehr schnellstmöglich die örtlichen Sicherheitskonzepte erstellt bzw. angepasst werden.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Rechtlich ergibt sich aus § 5 Abs. 3 Nr. 9 BlnDSG oder aus Nr. 9 der Anlage zu § 78a SGB X die Notwendigkeit, die Transportkontrolle zu gewährleisten, also zu verhindern, dass bei der Übertragung von Sozialdaten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Die Transportkontrolle bei der Übertragung kann entweder dadurch geschehen, dass hinreichend sicher verhindert werden kann, dass Unbefugte sich an den Leitungen zu schaffen machen können, um an die Daten - z. B. mit Abhörgeräten - heranzukommen, oder dadurch, dass die Daten durch kryptografische Verschlüsselung gegen unbefugte Kenntnisnahme, Veränderung oder Nutzung geschützt werden. Der Schutz der Leitungen kann - wenn überhaupt - nur durch die geeignete Verlegung der Leitungen in den Häusern oder durch permanenten Kontrolldruck erfolgen, der sich dadurch ergibt, dass jeder, der sich an Übertragungswegen unbefugt zu schaffen macht, damit rechnen muss, dabei ertappt zu werden. Wenn nicht absolut sichergestellt werden kann, dass die Daten über vollständig kontrollierbare Leitungen (inkl. aller Netzknoten) fließen, ist eine Verschlüsselung notwendig. Dies gilt zumindest immer dann, wenn die Daten hausübergreifend fließen.

Wenn zum Beispiel in einem Sozialamt eine strukturierte Verkabelung nach den in Berlin geltenden Verkabelungsvorschriften verwendet wird, kann in diesem LAN (Lokal Area Network) auf eine Verschlüsselung verzichtet werden, wenn eine Kontrolle über die Datenübertragungsleitungen gegeben ist. Wenn jedoch eine Fernadminstration des BASIS-Servers oder eine zentrale Datensicherung vom entfernten Rathaus aus erfolgt, so ist eine Verschlüsselung geboten.

### 4.4.4 Bauen, Wohnen, Umwelt

#### Übermittlung von Mieterdaten an Nachmietinteressenten

*Ein Mieter, der seine Wohnung fristgerecht gekündigt hatte, wurde von einer ihm unbekannten Person angerufen. Der Unbekannte hatte Kenntnis von der Wohnraumkündigung, befragte den Mieter zur Ausstattung der Wohnung und wann diese zu besichtigen sei. Auf Nachfrage gab der Anrufer an, dass er die Angaben vom Vermieter erhalten habe. Dieser bestätigte dem Mieter, dass er dem potenziellen Mietinteressenten eine Liste übersandt habe, in der neben wohnungsbezogenen Angaben (Anschrift und Lage der Wohnung, Größe, Anzahl der Zimmer, Höhe der Miete usw.) auch der Name und die Telefonnummer des Mieters genannt sind.*

Die Übermittlung der personenbezogenen Mieterdaten durch den Vermieter an einen potenziellen Nachmieter ist ohne die Einwilligung des Betroffenen unzulässig.

In den städtischen Wohnungsbaugesellschaften erfolgt die Weiterleitung der personenbezogenen Mieterdaten an einen potentiellen Nachmieter nur nach Einwilligung der Betroffenen. Diese Einwilligung wird – so-

Die Übermittlung kann nicht auf § 28 Abs. 1 Nr. 1 BDSG gestützt werden. Sie erfolgt nicht im Rahmen der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen. Die Zweckbestimmung hat sich an den von den Vertragspartnern mit dem Vertrag verfolgten Zielen zu orientieren. Die Parteien eines Mietvertrages verfolgen das Ziel, dem Mieter gegen Entrichtung des Mietzinses an den Vermieter den gewünschten Wohnraum zu überlassen, keinesfalls aber das Ziel, den Vermieter zur Übermittlung seiner Daten an Dritte zu berechtigen.

Die Übermittlung von Namen, Adresse und Telefonnummer eines Mieters - ohne dessen Einwilligung - an einen potenziellen (Nach-)Mietinteressenten ist auch nicht zur Wahrnehmung der berechtigten Interessen des Vermieters (§ 28 Abs. 1 Nr. 2 BDSG) erforderlich. Es mag durchaus sein, dass diese von vielen Vermietern bevorzugte Vorgehensweise die Aufgabenstellung eines Vermieters erleichtert. Subjektive Wünsche des einzelnen Vermieters sind jedoch nicht ausschlaggebend. Bei der Bewertung einer datenschutzrechtlich zulässigen Übermittlung ist vielmehr auf die objektive Erforderlichkeit der Datenverarbeitung abzustellen. Diese ist hier nicht gegeben, da der Vermieter (in Absprache mit dem Mieter) selbst einen Besichtigungstermin mit dem Mietinteressenten vereinbaren kann, ohne diesem die personenbezogenen Daten des Mieters zu offenbaren.

Unabhängig davon ist die Übermittlung der personenbezogenen Mieterdaten durch den Vermieter an den (Nach-)Mietinteressenten zulässig, wenn sie auf die Einwilligung des Mieters gestützt werden kann. Im Regelfall erfolgt diese nicht bereits mit der Unterzeichnung des Mietvertrages. Die Vertragsbestimmungen sehen zumeist lediglich vor, dass der Mieter eine Wohnungsbesichtigung des Vermieters mit einem Nachmietinteressenten zu dulden hat. Daraus lässt sich für den Mieter keine vertragliche Nebenpflicht ableiten, wonach er die Weitergabe seiner personenbezogenen Daten an einen (Nach-)Mietinteressenten zu dulden hat. Keinesfalls hat der Mieter mit der Unterzeichnung einer derartigen Bestimmung bzw. des Vertrages in die Weitergabe seines Namens, seiner Anschrift und seiner Telefonnummer an Dritte eingewilligt.

**Aktion „Wie gut ist Ihr Vermieter?“**

*In einer Umfrage, die von einer Interessenvertretung der Berliner Mieter durchgeführt wurde, sollten die Teilnehmer die Zufriedenheit mit ihren Vermietern zum Ausdruck bringen. Neben Angaben über die Einschätzung des Leistungs- und Serviceangebots war in dem Fragebogen “Wie gut ist Ihr Vermieter?“ u.a. auch der Name und die Adresse des Vermieters bzw. Verwalters anzugeben. Die Ergebnisse der Umfrage sollten veröffentlicht werden.*

weit sie nicht bereits vorliegt – unverzüglich nach Eingang der Wohnungskündigung eingeholt. Sollte dies nicht erfolgreich möglich sein, wird von der städtischen Wohnungsbaugesellschaft ein gemeinsamer Besichtigungstermin mit dem Mieter und dem Mietinteressenten vereinbart.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Bei den Angaben zu den Vermietern handelt es sich - soweit natürliche Personen betroffenen sind - um deren personenbezogene Daten. Die Verarbeitung derartiger personenbezogener Daten und deren Nutzung sind nach § 4 Abs. 1 BDSG nur zulässig, wenn das BDSG selbst oder andere Rechtsvorschriften dies erlauben oder anordnen oder soweit der Betroffene darin eingewilligt hat. Eine Einwilligung der Betroffenen (Vermieter, Verwalter) in die Datenverarbeitung und -nutzung lag nicht vor. Auch eine Rechtsgrundlage, auf die die Datenverarbeitung gestützt werden könnte, ist hier nicht ersichtlich.

Wir haben empfohlen, den Fragebogen zu anonymisieren und auf die Angaben zum Vermieter und Verwalter (Name, Adresse) zu verzichten. Der Veranstalter der Umfrage hat uns daraufhin versichert, dass die mit dem Fragebogen abgefragten Vermieter- und Verwalternamen nicht als solche gespeichert, sondern nur kategorisiert und anonymisiert erfasst würden. Ein entsprechender Hinweis auf dem Fragebogen sei versehentlich unterlassen worden. Bei etwaigen zukünftigen Fragebogenaktionen werde ein derartiger Hinweis aufgenommen.

**Der moderne Pranger**

*Ein Mitglied einer Wohnungsbaugenossenschaft beschwerte sich beim Bezirksamt über den ruhestörenden Lärm, der von einem Bolz- und Ballspielplatz in der Wohnanlage ausgeht. Das Bezirksamt ordnete die vorläufige Schließung des Spielplatzes an. Der Vorstand informierte die Mitglieder der Wohnungsbaugenossenschaft über diesen Sachverhalt in einem Rundschreiben. Darin benannte er den für die Schließung des Spielplatzes verantwortlichen Beschwerdeführer mit Namen und Adresse und erklärte, dass er diese jugendfeindliche Politik nicht unterstützen werde.*

Die Benennung von Namen und Adresse des Beschwerdeführers in dem Rundschreiben ist eine unzulässige Übermittlung von personenbezogenen Daten durch den Vorstand an die Leser des Rundschreibens.

Nach § 28 Abs. 1 Nr. 2 BDSG müsste die Übermittlung zur Wahrung berechtigter Interessen der Wohnungsbaugenossenschaft erforderlich gewesen sein, ohne dass schutzwürdige Interessen des betroffenen Mitgliedes überwiegen. Das berechtigte Interesse der Genossenschaft i.S.d. § 28 Abs. 1 Nr. 2 BDSG könnte darin liegen, dass diese anstrebt, für den Spielplatz eine Genehmigung zu erhalten bzw. dessen Wiedereröffnung zu erreichen. Die Veröffentlichung der Daten über den Beschwerdeführer in dem Rundschreiben ist zur Wahrung dieses Interesses jedoch weder geeignet noch erforderlich. Die namentliche Benennung des Beschwerdeführers hat hier vielmehr die Wirkung einer „Bloßstellung“ oder „Anprangerung“, wodurch in der Diskussion um die Wiedereröffnung des Spielplatzes eher Fronten geschaffen bzw. vertieft werden.

Bei den städtischen Wohnungsbaugesellschaften werden keine Rundschreiben mit Namen und Adressen von Beschwerdeführern versandt oder Aushänge über Mietschuldner angebracht, derartige Verfahrensweisen sind bei den städtischen Wohnungsbaugesellschaften nicht üblich.

Unabhängig davon werden durch die Vorgehensweise des Vorstandes der Genossenschaft schutzwürdige Belange des betroffenen Mitgliedes beeinträchtigt, die das berechtigte Interessen der Genossenschaft an einer Veröffentlichung der Daten überwiegen.

Wir haben die Wohnungsbaugenossenschaft aufgefordert, zukünftig vergleichbare Veröffentlichungen in Rundschreiben an die Mitglieder zu unterlassen.

*Eine Kleingärtnerin beschwerte sich beim Bezirksamt (Grünflächenamt) über eine Baumschnittaktion in ihrer Kleingartenkolonie. Das Bezirksamt ahndete die unzulässige Aktion, die durch den Vorstand des Kleingartenvereins veranlasst worden war, mit einem erheblichen Ordnungsgeld. Der Vereinsvorstand informierte alle Gartenfreundinnen und -freunde der Kolonie über diesen Sachverhalt in einem Rundschreiben und benannte darin die Anzeigenerstatterin mit Vor- und Nachnamen.*

Dadurch, dass alle Parzellisten in der Kolonie das Rundschreiben erhalten haben, wurde eine breite Öffentlichkeit über die Identität der Anzeigenerstatterin in Kenntnis gesetzt. Diese Übermittlung von personenbezogenen Daten erfolgte weder mit Einwilligung der Betroffenen noch kann sie auf § 28 BDSG gestützt werden.

Wir haben den Kleingartenverein aufgefordert, derartige Datenübermittlungen, die erkennbar auf eine Bloßstellung des Betroffenen abzielen, zukünftig zu unterlassen.

*In mehreren Eingaben beschwerten sich Mieter darüber, dass ihr Vermieter Aushänge mit Angaben über Mietschuldner angebracht habe. Diese seien in dem Schreiben mit Namen und Wohnungsnummer bezeichnet. Der Aushang sei in den Hauseingängen des Mehrfamilienhauses angebracht und damit für Dritte (z. B. andere Mieter, Besucher des Hauses) zugänglich.*

Eine derartige Veröffentlichung ist unzulässig. Es handelt sich bei den Angaben über Mietschulden um vertragsinterne Daten, die vom Vermieter nur unter bestimmten rechtlichen Voraussetzungen an Dritte (z. B. Sozialamt, Räumungsverfahren usw.) offenbart werden dürfen. Keine dieser rechtlichen Voraussetzungen ist im vorliegenden Fall gegeben. Es handelt sich hier - wie in den beiden vorgenannten Fällen - um einen erheblichen Eingriff in die schutzwürdigen Belange der Betroffenen. Diese werden durch die Bekanntgabe der Informationen in der Öffentlichkeit bloßgestellt, ohne das ihnen eine Möglichkeit zur Verteidigung bzw. Richtigstellung gegeben wird.

**Der Hauswart wird zum Boten**

*In mehreren Eingaben haben sich Mieter darüber beschwert, dass ihr Vermieter den Hauswart mit der Zustellung wichtiger Schreiben (z. B. Mahnungen über*

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

*Mietrückstände, Stellungnahmen zu Beschwerden usw.) beauftragt habe. Der Hauswart erhält die Schreiben vom Vermieter unverschlossen, um sie an den Empfänger/Mieter weiterzuleiten. Dadurch hat er die Möglichkeit, vom Inhalt der Schriftstücke Kenntnis zu nehmen.*

Der Schriftwechsel zwischen Vermieter und Mieter betrifft in der Regel das Mietvertragsverhältnis (z. B. bei Mahnungen über Mietrückstände, sonstigen Abmahnungen, Betriebskostenabrechnungen oder Schreiben über Mieterhöhungserklärungen, Kündigungen usw.). Im Rahmen der Zweckbestimmung dieses Vertragsverhältnisses ist die Übermittlung von personenbezogenen Daten nach § 28 Abs. 1 Nr. 1 BDSG zulässig. Dem Hauswart obliegt nicht die Kontrolle der Vertragseinhaltung, als Mitarbeiter des Vermieters beschränkt sich seine Aufgabe in der Regel auf Maßnahmen zur Einhaltung der Hausordnung, der „betriebstechnischen“ Wartung und Erhaltung des Hauses und die Reparatur kleinerer Mängel. Zur Erfüllung dieser Aufgaben sind Kenntnisse aus den vertraglichen Beziehungen zwischen Vermieter und Mieter grundsätzlich nicht erforderlich. Insofern findet § 28 Abs. 1 Nr. 1 BDSG hier keine Anwendung. Eine andere Rechtsvorschrift, auf die die Übermittlung von personenbezogenen Mieterdaten aus dem Schriftwechsel zwischen Vermieter und Mieter an den Hausmeister gestützt werden kann, ist nicht ersichtlich.

Wir haben daher empfohlen, dass die Hausmeister die an die Mieter gerichteten Schreiben nicht unverschlossen erhalten. Für eine Bestätigung, dass das Schreiben dem Empfänger zugegangen ist, ist eine Kenntnisnahme vom Inhalt der Schreiben durch den Hauswart nicht erforderlich.

Die Übermittlung von Schriftstücken an einzelne Mieter erfolgt bei den städtischen Wohnungsbaugesellschaften generell in verschlossenen Briefumschlägen, sei es durch die Post, durch Hauswarte oder durch sonstige Boten.

**Mietobergrenzen im Sanierungsgebiet**

*Zur Überprüfung der Mietobergrenzen in einem Sanierungsgebiet bat das zuständige Bezirksamt den Eigentümer eines Mehrfamilienhauses, Kopien der Mietverträge für einzeln benannte Wohnungen zu übersenden.*

Der Bezirk hatte für das betroffene Sanierungsgebiet Obergrenzen für die Mieterhöhung aufgrund von öffentlich geförderten Modernisierungsmaßnahmen beschlossen. Die zuständige Sanierungsverwaltungsstelle wurde damit beauftragt, die Einhaltung dieser Mietobergrenzen zu überwachen und gegebenenfalls durchzusetzen.

Sanierungsrechtliche Genehmigungen nach § 145 BauGB für Objekte in dem Sanierungsgebiet waren für die Eigentümer mit der Auflage verbunden worden, die festgesetzte Mietobergrenze einzuhalten und dies bei der Erstvermietung der Wohnungen gegenüber der Sanierungsverwaltungsstelle durch Vorlage der Mietverträge nachzuweisen. Kommt der Eigentü-

Die Darstellung des Berliner Beauftragten für Datenschutz und Akteneinsicht ist grundsätzlich zutreffend, der Senat weist jedoch darauf hin, dass die an dieser Stelle verwendete Formulierung “Objekte” nicht dem Gesetzeswortlaut des § 144 BauGB entspricht, der den Begriff “Vorhaben” verwendet. Da es sich bei den sanierungsrechtlichen Genehmigungen nach § 145

mer dieser Auflage nicht nach, erfolgt eine Prüfung von Amts wegen. Die Mietparteien werden - unter Hinweis auf den Grund - mit der Bitte angeschrieben, eine Kopie des Mietvertrages zu übersenden. Erst wenn die Mieter auf diese Bitte - und nach Erinnerung - nicht reagieren, werden die dann noch fehlenden Mietverträge beim Eigentümer angefordert.

Das Verfahren ist aus datenschutzrechtlicher Sicht nicht zu beanstanden.

Nach § 138 Abs. 1 Satz 1 BauGB unterliegen Eigentümer und Mieter eines Grundstückes, Gebäudes oder Gebäudeteils innerhalb eines Sanierungsgebiets sowie deren Beauftragte einer umfangreichen Auskunftspflicht gegenüber der Gemeinde hinsichtlich der Tatsachen, deren Kenntnis für die Beurteilung der Sanierungsbedürftigkeit eines Gebiets oder zur Vorbereitung oder Durchführung der Sanierung erforderlich ist.

An personenbezogenen Daten der Betroffenen können insbesondere Angaben zu deren persönlichen Lebensumständen im wirtschaftlichen und sozialen Bereich erhoben werden (§ 138 Abs. 1 Satz 2 BauGB). Hierzu zählen auch Angaben aus bestehenden Mietverträgen (z. B. Name, Vorname der Vertragspartner). Die Auskunftspflichten bestehen parallel nebeneinander. Auch hier gilt jedoch der Grundsatz, dass die Daten vorrangig beim Betroffenen selbst, mit seiner Kenntnis, zu erheben sind. Nur wenn dies aus bestimmten Gründen nicht oder aufgrund besonderer Umstände nur unter erschwerten Bedingungen möglich ist, können die Daten - in Anwendung des Verhältnismäßigkeitsgrundsatzes - bei anderen ebenfalls zur Auskunft verpflichteten Personen (z. B. Eigentümer, Verwalter) erhoben werden. Die Sanierungsverwaltungsstelle versucht, die erforderlichen Daten deshalb zunächst bei den betroffenen Mietern zu erheben. Erst wenn diese nicht reagieren, wird der Eigentümer mit der Bitte um Übersendung der Mietverträge angeschrieben.

Vorliegend umfasst die Auskunftspflicht die für die Überprüfung der Mietobergrenze erforderlichen Daten aus den Mietverträgen. Erforderlich in diesem Sinne sind Angaben zu den Vertragsparteien (Name, Vorname), der Höhe und Zusammensetzung der Miete, der Größe der Wohnung und der zuletzt ergangenen Mieterhöhung im Anschluss an die erfolgte Sanierung. Alle weiteren personenbezogenen Angaben (z. B. Geburtsdaten) können in den Unterlagen unkenntlich gemacht (geschwärzt) werden.

**Der gläserne Restmüll**

*Anlässlich der Einführung der BIOGUT-Sammlung hat die BSR ihre Kunden aufgefordert, sich entweder für die Eigenkompostierung ihres Bioabfalls oder die (kostenpflichtige) Entsorgung in einer BIOGUT-Tonne der BSR zu entscheiden. Sofern die Betroffenen*

BauGB, die mit einer Auflage zur Einhaltung der Mietobergrenzen verbunden wurden, durchweg um Vorhaben im Sinne von § 144 Abs. 1 Nr. 1 in Verbindung mit § 14 Abs. 1 und § 29 BauGB handelt, wäre an dieser Stelle die Verwendung des gesetzeskonformen Begriffs “Vorhaben” korrekt.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

*die Freistellung von der BIOGUT-Sammlung beantragten, sollten sie in dem von der BSR beigefügten Antwortschreiben ihr Einverständnis in eine stichprobenartige Überprüfung ihrer Restmülltonne erklären. Die Kunden befürchteten eine Kontrolle ihres Konsum- bzw. Verbraucherverhaltens.*

Um die Zulässigkeit und Reichweite einer Einwilligung in die Datenverarbeitung bestimmen zu können, kommt es darauf an, wie die betreffende Textpassage aus der Sicht des Empfängers zu verstehen ist. Bei der BIOGUT-Sammlung suggerierte die Formulierung der BSR dem Kunden eine Freiwilligkeit in die Entscheidung zur Datenerhebung (Untersuchung des Restmülls), die tatsächlich nicht gegeben war. Er hatte vielmehr nur die Möglichkeit, zwischen der Bestellung einer BIOGUT-Tonne oder der Eigenkompostierung seines Bioabfalls (einschließlich Überprüfung seines Restmülls) zu wählen.

Die Erklärung entsprach damit nicht den Anforderungen an eine datenschutzrechtliche Einwilligung i.S.d. § 6 Abs. 1 Nr. 3, Abs. 3 Satz 3 BlnDSG. Der Kunde wurde weder in geeigneter Weise über die Bedeutung seiner Erklärung - insbesondere den Verwendungszweck der Daten - aufgeklärt, noch wurde er ausreichend auf die Rechtsfolgen einer Verweigerung der Einwilligung in die Datenverarbeitung hingewiesen.

Unabhängig davon kann die Überprüfung des Restmülls derjenigen Kunden, die sich im Rahmen der BIOGUT-Sammlung für eine Eigenkompostierung ihrer Bioabfälle entschieden haben, auf § 19 Abs. 2 Berliner Betriebegesetz (BerlBG) i.V.m. § 2 Abs. 1 der Verordnung über die Verarbeitung personenbezogener Daten bei der BSR gestützt werden. In § 2 Abs. 1 Nr. 15 dieser Verordnung ist geregelt, dass die Verarbeitung von Daten über die Zusammensetzung des Abfalles zulässig ist.

Unserer Empfehlung, die *Untersuchung des Restmülls nur anlassbezogen* durchzuführen, kommt die BSR insofern nach, dass die standortbezogene, stichprobenartige Sortieranalyse für einzelne Behälterstandorte erst erfolgt, wenn flächenmäßige Sortieranalysen kompletter Fahrzeugladungen aus einem bestimmten Abfuhrgebiet einen Organikanteil von mehr als 20 % ergeben haben. Die stichprobenartige Einzelanalyse erfolgt dabei durch einen Sachverständigen, der das Ergebnis einer Behälternummer zuordnet und der BSR übergibt. Nur die BSR kann die Sortierergebnisse ihren Kunden zuordnen. Die Analysedaten werden nach Abschluss der Einführung der BIOGUT-Sammlung, spätestens nach drei Jahren, von der BSR gelöscht.

Das Verfahren ist datenschutzrechtlich nicht zu beanstanden. Die BSR wird unsere Empfehlung, die Kunden zukünftig schriftlich auf die Rechtsgrundlage, den Zweck der Datenverarbeitung hinzuweisen und umfassend über das Verfahren zu informieren, aufgreifen.

Die BSR haben die Anforderungen des Beauftragten für Datenschutz und Akteneinsicht bereits berücksichtigt und nunmehr auch wie folgt in die Anschreiben an die betroffenen Bürger zum Anschluß an die Biotonne bzw. zur Entscheidung für die Eigenkompostierung aufgenommen:

1. Rechtsgrundlage, auf die sich die Datenverarbeitung stützt;
2. Die Einzelheiten zur Durchführung des Sortierverfahrens.

Darüber hinaus wurden im Anschreiben an die Bürger auch die Informationen zur Überprüfung der Restmülltonnen und dem sich ggf. daraus ergebenden Anschluß an die BIOGUT-Sammlung vollständig von der Entscheidung "BIOGUT oder Eigenkompostierung" getrennt.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

**Fortschreibung des Emissionskatasters Hausbrand**

*Die Schornsteinfeger-Innung von Berlin wurde von der Senatsverwaltung für Stadtentwicklung gebeten, gebäudebezogene Daten (z. B. Kehrbezirkskennung, Postleitzahl, Straße, Hausnummer, Art der Anlage, Nennwärmeleistung in kW, Anzahl der versorgten Wohneinheiten usw.) über die Beheizung von Wohnungen auf elektronischen Datenträgern zu übermitteln. Als Zweck wurde von der Senatsverwaltung die Fortschreibung des Emissionskatasters Hausbrand angegeben.*

Nach § 19 Abs. 1 Nr. 1-5 Schornsteinfegergesetz hat der Bezirksschornsteinfeger in Bezug auf eine Feuerungsanlage Angaben u.a. zum Namen und der Anschrift des Eigentümers, Betreibers (usw.), Art der Anlage einschließlich ihrer technischen Daten und Angaben über ihren Betrieb und Standort aufzuzeichnen. Art und Standort der Feuerungsanlage sind u. a. in dem, für jedes Kalenderjahr zu führenden, Kehrbuch einzutragen. Diese vom Bezirksschornsteinfeger zu erhebenden Angaben entsprechen im Wesentlichen dem von der Senatsverwaltung erbetenen Datenkatalog. Er darf die Daten aus seinen Aufzeichnungen nach § 19 Abs. 3 Schornsteinfegergesetz an öffentliche Stellen übermitteln, soweit das für die Erfüllung seiner Aufgaben, die Bekämpfung der Luft-, Boden- und Gewässerverschmutzung, die rationelle Energieverwendung, die Bauaufsicht oder die Brandbekämpfung erforderlich ist.

Das ist der Fall. Die Datenübermittlung soll zum Zweck der Fortschreibung des Emissionskatasters Hausbrand genutzt werden. Das Kataster ist Teil des Emissionskatasters nach § 46 Bundes-Immissionsschutzgesetz (§ 1 Abs. 1 Ausführungsgesetz zum Bundes-Immissionsschutzgesetz). Es dient der Aufzeichnung von Luftverunreinigungen und damit der Bekämpfung von Luftverschmutzung.

Es bestehen somit keine datenschutzrechtlichen Bedenken; die Datenübermittlung durch die Schornsteinfeger-Innung an die Senatsverwaltung für Stadtentwicklung ist zulässig. Zur Klarstellung und insbesondere zur Transparenz in der Rechtsanwendung haben wir jedoch empfohlen, zum Zweck der Fortschreibung des Emissionskatasters Hausbrand für die Schornsteinfeger-Innung eine Befugnis zur Übermittlung von personenbezogenen Daten an die Senatsverwaltung für Stadtentwicklung in das Ausführungsgesetz zum Bundes-Immissionsschutzgesetz bzw. die Verordnung über die Verarbeitung personenbezogener Daten im Zusammenhang mit nicht genehmigungsbedürftigen Anlagen aufzunehmen.

Die vom Berliner Beauftragten für Datenschutz und Akteneinsicht ausgesprochene Empfehlung, in das Ausführungsgesetz zum Bundes-Immissionsschutzgesetz oder die Verordnung über die Verarbeitung personenbezogener Daten im Zusammenhang mit nicht genehmigungsbedürftigen Anlagen die Schornsteinfeger-Innung explizit aufzunehmen, wird zurzeit von der zuständigen Senatsverwaltung geprüft. Es besteht jedoch aus Sicht des Senats kein dringender Handlungsbedarf, da eine Fortschreibung des Emmissionskatasters Hausbrand nicht vor dem Jahre 2004 erforderlich ist. Bei weiterem Rückgang der kohlebeheizten Wohnungen wird es voraussichtlich nicht nötig sein, für die zukünftige Datenerhebung eine Befragung der Schornsteinfeger zu wiederholen.

## 4.5 Wissen und Bildung

### 4.5.1 Wissenschaft und Forschung

**Datennetze für die medizinische Forschung**

Man erinnere sich an solch euphorische Meldungen vor einem Jahr wie: „Genetischer Code des Menschen geknackt“. Auch wenn diese Meldungen verkannten, dass die lückenlose Auflistung mit einer fast 100%igen Genauigkeit noch nicht vorlag, war dieser Erfolg des *internationalen Human-Genom-Projekts (HGP)* nur dadurch möglich, dass 16 wissenschaftliche Zentren in Amerika, Europa und Asien kooperierten, die Aufgaben untereinander abstimmten und auf einheitliches genetisches Material zurückgreifen konnten, welches nicht von einem einzelnen Individuum stammte, sondern aus überlappenden Teilen der DNA zahlreicher Menschen hergestellt wurde. Neue Ergebnisse bei der Feststellung der Sequenz aller schätzungsweise 3 Milliarden Basenpaare wurden täglich für jeden abrufbar im Internet bereitgestellt. Durch diesen Wissenstransfer war eine erhebliche Beschleunigung des Projektes möglich geworden.

Solche Methoden des Wissenstransfers sind aber auch unabdingbar bei der Erforschung vieler Krankheiten. Um das Zusammenspiel verschiedenster Faktoren beispielsweise in der Krebsforschung und bei psychiatrischen Erkrankungen wie der Depression zu untersuchen, müssen klassische Mediziner, Humangenetiker, Pharmakologen, Pathologen oder Public-Health-Mediziner kooperieren. Es ist auch erforderlich, dass sie auf einen möglichst großen Datenbestand über Erkrankte und ggf. auch über potenziell für diese Krankheit veranlagte Verwandte von ihnen zurückgreifen können.

1997 wurde vom Bundesministerium für Bildung und Forschung der Wettbewerb „*Kompetenznetzwerke für die Medizin - MedNet*“ ausgeschrieben, um den Wissenstransfer aus der Grundlagenforschung in die Anwendungsforschung zu verbessern. Gegenwärtig sind 23 große Forschungsverbünde im Entstehen, die fast 200 Einzelforschungsvorhaben umfassen. Um für diese Forschungsverbünde tragfähige Vernetzungskonzepte zu entwickeln, erhielt das Berliner Frauenhofer-Institut Software- und Systemtechnik (ISST) den Auftrag, eine Grundlage für Telematikplattformen zu schaffen, die den Forschern hilft, durch die Nutzung modernster Informationstechnologien den angestrebten Wissenstransfer zu beschleunigen. Bereits Ende 1998 bat uns das ISST um beratende Begleitung, da viele Berliner Forschungseinrichtungen in die Kompetenznetze eingebunden werden.

Auch die vernetzte Forschung hat dafür Sorge zu tragen, dass personenbezogene Daten über die Gesundheit nur mit Einwilligung der Betroffenen übermittelt und genutzt werden dürfen, es sei denn, sie sind anonymisiert. *Anonymisierte Daten* wiederum erlauben es

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

dem Forscher lediglich, bereits erhobene Daten auszuwerten, nicht aber zusätzliche Informationen beispielsweise auch bei den Betroffenen selbst und mit deren Einwilligung zu erheben. Ein weiteres Problem ist, dass bei komplexen Forschungsansätzen die Einwilligungserklärungen nicht bis ins Detail die künftigen Verwendungsmöglichkeiten für die Forschung offen legen können, da diese häufig zum Zeitpunkt der Einwilligung noch unbekannt sind.

Für die Mehrzahl der Forschungsnetze bietet es sich an, die Möglichkeiten der *Pseudnonymisierung* zu nutzen. Dabei werden die Identifikationsdaten, wie Name und Geburtsdatum, durch Pseudonyme ersetzt, die es erlauben, dass für den Forscher selbst sich die medizinischen Angaben als anonymisiert darstellen. Wird nunmehr zwischen dem Forscher, der pseudonymisierte Daten erhält und der den Patienten behandelnden Einrichtung, die pseudonymisiert Daten liefert, ein Datentreuhänder eingeschaltet, so kann gesichert werden, dass nur nach gesicherten Regelungen eine Aufhebung der Pseudonymisierung und ein Rückbezug auf den Patienten möglich ist.

Grob skizziert ist der geplante Ablauf wie folgt:

Der behandelnde Arzt erläutert die Ziele des Kompetenznetzwerkes, versorgt den Patienten mit Informationsmaterial und nimmt seine schriftliche Einwilligung entgegen, die in den Patientenunterlagen dokumentiert wird. Der Arzt lässt sich unter Verwendung des Namens und anderer unmittelbar personenbezogener Merkmale von einem zentralen oder dezentralen Pseudonymisierungsdienst ein erstes Pseudonym bereitstellen. Die medizinischen Daten werden dann pseudonymisiert an den Datentreuhänder elektronisch versandt. Dieser kann die medizinischen Daten jedoch nicht lesen, ersetzt aber das erste Pseudonym durch ein zweites. Die medizinischen Daten werden von ihm an den Datenbank- bzw. Registerrechner des Kompetenznetzwerkes durchgereicht und dort unter dem zweiten Pseudonym entschlüsselt. Das zweite Pseudonym wird durch eine fortlaufende Nummer ersetzt und gesondert verwahrt. Vorausgesetzt, die medizinischen Daten selbst enthalten keine unmittelbar auf die Person deutenden Angaben, stellen sich diese Angaben für den Forscher somit als faktisch anonymisiert dar.

Ein wissenschaftliches Gremium des Kompetenznetzwerkes (Konsenskonferenz) entscheidet über die Nutzung der medizinischen Daten für die einzelnen Forschungsprojekte, über eine Aufspaltung in vertiefte medizinische Daten und einen Minimaldatenbestand, nachdem für die Forscher Vorauswahlen möglich sind. Ergibt sich dann die Notwendigkeit für den Forscher, mit dem Patienten in Kontakt zu treten, so kann er dies nach Genehmigung durch die Konsenskonferenz in einem rechtlich-vertraglich geregelten Verfahren über den Datentreuhänder und die Be-

Die Ausführungen zum Datenschutz und zur Pseudonymisierung erscheinen plausibel. Allerdings ist mit diesem Verfahren offenkundig ein erheblicher Verwaltungsaufwand verbunden. Inwieweit dieser sich nachteilig auf die Forschung auswirkt und ob andere Gründe gegen ein solches Verfahren sprechen, kann erst nach Beteiligung betroffener Forschungseinrichtungen beurteilt werden. Diese Beteiligung sollte vor Gesetzesänderungen (Datenschutzgesetz) unbedingt erfolgen.

handlungseinrichtung tun. Der Patient entscheidet dann frei darüber, ob weitere Aufgaben für dieses spezielle Forschungsanliegen erhoben und genutzt werden dürfen.

Auch die *Rechte der Patienten auf Auskunft und Widerspruch* einschließlich einer Löschung der gespeicherten Forschungsdaten sind gut durchsetzbar, da der Patient unter Nutzung der Erstpseudonymisierung unmittelbar beim Datentreuhänder seine Rechte geltend machen kann. Er braucht somit den ihn behandelnden Arzt von seinem Widerspruch nicht zu informieren. Der Datentreuhänder selbst ist, insbesondere wenn diese Aufgabe von einem Anwalt oder Notar ausgeübt wird, vertraglich und standesrechtlich dem Patienten verpflichtet. Dieses Verfahren erlaubt auch bei Zweifeln an der wissenschaftlichen Redlichkeit von Forschern, die Ergebnisse im Rahmen der Selbstkontrolle der Wissenschaft zu überprüfen, ohne dass beim Forscher selbst die unmittelbar auf die Person zeigenden Daten für einen langen Zeitraum hinterlegt werden müssen.

Die beim Treuhänder/Anwalt oder Notar hinterlegten Anonymisierungsdaten unterliegen einer besonderen Schweigepflicht und sind gegen eine Kenntnisnahme durch Dritte und auch gegen eine etwaige Beschlagnahme gesetzlich geschützt.

Am Weitesten fortgeschritten sind bei der Umsetzung eines solchen Modells gegenwärtig die Arbeiten am *Kompetenznetz Parkinson* mit Sitz in Hessen. Der Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder diskutiert mit Vertretern verschiedener Forschungsnetze die speziellen Aspekte dieses Netzes sowie mit dem Koodinierungsbüro der Telematikplattform am Frauenhofer-ISST die datenschutzrechtlichen Anforderungen verschiedener Konzepte.

Die Synergieeffekte bei der datenschutzrechtlichen Beratung von Forschungsprojekten wurden im vergangenen Jahr besonders deutlich. Seit vielen Jahren begleiten wir das Projekt „Qualitätssicherung in der Nierenersatztherapie - *QuaSiNiere*“, das gegenwärtig ein mehrstufiges Chipkarten-gestütztes, internetbasiertes Verschlüsselungs- und Pseudonymisierungsverfahren erprobt. Die dort gewonnenen rechtlichen und technischen Erkenntnisse flossen sowohl in die Beratung des ISST als auch anderer Einzelprojekte, wie beispielsweise des am Deutschen Herzzentrum und der Charité im Entstehen begriffenen nationalen Registers für Patienten mit angeborenen Herzfehlern, ein. Auch für dieses Register soll das *Treuhänderverfahren* genutzt werden.

Zwischen den Datenschutzbeauftragten von Bund und Ländern besteht Einvernehmen darüber, dass *Forschungsregister*, die sensitive Daten im Sinne der Datenschutzrichtlinie - wie dies beispielsweise Daten über Erkrankungen sind - personenbezogen vorhalten,

im Regelfall eine *spezialgesetzliche Grundlage für die Registerführung* erfordern. Es müssen besondere Rechtfertigungsgründe bestehen, wenn derartige Daten unverschlüsselt verarbeitet werden sollen, statt anonymisiert oder pseudonymisiert zu werden. Als Beispiel für solche Rechtsvorschriften sind die Landeskrebsregistergesetze anzusehen. Der Aufbau personenbezogener Register ausschließlich auf der Grundlage einer Einwilligung der Betroffenen ist auch nicht datenschutzgerecht, weil für den Betroffenen nicht übersehbar ist, wer welche Daten wann und wo für welche Zwecke verwenden wird. Die Charakteristik von Registern ist gerade ihre künftig vielfältige, aber noch unbestimmte Nutzung und damit nicht eine unmittelbare Zweckbindung. Verzichtbar sind aber spezialgesetzliche Regelungen, wenn die Daten, wie oben dargestellt, anonymisiert oder pseudonymisiert gespeichert werden, und weitere Verfahrensvorschriften, wie beispielsweise die *Einrichtung von Datentreuhändern*, ihre Reidentifizierung verhindern. Grundsätzlich soll bei den Registern der Kompetenznetzwerke die Einwilligung der Betroffenen mit flankierenden Datenschutzmaßnahmen so verbunden werden, dass sich der zu beforschende Datenbestand für den Forscher als anonymisiert darstellt. Sind diese Verfahrensvorschriften für den Betroffenen transparent, so – wie die Erfahrungen der vergangenen Jahre zeigen – gibt es auch nur wenig Probleme, die Einwilligung einzuholen.

Die gegenwärtige Praxis der Forschungsfinanzierung kann in Zukunft dazu führen, dass nach dem Auslaufen der Förderung von Kompetenznetzwerken die Kontinuität der Registerführung nicht mehr, wie ursprünglich gegenüber dem Betroffenen versichert, gewahrt werden kann. Aus datenschutzrechtlicher Sicht sollten frühzeitig rechtlich verbindliche Versicherungen gegeben werden, die bei finanziellen Engpässen „herrenlose“ Sammlungen medizinischer Daten verhindern. Ein Weg wäre, dass durch das Bundesforschungsministerium eine Bund-Länder-Institution geschaffen wird, die als gemeinsame Einrichtung die Daten im öffentlichen Bereich belässt und archiviert sowie der künftigen Forschung möglicherweise erneut bereitstellen kann.

**Novellierung der Forschungsklausel im Berliner Datenschutzgesetz**

Parallel zur anstehenden Novellierung des Berliner Hochschulgesetzes möchten wir diese Erfahrungen auch berücksichtigen und schlagen daher eine umfassende Neufassung des § 30 Berliner Datenschutzgesetz (BlnDSG) - Datenverarbeitung für wissenschaftliche Zwecke - vor. Die bisherigen Festlegungen, die insbesondere als so genanntes Forschungsprivileg den Rechtsrahmen dafür setzten, unter welchen Umständen Forscher auch ohne Einwilligung der Betroffenen personenbezogene Daten nutzen dürfen, sollten ergänzt werden um die Möglichkeiten der Pseudonymi-

Die angeregte Novellierung des § 30 Berliner Datenschutzgesetz ist vorbehaltlich der vorherigen Beteiligung betroffener Forschungseinrichtungen zu unterstützen. § 30 sollte ergänzt werden um: Pseudonymisierung der Daten, Nutzung von Datentreuhändern, Verpflichtung zur Verschwiegenheit.

Im Rahmen der Selbstkontrolle redlichen wissenschaftlichen Verhaltens ihres wissenschaftlichen Personals soll den Hochschulen im Zuge der allgemein anstehenden Novellierung des Berliner Hochschulge-

sierung, der Nutzung von Datentreuhändern, aber auch um die Möglichkeit, Forscher besonders zur Verschwiegenheit zu verpflichten. Durch die Einbeziehung unabhängiger Treuhänder kann damit auch die Selbstkontrolle der Wissenschaft oder für spätere Forschungszwecke eine Depseudonymisierung unter bestimmten Umständen erlaubt werden. Mit der Befugnis, pseudonymisierte Daten zum Zwecke der wissenschaftlichen Selbstkontrolle datenschutzgerecht nutzen zu dürfen, korrespondiert eine solche Vorschrift mit einer entsprechenden Novellierung des Berliner Hochschulgesetzes, die den Hochschulen den Erlass von Regelungen zur Sicherung guter wissenschaftlicher Praxis auferlegt.

**Neue Probleme bei der Genomforschung**

Auch in Berlin entstehen auf dem Gebiet der Genomforschung nicht nur Forschungseinrichtungen, sondern auch Gentechnologie-Firmen, die zunächst sehr viele medizinische „Rohdaten“ personenbezogen sammeln, um die inhaltlichen Zusammenhänge und damit auch die Funktionsweise im Genom erkennbar zu machen. Neue Forschungsansätze führen dabei zu datenschutzrechtlich veränderten Konstellationen. In der Vergangenheit wurde häufig von bereits erkrankten Personen ausgegangen und nach verschiedensten Therapiemöglichkeiten gesucht, die ausgebrochene Krankheit zu bekämpfen. Resultierend aus ersten Ergebnissen der genetischen Forschung tritt die Erforschung der Möglichkeiten zur Verhinderung von Erkrankungen stärker in den Vordergrund.

Für die Forscher heißt dieses, dass im genetischen wie im realen Umfeld der erkrankten Person nach Risikofaktoren und Risikoträgern gesucht wird. Bei solchen Forschungsansätzen steht aber nicht das reine Sammeln von Blut und daraus extrahierter DNA im Vordergrund, sondern die *Analyse des genetischen Risikos in der Familie, der Umweltfaktoren und Lebensgewohnheiten* sowie anderer Risiken. Bei solchen Forschungsansätzen kann eine hohe Mitwirkungsbereitschaft der betroffenen erkrankten und nichterkrankten Familienangehörigen bzw. Lebenspartner dadurch erreicht werden, dass die Ergebnisse unmittelbar auch Nichterkrankten helfen können, bestehen-

setzes eine generelle Satzungsbefugnis zur Sicherung guter wissenschaftlicher Praxis eingeräumt werden. Die Einzelheiten dazu (hinsichtlich Verfahren, Zuständigkeiten und eventuellen Sanktionen) sollen den Regelungen in den jeweiligen Hochschulsatzungen überlassen bleiben. Die für die Hochschulen in diesem Zusammenhang zu beachtenden datenschutzrechtlichen Aspekte sollen durch die Neufassung der Forschungsklausel in § 30 BlnDSG abgedeckt werden. Insoweit hat bereits eine Verständigung auf Arbeitsebene zwischen dem Berliner Beauftragen für Datenschutz und Akteneinsicht und der für die Hochschulen zuständigen Senatsverwaltung stattgefunden. Aufgrund der Bedeutung der Vorschrift und des daraus resultierenden weiteren Abstimmungsbedarfs ist eine Neufassung des § 30 BlnDSG im Rahmen der anstehenden Novellierung des Berliner Datenschutzgesetzes aus Zeitgründen jedoch unwahrscheinlich. Hinsichtlich der Einzelheiten bei der Neufassung der Forschungsklausel wird darauf zu achten sein, dass die datenschutzrechtlichen Vorkehrungen auch unter Kosten- und Praktikabilitätsgesichtspunkten für die Hochschulen handhabbar bleiben, damit diese ihrer im Rahmen der internationalen Wettbewerbsfähigkeit notwendigen Verpflichtung, im Zweifelsfall die Redlichkeit der in ihrem Bereich stattfindenden Forschung zu überprüfen und nachzuweisen, nachkommen können.

de Risiken zu reduzieren. Mit solchen Erkenntnissen beginnt jedoch die klassische Trennung zwischen „Gesund“ und „Krank“ zu schwinden. Im Ergebnis der Untersuchung „gesunder“ Probanden werden sich also früher oder später Krankheitsdispositionen herausstellen. Der betroffene Proband kann natürlich frei entscheiden, ob er über diese Disposition informiert werden möchte oder nicht. Inwieweit aber heutige Anforderungen an eine Einwilligungserklärung den sich gravierend verändernden Dimensionen der Erkenntnisse aus der Genomforschung und der damit möglichen Aussagen über die „beforschte“ Person entsprechen, muss neu diskutiert werden.

Da man heute damit rechnet, dass auch geringe Mengen von Blutproben für die genetische Forschung für vielfältigste genetische Projekte über 20 und mehr Jahre hinweg genutzt werden können, ohne verbraucht zu sein, sollen Daten solcher Proben mit Krankheitsgeschichten und Abstammungsdaten verbunden werden. Dies führt zu Persönlichkeitsprofilen ungeahnter Tiefe einschließlich der Aussagen über Verwandte. Selbst wenn *genetische Proben* selbstverständlich nichts über den konkreten Lebensweg einer Person sagen, so werden doch in einigen Jahren nicht nur Kenntnisse und virtuelle Abbilder des Äußeren einer Person möglich sein, sondern auch Aussagen über Veranlagungen zu bestimmten Charaktereigenschaften und sozialen Verhaltensweisen.

Inwieweit solchen potenziellen Gefährdungen der Persönlichkeitsrechte vom Gesetzgeber eine Grenze gesetzt werden kann, ist auch zwischen den Datenschutzbeauftragten intensiv zu diskutieren. Die 60. Konferenz der Datenschutzbeauftragten von Bund und Ländern hat daher beschlossen, eine Arbeitsgruppe zu den datenschutzrechtlichen Konsequenzen der Entschlüsselung des menschlichen Genoms zu bilden. Diese Arbeitsgruppe wird sich mit den bereits vorhandenen Gesetzgebungsaktivitäten und mit den jetzt entstehenden Technologien zur beschleunigten Auswertung genetischer Informationen wie beispielsweise mittels Genchip befassen.

**Datenschutzgerechte Forschung**

Wie in jedem Jahresbericht wollen wir auch diesmal eine Auswahl von Forschungsprojekten kurz vorstellen, für die es mit zum Teil erheblichem Beratungsaufwand gelang, bei Wahrung der informationellen Selbstbestimmung der Betroffenen den Forschern einen optimalen Datenzugang zu ermöglichen.

Von Forschern befragt wurden:

- Kinder und Jugendliche sowie Eltern zur gesundheitlichen Situation,
- Schüler und Eltern zum so genannten Expressabitur,
- Schüler und Lehrer zum kooperativen Lernen,

- Jugendliche, deren Eltern, Lehrer und Freunde zu typischen Lebenswegen und Zukunftsvorstellungen,
- behinderte Jugendlichen zum Umgang mit sexueller Selbstbestimmung und sexueller Gewalt in Wohneinrichtungen,
- Kinder und Jugendliche zum Freizeitverhalten und Freizeitangebot im einem Berliner Bezirk,
- an der Wirbelsäule Verletzte zu Ergebnissen der ambulanten orthopädisch-traumatologischen Rehabilitation,
- Krebskranke zum Medienthema Krebsmedizin,
- Schüler, Lehrer und Eltern im Rahmen einer Evaluation des gesamten Schulbetriebes,
- Schüler zu gesundheitsfördernden Aktivitäten der Schule,
- ältere Menschen zu ihrer persönlichen Mobilität,
- Mieter zur Wohnfeldarchitektur aus der Sicht der Nutzer,
- Schwangere zu ihren Gesundheitsrisiken einschließlich einer individuellen Analyse der Risiken (Projekt BabyCare),
- Absolventen der Erziehungswissenschaften zu ihrer beruflichen Mobilität.

Akteneinsicht wollten Forscher nehmen in Unterlagen über:

- drohenden Wohnungsverlust infolge Mietschulden, anhand von Unterlagen der sozialen Wohnhilfe und der Wohnungsbaugesellschaft,
- die Arbeit des Berliner Krisendienstes zur psychosozialen Versorgung,
- die Geschichte von Kinder- und Jugendsportschulen in der DDR,
- die heutigen Lebensumstände von früheren Antragstellern auf Ausreise aus der DDR,
- Wiedergutmachung für verfolgte Homosexuelle in Ost- und Westdeutschland bis 1970,
- Tierfortnahmen durch das Veterinärwesen nach dem Tierschutzgesetz.

**Studentenausweis als Chipkarte rechtmäßig**

In die *Studentendatenverordnung* wurde im vergangenen Jahr auf unsere Forderungen hin eine *Regelung zu den Studienausweisen* aufgenommen. Diese Regelung differenziert nach einem für jedermann optisch lesbaren Teil und der Möglichkeit, diesen Ausweis auch als mobiles personenbezogenes Datenverarbeitungssystem (multifunktionale Chipkarte) zu nutzen. Mit diesem Ausweis können neben der hochschulbe-

zogenen Nutzung künftig Funktionen weiterer öffentlicher wie nicht-öffentlicher Stellen ausgeführt werden, wenn die Freiwilligkeit dieser Nutzungen sichergestellt ist. Für die Studierenden wurde das Recht festgeschrieben, jederzeit Auskunft über die durch dieses mobile Datenverarbeitungssystem aktivierten personenbezogenen Speicherungen zu verlangen. Die Kommunikation muss für die nutzende Person erkennbar sein. Einen „gläsernen Studenten“[87] wird es damit nicht geben[88].

**Prüfungsbelastungen als Evaluationskriterium**

Durch die Hochschulverträge des Landes Berlin mit den Hochschulen, die auch deren finanziellen Rahmen absteckten, wuchs das Bedürfnis, zum Zweck der Qualitätsverbesserung von Lehre und Forschung verschiedene Evaluationsmaßnahmen durchzuführen. Zur Bewertung der Qualität von Lehre und Forschung wurde daher gefordert, die reale Prüfungsbelastung der Hochschullehrerinnen und Hochschullehrer zu berücksichtigen. Den Hochschulen liegen aber über diese Belastungen keine unmittelbaren Informationen vor, da diese Daten lediglich bei den Prüfungsämtern anfallen. Weder das Hochschulgesetz noch die Rechtsvorschriften für die Prüfungsämter enthalten eine Erhebungs- bzw. Übermittlungsbefugnis für diese als Personaldaten einzustufenden Angaben. Nach einer mit den betreffenden Hochschulen, insbesondere deren behördlichen Datenschutzbeauftragten geführten Diskussion wurde ein Vorschlag unterbreitet, der sowohl eine Erhebungs- und Übermittlungsbefugnis als auch eine Zweckbindung umfasst.

Im Rahmen der Hochschulverträge mit dem Land Berlin haben die Hochschulen die Verpflichtung, sich umfassenden Evaluierungsmaßnahmen auch im Bereich der Lehre zu unterziehen. Ein Kriterium ist dabei die Ermittlung der Prüfbelastung der einzelnen Hochschullehrer bzw. der Bereitschaft der dafür zuständigen Dozenten zur Teilnahme an Prüfungen. Die entsprechenden Ergebnisse können bei der Finanzausstattung der Hochschulen bzw. der einzelnen Bereiche innerhalb der Hochschulen Berücksichtigung finden. Auch im Hinblick auf die sich anbahnende Neustrukturierung der Hochschullehrerbesoldung mit der (bundesrechtlich) unter anderem geplanten Einführung von sog. Leistungszulagen kann dieser Punkt Bedeutung erlangen. Dies betrifft auch die Teilnahme an Staatsprüfungen, d.h. solchen Prüfungen, die nicht von den Hochschulen selbst, sondern von staatlichen Prüfungsämtern abgenommen werden.

Auf der Grundlage des im Datenschutzbericht erwähnten Vorschlags soll daher bei der anstehenden Gesamtnovellierung des Berliner Hochschulgesetzes eine Regelung verankert werden, die den Bedürfnissen der betroffenen Hochschulen zur diesbezüglichen Datenerhebung bei den staatlichen Prüfungsämtern Rechnung trägt. Die dazu korrespondierende Datenübermittlungsbefugnis seitens der staatlichen Prüfungsämter müßte allerdings in die entsprechenden, die Staatsprüfungen regelnden Ausbildungsgesetze (z.B. Juristenausbildungsgesetz oder Lehrerbildungsgesetz) eingefügt werden.

**4.5.2 Schule und Sport**

Mit Beginn des Schuljahres 2000/2001 ist die von uns seit Jahren angemahnte *Verordnung über die Sonderpädagogische Förderung* endlich in Kraft getreten[89]. Die mit dieser Rechtsvorschrift korrespondierende Schuldatenverordnung wurde leider nicht zeitgleich verabschiedet, obwohl wir bereits im Dezember 1999 einen Änderungsvorschlag unterbreiteten. Es bedurfte

Die Schuldatenverordnung soll noch in diesem Schuljahr erlassen werden.

[87] JB 1997, 4.5.1

[88] JB 1998, 4.5.1

[89] GVBl. S. 371

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

zur Beschleunigung erst eines Beschlusses des Unterausschusses des Abgeordnetenhauses. Der im September vorgelegte Entwurf der Senatsverwaltung für Schule, Jugend und Sport berücksichtigte im Wesentlichen alle von uns gegebenen Hinweise und Anregungen. Wir erwarten, dass die Änderungen noch im Schuljahr 2000/2001 rechtswirksam werden können.

**Schulen - nunmehr im Netz**

Die Skizzierung der vielfältigen möglichen Probleme bei der Internet-Nutzung durch die Berliner Schulen im Jahresbericht 1999[90] führte dazu, dass durch das Landesschulamt für die dem Amt direkt unterstellten Oberstufenzentren eine *Musterbenutzerordnung* erarbeitet wurde. Parallel dazu hatten wir uns gegenüber dem Landesschulamt und der Senatsverwaltung für Schule, Jugend und Sport bereit erklärt, ein Rundschreiben zu datenschutzrechtlichen Aspekten der Internet-Nutzung für alle Berliner Schulen zu verfassen. Zusammenfassend ergab die rechtliche Prüfung, dass die Schule fast keine datenschutzrechtlichen Probleme hat, wenn sie die Teledienste des Internets nur ausschließlich für schulische Zwecke nutzt. Öffnet sie sich hingegen auch einer privaten Nutzung, beispielsweise nachmittags in Form von Internet-Cafés, so entsteht zwischen der Schule und den Schülern bzw. Lehrern ein Anbieter-Nutzer-Verhältnis. Die Regelungen des Teledienstegesetzes bzw. Teledienstedatenschutzgesetzes bilden dann den rechtlichen Rahmen. Wird die Schule darüber hinaus durch eigene Internet-Angebote als Schule selbst oder für einzelne Schüler, Lehrer oder Gruppen zum Internet-Anbieter, so sind dieses rechtlich Mediendienste und die Schule steht in der Verantwortung zu prüfen, dass die Veröffentlichungen rechtmäßig sind.

Auch wenn die rechtlich klarste Situation für die Schule darin besteht, keine eigenen oder fremden Angebote zu veröffentlichen und lediglich den Internet-Zugang für schulische Zwecke zu nutzen, dürfte dies wohl kaum den Erwartungen entsprechen, die an die Ausstattung der Schulen mit moderner Informationstechnik gestellt werden. Sollen die Schüler mit einem verantwortlichen Umgang mit modernen Informationstechniken vertraut gemacht werden, so ist dies kaum mit einer Reduzierung der Nutzungsmöglichkeit vereinbar. Der Unterausschuss Datenschutz hat daher gefordert, dass der Erlass von Nutzerordnungen durch Schulen mit Internet-Anschlüssen umgehend durchzusetzen ist.

Eine Empfehlung für eine Benutzerordnung, die den Umgang mit dem Internet für private und schulische Nutzung regelt, wird von der "Beratungsstelle für Informationstechnik und Computereinsatz in der Berliner Schule (bics)" zur Zeit erarbeitet. Rechtliche Hinweise zur Erstellung von Internet-Seiten befinden sich bereits auf dem Berliner Bildungsserver sowie auf den Webseiten der bics.

**Deutsche Sprache - schwere Sprache**

*Ein Oberstufenzentrum in Berlin: Alljährlich im Oktober sinniert Studienrat L. über die Möglichkeiten für die Schülerstatistik, bei seinen Berufsschülern zu erfahren, wer von ihnen deutscher oder nichtdeut-*

[90] JB 1999, 4.5.2

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

*scher Herkunftssprache ist. Die Schülerpersonalblätter enthalten derartige Informationen nicht. Kontakt zu den Eltern besteht bei diesen jungen Erwachsenen auch nicht mehr. Bei René, Mike und Andrej hegt er den Verdacht, dass zu Hause möglicherweise nicht deutsch gesprochen wird, aber soll er sie deshalb vor versammelter Klasse danach befragen - und wenn: Würde er eine ehrliche Antwort bekommen? Auch eine weitere Fragestellung der Schülerstatistik ist nur schwer zu beantworten. So soll erhoben werden, wieviele Schüler in den „westlichen" oder in den „östlichen" Bezirken wohnen. Dies ist nur durch ein akribisches Studium des Stadtplanes beantwortbar. Postleitzahlen nehmen bekanntlich auf die frühere Mauer auch keine Rücksicht mehr.*

Soll die Berliner Schule ihrer Unterrichts- und Erziehungsaufgabe gerecht werden, ist es unstrittig, dass Schüler einer nichtdeutschen Herkunftssprache oft einer besonderen Förderung bedürfen, insbesondere wenn sie die deutsche Sprache gar nicht oder nur so wenig beherrschen, dass sie dem Unterricht nicht oder nicht ausreichend folgen können. § 35 a Abs. 4 Schulgesetz für Berlin (SchulG) sieht bei der Aufnahme solcher Schüler in die Berliner Schule vor, die Kenntnisse in der deutschen Sprache festzustellen. Damit dürfte auch die statistische Erfassung der Anzahl der Schüler nichtdeutscher Herkunftssprache in der Grundschule und in der Sekundarstufe I insbesondere bei einem engen Kontakt mit den Eltern durch den Lehrer nur wenig problematisch sein. Bei den acht bis zwölf wöchentlichen Unterrichtsstunden an der Berufsschule hingegen ist eine solche statistische Größe kaum zu erheben. Wir regten an, im Bereich der Berufsschulen, für den ohnehin kaum eine sprachbedingte Förderung erfolgt, ein anderes, aber geeignetes Merkmal - wie die Sprachkenntnisse in Deutsch im Zusammenhang mit der Fähigkeit, dem Unterricht folgen zu können - abzufragen und ggf. durch eine Selbsteinschätzung der betroffenen Schüler zu ergänzen. Ob eine solche Datenerhebung zu einer Ergänzung der Schuldatenverordnung führen muss, hängt vom Ergebnis der fachlichen Diskussionen in der Senatsschulverwaltung und im Landesschulamt ab. Die Senatsverwaltung für Schule, Jugend und Sport sagte im Weiteren zu, ab dem Schuljahr 2001/2002 nicht mehr die Anzahl von Schülern mit Wohnort in den westlichen bzw. östlichen Bezirken zu erfragen. Durch die Bezirksreform dürfte auch dieses Datum kaum noch feststellbar sein.

*Zum Elternsprechtag bekommen die Eltern vom Klassenlehrer offeriert, dass die Grundschule ihrer Tochter für die Sekundarstufe I eine, wenn auch schwache Empfehlung zum Gymnasium aussprechen wird. Auf der einige Tage später folgenden Zeugniskonferenz ergibt die Abstimmung jedoch eine Realschulempfehlung. Die Eltern werden zunächst nicht informiert und zur Zeugnisausgabe erhält die Schülerin nicht*

Die Länder haben sich in dem Unterausschuss „Schuldaten" der KMK verständigt und vereinbart, in den jeweiligen Ländern ein Minimaldatenprogramm zu erheben und die erhobenen Daten den jeweiligen statistischen Landesämtern bzw. dem Statistischen Bundesamt zur Verfügung zu stellen. Diese Daten dienen zur Koordinierung und der Vereinheitlichung der Beschulung ausländischer Schülerinnen und Schüler: z.B. als Planungsgrundlage für geeignete Maßnahmen der schulischen Betreuung, für demografische Analysen, für OECD-Studien etc.

Das Recht zur Erhebung und Speicherung der Staatsangehörigkeit einer Schülerin oder eines Schülers im berufsbildenden Bereich ergibt sich aus den §§ 1 Abs. 5 und 3 i.V.m. § 2 Abs. 2 SchuldatenVO. Danach darf in das Schülerpersonalblatt, das an berufsbildenden Schulen den Schülerbogen ersetzt, ausdrücklich die Staatsangehörigkeit aufgenommen werden.

Bei der Prüfung einer Änderung wird der BlnBDA in den Diskussionsprozess eingebunden.

*nur die an die Eltern gerichtete Empfehlung, sondern vor der gesamten Klasse werden die Empfehlungen für alle Schüler verlesen.*

Dass in einem solchen Fall die Schülerin verstört nach Hause kommt, bedarf keiner weiteren Erklärung. Übereinstimmend mit dem Landesschulamt stellten wir fest, dass es für die *Praxis, Oberschulempfehlungen vor der Klasse zu verlesen*, im Unterschied zum Verlesen von Noten aller Schüler[91], keine Rechtsgrundlage gibt. Im Unterschied zu den einzelnen Noten oder dem Zeugnis ist die Oberschulempfehlung kein Instrument, mit dem die Lehrer die Leistungen der Schüler gemäß ihrer fachlichen Ausbildung und in eigener Verantwortung zu beurteilen haben. Nach § 29 Abs. 2 SchulG obliegt die Wahl zwischen den Oberschulzweigen den Erziehungsberechtigten des Schülers. Zuvor hat eine Beratung der Erziehungsberechtigten durch den Klassenlehrer oder Schulleiter zu erfolgen und der Schüler ist zu hören. Damit wird deutlich, dass Adressat der Oberschulempfehlung die Erziehungsberechtigten und keinesfalls die Schüler der gesamten Klasse sind. Selbst wenn einzelne Lehrer einem solchen Vorhaben pädagogische Aspekte abgewinnen können, ist datenschutzrechtlich von Relevanz, dass damit einer Bloßstellung im Sinne einer *Stigmatisierung* Vorschub geleistet werden dürfte. Das Landesschulamt hat die Angelegenheit aufgegriffen und anlässlich einer Schulaufsichtskonferenz für den Grundschulbereich generell darauf hingewiesen, dass das Verlesen von Oberschulempfehlungen zu unterbleiben hat.

**Elektronisches Kassensystem der Berliner Bäder-Betriebe**

*Bereits 1998 hatte ein Bürger vermutet, die Berliner Bäderbetriebe wollten zumindest bei den Sammelkarten den „gläsernen Badegast“ einführen. Die Datenerhebung beim Kauf einer solchen Karte, die Angabe des Namens auf den Sammelkarten und die Angaben, die den Benutzern beim Zutritt über Badezeiten und verbleibende Eintrittberechtigungen angezeigt wurden, hatten zu Mißtrauen über den Umgang mit personenbezogenen Daten geführt. Nach unserer Prüfung empfahlen wir eine bessere Aufklärung der Kunden[92]. Nunmehr wurde die Angelegenheit Gegenstand einer parlamentarischen Anfrage.*

Die Berliner Bäder-Betriebe (BBB) lieferten mit der Einführung ihres elektronischen Ticket-Systems „Cassa Nova“ geradezu ein Paradebeispiel dafür, wie man durch mangelnde Transparenz des Verfahrens gegenüber den Betroffenen einen erst mit diesem System möglichen Kundenservice ins Zwielicht rücken kann. Die BBB bieten ihren Badegästen die Möglichkeit,

[91] JB 1994, 4.10

[92] JB 1998, 4.6.3

beim Verlust von Mehrfachkarten unter bestimmten Voraussetzungen eine Ersatzkarte auszustellen, da die dazu notwendigen Daten wie Verfallsdatum bzw. Anzahl der noch nicht in Anspruch genommenen Besuche im Zusammenhang mit der Kartenausgabe und der anschließenden Nutzung im System gespeichert werden. Einzige Voraussetzung für das Ausstellen einer Ersatzkarte ist allerdings die Angabe ihres Namens, gegebenenfalls auch des Vornamens, zur Speicherung im Kassensystem.

Bereits 1998 haben wir aufgrund der Eingabe eines Badegastes das Ticket-System geprüft und im Ergebnis den BBB empfohlen, ihre Kunden auf die Notwendigkeit der Namensspeicherung im Zusammenhang mit der Inanspruchnahme des Ersatzkarten-Services aufzuklären, so dass diese dann frei entscheiden können, ob sie von dieser Dienstleistung unter Umständen Gebrauch machen möchten oder nicht. Offenbar haben die BBB unsere damalige Empfehlung nicht so ernst genommen, durch eine gezielte Aufklärung ihrer Badegäste - z. B. durch einen entsprechenden Aushang an den Kassen - eine datenschutzgerechte informierte Einwilligung der Betroffenen zu bewirken. Nur so ist es erklärbar, dass in diesem Jahr im Abgeordnetenhaus eine Kleine Anfrage zum Thema „Gläserne Besucher der Berliner Bäder-Betriebe“ gestellt wurde.

Eine erneute Überprüfung des Ticket-Systems ergab hinsichtlich der in der Anfrage geäußerten Befürchtungen keine Anhaltspunkte. Die alleinige Namensspeicherung ist zur Erstellung eines personenbezogenen Besucherprofils nicht hinreichend und es liegt den BBB fern, solche Profile überhaupt in Erwägung zu ziehen. Eine derartige Profilbildung und ihre Nutzung z. B. für Marketingzwecke setzt voraus, dass über den Namen hinausgehende personenbezogene Daten wie z. B. Adresse, Alter, Telefonnummer usw. gespeichert würden. Nachdem die BBB seit September dieses Jahres ihre Kunden durch Aushänge in ihren Bädern auf den Zweck der Erhebung und Speicherung personenbezogener Daten bei Sammelkarten aufklärt, sahen wir keinen datenschutzrechtlichen Grund, den Ersatzkarten-Service zu unterbinden.

**Videoüberwachung in Schwimmbädern der Berliner Bäder-Betriebe (BBB)**

*In der Tagespresse wurde berichtet, dass im Stadtbad Lankwitz die Umkleideräume der Herren mit Videokameras überwacht würden, da insbesondere hier die Diebstähle aus Umkleidekabinen und -schränken in jüngster Zeit signifikant zugenommen hätten.*

Aus der Stellungnahme des BBB Vorstandes ging hervor, dass in zehn Bädern Videoüberwachungsanlagen unterschiedlicher Ausprägung betrieben werden, mit der Personalvertretung entsprechende, die Rechte der Beschäftigten wahrende Dienstvereinbarungen abgeschlossen wurden und „in keinem Fall Örtlich-

Durch die Videoüberwachungsanlagen, die in den Berliner Bädern installiert wurden, wird die Intimsphäre der Besucher nicht verletzt. Die eingeleiteten Maßnahmen dienen dazu, dem Sicherheitsbedürfnis der Badebesucher unter Wahrung ihrer Persönlichkeitsrechte gerecht zu werden.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

keiten beobachtet und aufgezeichnet werden, die eine Sensibilität hinsichtlich intimer Persönlichkeitsbereiche aufweisen“.

Anhand der uns zur Verfügung gestellten Dienstvereinbarungen war erkennbar, dass in den meisten Bädern die Kameras lediglich der Beobachtung gefahrgeneigter Einrichtungen (z. B. Rutschen) oder vom Kassenpersonal nicht unmittelbar einsehbarer Zugänge (z. B. zur Sauna) dienen. Hier wird konsequent das reine Kamera-Monitor-Prinzip - das sog. „verlängerte Auge“ - verwirklicht, d. h., die Kamerabilder werden nicht aufgezeichnet. In drei Hallenbädern und einem Sommerbad wird hingegen auch von den dort vorhandenen Aufzeichnungsmöglichkeiten Gebrauch gemacht. Aus jahreszeitlich bedingten Gründen haben wir uns bei unseren Überprüfungen vor Ort zunächst auf die drei Hallenbäder - Stadtbad Lankwitz, Kombibad Gropiusstadt und die Schwimm- und Sprunghalle im Europasportpark an der Landsberger Allee – konzentriert.

Kontinuierliche Aufzeichnungen werden nur in denjenigen Bädern vorgenommen, in deren Umkleidebereichen es in der Vergangenheit zu einer massiven Häufung von Straftaten gekommen ist. Überwacht werden nur die Gänge zwischen den Umkleidekabinen bzw. Schränken, also Bereiche, die auch von jedem anderen Badegast jederzeit eingesehen werden können. Alle Kameras sind erkennbar. Versteckte Kameras gibt es nicht. Auf die Videokameras in den Bädern wird durch entsprechende Hinweisschilder aufmerksam gemacht.

Bei der letztgenannten Einrichtung gehört die Videoüberwachung zu einem Komplex von Sicherheits- und Überwachungsmaßnahmen, mit dem ein Sicherheitsdienst beauftragt wurde. Die Mitarbeiter dieses Dienstes beobachten an den in einer Zentrale aufgestellten Monitoren kontinuierlich das Geschehen an neuralgischen, öffentlich zugänglichen Bereichen und sind seitens der BBB angewiesen, Aufzeichnungen nur dann zu veranlassen, wenn sich Anhaltspunkte für strafbare Handlungen oder sonstige den Betriebsablauf gefährdende Ereignisse ergeben. Sensible Bereiche wie Umkleideräume liegen nicht im Blickfeld der Kameras. Zu bemängeln war hier lediglich, dass an einigen Stellen – z. B. am Fußgängertunnel von und zur S-Bahn - auf die Videoüberwachung nur unzureichend durch eine entsprechende Beschilderung hingewiesen wurde. Die Vertreter der BBB haben uns zugesagt, diesem Mangel umgehend abzuhelfen.

Zur noch fehlenden Beschilderung am Fußgängertunnel von der Schwimm- und Sprunghalle Landsberger Allee zur S-Bahn und umgekehrt haben die BBB mit der Firma Velomax Kontakt aufgenommen mit dem Ziel, dass eine entsprechende Informationstafel mit Hinweis auf die Videoüberwachung aufgestellt wird.

Anders stellte sich die Situation in den beiden anderen von uns überprüften Bädern dar. Entgegen der Aussage des BBB-Vorstands wurden hier tatsächlich sensible, die Intimsphäre der Badbesucher berührende Bereiche von den installierten Videokameras erfasst. Während in den Räumlichkeiten, in denen sich die Einzelumkleidekabinen bzw. -schränke befinden, lediglich die Gänge und die Kabinen- bzw. Schranktüren von den Kameras erfasst werden, können sich die Nutzer der „Sammelumkleiden“ - insbesondere im Stadtbad Lankwitz - beim Umziehen kaum den Blicken der Videokameras entziehen. Zwar weisen in beiden Bädern zahlreiche Schilder vor und in den Umkleideräumen auf die Videoüberwachung hin, jedoch ist ein derartiger Eingriff in die Intimsphäre der Badegäste nicht hinnehmbar. Zudem fehlte auf den Schildern generell der Hinweis auf die zum Zeitpunkt unserer Überprüfung praktizierte kontinuierliche Aufzeichnung der Videobilder. Dass zu diesem Termin

Die Darstellung, im Kombibad Gropiusstadt und im Stadtbad Lankwitz würden die Besucher in den Innenräumen der Sammelumkleidekabinen überwacht, entspricht nicht den Tatsachen. Im Stadtbad Lankwitz befinden sich zwar im Sammelumkleidebereich funktionsfähige Kameras, diese sind aber ständig weggeschaltet. Die Berliner Bäder-Betriebe werden jedoch dafür sorgen, dass durch geeignete technische Maßnahmen (Abklemmen von Kabeln o.ä.) die Kameras zukünftig nicht mehr ohne weiteres in Betrieb gesetzt werden können.

Eine Überprüfung im Kombibad Gropiusstadt ergab, dass die Sichtblenden in den dortigen Sammelumkleidebereichen die Beobachtung sich umkleidender Personen in hinreichender Weise einschränken. Im Erfassungsbereich befinden sich nur die Schranktüren.

die fragwürdigen Kameras abgeschaltet waren, spielt nur eine untergeordnete Rolle, da sie sofort wieder aktiviert werden konnten. Wir haben daher den BBB dringend empfohlen, zumindest bis zur Veränderung der baulichen Gegebenheiten in den Sammelumkleiden (Sichtblenden, Kamerapositionierung) diese Kameras technisch außer Betrieb zu setzen. Für den Fall, dass auf diese Weise ein unbeobachtetes Umziehen der Badbesucher nicht gewährleistet werden kann, wären diese Kameras vollständig zu demontieren.

### 4.5.3 Statistik

**Statt Volkszählung: rechnergestützter Zensus**

Eine Volkszählung ist ein erheblicher Eingriff in das Selbstbestimmungsrecht aller Einwohner. Wir befürworten daher alle Bemühungen, ein milderes Mittel als eine Volkszählung als Totalerhebung zu finden. Fraglich bleibt jedoch, ob die personenbezogene Zusammenführung der Daten verschiedener Register das mildere Mittel gegenüber einer Totalerhebung unter Mitwirkung der Betroffenen ist. Dieses hängt entscheidend von den Rahmenbedingungen ab. Ein Testgesetz, für das Ende 1999 eine Arbeitsgruppe der statistischen Ämter von Bund und Ländern Vorschläge für die inhaltlichen Aspekte erarbeitet hat, sieht die Entwicklung und Überprüfung von Methoden der Zusammenführung der Daten der Meldedateien, der Bundesanstalt für Arbeit sowie die stichprobenhafte Ergänzung durch Einwohnerbefragungen vor.

*Ein angenommenes und gekürztes Beispiel:*

*Die gemeldeten Bewohner der Müllerstraße XYZ werden aufgrund der Daten im Melderegister zu statistischen Haushalten zusammengerechnet.*

*Dabei „entsteht" folgender Haushalt:*

*Karin L. (42) und Martin B. (44) bilden den Kernhaushalt, weil sie ein gemeinsames Datum der letzten Eheschließung und der letzten Ehescheidung haben. Dem Haushalt zugeordnet wird Tom L. (12), weil Karin L. den gleichen Nachnamen hat und die Geburtsdaten von Karin L. und Martin B. mit denen des gesetzlichen Vertreters von Tom L. übereinstimmen. Agnes V. (67) wird dem Haushalt auch zugerechnet, weil ihr Geburtsname (Agnes M.) mit dem Geburtsnamen von Karin L. (geborene M.) übereinstimmt und beide das gleiche Einzugsdatum in die Wohnung haben. Agnes V. ist verwitwet.*

*Alle vier Personen haben keine weitere Nebenwohnung und die deutsche Staatsangehörigkeit. Ihr Haushalt ist statistisch plausibel und noch einfach generierbar.*

Bei den Tests sollen *bis zu 30 verschiedene Hilfsmerkmale*, insbesondere aus den Meldedateien, über die Betroffenen erhoben und verarbeitet werden. Die-

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

se Hilfsmerkmale können in ihrer Gesamtheit wie ein Substitut eines Personenkennzeichens wirken. Es werden also Methoden getestet, die es erlauben, flächendeckend auch außerhalb der Statistik den einzelnen Bürger in weiten Bereichen seiner Persönlichkeit zu registrieren und zu katalogisieren. Solche Methoden hat das Bundesverfassungsgericht im Volkszählungsurteil von 1983[93] als unzulässig bezeichnet und festgestellt, dass die Verknüpfung vorhandener Dateien auch nicht das mildere Mittel sei. Diese große Zahl von Hilfsmerkmalen (beispielsweise soll über Eltern-Kind-Verknüpfungen, gemeinsame Einzugsdaten u. Ä. der Haushaltszusammenhang von Bewohnern simuliert werden) sind damit nicht mehr Hilfsmerkmale im klassischen statistischen Sinne, die der Durchführung von Bundesstatistiken dienen.

Diese Merkmale stellen zugleich *Roherhebungsmerkmale* dar, die bei einer klassischen Volkszählung erst gar nicht anfallen, da die Betroffenen selbst Auskunft zu dem entsprechenden Erhebungsmerkmal (beispielsweise die Erklärung zu einem gemeinsamen Haushalt) geben. Die Grenze zwischen Hilfs- und Erhebungsmerkmal und damit auch die datenschutzrechtlich gebotene frühzeitige Trennung von den Erhebungsmerkmalen droht unterlaufen zu werden. In der technischen Durchführung könnte sich das so darstellen, dass für die eine Aufbereitung bestimmte Hilfsmerkmale frühzeitig gelöscht werden, sie für eine andere Aufbereitung jedoch komplett erhalten werden müssen, um plausible Erhebungsdaten zu gewinnen. So verwendete Hilfsmerkmale bilden damit ein *Surrogat eines intelligenten Personenkennzeichens*, mit dem nicht nur die Person selbst identifiziert, sondern auch ein komplexer Zusammenhang zusammenlebender Personen abgebildet wird, um abschließend das Merkmal der Haushaltszugehörigkeit zu bestimmen.

Daher schlugen wir vor, nicht nur das technische Instrumentarium der Registerzusammenführung und intelligenter Registerauswertung zu testen, sondern zugleich auch *Pseudonymisierungsverfahren zu erproben*, die die Eingriffstiefe vermindern zu können. Wir empfahlen, unmittelbar identifizierende Daten wie Namen und Anschrift sowie definierte Ordnungsangaben wie den Geburtstag oder den Geburtsort derartig zu verändern, dass durch Verschlüsselung ein Pseudonym entsteht. Diese Tests könnten parallel zum Registerabgleich und zur Registerzusammenführung erprobt werden. Es wäre sehr bedauerlich, wenn das *Zensus-Testgesetz* auf die Erprobung datenschutzfreundlicher Technologien verzichten und nur die unmittelbare Zusammenführung der verschiedenen Datenbestände zum Ersatz einer klassischen Volkszählung erlauben würde. Einmal entwickelt, können solche Instrumente, die für „harmlose“ Zwecke wie

Der Entwurf eines Gesetzes zur Erprobung eines registergestützten Zensus (Zensustestgesetz) wird nach Beteiligung des Bundesrates zur Zeit im Bundestag behandelt. Das Ergebnis des Gesetzgebungsverfahrens bleibt abzuwarten.

[93] BVerfGE 65, 57

die Statistik entwickelt wurden, die Nutzungsbegehrlichkeiten anderer öffentlicher oder privater Stellen hervorrufen. Es kann dabei nicht ausgeschlossen werden, dass diese Instrumente eine mit der Würde des Menschen unvereinbare Registrierung und Katalogisierung der Persönlichkeit durch Persönlichkeitsabbilder ermöglichen. Zumindest sollte gesichert werden, dass das zu testende Know-How der Zusammenführung von Hilfsmerkmalen ebenfalls der strikten statistischen Geheimhaltung unterworfen wird und ausschließlich im Bereich der statistischen Ämter genutzt werden darf.

**Offene Türen für die Forschung?**

Im Jahresbericht 1998[94] informierten wir über eine anfangs heftig geführte Diskussion über den Zugang der Wissenschaft zu statistischen Einzeldaten. In einer Reihe von Beiträgen wurde gefordert, das Statistikgeheimnis für die wissenschaftliche Forschung weitgehend einzuschränken. Wir betonten in dieser Diskussion, dass die Sicherung des Statistikgeheimnisses entscheidend für die Akzeptanz der amtlichen Statistik bei den Auskunftspflichtigen ist[95]. Mitte 1999 fand auf Anregung des Bundesministeriums für Bildung und Forschung ein Symposium zum Thema „Kooperation zwischen Wissenschaft und amtlicher Statistik“ statt, auf dem wir unsere Erfahrungen mit der Verarbeitung sensitiver Daten durch Datentreuhänder als eine Möglichkeit, in neuen Wegen für die amtliche Statistik zu denken, vortrugen. Als Reaktion auf das Symposium setzte die Bundesministerin für Bildung und Forschung eine Kommission ein, die bis Anfang 2001 Lösungsvorschläge erarbeitet hat. Diese „Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik“ (KVI) führte im Oktober 2000 ein Hearing durch, zu dem auch wir geladen wurden. Es zeigte sich, dass die angesprochenen Probleme des Datenzugangs in keiner Weise ein speziell deutsches Problem sind, sondern berühren neben den europäischen Staaten genauso Kanada und die USA und es zeichnet sich ab, dass dort ähnliche Lösungen angestrebt werden. Wir unterbreiteten Vorschläge für

- die Erhöhung der Flexibilität der statistischen Erhebungen, ohne das Prinzip „Keine amtliche Statistik ohne eine sie legalisierende Rechtsvorschrift“ im Kern zu unterlaufen,
- die Lösung des Archivproblems bei statistischen Einzeldaten,
- die Stärkung der Analyse und Eigenforschung durch die amtliche Statistik einschließlich rechtlich gesi-

[94] JB 1998, 4.5.1

[95] Allgemeines Statistisches Archiv, Heft 1/1999, S. 152-157

cherter Möglichkeiten für die Durchführung des Gastwissenschaftlermodells,

- rechtliche Möglichkeiten der Bildung einer Vermittlungsstelle für Mikrodaten als gemeinsame Einrichtung von Bund und Ländern.

Beim Hearing war von besonderer Bedeutung die Frage, ob es in Deutschland möglich ist, ein *Forschungsgeheimnis* zu installieren. Dies setzt auf der einen Seite die Möglichkeit voraus, den Forscher, der Zugang zu Einzeldaten erhält, besonders und strafbewehrt auf die Geheimhaltung und Verschwiegenheit bezüglich dieser Einzelangaben zu verpflichten und auf der anderen Seite die von ihm erlangten Erkenntnisse vor jeglicher Kenntnisnahme durch Dritte einschließlich eines Beschlagnahmeverbotes zu schützen. Für die Verpflichtung der Wissenschaftler ist durch das Strafverfahrensänderungsgesetz (§ 203 Abs. 2 Ziff. 6 StGB) eine formale Möglichkeit der Bestrafung bei unbefugtem Offenbaren geschaffen. In welchen Fällen die Offenbarung befugt ist, muss jedoch entweder einzelgesetzlich wie im Bundesstatistikgesetz oder allgemein z. B. im Berliner Datenschutzgesetz festgelegt werden.

**Repräsentativität ohne Auskunftspflicht?**

Spätestens seit dem Volkszählungsurteil sind die Statistiker gefordert, ihr Methodenarsenal stetig weiter zu entwickeln. Dies hat auch der Gesetzgeber zu berücksichtigen. Nachdem über viele Jahre hinweg nie ernsthaft in Zweifel gezogen wurde, dass repräsentative Daten der amtlichen Statistik nur mit Auskunftspflicht gewonnen werden können, scheint nun wenigstens bei der Weiterentwicklung des Systems der *Haushaltsstichproben* ein neuer Ansatz diskussionswürdig zu sein. Bekanntermaßen ist alljährlich 1 % der Bevölkerung gefordert, mit Auskunftspflicht im Rahmen des Mikrozensus statistische Daten über die in einem Haushalt zusammenlebenden Personen gegenüber der amtlichen Statistik zu offenbaren. Jährlich wird ein Viertel der Befragten ausgetauscht, so dass die Haushalte in einer Wohnung viermal, d. h. damit auch vier Jahre hintereinander befragt werden. Auch wenn die Aufregung und Überraschung bei der ersten Erhebung groß sind, zeigt sich aus unserer Beratungspraxis, dass bei der Zweit- oder Drittbefragung die Akzeptanz gewachsen ist. Häufig haben die Betroffenen erstmals durch diese Erhebung gesehen, mit welcher Genauigkeit und welchem wissenschaftlichen Anspruch die statistischen Ämter diese Datenerhebung durchführen. Warum sollen die Haushalte nicht nach vier Jahren gefragt werden, ob sie bereit sind, Namen, Anschrift und einige Haushaltsmerkmale in einer gesonderten Datei zum Zwecke der Durchführung von Datenerhebungen ohne Auskunftspflicht bei der amtlichen Statistik zu hinterlegen? Durch die Auswahl der zu Befragenden könnten repräsentative Stichproben durchgeführt werden. Des Weiteren bietet dies die Mög-

lichkeit, mit Einwilligung der Betroffenen Daten verschiedener Bereiche auf den Haushalt bezogen kurzzeitig für Auswertungszwecke zu verbinden und damit den Weg zu integrierten Informationssystemen zu gehen, die auch von der wissenschaftlichen Forschung gefordert werden. Wir begrüßen daher diesen Vorschlag des Statistischen Bundesamtes und gehen davon aus, dass er bei der Diskussion des im Jahre 2004 auslaufenden und dann zu erneuernden Mikrozensusgesetzes Berücksichtigung finden kann.

## 4.6 Wirtschaft

### 4.6.1 Geld und Kredit

**Der gläserne Aktionär**

Im Vorjahr[96] berichteten wir über die datenschutzrechtlichen Probleme, die durch die inzwischen übliche *Umstellung von Inhaberaktien in Namensaktien* aufgetreten sind. Der Gesetzgeber hat inzwischen reagiert und ein Gesetz zur Namensaktie verabschiedet[97], durch welches die Datenschutzbelange der Aktionäre zufrieden stellend gelöst werden.

In der Begründung zu § 67 Abs. 1 Aktiengesetz stellt der Gesetzgeber klar, dass der Beruf nicht zu den in das Aktienregister (bisher: Aktienbuch) aufzunehmenden Daten gehört. Anstelle der postalischen Anschrift kann der Aktionär zukünftig auch eine Büroadresse, einen Zustellungsbeauftragten oder eine E-Mail-Adresse angeben.

In § 67 Abs. 6 Aktiengesetz wird der *Umfang des Einsichtsrechts* in das Aktienregister erheblich eingegrenzt. Das bisherige umfassende Einsichtsrecht aller Aktionäre bezüglich der Daten aller übrigen Aktionäre wurde gestrichen. Zukünftig kann der Aktionär von der Gesellschaft nur Auskunft über die zu seiner Person in das Aktienregister eingetragenen Daten verlangen. Für die Aktionärsdaten gilt eine klare Zweckbindung. Die Gesellschaft darf die Registerdaten nur für ihre Aufgaben im Verhältnis zu den Aktionären verwenden. Zur Werbung für das Unternehmen darf sie die Daten nur verwenden, soweit der Aktionär nicht widerspricht. Besonders begrüßenswert ist die Regelung, dass die Aktionäre in angemessener Weise auf ihr Widerspruchsrecht hinzuweisen sind.

**Statt Kredit Eintragung in Warndatei und Werbung**

*Eine Bürgerin beantragte bei einer Bank einen Kredit, den diese ablehnte. Die von ihr für die Kreditbeantragung vorgelegten Unterlagen wurden ein halbes Jahr lang aufbewahrt und ihre Daten außerdem in*

---

[96] JB 1999, 4.6.1

[97] BGBl. I 2001, S. 123

*einer Warndatei gespeichert, zu der alle Filialen der Bank Zugriff haben. Laut Auskunft der Bank sei dies erforderlich, da nicht auszuschließen sei, dass sich die Kundin an eine andere Filiale der Bank wendet. Hierbei bestünde die „Gefahr, dass Kunden lernfähig" seien und bei einer späteren Kreditbeantragung nicht die gleichen vollständigen Informationen zur Verfügung stellen. Nach Ablauf eines halben Jahres werden nur noch Name, Anschrift, die beantragte Kredithöhe sowie das Geburtsdatum für Werbezwecke gespeichert.*

Da es in Deutschland zahlreiche Banken gibt, ist es schon nicht sehr wahrscheinlich, dass sich ein Kunde ausgerechnet ein zweites Mal an eine (eher unbedeutende) Bank wendet, die seinen Kreditantrag abgelehnt hat. Selbst wenn diese „Gefahr" bestehen würde, wäre nicht ersichtlich, aus welchem Grund der Sachbearbeiter der Bank über den vorhergehenden Kreditwunsch eines potentiellen Kunden informiert werden müsste, zumal sich die wirtschaftlichen Verhältnisse eines Betroffenen innerhalb eines halben Jahres ändern können und jeweils die aktuellen Vermögensverhältnisse zu überprüfen sind. In der Regel wird der Betroffene bei einem Kreditantrag alle Angaben zu dokumentieren haben, so dass kaum Raum für Falschangaben ist. Auch ist zu berücksichtigen, dass eine so genannte „Lernfähigkeit" der Kreditinteressenten auch bei Kreditanträgen bei anderen Banken oder durch Gespräche mit anderen Betroffenen möglich ist. Die Warndatei der Bank wird also auch kaum dazu führen, dass „Spezialisten" ihre Vermögensverhältnisse besser darstellen, als sie in Wahrheit sind. Da die Nutzung der Kundendaten für die Warndatei weder im Rahmen der Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen erforderlich ist (§ 28 Abs. 1 Nr. 1 BDSG) und eine Berufung auf die Wahrung berechtigter Interessen der speichernden Stelle zumindest an den überwiegenden schutzwürdigen Interessen des Betroffenen an dem Ausschluss der Nutzung scheitert (vgl. § 28 Abs. 1 Nr. 2 BDSG), ist die Warndatei rechtswidrig.

Gegen die Umwidmung von Vertragsdaten in *Werbedaten* bestehen keine grundsätzlichen Bedenken, soweit sich die Werbedatei auf die in § 28 Abs. 2 Nr. 1 b BDSG erwähnten Daten beschränkt. Wir haben dem Kreditinstitut deshalb empfohlen, anstelle des Geburtsdatums nur das Geburtsjahr zu speichern und auf die beantragte Kredithöhe als Datum zu verzichten. Da auch bei den in § 28 Abs. 2 Nr. 1 b BDSG angegebenen Daten zu prüfen ist, ob kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung seiner Daten (für Werbezwecke) hat, haben wir der Bank außerdem empfohlen, in den Fällen, in denen die Nichtgewährung des Kredits zu Missstimmigkeiten geführt hat, auf die Aufnahme der Kundendaten in eine Werbedatei zu verzichten. Da-

ten, die nicht für die Werbedatei verwendet werden, sind zu löschen (vgl. § 35 Abs. 2 Satz 2 Nr. 3 BDSG).

**Personalausweiskopie bei Kontoeröffnung**

*Bei der Eröffnung eines Girokontos verlangen einige Banken die Fotokopie des Personalausweises. Auf Nachfrage wird den Bankkunden mitgeteilt, die Banken seien aufgrund des Geldwäschegesetzes, der Abgabenordnung und aufgrund der Verlautbarung des Bundesaufsichtsamtes für das Kreditwesen vom 30. März 1998 über Maßnahmen der Kreditinstitute zur Bekämpfung und Verhinderung der Geldwäsche dazu verpflichtet, Personalausweiskopien zu erstellen.*

Nach dem in § 154 Abgabenordnung (AO) konstituierten *Grundsatz der Kontenwahrheit* sind Kreditinstitute bei der Eröffnung eines Kontos verpflichtet, sich Gewissheit über die Person und die Anschrift des Verfügungsberechtigten zu verschaffen. Gewissheit über die Person besteht, wenn dem Bankangestellten der vollständige Name, das Geburtsdatum und der Wohnsitz bekannt sind. Nach der Abgabenordnung hat der Bankangestellte deshalb die Verpflichtung, sich einen Personalausweis vorlegen zu lassen und die o. g. Daten festzuhalten (vgl. § 154 Abs. 2 Satz 1 AO). Eine Berechtigung oder Verpflichtung, einen Personalausweis zu kopieren oder sämtliche in dem Personalausweis enthaltenen personenbezogenen Daten festzuhalten, enthält die Abgabenordnung nicht.

Ein *Identifizieren i.S.d. Geldwäschegesetzes* ist nach § 1 Abs. 5 Geldwäschegesetz (GwG) das Festhalten des Namens aufgrund eines Personalausweises oder Reisepasses sowie des Geburtsdatums und der Anschrift, soweit sie darin enthalten sind, und das Feststellen der Art, Nummer und ausstellender Behörde des amtlichen Ausweises. Nach § 9 Abs. 1 Satz 2 GWG sollen nach dem Geldwäschegesetz erforderliche Aufzeichnungen, soweit möglich, durch Kopie der zur Feststellung der Identität vorgelegten Dokumente erfolgen. Die Identifizierungspflichten sowie die anschließenden Aufzeichnungs- und Aufbewahrungspflichten nach dem Geldwäschegesetz entstehen allerdings erst bei geldwäscherelevanten Vorgängen. Geldwäscherelevant sind insbesondere Finanztransaktionen, die den Schwellenwert von 30.000 DM überschreiten (vgl. § 2 Abs. 1 GwG). Da die bloße Eröffnung eines Girokontos kein geldwäscherelevanter Vorgang ist, scheidet das Geldwäschegesetz als Rechtsgrundlage für die geforderte Kopie des Personalausweises aus.

Die *Verlautbarung des Bundesaufsichtsamtes für das Kreditwesen* kommt als Rechtsgrundlage für die Erstellung von Ausweiskopien schon deshalb nicht in Betracht, da nach § 4 Abs. 1 BDSG nur eine Rechtsvorschrift als Ermächtigungsgrundlage für die Bearbeitung personenbezogener Daten in Betracht kommt.

Da es für die Erstellung einer Ausweiskopie bei der Eröffnung eines Girokontos keine Rechtsgrundlage gibt, ist diese nur dann rechtmäßig, wenn der Betroffene hierin eingewilligt hat. Ein informierte Einwilligung liegt allerdings dann nicht vor, wenn der Betroffene aufgrund einer falschen Information der Bank davon ausgeht, dass er gesetzlich zur Preisgabe der in dem Personalausweis enthaltenen Daten verpflichtet sei.

### 4.6.2 Auskunfteien

**Selbstauskunft verschlechtert Bonität**

*Wer bei der SCHUFA von seinem Recht Gebrauch macht, eine Selbstauskunft einzuholen, wird hierfür mit einer Verschlechterung seiner Bonität bestraft. Der SCHUFA-Score-Wert, mit dessen Hilfe das zukünftige Verhalten von Kreditnehmern prognostiziert wird[98], verschlechtert sich nämlich mit jeder Selbstauskunft.*

Die SCHUFA begründete die negative Beeinflussung des Score-Wertes durch Selbstauskünfte damit, dass die Häufigkeit der Selbstauskünfte nach den empirischen, statistisch-mathematisch ermittelten Ergebnissen bis zu einer Verzehnfachung des Risikos von Kreditausfällen führen würde. Ursache hierfür sei, dass SCHUFA-Selbstauskünfte häufig in wirtschaftlichen Umbruchsituationen (neue Wohnung, neue Tätigkeit) für wirtschaftliche Zwecke und nicht so sehr zur Kontrolle des Datensatzes verwendet würden.

Selbst wenn die statistischen Ergebnisse zutreffend sind, ist die negative Beeinflussung des Score-Wertes durch Selbstauskünfte rechtswidrig. Das in § 34 BDSG konstituierte Recht, Auskunft zu verlangen über die zu seiner Person gespeicherten Daten, ist von zentraler Bedeutung für das informationelle Selbstbestimmungsrecht und kann deshalb als Teil der „Magna Charta“ des Datenschutzes gewertet werden. Dieses Recht wurde vom Gesetzgeber so hoch bewertet, dass es nach § 6 Abs. 1 BDSG auch nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden kann. Die Wahrnehmung eines derartigen Rechts darf - dies gilt im Übrigen auch für die Wahrnehmung anderer datenschutzrechtlicher Rechte - nie zu einem Nachteil für den Betroffenen führen.

Die SCHUFA hat zugesagt, die rechtswidrige negative Beeinflussung des Score-Wertes durch Selbstauskünfte bis Mitte 2001 zu beenden.

[98] JB 1998, 4.6.2

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

**Datenschutzprobleme einer Auskunftei**

Bei der Überprüfung einer Auskunftei wurden verschiedene Datenschutzverstöße festgestellt.

*Wenn die Auskunftei nicht in der Lage ist, alle für die Bonität eines Unternehmens relevanten Daten zu erheben, also insbesondere dann, wenn die Betroffenen nicht zu einer Selbstauskunft bereit sind, verwendet die Auskunftei so genannte Schätzdaten, die sich nach dem Branchendurchschnitt richten. Die Schätzdaten sind nicht als solche erkennbar.*

Die Verwendung von nicht gekennzeichneten *Schätzdaten* ist rechtswidrig, denn letztendlich ist der Branchendurchschnitt bei jedem Unternehmen falsch, das nicht (genau) dem Durchschnitt entspricht. Da Schätzdaten insbesondere bei Betroffenen verwendet werden, die nicht bereit sind, mit der Auskunftei zusammenzuarbeiten und ihr eine Eigenauskunft zu geben, fühlen sich viele Unternehmer durch die Schätzdatenangabe genötigt. Um keine nichtgekennzeichneten (und für sie nicht als solche erkennbaren) statistischen Daten in ihrem Datensatz zu haben, fühlen sie sich gezwungen, zur Substanziierung der Unrichtigkeit der Daten die richtigen Daten zu nennen. Die Einlassung der Auskunftei, der geübte Leser sei in der Lage, Schätzdaten zu erkennen, da Schätzdaten aufgerundet seien, ist schon deshalb nicht zutreffend, da die Betroffenen selbst bei Auskünften oftmals gerundete Zahlen angeben.

Kunden von Auskunfteien, die über eine bestimmte Person Informationen erhalten möchten, müssen ein *berechtigtes Interesse* an der Kenntnis dieser Daten haben (§ 29 Abs. 2 Nr. 1 a BDSG). Ein berechtigtes Interesse liegt in der Regel dann vor, wenn man einem anderen gegenüber vertraglich in Vorleistung treten will (Darlehen, Leasing etc.) und sich vor dem Abschluss des Vertrages über die Bonität des Kunden informieren möchte.

*In einem Fall hatte ein Kunde der Auskunftei eine Auskunft über einen potentiellen Vertragspartner eingeholt, obwohl dieser über den Vertragsabschluss erst nach einem 14-tägigen Urlaub entscheiden wollte.*

Hier liegt offensichtlich das berechtigte Interesse noch nicht vor.

*Eine Bank wollte einen Makler dafür gewinnen, ihm Kunden mit Kreditbedarf zuzuführen.*

Ob hier überhaupt ein berechtigtes Interesse zu einer Bonitätsüberprüfung vorliegt, erscheint schon mangels eines Vorleistungsverhältnisses zweifelhaft. Die Bank jedenfalls hat die Auskunft eingeholt, bevor überhaupt erste Gespräche mit dem Makler geführt wurden (der im Übrigen zu keinem Zeitpunkt Interesse an einer Zusammenarbeit mit der Bank hatte).

Auch hier war die Datenabfrage der Auskunfteikunden rechtswidrig.

Die in dem Jahresbericht 1999 geschilderten rechtswidrigen *Nachbarschaftsbefragungen*[99] wurden von der Auskunftei bisher nicht abgestellt. Insbesondere ist bedauerlich, dass es jedem einzelnen Rechercheur freigestellt ist, auf eine datenschutzrechtlich wünschenswerte Selbstbefragung zu verzichten und stattdessen eine Nachbarschaftsbefragung durchzuführen. Kriterien, in welchen Fällen auf eine Selbstbefragung verzichtet werden kann, existieren in der Auskunftei nicht.

### 4.6.3 Marketing

**Data Warehouse und Data Mining**

Im Zeitalter der Informationstechnologie eröffnen sich für Unternehmen Möglichkeiten, Technologien einzusetzen, die Datenbestände eines Unternehmens in einer Weise für das Unternehmen nutzbar machen, die es vorher nicht gegeben hat. Es ist möglich geworden, alle Unternehmensdaten zu einem großen *Datenpool* zusammenzuführen, der mit Hilfe verschiedenster *Auswertungssysteme* ausgewertet werden kann, um die Daten für das Unternehmen in vollkommen neuen Zusammenhängen zu nutzen. Data Warehouse und Data Mining sind die Stichwörter, die inzwischen die Debatten um den Einsatz von Informationstechnik beherrschen[100].

*Data Warehouse* bedeutet „Daten-Lagerhaus“. Es werden alle in einem Unternehmen anfallenden Informationsstränge (so genannte operative Datenbanken, wie Vertriebsdaten, Buchhaltungsdaten, Personaldaten, Marktforschungsdaten) mit dem Ziel zusammengeführt, eine zielgerichtete Verfügbarkeit, Abrufbarkeit und Aufbereitung der Daten des gesamten Unternehmens zu ermöglichen. Die *Zusammenführung der Datenbanken* setzt voraus, dass die Speicherung nach einheitlichen Kriterien erfolgt, um eine umfassende Analyse des Datenbestandes durchführen zu können.

Bei *Data Mining* („Datenbergbau“) werden die Daten des Data Warehouse in neue Zusammenhänge gestellt. Mit Hilfe einer *automatisierten Auswertung* können Vorhersagen getroffen werden über Trends, Verhaltensmuster - es können unbekannte Strukturen und Zusammenhänge aufgedeckt werden.

Ausgewertet werden kann insbesondere das Kundenverhalten, aber auch Personaldaten könnten für eine Datenauswertung von Interesse sein. Beispiele:

---

[99] JB 1999, 4.6.2

[100] JB 1998, 2.1

- Erfassung von Konsumverhalten der Kunden zu Werbezwecken,
- Auswertung der Daten auf Kundenpräferenzen, Zahlungswahrscheinlichkeit, Kundenprofitabilität,
- Erstellung von Prognosen für Abwerbung von Mitarbeitern des eigenen Unternehmens.

Data Warehouse und Data Mining werden in der Regel für eigene Geschäftszwecke betrieben. Als Rechtsgrundlage kommt somit § 28 Bundesdatenschutzgesetz (BDSG) in Betracht. Nach § 28 Abs. 1 Nr. 1 BDSG ist die Datenverarbeitung oder -nutzung als Mittel für die Erfüllung eigener Geschäftszwecke im Rahmen eines Vertragsverhältnisses mit dem Betroffenen zulässig. Da sich das Data Warehouse in der Regel außerhalb des operativen Geschäfts bewegt, dürfte es in der Regel nicht unter § 28 Abs. 1 Nr. 1 BDSG zu subsumieren sein. Ein Kunde schließt etwa einen Vertrag über einen bestimmten Kaufgegenstand ab, die Analyse seines Kaufverhaltens mit dem Ziel, ihn möglichst optimal zu bewerben, fällt nicht mehr unter den Vertragszweck. Bei einem Arbeitsvertrag (Dauerschuldverhältnis) fallen alle Daten unter § 28 Abs. 1 Nr. 1 BDSG, die der Arbeitgeber benötigt, um seinen daraus resultierenden Pflichten zu entsprechen. Die Erstellung von Prognosen für die Abwerbung von Mitarbeitern z. B. geht aber über das Erfordernis der Fürsorgepflicht hinaus und fällt nicht mehr unter § 28 Abs. 1 Nr. 1 BDSG.

Datenverarbeitung und -nutzung für eigene Zwecke ist auch zulässig, soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Sowohl *Marketinginteressen* als auch etwa das Interesse, dass qualifizierte Mitarbeiter nicht abgeworben werden, sind berechtigte Interessen i.S.d. § 28 Abs. 1 Nr. 2 BDSG. Man wird allerdings in der Regel davon ausgehen müssen, dass hier die *schutzwürdigen Belange der Betroffenen überwiegen*, da diese ein schutzwürdiges Interesse dahingehend haben, dass keine personenbezogenen Profile erstellt werden, mit deren Hilfe ihr Verhalten analysiert werden kann. Ein zusätzliches rechtliches Hindernis für Data Warehouse/Data Mining ist, dass nach § 35 Abs. 2 Nr. 3 BDSG personenbezogene Daten zu löschen sind, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Außerhalb von Dauerschuldverhältnissen sind demnach in der Regel die personenbezogenen Daten von Betroffenen zu löschen bzw. zu sperren. Nur ein begrenzter Datensatz wird für Werbezwecke in eine Werbedatei eingebracht werden können.

Die Errichtung eines Data Warehouses und Data Minings ist allerdings bei Vorliegen einer *Einwilligung*

(§ 4 Abs. 1 BDSG) rechtmäßig. Voraussetzung hierfür ist, dass der Zweck der Datenverarbeitung hinreichend spezifiziert werden kann. Noch weitgehend ungeklärt ist, ab wann eine Profilbildung so weit geht, dass trotz Einwilligung von einer *Sittenwidrigkeit* i.S.v. § 138 BGB auszugehen ist. Auch ist zu prüfen, inwieweit eine Einwilligung zur Betreibung eines Data Warehouses gegen § 6 Abs. 1 BDSG verstößt, da hierdurch das Recht auf die eigentlich nach § 35 BDSG vorgesehene Löschung beschränkt werden kann.

Die oben beschriebenen datenschutzrechtlichen Probleme entstehen nicht, wenn das Data Warehouse *anonymisiert* betrieben wird. Gegen die Einbringung von operativen Daten in ein anonymisiertes Data Warehouse bestehen keine Bedenken. Allerdings ist bei einer Rückführung der bei einer anonymisierten Analyse gewonnenen Erkenntnisse zu einer bestimmten Personengruppe zu überprüfen, ob eine entsprechende Datennutzung den Vorgaben des § 28 BDSG entspricht.

**Reichweite des Werbeverbotes**

*Wer bei der Deutschen Bahn AG eine BahnCard beantragt, hat die Möglichkeit (wie auch sonst in der Privatwirtschaft), bei der Antragstellung oder zu einem späteren Zeitpunkt bei der speichernden Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung zu widersprechen. Die Deutsche Bahn AG berücksichtigt den Widerspruch zwar für die Zeit der Geltungsdauer der BahnCard, nicht jedoch bei Folge- bzw. Neuverträgen, die nach Ablauf der Geltungsdauer der alten BahnCard abgeschlossen wurden.*

Der Widerspruch gegen die Nutzung oder Übermittlung personenbezogener Daten für Zwecke der Werbung nach § 28 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) ist bezüglich seiner Reichweite nach Treu und Glauben und mit Rücksicht auf die Verkehrssitte auszulegen (§ 242 BGB). Danach ist zu klären, ob ein objektiver Beobachter, der die Erklärung des Widersprechenden auslegt, davon ausgehen muss, dass der Widersprechende eine *Fortdauer der Widerspruchswirkung* über den Zeitpunkt der Gültigkeit der BahnCard hinaus wünscht. Die Vermutung der Deutschen Bahn AG, ein Kunde würde seine Meinung über Werbung bei jedem neuen BahnCard-Erwerb wechseln, erscheint jedenfalls nicht plausibel. Insbesondere bei Kunden, die zum Abschluss des Folgevertrages ein von der Deutschen Bahn AG vorbereitetes, ausgefülltes Antragsformular verwenden (Erneuerungsantrag), muss davon ausgegangen werden, dass der Betroffene von der Beibehaltung aller Vertragsmodalitäten des Altvertrages ausgeht. Die Deutsche Bahn AG hat unsere Bedenken aufgegriffen und berücksichtigt nunmehr alle Widersprüche, sofern der

Antrag innerhalb eines Jahres nach der Ungültigkeit der alten BahnCard gestellt wird.

**Kundenbefragung**

*Die Bewag führte eine Kundenbefragung durch. In dem Anschreiben wurde erwähnt, man wolle den Kunden besser kennen lernen, um ihm weitere Serviceangebote zu machen, die über die Stromversorgung hinausgingen. Abgefragt wurden Daten wie Beruf, Besitz von Haustieren, Freizeitverhalten, Vereinsmitgliedschaften, Interesse an Fallschirmspringen, Organisation des Urlaubs etc.***.**

Die Bewag hat den Fragebogen an ihre 350.000 besten Kunden (Kunden mit dem höchsten Stromverbrauch) versandt. Um diese Kunden langfristig an die Bewag zu binden, ist beabsichtigt, an diese Kunden *Geschenkgutscheine* zu versenden. Der Fragebogen soll dazu dienen, die Kunden entsprechend ihren Neigungen und „Erlebniswelten" in Geschenkgutscheinklassen einzuteilen. Eine weitere Nutzung der personenbezogenen Daten ist nicht beabsichtigt.

Da die Fragebogenaktion der Bewag nicht auf eine gesetzliche Ermächtigungsnorm gestützt werden kann, ist sie nur rechtmäßig, wenn eine wirksame Einwilligung des Betroffenen vorliegt. Dies setzt voraus, dass der Betroffene auf den Zweck der Speicherung hinzuweisen ist (vgl. § 4 Abs. 2 Satz 1 BDSG). Für die Kunden war aus dem Anschreiben der Bewag nicht nachvollziehbar, was genau mit den Daten geschehen sollte. Zu einer vollständigen Aufklärung waren die verwendeten Begriffe „interne Kundenbetreuung" bzw. „tolle Serviceangebote" zu unbestimmt. Wir haben der Bewag deshalb empfohlen, bei zukünftigen Befragungen den Zweck der Speicherung näher zu spezifizieren. Die Bewag hätte von Anfang an deutlich machen müssen, dass die *Befragung zur Zuordnung von Werbegeschenken* erforderlich ist. Hierdurch wären im Übrigen auch Irritationen vermieden worden, durch die der Wert der Werbekampagne geschmälert wurde.

**4.6.4 Informationsfreiheit im Wirtschaftsamt**

**Informationsfreiheit und Pachtvertrag**

*Der Verpächter einer Gaststätte möchte den Pächter auf Schadensersatz verklagen. Allerdings hat er den Pachtvertrag verloren. Er weiß, dass sein Pächter den Pachtvertrag in Kopie im Rahmen des gaststättenrechtlichen Genehmigungsverfahrens eingereicht hat. Das Wirtschaftsamt verweigert die Akteneinsicht mit Hinweis auf § 6 Abs. 1 Informationsfreiheitsgesetz (IFG), da der Vertrag personenbezogene Daten enthält und der Verpächter überwiegend Privatinteressen verfolge.*

Das Informationsfreiheitsgesetz ist eine besondere Rechtsvorschrift i. S. d. § 6 Abs. 1 Berliner Daten-

Der Senat verweist auf die allgemeinen Ausführungen zu Ziffer 3.5.(Informationsfreiheit- eine erste Bilanz);

schutzgesetz (BlnDSG). Es stellt sich deshalb die Frage, ob sich die Zulässigkeit der Akteneinsicht schon aus § 6 Abs. 1 Satz 2 BlnDSG herleiten lässt. Danach ist die Verarbeitung personenbezogener Daten nach dem Berliner Datenschutzgesetz zulässig, wenn wegen der Art der Verwendung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden (so genannte Trivialdaten). Bei Vorliegen dieser Voraussetzung macht das Informationsfreiheitsgesetz aus der Befugnis zur Datenoffenbarung eine Verpflichtung. Vorliegend soll der Vertrag von dem Vertragspartner entsprechend seinem Sinn, nämlich zur Durchsetzung von Rechtsansprüchen, verwendet werden. Es ist nicht erkennbar, wie hierdurch schutzwürdige Belange des Betroffenen beeinträchtigt werden können. Somit kann schon aus § 6 Abs. 1 Satz 2 BlnDSG ein Akteneinsichtsrecht des Verpächters hergeleitet werden. Auch nach dem Informationsfreiheitsgesetz besteht ein Einsichtsrecht, da § 6 Abs. 1 IFG nicht zu einem Ausschluss des Einsichts- bzw. Auskunftsrechts führt. Der Gesetzgeber wollte durch die Einschränkung des § 6 Abs. 1 Erste Alt. IFG nur vermeiden, dass Ersuchen auf Auskunft aus Neugier, Rachegelüsten, Querulanz etc. gestellt werden. Der Begriff „Privatinteressen“ ist deshalb im Rahmen einer teleologischen Reduktion so auszulegen, dass die Akteneinsicht zur Durchführung eines Zivilprozesses nicht durch den Gesetzgeber mit § 6 Abs. 1 Erste Alt. IFG verhindert werden sollte. Vorliegend ist vielmehr davon auszugehen, dass das Informationsinteresse des Antragstellers etwaige schutzwürdige Belange des Betroffenen an der Geheimhaltung überwiegt (vgl. § 6 Abs. 1 Zweite Alternative IFG).

vgl. hier insbesondere zum 2. Absatz unter der Überschrift „Einschränkungen“ (ab S. 46).

### 4.7 Europäischer und internationaler Datenschutz

Der Berliner Beauftragte für Datenschutz und Akteneinsicht hat im Auftrag der Konferenz der Datenschutzbeauftragten des Bundes und der Länder als Nachfolger für den Bremischen Landesdatenschutzbeauftragten die Aufgabe übernommen, als stellvertretender Delegationsleiter die Landesbeauftragten für den Datenschutz in der Gruppe nach Art. 29 Datenschutzrichtlinie zu vertreten. Diese Aufgabe auf europäischer Ebene ergänzt die Koordinierung der Tätigkeiten der deutschen Aufsichtsbehörden beim Datentransfer ins Ausland, die von uns bereits seit mehreren Jahren durch den Vorsitz in der Arbeitsgruppe „Internationaler Datenverkehr“ des Düsseldorfer Kreises wahrgenommen wird.

**Der sichere Hafen**

Das wichtigste Ergebnis der Arbeit der europäischen Datenschutzgremien ist der nach mehr als zwei Jahren erfolgte Abschluss der Verhandlungen der Europäischen Kommission mit dem US-Handelsministerium über die *„Safe-Harbor-Prinzipien“*. Wir haben im

letzten Jahr ausführlich über die Debatte berichtet[101]. Nachdem zunächst die Art. 29-Gruppe, sodann der Ausschuss der Regierungsvertreter nach Art. 31 der Richtlinie jeweils ein positives Votum zu den erarbeiteten Entwürfen abgegeben hatten, befasste sich das Europäische Parlament mit der Angelegenheit. In seiner Entschließung[102] vertrat es den Standpunkt, dass das Safe-Harbor-Paket nur dann ein angemessenes Datenschutzniveau gewährleiste, wenn es noch in verschiedenen Punkten abgeändert und insbesondere die Aussagen zu Durchsetzungsmechanismen in den USA konkretisiert würden (u. a. Einrichtung einer unabhängigen Beschwerdeinstanz, die zur Überprüfung der Eingabe wegen etwaigen Verstoßes gegen die Grundsätze verpflichtet sei ; Verpflichtung der beigetretenen Unternehmen zum Schadensersatz bei verursachten Schäden; Darlegung der einzelnen Schritte, die für die Löschung von Daten und die Geltendmachung von Schadensersatz erforderlich sind). Die Kommission hat die Bedenken des Europäischen Parlaments dem US-Handelsministerium mitgeteilt, aber ungeachtet dessen Ende Juli 2000 eine Entscheidung nach Art. 25 Abs. 6 Datenschutzrichtlinie getroffen[103].

Festgestellt ist nun, dass unter Berücksichtigung der Grundsätze des „sicheren Hafens“ von einem angemessenen Schutzniveau in den USA, genauer: bei dem die Daten empfangenden US-Unternehmen ausgegangen werden kann, wenn sich dieses Unternehmen in den „sicheren Hafen“ begeben, d. h. sich den Prinzipien unterworfen hat. Entgegen einer gerade bei Vertretern amerikanischer Organisationen weit verbreiteten Ansicht bedeutet dies jedoch nicht, dass die Datenübermittlung an Stellen, die sich den Safe-Harbor-Prinzipien unterworfen haben, nunmehr völlig unbeschränkt zulässig ist. Durch die Entscheidung der Kommission steht lediglich fest, dass hinsichtlich des Datenschutzniveaus in die USA ein Übermittlungshindernis nicht besteht. In einer zweiten Stufe ist aber nach Maßgabe des einzelstaatlichen Rechts zu prüfen, ob die Datenübermittlung im Einzelfall durch einen Erlaubnistatbestand gedeckt ist. Wäre die Auffassung richtig, dass eine Einzelfallprüfung wegen der Safe-Harbor-Entscheidung nicht mehr erforderlich sei, so hieße dies, dass ein Datentransfer in die USA leichter

---

[101] JB 1999, 4.7

[102] vom 5. Juli 2000, BR-Drs. 478/00

[103] Entscheidung vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. EG, L 215/7, vgl. Anlagenband „Dokumente zum Datenschutz 2000“, S. 23

zu vollziehen wäre als derjenige von einem europäischen Mitgliedsstaat in den anderen.

Nach der Veröffentlichung des Safe-Harbor-Konzeptes durch das US-Handelsministerium[104] wurde eine Liste für beigetretene „Harborites“ eingerichtet, die seit dem 1. November öffentlich zugänglich und online abrufbar ist[105]. Eingetragen waren zum Beginn des Jahres 2001 ein Duzend Unternehmen, im Wesentlichen solche, die Personaldaten verarbeiten. Aus der Liste soll auch hervorgehen, ob ein Unternehmen den ihm einmal verliehenen Safe-Harbor-Status verloren hat, etwa weil es die Datenschutzgrundsätze missachtet hat. Die US-Unternehmen können sich im Wege sog. Selbstzertifizierung gegenüber dem US-Handelsministerium oder einer von diesem benannten Stelle auf die Einhaltung der Grundsätze verpflichten. Der Beitritt zu Safe-Harbor ist freiwillig. Ist er jedoch erfolgt, so sind die Regelungen verbindlich.

Die US-Organisationen, die dem Safe-Harbor beitreten, müssen sich einem Durchsetzungsmechanismus unterwerfen. Hierzu können sie sich zur Zusammenarbeit mit den europäischen Datenschutzbehörden verpflichten. Diese Zusammenarbeit erfolgt durch Beratung, die von einem informellen Gremium (dem „Panel“) durchgeführt wird, dem diese beitreten können. Das „Panel“ wird in den Fällen tätig, in denen der nationalen Aufsichtsbehörde die Beilegung des Streits nicht möglich gewesen ist. Die Koordinierung der Verfahrensweisen der nationalen Aufsichtsbehörden erfolgt auf der Grundlage eines von der Art. 29-Gruppe am Ende des Jahres verabschiedeten Papiers[106]. Der Berliner Beauftragte für Datenschutz und Akteneinsicht hat die bundesweite Koordinierung der strittigen Fälle, die von den Aufsichtsbehörden zur Einbringung in das „Panel“ vorgesehen sind, ebenso wie die Mitarbeit im „Panel“ als Vertreter der deutschen Aufsichtsbehörden übernommen.

**Übermittlung in Drittländer**

Die Europäische Kommission hat sich Ende Juli auch zur *Angemessenheit des Schutzniveaus* in den Ländern *Schweiz* und *Ungarn*[107] geäußert und auch hier positive Entscheidungen nach Art. 25 Abs. 6 Europäische Richtlinie getroffen. Entsprechende Entscheidungen über das Datenschutzniveau in Kanada und Australien sind in Vorbereitung.

---

[104] Department of Commerce, Federal Register / Vol. 65, No. 142, 45666, 24. Juli 2000

[105] http://www.export.gov/safeharbor/

[106] Anlagenband „Dokumente zum Datenschutz 2000“, S. 51

[107] vom 26. Juli 2000, ABl. EG vom 25. August 2000, L 215/1 und L 215/4

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Solange eine Entscheidung über das Datenschutzniveau im Drittland von der Kommission nicht getroffen worden ist, können Datenübermittlungen auch unter den Voraussetzungen des Art. 26 Abs. 2 erfolgen. Hier kommt insbesondere eine Datenschutzvereinbarung zwischen Datenexporteur und Datenimporteur in Betracht, die ausreichende *Datenschutzgarantien* vorsehen muss. Die Bemühungen, einen *Modellvertrag* zu entwerfen, der die Mindestkriterien in diesem Sinne berücksichtigt, sind zahlreich und vielfältig, jedoch kaum jemals bis zum Ende betrieben worden. Kurz vor der Verabschiedung steht aber eine Entscheidung der Europäischen Kommission nach Art. 26 Abs. 4 Datenschutzrichtlinie, nach dem festgestellt werden kann, dass bestimmte Standardvertragsklauseln ausreichende Garantien vorsehen. Die Standardklauseln, die u.a in enger Anlehnung an Modellvertragsentwürfe des International Chamber of Commerce (ICC) und der Chamber of British Industries (CBI) entwickelt worden sind, sind in einem Anhang zur Entscheidung behandelt (Annex). In einem Vertragsanhang müssen Datenexporteur und -importeur insbesondere den Übermittlungszweck und die Kategorie übermittelter Daten (z. B. Arbeitnehmerdaten) näher bezeichnen. Verbindliche Datenschutzgrundsätze (z. B. Zweckbindung, Transparenz) sind ebenfalls in einem Anhang zum Vertrag enthalten und als Mindestanforderungen für den Datenschutz zu vereinbaren. Die Beratungen der Datenschutzgruppe nach Art. 29 und die Beteiligung des Ausschusses der Regierungsvertreter nach Art. 31 waren zum Jahresende noch nicht abgeschlossen.

Die Initiativen, die auf europäischer Ebene in jüngster Zeit entwickelt worden sind, zeigen, dass die nationalen Aufsichtsbehörden viel Arbeit erwartet, insbesondere dann, wenn die Umsetzung der Europäischen Datenschutzrichtlinie in das nationale Recht erfolgt ist und die internationalen Datentransfers von der Aufsichtsbehörde genehmigt werden müssen. Die entsprechenden Regelungen werden voraussichtlich in §§ 4 b) und 4 c) des neuen BDSG enthalten sein, mit dessen Verabschiedung nach derzeitigen Erkenntnissen im nächsten Frühjahr gerechnet wird.

Der Senat hat das Problem der Übermittlung von Daten in Drittländer in seinem Gesetzentwurf zur Novelle des Berliner Datenschutzgesetzes besonders berücksichtigt.

**Anwendbares Recht**

*Ein französisches Markt- und Meinungsforschungsinstitut führt in Deutschland eine Umfrageaktion durch, ohne eine eigene Niederlassung zu betreiben oder auf Datenverarbeitungsmöglichkeiten zurückzugreifen, die hier „belegen" sind (so der Wortlauf der Richtlinie).*

Dieser Fall zeigt, dass bei der datenschutzrechtlichen Bewertung für die deutsche Aufsichtsbehörde künftig nicht immer nur deutsches Recht maßgeblich sein muss. Nach § 1 Abs. 5 Satz 1 BDSG n. F. findet dieses Gesetz keine Anwendung, sofern eine in einem anderen Mitgliedsstaat der Europäischen Union bele-

gene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Die deutsche Aufsichtsbehörde hat also bei der Prüfung, ob die bei den in Deutschland durchgeführten Umfragen erfolgte Datenerhebung zulässig ist, nicht deutsches, sondern französisches Datenschutzrecht anzuwenden. In der Art. 29-Gruppe wurde vereinbart, dass in derartigen Fällen die jeweilige nationale Aufsichtsbehörde um Unterstützung bei der datenschutzrechtlichen Bewertung gebeten werden kann.

Dass die Frage des anwendbaren Rechts derzeit unter Berücksichtigung der in Art. 4 Abs. 1 a) Europäische Richtlinie enthaltenen Regelung nicht immer so leicht zu beantworten ist, zeigt folgender Fall:

*Wenn ein Kunde in Deutschland eine Kreditkarte von American Express haben will, wird der Antrag mit den erforderlichen personenbezogenen Daten (zumeist durch die ortsansässige Bank) an die deutsche Dependance von American Express International (Sitz in Frankfurt a.M.) weitergegeben. Diese Einrichtung nimmt die Daten des Kunden entgegen und gibt sie an die in England ansässige Niederlassung weiter, mit der der Kunde auch den Kreditkartenvertrag schließt. Von hier werden die Daten in das in den USA befindliche Rechenzentrum der Muttergesellschaft gegeben. Für das Vertragsverhältnis gilt nach den AGB deutsches Recht.*

Nach Art. 4 Abs. 1 a) Europäische Richtlinie gilt für die Datenverarbeitung der verantwortlichen Stelle das Recht des Landes, in dem sie ihre Niederlassung hat. In der Arbeitsgruppe „Internationaler Datenverkehr“ des Düsseldorfer Kreises wurde diskutiert, unter welchen Beteiligten eine Datenübermittlung im Sinne von Art. 25, 26 Europäische Richtlinie stattfindet. Zum Teil wurde die Auffassung vertreten, dass das in Deutschland befindliche Büro die Daten der deutschen Kunden nur als Übermittlungsbote für das in England befindliche Unternehmen entgegennehme und eine Datenübermittlung aus Deutschland nicht stattfinde. Nach überwiegender Ansicht schließt jedoch allein die beschränkte Funktion des Büros das Vorliegen einer Niederlassung nicht aus. Vielmehr spricht schon der Umstand, dass offenbar Geschäftsräume unterhalten werden und Personal beschäftigt wird, für die Annahme einer Niederlassung. Insofern ist deutsches Recht für die durch das Frankfurter Büro erfolgende Datenverarbeitung zu berücksichtigen. Käme man zu der Auffassung, dass das Büro in Deutschland nicht die (von der Richtlinie nicht näher definierten) Kriterien einer Niederlassung erfüllt, so hieße dies, dass angesichts der vorhandenen englischen Niederlassung als für das Kundenvertragsverhältnis maßgebliches nationales Datenschutzrecht das englische gelten müsste. Dieses kann dann aber nicht - anders als im internationalen Kaufrecht - von den Parteien (zugunsten deutschen Rechts) abbedungen

werden, denn das europäische Datenschutzrecht ist zwingend.

### 4.8. Organisation und Technik

#### 4.8.1. Sicherheit vor Viren und sicheres Surfen im Internet

Anfang Mai 2000 verbreitete sich der *Computerwurm* „ILOVEYOU“ in rasender Geschwindigkeit über die ganze Welt. Dies führte zu erheblichen Beeinträchtigungen bei der Nutzung des Internet. Das Surfen im Internet oder der Versand von elektronischer Post (Email) erfolgte nur noch sehr schleppend, weil die Mail-Server so überlastet waren, dass sie eine Weiterarbeit nicht mehr zuließen. Außerdem verursachte der Wurm noch weitere Schäden, weil er Dateien auf den Computern löschte bzw. unbrauchbar machte.

Die Verbreitung wurde wesentlich dadurch begünstigt, dass nicht hinreichend informierte oder geschulte Personen die Erfahrungen unbeachtet ließen, die aus früheren Virusattacken, z. B. des Melissa-Wurms im März 1999, gezogen werden mussten. Obwohl bei „ILOVEYOU“ viele Merkmale vorhanden waren, die Verdacht hätten auslösen können, wurde das Attachment der ILOVEYOU-Email unbedacht geöffnet. Es enthielt eine Visual Basic Skript-Datei, die mit ihrer Öffnung ausgeführt wurde und sich damit an alle im Adressbuch von Microsoft Outlook gespeicherten Nutzer versandte und dort wieder auf unachtsame Benutzer wartete.

Dieses spektakuläre Ereignis, welches für kurze Zeit das Thema der informationstechnischen Sicherheit in die Schlagzeilen brachte, war für uns Anlass, ein Faltblatt herauszugeben, dessen Schwerpunkt Schutzmaßnahmen gegen den Befall mit schadenverursachender Software und Sofortmaßnahmen nach einem Befall bildeten[108].

Es werden folgende vorbeugende Maßnahmen empfohlen:

- Die Installation eines speicherresidenten Virenschutzprogramms zur Entdeckung virenartigen Verhaltens, zur Untersuchung von beweglichen Datenträgern und aus dem Internet (z. B. per E-Mail) empfangener Dateien und zur regelmäßigen Untersuchung der eingebauten Massenspeicher ist die wichtigsten vorbeugende Maßnahme. Das Virenschutzprogramm ist ständig über die Aktualisierungsdienste der Hersteller auf dem aktuellen Stand zu halten.
- Die Aktivierung der Anzeige aller Dateitypen in Dateiverwaltungsprogrammen, wie z. B. dem Win-

Der Schutz vor den Risiken, die aus Viren oder ähnlicher Software mit Schadenswirkung oder aus dem Einsatz so genannter aktiver Inhalte bei der Internet-Nutzung entstehen, hat für den Senat eine hohe Priorität.

Die entstehenden Risiken und entsprechende Maßnahmen werden u. a. auch in den IT-Sicherheitsberichten der Jahre 1999 und 2000 angesprochen. Die gültigen IT-Sicherheitsstandards legen vielfältige Maßnahmen fest, mit denen ein Schutz vor diesen Risiken erreicht werden kann. Die inhaltliche Ausrichtung dieser Maßnahmen stimmt in allen wesentlichen Punkten mit den Empfehlungen des Berichtes überein.

Es kann insgesamt eingeschätzt werden, dass die durchgeführten Maßnahmen in vielen Bereichen bereits einen adäquaten Schutz gewährleisten. So war zwar z. B. auch die Berliner Verwaltung vom „ILOVEYOU“ –Virus betroffen, ein relevanter Schaden entstand jedoch nur in vereinzelten Fällen.

Den Empfehlungen ist in vollem Umfang zuzustimmen. Die technischen Maßnahmen in einigen Dienstgebäuden entsprechen den Empfehlungen nicht nur, sondern gehen sogar teilweise darüber hinaus.

[108] BlnBDA: Ratgeber zum Datenschutz Nr. 4, Computerviren und andere Softwareangriffe, Dezember 2001

dows Explorer, hilft bei der Entdeckung der riskanten ausführbaren Dateitypen .

- Die Erkennung und Beseitigung von Makroviren in den Makro-Ergänzungen von Dateien, die mittels Standardanwendungsprogrammen erzeugt werden (z. B. Dokumenten aus Textprogrammen, Tabellen und Mappen aus Tabellenkalkulationsprogrammen, Präsentationen aus Präsentationserstellungsprogrammen), mit Hilfe der aktuellen Virenschutzprogramme ist ebenfall dringend zu raten. In der Regel haben die Makros, die solchen Dateien anhängen, für die Nutzung der Dateien keine besondere Bedeutung, so dass ihre Ausführung unterbunden werden kann. Die Anwendungsprogramme (z. B. bei WinWord) verfügen z. T. über Mechanismen, die vor angehängten Makros warnen können, wenn sie aktiviert werden, bzw. die das automatischen Ausführen von Makros unterbinden.

Bei der Übertragung von Texten als Anlage von E-Mails sollte darauf geachtet werden, dass Dokumente in einem Format übersandt werden, welches keine Makros enthält. Zum Beispiel heißt dies, dass WinWord-Dokumente als RTF- oder - mit erheblichen Qualitätseinbußen - TXT-Dokumente übertragen werden sollten. Für Textsysteme anderer Hersteller stehen ebenfalls internationale Austauschformate zur Verfügung, die keine Makros übertragen.

Sofern Dokumente in Formaten empfangen werden, die die Mitsendung von Makros nicht unterbinden, kann man der Gefahr der Öffnung virenverseuchter Makros dadurch entgehen, dass die Dokumente nur mit Viewern geöffnet werden, die die Makros unberücksichtigt lassen. Bei WinWord-Dokumenten aus älteren Versionen (bis Word 95) entsteht ein solcher Sicherheitseffekt auch, wenn sie mit WordPad geöffnet werden. Viewer stehen auch für Präsentationssoftware (z. B. PowerPoint) oder Tabellenkalkulationssoftware (z. B. Excel) zur Verfügung.

- Internet-Browser bieten einen gewissen Schutz gegen Viren, wenn ihre Sicherheitseinstellungen auf ein hohes Schutzniveau reguliert werden, damit aktive Inhalte (ActiveX, Java und Java Skript), die Viren enthalten können, deaktiviert sind. Allerdings sind diese Funktionen vom Hersteller standardmäßig aktiviert, da ihre Deaktivierung zu Beeinträchtigungen bei der Internetnutzung führt. Dies bedeutet, dass die Browser eine Schutzwirkung nur dann entfalten, wenn der Benutzer vorher die Grundeinstellungen entsprechend angepasst hat.

Wenn man aber differenzierter auf aktive Elemente reagieren will, also im Einzelfall entscheiden will, ob man den aktiven Elementen einer angewählten Homepage vertrauen will oder nicht, ohne jedes Mal die Sicherheitseinstellungen des Internet-Browsers umständlich modifizieren zu müssen, so ist der Einsatz spezieller „Surf-“Schutzsoftware“ zu empfehlen. Sie

erlaubt den flexibleren Umgang mit aktiven Elementen. Dies ist sinnvoll, weil viele wichtige Websites ohne Zulassung aktiver Elemente nicht gelesen werden können.

- Die regelmäßige Datensicherung zum Schutz der Daten vor Verlust oder Beschädigungen sollte selbstverständlich sein. Je wichtiger die Daten sind, desto kürzer sollte der Abstand zwischen den einzelnen Sicherungsläufen sein.

- Es sollten eine oder mehrere Notfalldisketten (SOS-Disketten) nach den Vorgaben des Herstellers von Virenschutz-Programmen angelegt werden, mit welchen der Computer virenfrei gestartet werden kann. Nach dem virenfreien Start muss dann das Virenschutz-Programm ausgeführt werden.

Wie der Trojaner ILOVEYOU zeigte, stellen E-Mails inzwischen die größte Ansteckungsgefahr dar. In der Zwischenzeit gibt es Erfahrungen darüber, unter welchen Umständen man mit Virusattacken rechnen sollte. Wenn z. B. der Text nicht zum Absender passt (z. B. englischer Text vom deutschen Bekannten), der fehlende Bezug zu vorausgegangenen Schreiben auffällt, weitere Kopien zu unbekannten Adressaten gesandt wurden, mehrere Nachrichten mit gleich lautendem Betreff eingehen und Begriffe wie „Geld“, „Sex“, „Geheim“ usw. in der Betreffzeile auftreten, sollte man Vorsicht walten beim Öffnen der Anhänge, besser sogar der ganzen Sendung.

Wir empfehlen, ausführbaren Code (z. B. Programme, Skripte oder Makros) erst lokal abzuspeichern, auf Computeranomalien zu prüfen und anschließend auszuführen oder zu öffnen, wenn keine Gefahr besteht. Offensichtlich inkorrekte E-Mails oder so genannte Spam-Mails (z. B. Werbung per E-Mail) sollten ungeöffnet gelöscht werden.

Getreu der Vermutung, dass jedes Aktivieren unbekannten ausführbaren Codes mit Vorsicht erfolgen soll, sollte das Herunterladen von Programmen aus dem Internet ausschließlich von vertrauenswürdigen Internetseiten erfolgen, wie z. B. die Originalseiten von Hard- und Softwareherstellern. Sammlungen von Treibern und Softwaretools auf privaten Homepages stellen hierbei eine besondere Gefahr dar, denn mit ihnen wird häufig schadensverursachende Software verbreitet. Wie bei E-Mails gilt auch beim Downloaden, dass die Dateien erst auf die lokale Festplatte gespeichert werden sollten. Bei gepackten Dateien kommt hinzu, dass diese zuerst nach dem Download entpackt , dann auf Computeranomalien geprüft und erst zum Schluss ausgeführt werden sollten.

Für das sichere Surfen werden noch folgende *Tipps* zur Hand gegeben:

- Unter der Internet-Adresse des Landesbeauftragten für Datenschutz in Niedersachsen „www.lfd.niedersachsen.de“ kann ein Selbsttest, mit

Dieser Selbsttest kann falsche Ergebnisse liefern, sofern sich der zu prüfende Client hinter einem (korrekt konfigurierten) Firewall-Server befindet.

dem die Sicherheit eines PC-Systems geprüft und verbessert werden kann, durchgeführt werden. Auch auf den Internet-Seiten von „heise-online“ kann unter der Adresse „www.heise.de/browsercheck/“ ein Browser-Check durchgeführt werden. Hierbei werden z. B. die einzelnen Browser-Funktionen erläutert oder deren Missbrauchspotenzial demonstriert. Natürlich sollten die Sicherheitseinstellungen der Browser den Ansprüchen des Surfers angepasst eingestellt werden. Hierfür sollte eine hohe Sicherheitsstufe gewählt werden und z. B. JavaScript und ActiveX abgestellt bzw. auf lokale Adressen begrenzt werden.

- Insbesondere sollte beim Online-Banking darauf geachtet werden, dass z. B. Überweisungen nur über eine verschlüsselte WWW-Seite erfolgen. Dies ist an den Hinweisen zu erkennen, wenn der Internet-Browser bei der URL-Adresse ein s - „shttp://www.banke.de/...“ - vorangestellt hat und in der linken unteren Ecke des Browserfensters ein Schloss zu sehen ist. Aber natürlich ist es auch ratsam, E-Mails zu verschlüsseln. Hierfür werden Privatleuten kostenfreie Tools wie z. B. ‘PGP’ angeboten.
- Zur Sicherung von Netzverbindungen oder Konfigurationseinstellungen werden Passwörter vergeben. Beispielsweise sendet der Internetprovider dem Nutzer für die Einwahl in das Internet eine Nutzerkennung und ein dazugehörendes Passwort. Dieses Passwort sollte beim ersten Anmelden unmittelbar geändert und nicht im Anmeldeprogramm, also auf der Festplatte, gespeichert , sondern bei jeder Anmeldung erneut eingeben werden. Bei Hardware-Komponenten wie z. B. Routern, sind die Passwörter vom Hardwarehersteller voreingestellt. Natürlich sollten diese Standardvorgaben nach der erfolgreichen Installation unverzüglich verändert werden. Zur Auswahl sicherer Passwörter verweisen wir auf unser Faltblatt[109].

### 4.8.2 Behördliche Datenschutzbeauftragte

Zu den wichtigsten Multiplikatoren des Datenschutzgedankens in der Berliner Verwaltung gehören die behördlichen Datenschutzbeauftragten, die in den Behörden des Landes gesetzlich festgelegte Aufgaben und Pflichten wahrzunehmen haben. Auch im Berichtsjahr gehörte es zu unseren wichtigsten Tätigkeiten, die behördlichen Datenschutzbeauftragten bei ihrer Arbeit zu unterstützen und zur Verbesserung der Bedingungen, unter denen sie - meist im Nebenamt und gegen mehr oder weniger offenen Widerstand ihrer Dienstherren - ihren Pflichten nachkommen, beizutragen.

---

[109] BlnBDA: Empfehlungen für die Vergabe von Passwörtern, Ratgeber zum Datenschutz Nr. 3, Oktober 2000

**Koordinierungsrunde der bezirklichen Datenschutzbeauftragten**

Regelmäßig zwei bis dreimal im Jahr finden Koordinierungbesprechungen der bezirklichen Datenschutzbeauftragten statt, die wir logistisch und mit fachlicher Beratung unterstützen.

Im Berichtsjahr lag ein Schwerpunkt auf den Fragen zu Auslegung und Anwendung des Informationsfreiheitsgesetzes (IFG). Einen breiten Raum nahmen naturgemäß die Fragen zum Verhältnis von Informationsfreiheit und Datenschutz ein.

Weiterhin wurde die vom Landesbetrieb für Informationstechnik entwickelte Benutzerrichtlinie für die Nutzung von Online-Diensten diskutiert, die bereits in mehreren Bezirksverwaltungen Anwendung findet. Bei den komplexen rechtlichen Rahmenbedingungen der Telekommunikation gibt es in der Praxis erhebliche Abgrenzungsschwierigkeiten. Für die Bezirksvertreter waren die Fälle von besonderem Interesse, in denen die Verwaltung als Informationsanbieter auftritt. Hier kommt mit dem Telekommunikationsgesetz (TKG) für den Bereich der Telekommunikation, dem Informations- und Kommunikationsdienstegesetz (IuKDG) mit dem Teledienstegesetz (TDG), dem Teledienste-Datenschutzgesetz (TDDSG) und dem Signaturgesetz (SigG) sowie dem Mediendienste-Staatsvertrag (MDStV) für die Individualkommunikation eine Vielzahl schwieriger Rechtsgrundlagen zum Tragen. Hinzu kommen die Gesetze, die für die Inhalte von Informationsangeboten gelten wie z. B. das Strafgesetzbuch.

Aus nahe liegenden Gründen wurde in diesem Kreis auch die Stellung des behördlichen Datenschutzbeauftragten nach der Fusion in den künftigen Großbezirken diskutiert. Von einem der Teilnehmer wurde hierzu ein Diskussionspapier entwickelt, das drei künftige Modelle skizziert, die darauf abzielen, die nach der Fusion überzähligen behördlichen Datenschutzbeauftragten in eine neue Datenschutzinfrastruktur mit hauptamtlichen Datenschutzbeauftragten und ggf. ein bis zwei Stellvertretern zu integrieren. Die Modelle unterschieden sich hauptsächlich dadurch, ob die Datenschutzbeauftragten nach dem Ressortprinzip, also für die einzelnen Ämter/LUV´s, oder nach dem Funktionsprinzip, also nach den Sachgebieten Recht und Informatik, zuständig sein sollten. In jedem Fall sollten die Aufgaben des Datenschutzbeauftragten nach SGB X nicht mehr getrennt wie früher von einem eigenständigen SGB-Datenschutzbeauftragten wahrgenommen werden, sondern nunmehr von dem bezirklichen Datenschutzbeauftragten in Personalunion erledigt werden. Favorisiert wurde von den Teilnehmern letztlich das Modell, wonach der bezirkliche Datenschutzbeauftragte für alle LUV´s und Serviceeinheiten zuständig sein soll. Von ihm sollen auch Ansprechpartner für Datenschutzfragen

Der Senat beabsichtigt, im Jahre 2001 eine Rahmendienstvereinbarung mit dem Hauptpersonalrat zur Nutzung des Internet abzuschließen. Dabei werden insbesondere auch die sich aus den rechtlichen Grundlagen ergebenden Aspekte zum Datenschutz berücksichtigt. Der Text der Vereinbarung wird dazu u. a. auch mit dem BlnBDA intensiv abgestimmt.

Auf der Grundlage einer solchen allgemeinen Regelung können dann die bisher teilweise bereits vorhandenen behördenspezifischen Regelungen zur Nutzung des Internet aktualisiert werden.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

aus jedem LUV bzw. aus großen Standorten ausgewählt werden, die vor Ort auf die spezifischen Datenschutzbelange zu achten haben und mit denen er sich in regelmäßigen Abständen zur Koordinierung der Tätigkeiten zusammensetzt.

Von unserer Seite wurde insbesondere darauf hingewiesen, dass durch den Aufgabenzuwachs der Arbeitsaufwand nicht mehr nebenbei erledigt werden kann und dass es unbedingt erforderlich ist, einen Stellvertreter benennen, damit in Zeiten der Abwesenheit des hauptamtlichen Datenschutzbeauftragten die Sicherstellung des Datenschutzes in der Daten verarbeitenden Stelle gewährleistet werden kann.

Siehe hierzu Stellungnahme des Senats zu 4.8.2 „Stellung des behördlichen Datenschutzbeauftragten in den Fusionsbezirken“ (S. 165).

Einzelne Fragestellungen, die bisher nicht so sehr im Blickpunkt standen, erlangten mit der Bezirksfusion ungeahnte Bedeutung:

**Mitwirkung bei der Personalauswahl**

In den meisten Behörden wird die Vorschrift, wonach der behördliche Datenschutzbeauftragte bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen beratend mitwirken soll,[110] nicht praktisch umgesetzt. Häufig erschließt sich auch nicht der Sinn dieser Vorschrift, weil nicht klar ist, auf welche Dinge der behördliche Datenschutzbeauftragte bei der Personalauswahl eigentlich zu achten hat. Dies ist gerade bei Stellenbesetzungen, die nicht intern vorgenommen werden, auch sehr gut nachzuvollziehen. Anders ist dies bei der internen Besetzung von Stellen, wenn also auf Positionen, in denen die Einstellung zum Datenschutz und die Bereitschaft zur Beachtung der einschlägigen Gesetze eine große Bedeutung haben, Mitarbeiter gesetzt werden sollen, zu denen sich die behördlichen Datenschutzbeauftragten ein Bild machen können. Im Zusammenhang mit der Neubesetzung der Führungspositionen in den Fusionsbezirksämtern haben einige behördliche Datenschutzbeauftragte ihren Rechtsanspruch auf Beteiligung bei der Personalauswahl geltend gemacht. In vielen Fällen wurde dies entgegen eindeutiger Gesetzeslage abgelehnt.

Aufgrund der Weisungsfreiheit, die der behördliche Datenschutzbeauftragte nach § 36 Abs. 3 Satz 2 BDSG i.V.m. § 19 Abs. 5 BlnDSG genießt, ist es seiner Entscheidung zu überlassen, in welcher Form er mitwirken will. In jedem Fall ist ihm durch rechtzeitige Unterrichtung Gelegenheit zu geben, sich an der Auswahl zu beteiligen.

Wird dem behördlichen Datenschutzbeauftragten die Mitwirkung bei der Personalauswahl verweigert, liegt ein Grund für eine Beanstandung nach § 26 BlnDSG vor. Dies könnte auch bedeuten, dass ein Stellenbesetzungsverfahren wegen dann vorliegender rechtlicher Mängel angefochten werden könnte.

Die unter Hinweis auf § 37 Abs. 1 Nr. 3 BDSG i.V.m. § 19 Abs. 4 BlnDSG vertretene Auffassung, wonach die Mitwirkung des behördlichen Datenschutzbeauftragten bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen ein Mitwirkungsrecht des behördlichen Datenschutzbeauftragten bei der Personalauswahl für Stellenbesetzungen gewährleiste und die daran geknüpfte Vermutung, die Verweigerung dieser Mitwirkung des Datenschutzbeauftragten „könnte auch bedeuten, dass ein Stellenbesetzungsverfahren wegen dann vorliegender rechtlicher Mängel angefochten werden könnte“, ist fernliegend.

Hierbei kann das Ausmaß des Beteiligungsrechts des behördlichen Datenschutzbeauftragten (beratende Mitwirkung bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen) unerörtert bleiben. Soweit hier unterschiedslos von Stellenbesetzungen gesprochen wird, sind Abordnungen, Umsetzungen bzw. konkrete Vergaben von Dienstposten genauso mitumfasst wie Beförderungen. Wenn eine Anfechtung wegen vorliegender rechtlicher Mängel für möglich gehalten wird, ist hierbei jedoch zu unterscheiden.

Abordnungen gem. § 62 LBO sind rechtlich zulässig, wenn ein dienstliches Bedürfnis besteht. Eine rechtliche Anfechtung ist hier lediglich durch den abgeordneten Beamten denkbar. Rechtlich zu diskutieren ist hier das dienstliche Bedürfnis und nicht eine interne Beteiligungsvorschrift.

Umsetzungen und konkrete Dienstpostenzuweisungen stehen im weiten Direktionsrecht des Dienstherrn. Ein Beamter hat keinen Anspruch auf unveränderte und ungeschmälerte Ausübung des ihm übertragenen konkret-funktionalen Amtes.

[110] § 37 Abs.1 Nr. 3 BDSG i.V.m. § 19 Abs. 5 BlnDSG

Vielmehr kann der Dienstherr aus jedem sachlichen Grund den Aufgabenbereich des Beamten verändern, solange diesem ein amtsangemessener Aufgabenbereich verbleibt. Bei der Ermessensausübung sind dem Dienstherrn sehr weite Grenzen gesetzt. Aus diesen Gründen kann die Rechtmäßigkeit einer Umsetzung im allgemeinen nur darauf überprüft werden, ob sie maßgebend durch einen Ermessensmissbrauch geprägt ist. Deshalb ist die Prüfung grundsätzlich darauf beschränkt, ob die Gründe des Dienstherrn nicht nur vorgeschoben sind, um eine in Wahrheit allein oder maßgebend auf anderen Beweggründen beruhende Entscheidung zu rechtfertigen oder ob sie aus anderen Gründen willkürlich ist. Verwaltungsinterne Beteiligungsrechte könnten, wenn überhaupt, nur innerhalb der vorgenannten Grenzen von Bedeutung sein. Soweit eine Maßnahme nicht im Ergebnis willkürlich ist, kann die etwaige Verletzung interner Beteiligungsrechte nicht durchgreifen. Stellenbesetzungen, die mit einer Beförderung einhergehen, sind aufgrund von Art. 33 Abs. 5 nach dem Leistungsgrundsatz („Bestenauslese“) durchzuführen. Bei der Bewertung der Bewerber nach Eignung, Befähigung und fachlicher Leistung steht dem Dienstherrn eine Beurteilungsermächtigung zu. Sie umfasst die Festlegung und Gewichtung der in Betracht kommenden Auswahlkriterien. Ob die Eignung eines Bewerbers vom Dienstherrn zutreffend beurteilt worden ist, kann gerichtlich nur daraufhin überprüft werden, ob der Dienstherr den gesetzlichen Rahmen seiner Beurteilungsermächtigung verkannt hat, von einem falschen Sachverhalt ausgegangen ist, allgemeine Wertmaßstäbe nicht berücksichtigt oder sachwidrige Erwägungen angestellt hat oder verfahrensfehlerhaft vorgegangen ist. Verfahrensfehler können danach nur von Bedeutung sein, soweit sie sich auf den Leistungsgrundsatz auswirken könnten.

Die Auswahlentscheidung über die Besetzung einer Beförderungsstelle ist aufgrund eines aktuellen Leistungs- und Eignungsvergleichs der Bewerber vorzunehmen. Hierbei sind alle Gesichtspunkte zu berücksichtigen, die für die Beurteilung von Eignung, Befähigung und fachlicher Leistung bedeutsam sind. Wesentliche Grundlage sind die Personalakten der Bewerber, aus denen sich deren schulische und berufliche Aus- und Fortbildung einschließlich der Abschluss- und etwaiger Laufbahnprüfungen, der berufliche Werdegang und auch bisherige Leistungsbeurteilungen ergeben. Aufgrund dieses von der höchstrichterlichen Rechtsprechung allgemein anerkannten Prüfungsansatzes ist es fernliegend, einer unterlassenen Mitwirkung des behördlichen Datenschutzbeauftragten bei der Personalauswahl einen durchgreifenden Anfechtungsgrund zu entnehmen.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

**Stellung des behördlichen Datenschutzbeauftragten in den Fusionsbezirken**

Die Bezirksreform und die damit zusammenhängende Fusion von jeweils 2 bis 3 Bezirken zu Großbezirken haben wir zum Anlass genommen, den Bezirksbürgermeistern in einem Rundschreiben zu empfehlen, die Stellung und die qualitative Ausstattung des behördlichen Datenschutzbeauftragten neu zu überdenken.

Da sich mit den Vorgaben der EG-Datenschutzrichtlinie und der im Entwurf des neuen Bundesdatenschutzgesetzes erkennbaren Zielrichtung neue und umfangreiche Aufgaben für den behördlichen Datenschutzbeauftragten ergeben (u. a. Durchführung einer Vorabkontrolle bei Einführung neuer und grundlegender Änderung alter Verfahren), gehen wir davon aus, dass die künftigen Großbezirke in Anbetracht ihrer stark gewachsenen Mitarbeiterzahl und der hohen Zahl der zu betreuenden Bürger folgende Voraussetzungen für ihre Datenschutzbeauftragten schaffen müssen:

Es ist ein behördlicher Datenschutzbeauftragter zu bestellen, der seine Aufgaben als Vollzeitkraft erfüllen kann und der dem Bezirksamt unmittelbar berichtspflichtig ist. Damit entfallen auch alle bisherigen Probleme der Kompatibilität mit anderen Ämtern.

Daneben ist eine Stellvertreterregelung zu schaffen, bei der bei Abwesenheit des hauptamtlichen Datenschutzbeauftragten eine Person seines Vertrauens seine Aufgaben übernehmen kann. Diese Funktion könnte nebenamtlich übernommen werden.

Dem behördlichen Datenschutzbeauftragten ist die Möglichkeit zu geben, eine interne Datenschutzinfrastruktur aufzubauen, die ihn dabei unterstützt, seine Aufgaben in allen Ämtern (LUV´s) und in den verschiedenen bezirklichen Standorten ordnungsgemäß und zeitgerecht wahrzunehmen. In diesem Zusammenhang wäre es denkbar, wenn zu diesem Zweck aus jedem Amt (LUV), aber auch aus jedem größeren örtlichen Bereich eine Kontaktperson benannt wird, die in ihrem Bereich auf die Belange des Datenschutzes achtet und dem behördlichen Datenschutzbeauftragten beratend und unterstützend zuarbeitet. Der hauptamtliche Datenschutzbeauftragte hätte dann die Prüf- und Beratungstätigkeiten seiner Helfer und die Organisation regelmäßiger Zusammenkünfte und Abstimmungen zu koordinieren. Der Stellvertreter könnte aus dem Kreis der Kontaktpersonen benannt werden.

Wir haben den Bezirksbürgermeistern ein abgestimmtes und einheitliches Vorgehen in allen Bezirksverwaltungen empfohlen.

Mit der Frage der Einrichtung bezirklicher Datenschutzbeauftragter und deren Vertretern aufgrund der geänderten europarechtlichen Vorschriften hat sich der Senat bereits im Rahmen der Behandlung der Vorlage Nr. 925/01 („Gesetz zur Änderung des Berliner Datenschutzgesetzes und anderer datenschutzrechtlicher Regelungen“) befasst. Darin wird festgestellt, dass personeller Mehrbedarf nicht anerkannt werden kann, sondern die Aufgabenwahrnehmung im Rahmen der bestehenden Möglichkeiten finanziert werden muss. Zudem erlaubt die neue Regelung, dass mehrere Behörden einen gemeinsamen Datenschutzbeauftragten bestellen, was zu personalwirtschaftlicher Entlastung führen kann.

**4.8.3 Prüfungen im privaten Bereich**

Die zahlreichen Kontrollen bei Unternehmen, die nach § 32 BDSG meldepflichtig sind und daher der Kontrolle vom Amts wegen unterliegen, haben unseren Eindruck aus den Vorjahren bestätigt, dass Firmen, deren Existenzgrundlage die Verarbeitung und Nutzung von personenbezogenen Daten ist, dem Datenschutz und der Datensicherheit überwiegend eine hohe Priorität einräumen.

Natürlich wurden auch Mängel vorgefunden:

Entgegen der aus § 11 Abs. 2 Satz 2 BDSG folgenden Verpflichtung, bei der Beauftragung von Serviceunternehmen zur Durchführung von Datenverarbeitung mit dem Auftragnehmer schriftliche Verträge abzuschließen, ist es zwischen kleineren Unternehmen üblich geworden, im Falle von *Auftragsdatenverarbeitung* Verträge „per Handschlag“ zu machen. Dies wird mit branchenüblichen Gebaren begründet. Der Auftraggeber hat jedoch nicht nur auf die besondere Eignung des Auftragnehmers für die von ihm ausgelagerten Arbeiten zu achten, sondern auch Vorgaben zu machen, in denen die einzelnen Schritte der Datenverarbeitung, die technischen und organisatorischen Datenschutzmaßnahmen und auch etwaige Unterauftragsverhältnisse genau festzulegen sind. Nur wenn diese Festlegungen schriftlich vorliegen, können sie Gegenstand der Kontrolle durch die interne Revision, den Auftraggeber oder die Aufsichtsbehörde werden und kann die Ordnungsmäßigkeit der Datenverarbeitung gewährleistet werden. Aus diesem Grunde wird eine Abweichung vom Schriftlichkeitsgebot von uns beanstandet.

Mit der Verbreitung von *Internetanwendungen* ist festzustellen, dass viele Firmen dieses Medium zwar gern und häufig benutzen, dabei aber teilweise die erforderlichen Sicherungsmaßnahmen außer Acht lassen. So wurde bei zwei kleineren Firmen festgestellt, dass der einzige Rechner sowohl für Firmenzwecke als auch privat genutzt wurde und für die private Nutzung ein Internetzugang installiert war, ohne dass die Firmenanwendung hinreichend gegen Angriffe aus dem Internet geschützt war. Wir haben dies beanstandet und vorgeschlagen, für die firmeneigene bzw. die private Nutzung jeweils getrennte Rechner einzusetzen. Anderenfalls müssten umfangreiche Hard- bzw. Softwaremaßnahmen ergriffen werden, um einem möglichen Missbrauch zu begegnen. Zum Beispiel könnte der einzige Rechner mit austauschbaren Festplatten nachgerüstet werden, die keinen Zugriff untereinander ermöglichen und auf denen jeweils ein autarkes Betriebssystem installiert worden ist. Ein Zugriff auf weitere feste Datenträger (z. B. Festplatten) wäre dann zu unterbinden. Nur wenn auf dem Datenträger, mit dem die Firmendaten verarbeitet werden, das Betriebssystem keinen Internetzugang ermöglicht, kann von einer hinreichenden Sicherheit ausgegangen werden.

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Eine Firma, die im Auftrag Daten für andere Firmen erfasst und aufbereitet, lässt sich von einigen Auftragnehmern die zu verarbeitenden Daten per E-Mail zusenden. Wir mussten beanstanden, dass dies in nicht verschlüsselter Form erfolgte und damit die Vertraulichkeit der zu übermittelnden Daten besonders gefährdet war. Zur Gewährleistung einer hinreichenden *Transportkontrolle* nach Nr. 9 der Anlage zu § 9 BDSG haben wir der Firma empfohlen, die Daten auf dem Leitungsweg zu verschlüsseln; als geeignetes Verschlüsselungsverfahren bietet sich hierbei das PGP-Verfahren an, für das bei kommerziellen Anwendern jedoch eine Lizenz erforderlich ist.

Ein Schwachpunkt bei fast allen geprüften Stellen ist nach wie vor die mangelhafte Führung von *Dokumentationen*, die die Datenverarbeitungsabläufe nachvollziehbar machen. Vor allem betrifft dies die Systemdokumentation und die schriftliche Festlegung von internen Verfahrensregelungen und Arbeitsabläufen. In der Regel existieren nur die für die laufende Arbeit unbedingt erforderlichen Anweisungen (Bedienungsanleitung, Benutzerhandbuch), weiter gehende schriftliche Festlegungen (z. B. Zugriffs-, Passwortregelungen, Schlüsselplan) fehlen jedoch zumeist oder sind unvollständig vorhanden. Auch Datei- und Geräteübersichten, die eigentlich den Überblick über die interne Hard- und Software erst ermöglichen, sind nur bei wenigen Stellen vorhanden, und dann meist nicht im aktuellen Zustand.

Wir raten diesen Stellen, ein *Datenschutzkonzept* zu erarbeiten bzw. zusammen zu stellen, das alle internen und externen Datenschutzregelungen erfasst. In diesem Konzept sollten neben den gesetzlichen Datenschutzregelungen auch Festlegungen der Funktionen von Verantwortlichen und Mitarbeitern in der Datenverarbeitung und - wenn kein IT-Sicherheitskonzept existiert - auch die Zugangs- und Zugriffsregelungen, die System- und Programmdokumentation, die Bediener- und Benutzeranweisungen, die Richtlinien über die Datenträgeraufbewahrung und -vernichtung und der Gebäude- und Notfallplan niedergelegt werden.

## 5. Telekommunikation und Medien

### 5.1 Telekommunikationsnetze und -dienste

#### Neue Telekommunikations-Datenschutzverordnung - kein Fortschritt für den Datenschutz

Mit mehr als zweijähriger Verspätung hat die Bundesregierung nunmehr die Europäische Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation[111] durch Erlass der *Telekommunikations-*

Der Bundesrat hat abschließend am 29.09.2000 einen Beschluss mit Änderungsvorgaben zur Telekommunikationsdatenschutzverordnung verabschiedet.
Das Bundeskabinett hat daraufhin in seiner Sitzung am 22.11.2000 eine geänderte Fassung der Telekommuni-

[111] Richtlinie 97/66/EG, ABlEG L 24/1

*Datenschutzverordnung*[112] (TDSV) in nationales Recht umgesetzt. Die Verordnung ersetzt die bis dahin geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996, die bereits bei ihrem In-Kraft-Treten durch das beinahe zeitgleich in Kraft getretene Telekommunikationsgesetz wieder novellierungsbedürftig geworden war. Die neue TDSV regelt den Schutz personenbezogener Daten bei Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen. Sie gilt insbesondere für den Sprachtelefondienst und stellt damit die zentrale Regelung überhaupt für den Datenschutz im Bereich der Telekommunikation dar.

Trotz des langen Vorbereitungszeitraums und dem zwischenzeitlichen Wechsel der Bundesregierung kann jedoch von einer Verbesserung des Datenschutzes für die Nutzer von Telekommunikationsdiensten durch die neue TDSV keine Rede sein. Vielmehr wurden die bisher geltenden Bestimmungen zugunsten einer Ausweitung der Befugnisse zur Verarbeitung personenbezogener Daten durch die Anbieter von Telekommunikationsdienstleistungen in verschiedener Hinsicht aufgeweicht.

So ist die Verpflichtung der Diensteanbieter, die Anrufer darüber zu unterrichten, wenn ein Anruf an einen anderen Anschluss *weitergeschaltet* wird (§ 9 Abs. 4 der alten TDSV) nunmehr ersatzlos entfallen. Damit ist künftig nicht mehr sichergestellt, dass die Anrufer darüber informiert werden, wenn ihr Anruf auf einen anderen Anschluss weitergeleitet wird als den, dessen Nummer sie gewählt hatten. Der ersatzlose Wegfall dieser Vorschrift schmälert somit die Transparenz für die Anrufer.

Die gravierendste Verschlechterung des Datenschutzniveaus im Telekommunikationsbereich ist jedoch die Ausweitung des Zeitraums, in dem Anbieter von Telekommunikationsdiensten Verbindungsdaten ihrer Kunden bei der Abrechnung mittels *Einzelverbindungsnachweisen* speichern dürfen: Während die alte TDSV bestimmte, dass diese Daten spätestens 80 Tage nach Versendung der Rechnung zu löschen sind, dehnt die neue Verordnung diesen Zeitraum auf 6 Monate nach Versendung der Rechnung aus. Die Begründung vermerkt hierzu lapidar, die neue Speicherungsregelung entspreche Vorstellungen aus der Praxis, die infolge der vorzunehmenden Abrechnung der einzelnen Netzbetreiber untereinander längere Speicherungsfristen erfordert. Hier kann man nur mit Erstaunen zur Kenntnis nehmen, dass Anbieter von Telekommunikationsdienstleistungen im Zeitalter elektronischer Datenverarbeitung offensichtlich nicht in der Lage sind, die Abrechnung untereinander in einem Zeitraum von mehr als zweieinhalb Monaten nach Rechnungsversand zu bewerkstelligen und die Bunkationsdatenschutzverordnung unter Berücksichtigung der Änderungswünsche des Bundesrates verabschiedet.

Die neue Telekommunikationsdatenschutzverordnung regelt den Schutz personenbezogener Daten bei Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen. Über die entsprechenden Beratungen im Bundesrat hat das Land Berlin an der Gestaltung der TDSV mitgewirkt. In der jetzigen Verordnung sind nach Ansicht des Senats die vielfältigen und unterschiedlichen Interessen aller Beteiligten in geeigneter Weise berücksichtigt.

[112] TDSV vom 18. Dezember 2000; BGBl. I, S. 1740

desregierung dies zum Anlass nimmt, weitere Beschränkungen des Fernmeldegeheimnisses zu verordnen.

Bei den Beratungen im Bundesrat zeigte sich jedoch, dass der Wind hier auch noch aus einer ganz anderen Richtung geweht haben muss: Ein mühsam zwischen Vertretern der Datenschutzbeauftragten und dem Länderarbeitskreis „Telekommunikation, Informationswirtschaft, Post“ des Wirtschaftsausschusses des Bundesrates vereinbarter Kompromiss, nach dem die Speicherungsdauer immerhin auf bis zu drei Monate nach Rechnungsversand, höchstens jedoch bis sechs Monate nach Beendigung der Verbindung beschränkt werden sollte, wurde im mitberatenden Innenausschuss des Bundesrates mit dem Hinweis abgelehnt, durch diese Empfehlung werde die Arbeit der Strafverfolgungsbehörden unangemessen beeinträchtigt[113]. In der Tat können die Strafverfolgungsbehörden nach den Vorschriften des § 12 Fernmeldeanlagengesetz in Strafermittlungsverfahren nahezu unbegrenzt auf bei den Telekommunikationsdiensteanbietern gespeicherte Verbindungsdaten zugreifen[114]. Dem Innenausschuss des Bundesrates scheint jedoch entgangen zu sein, dass selbst der oben beschriebene Kompromiss die bisherigen Befugnisse der Strafverfolgungsbehörden in keiner Weise beschränkt hätte. Somit war der Innenausschuss des Bundesrates offensichtlich der Ansicht, die Arbeit der Strafverfolgungsbehörden werde bereits dann unangemessen beeinträchtigt, wenn die Speicherungsbefugnisse der Telekommunikationsdiensteanbieter nicht entsprechend den ursprünglichen Vorschlägen ausgeweitet werden.

Die Bundesregierung ist nach wie vor in der Pflicht, § 12 des *Fernmeldeanlagengesetzes* durch eine verfassungskonforme Regelung im Rahmen der Strafprozessordnung zu ersetzen (der Geltungszeitraum des § 12 FAG ist befristet bis zum 31. Dezember 2001). Mit dem wesentlich erweiterten Datenvolumen, das den Strafverfolgungsbehörden jetzt zur Verfügung steht, wird es umso mehr darauf ankommen, die bisher beinahe schrankenlosen Nutzungsmöglichkeiten durch die Strafverfolgungsbehörden entsprechend den Regelungen des § 100 a StPO zu beschränken[115].

Auch das *Wahlrecht der Kunden* hinsichtlich Speicherumfang und -dauer der Verbindungsdaten ist nach

---

[113] BR-Drs. 300/2/00, Punkt 5

[114] Diese Vorschrift wird von den Datenschutzbeauftragten bereits seit Jahren als wesentlich zu weit gehend kritisiert; vgl. zuletzt JB 1999, 5.1

[115] vgl. Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 „Für eine freie Telekommunikation in einer freien Gesellschaft“:
http://www.datenschutz-berlin.de/doc/de/konf/59/tele.htm

der neuen TDSV wesentlich beschränkt worden: Während vorher alle Telekommunikationsdiensteanbieter verpflichtet waren, Verbindungsdaten nach Wahl des Kunden nicht nur verkürzt, sondern auch mit vollständigen Zielnummern zu speichern bzw. nach Versendung der Rechnung zu löschen, gilt dieses Wahlrecht der Betroffenen nunmehr nur noch gegenüber dem rechnungstellenden Diensteanbieter. Der Kunde hat damit nunmehr faktisch auf die Speicherung von Verbindungsdaten bei Diensteanbietern, die ihm nicht selbst eine Rechnung stellen, sondern Verbindungsdaten im Rahmen z. B. von Zusammenschaltungsvereinbarungen oder als Anbieter von Call-by-Call-Dienstleistungen speichern, keinen Einfluss mehr. Hinsichtlich der letztgenannten Anbieter ist dieses Manko nur dadurch zu beheben, dass sich der Kunde von jedem der Anbieter eine Rechnung stellen lässt. Wer diese Dienste zukünftig nutzen und gleichzeitig die Verarbeitung von Verbindungsdaten beschränken will, muss damit wesentlich mehr Aufwand treiben. Diese Lösung ist weder datenschutz- noch kundenfreundlich.

Auch die Verpflichtung der Diensteanbieter, Verbindungsdaten unmittelbar nach Beendigung der Verbindung zu *löschen*, soweit sie nicht zum Aufbau weiterer Verbindungen oder für andere durch die TDSV erlaubte Zwecke erforderlich sind, ist ohne Begründung gelockert worden. Mussten diese Daten bisher mit Ende der Verbindung gelöscht werden, so ist dies jetzt erst „spätestens am Tag nach Beendigung der Verbindung“ erforderlich. Dafür dann aber unverzüglich (vgl. § 6 Abs. 2 Satz 2 TDSV).

Schließlich sind auch die Befugnisse der Diensteanbieter zur Verarbeitung personenbezogener Daten wesentlich erweitert worden: Während bereits bisher Anbieter von Telekommunikationsdienstleistungen im Vorfeld des Vorliegens tatsächlicher Anhaltspunkte für *Leistungserschleichung* oder sonstige rechtswidrige Inanspruchnahme von Telekommunikationsnetzen und -diensten den Gesamtdatenbestand aller Verbindungsdaten eines Monats „rastern“ durften, um nach nicht näher bestimmten Kriterien entsprechende Anhaltspunkte zu gewinnen, ist dieser Zeitraum jetzt auf den Gesamtdatenbestand aller Verbindungsdaten, die nicht älter als 6 Monate sind, ausgedehnt worden (§ 9 Abs. 2 Satz 1 TDSV neu). Die Begründung vermerkt hierzu lapidar, diese Frist entspreche der in § 7 Abs. 3 vorgesehenen Frist für die Speicherung von Verbindungsdaten zu Abrechnungszwecken. Ob diese Begründung als hinreichend gelten kann, den Anbietern erweiterte Befugnisse zum Eingriff in das Fernmeldegeheimnis ihrer Kunden einzuräumen, darf bezweifelt werden. Hier setzt sich einmal mehr der Trend fort, bestehende Sicherheitslücken bei Telekommunikationsnetzen und -diensten durch Einschränkung des Fernmeldegeheimnisses der Kunden bekämpfen zu wollen, anstatt es den Anbietern aufzugeben, die Si-

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

cherheitsstandards ihrer Dienstleistungen so zu erhöhen, dass derartige vorbeugende Überwachung aller - und damit auch der überwiegenden Mehrzahl der Kunden, die die in Anspruch genommene Leistung ordnungsgemäß bezahlen - entbehrlich ist. Positiv hervorzuheben ist, dass immerhin die bisher zur Missbrauchsbekämpfung in § 7 Abs. 4 der alten TDSV enthaltene Befugnis zur Verarbeitung von Nachrichteninhalten (also z. B. auch dem Abhören von Telefongesprächen) durch die Diensteanbieter zur Missbrauchsbekämpfung nunmehr auf die Verarbeitung von Steuersignalen begrenzt wurde.

Die Vorgabe der Telekommunikationsrichtlinie der Europäischen Union, nach der die Mitgliedstaaten darauf hinwirken sollen, dass für öffentliche zugängliche Telekommunikationsdienste Funktionen entwickelt werden, die den anonymen Zugang zu diesen Diensten ermöglichen (Erwägungsgrund 19 der Richtlinie), wird durch die neue TDSV nicht in erkennbarer Weise umgesetzt.

Insgesamt ist festzustellen, dass die von jeher problematische Tendenz andauert, für Verbindungsdaten von Telekommunikationsdienstleistungen ungleich umfangreichere Eingriffe in das Fernmeldegeheimnis der Nutzer zu erlauben als bei Inhaltsdaten, obwohl Inhalts- und Verbindungsdaten in gleicher Weise durch das Fernmeldegeheimnis des Art. 10 GG geschützt werden.

In seiner Stellungnahme zu unserem Jahresbericht 1999 hatte der Berliner Senat angekündigt, bei der Beratung des Entwurfs der TDSV im Bundesrat eng mit dem Berliner Beauftragten für Datenschutz und Akteneinsicht zusammenzuarbeiten[116]. Wir hatten gegenüber den zuständigen Senatsverwaltungen im Zuge der Beratung des Entwurfs der TDSV in den Ausschüssen und im Plenum des Bundesrates verschiedentlich Stellungnahmen mit Verbesserungsvorschlägen abgegeben und die Senatsverwaltungen gebeten, sich im Bundesrat für entsprechende Verbesserung der Verordnung einzusetzen. Entsprechende Änderungsanträge im Bundesratsverfahren hat der Senat von Berlin allerdings trotzdem bedauerlicherweise nicht eingebracht.

**Weitergehende Forderungen**

Bedenklich stimmt in diesem Zusammenhang auch eine im November 2000 erhobene Forderung der Innenministerkonferenz, für Zwecke der Strafverfolgung „den Providern und Betreibern von Servern eine Protokollierungspflicht hinsichtlich der IP-Adresse und des Nutzungszeitraumes sowie eine angemessene Aufbewahrungszeit ... “ von Nutzungsdaten vorzuschreiben. Diese Forderung wurde von den Landesbeauftragten für den Datenschutz nahezu einhellig ab-

Die Überarbeitung der Telekommunikationsdatenschutzverordnung erfolgte auf Grund der Initiative verschiedener Bundesländer, u. a. Berlins, im Länderarbeitskreis Telekommunikation, Informationswirtschaft, Post sowie der Stellungnahme der beteiligten Fachausschüsse des Bundesrates.

In diese Überarbeitung sind z.T. auch die Anregungen und Forderungen der Landesbeauftragten für den Datenschutz eingeflossen.

[116] vgl. Abghs.-Drs. 14/423, S. 139 f.

gelehnt. In einer gemeinsamen Presseerklärung haben 15 der Landesdatenschutzbeauftragten Bedenken an der Verfassungsmäßigkeit einer solchen Verpflichtung geäußert[117]. Das Bundesverfassungsgericht hat wiederholt festgestellt, dass die Speicherung personenbezogener Daten nicht zu einer Rundumbeobachtung der Bürger führen darf. Das wäre aber im Bereich der Internetnutzung mit der angestrebten Regelung der Fall. Dieses Verfahren würde nach Auffassung der 15 beteiligten Landesbeauftragten für den Datenschutz den mit den Vorschriften über Tele- und Mediendienste gewährleisteten Datenschutz in unvertretbarer Weise abbauen. Es widerspräche auch dem von der Bundesregierung selbst vorgelegten Entwurf einer Novelle zum Bundesdatenschutzgesetz, das die Entwicklung und den Einsatz von technischen Verfahren vorsieht, die mit einem Minimum an personenbezogener Datenverarbeitung betrieben werden können.

Die Forderung der Innenministerkonferenz lässt sich vergleichen mit einer Verpflichtung der Post, sämtliche Absender- und Empfängerangaben im Briefverkehr für Zwecke einer möglichen späteren Strafverfolgung zu speichern und für den Zugriff der Sicherheitsbehörden bereitzuhalten. Die bestehenden Befugnisse der Strafverfolgungsbehörden gewährleisten schon jetzt eine effektive Strafverfolgung im Internet, denn es ist den Providern ohne weiteres technisch möglich, IP-Nummern ab dem Zeitpunkt des Vorliegens eines entsprechenden richterlichen Beschlusses - oder bei Gefahr im Verzug einer staatsanwaltlichen Anordnung - vorzuhalten.

**Novellierung der Europäischen Telekommunikations-Datenschutzrichtlinie**

Während die Bundesregierung im zurückliegenden Berichtszeitraum immer noch mit der Umsetzung der Vorschriften der Telekommunikations-Datenschutzrichtlinie von 1997 beschäftigt war, bereitet die Kommission der Europäischen Union unterdessen eine Novellierung eben dieser Richtlinie im Zusammenhang mit den Bestrebungen zur Schaffung eines gemeinsamen Rechtsrahmens für elektronische Kommunikationsnetze und -dienste vor[118]. Ausgehend von den von der Kommission festgelegten Leitlinien für den neuen Rechtsrahmen[119] sollen die Regelungen der Europäischen Union für elektronische Kommunikationsnetze und -dienste in einer Rahmenrichtlinie und vier spezifischen Richtlinien zusammengefasst werden, die sich mit Genehmigungen, Zugang und Zu-

[117] http://www.datenschutz-berlin.de/aktuelle/presse00/presse08.htm

[118] vgl. den entsprechenden Vorschlag für eine Richtlinie KOM (2000)393 endg. vom 12. September 2000

[119] vgl. die entsprechende Mitteilung der Kommission KOM (2000)239 vom 26. April 2000

sammenschaltung Universaldienst- und Verbraucher- und Benutzerrechten sowie Datenschutz im Kommunikationsbereich beschäftigen.

Die Kommission hat im Juli 2000 einen Vorschlag für eine Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation[120] vorgelegt, der die Telekommunikations-Datenschutzrichtlinie 97/66/EG ersetzen soll. Danach ist geplant, den Geltungsbereich der Richtlinie 97/66/EG, der auf Telekommunikationsdienste und -netze beschränkt war, auf alle Arten der Übertragung elektronischer Nachrichten - unabhängig von der zugrunde liegenden Technologie - auszuweiten. Gleichzeitig sollen die Bestimmungen an neue Entwicklungen auf dem Gebiet elektronischer Kommunikationsdienste und -technologien angepasst werden.

Neu aufgenommen werden soll insbesondere eine Bestimmung, in der die Befugnisse der Diensteanbieter zur Verarbeitung von Standortdaten der Nutzer und Teilnehmer in elektronischen Kommunikationsnetzen geregelt wird. Solche Standortdaten, die den geografischen Standort eines mobilen Endgerätes und damit auch des entsprechenden Nutzers angeben, werden bereits in heutigen Mobilfunknetzen verarbeitet; sie sind technisch für die Nachrichtenübermittlung von und zu einem Nutzer ohne festen Standort erforderlich. Hing bisher die Genauigkeit dieser Standortdaten in zellularen Netzen von der Fläche der Zelle ab, in der sich der mobile Nutzer befindet, so gestatten neue Dienstmerkmale in zellularen und satellitengestützten Netzen unterdessen eine wesentlich genauere Ortung von Endgerät und Nutzer. Die Entwicklung genauerer Methoden zur Standortbestimmung von Mobilfunkteilnehmern wird unter anderem auch durch Regulierungsvorgaben der Regierungen in verschiedenen Staaten vorangetrieben. So hat die amerikanische Federal Communications Commission (FCC) die Anbieter von Mobilfunkdiensten verpflichtet, die Ortungsmöglichkeiten für Mobilfunkendgeräte bis Oktober 2001 auf eine Genauigkeit von 1000 Fuß zu verbessern. Damit soll nach offiziellen Angaben zunächst sichergestellt werden, dass Rettungsdienste in Zukunft besser in der Lage sind, hilfsbedürftige Besitzer von Mobilfunkendgeräten auch dann aufzufinden, wenn diese nicht selbst in der Lage sind, ihren Standort präzise anzugeben.

Über den Einsatz für die Zwecke von Rettungsdiensten hinaus eröffnen sich darüber hinaus zahlreiche weitere Einsatzmöglichkeiten im Rahmen der Entwicklung des mobilen elektronischen Geschäftsverkehrs (erste Eindrücke lassen sich hier bereits jetzt bei den angebotenen Diensten zum mobilen Internetzugriff gewinnen, die das „Wireless Application Pro-

[120] KOM (2000)385 endg. vom 12. Juli 2000

tocol“ (WAP) nutzen). Hier ist die Einführung zahlreicher neuer Dienstleistungen geplant, für die präzise Aufenthaltsinformationen der Teilnehmer verarbeitet werden sollen. Beispielhaft seien hier nur elektronische Landkarten zur genauen Bestimmung der eigenen Position und alle Arten von ortsbezogenen Informationsdiensten (wo befindet sich von meinem Standort aus gesehen das nächste Restaurant?) genannt[121].

Die Aufenthaltsinformationen von Mobilfunkteilnehmern werden damit in Zukunft nicht nur wesentlich präziser sein; die Daten werden auch zukünftig einem wesentlich größeren Kreis von Anbietern zur Verfügung stehen, während bisher die Kenntnis der Aufenthaltsinformationen auf die Netzbetreiber der Mobilfunknetze beschränkt war.

Es liegt auf der Hand, dass mit solchen präzisen Bewegungsprofilen neue Gefährdungen des Persönlichkeitsrechts der Mobilfunknutzer verbunden sein können. Nach Einführung der technischen Voraussetzungen wird - technisch gesehen - jeder Nutzer eines Mobilfunkgeräts de facto einen Peilsender mit sich herumtragen, der im Prinzip - soweit das Gerät nicht ausgeschaltet ist - die jederzeitige genaue Bestimmung des Standortes seines Endgeräts - unter Umständen bis auf die Straße und Hausnummer genau - ermöglicht.

Bereits jetzt deutet sich an, dass die Chancen, solche Funktionen in datenschutzfreundlicher Weise unter alleiniger Kontrolle des Nutzers zu realisieren, bei der Entwicklung der entsprechenden Technologie wiederum nicht genutzt worden sind: So ist geplant, dass die Standortbestimmung - wie bereits bisher - weiterhin automatisch bei der Einbuchung des mobilen Endgeräts in das jeweilige Funknetz erfolgen wird, ohne dass der Benutzer dies am Endgerät entscheidend beeinflussen kann. Hier ist - ähnlich wie bereits bei Einführung der Rufnummernübermittlung - erneut der Fehler gemacht worden, solche Funktionen direkt in die Netze zu implementieren, wo sie der Kontrolle der Netzbetreiber, nicht aber der Kontrolle der Nutzer unterliegen. Die datenschutzfreundlichere technologische Alternative, zur Positionsbestimmung in das mobile Endgerät implementierte GPS-Empfänger zu nutzen, dürfte aufgrund der systemimmanenten Beschränkungen der Ortungsmöglichkeiten (schlechter Empfang in geschlossenen Gebäuden, Tunneln und anderen Situationen, in denen keine ausreichende Freisicht zum Himmel besteht) verworfen werden. Aus Sicht des Datenschutzes wären Technologien vorzuziehen, die eine passive Ortung des Nutzers vorsehen, bei denen der Nutzer selbst kontrollieren könnte, ob diese präzise Aufenthaltsinformation überhaupt in das Netz eingespeist wird.

---

[121] vgl. 2.1

Nachdem es im Nachhinein kaum noch möglich sein wird, hier eine technologische Änderung zu bewirken, kommt es jetzt entscheidend darauf an, die Voraussetzung für die Übermittlung präziser Aufenthaltsinformationen durch die Betreiber von Mobilfunknetzen an andere Diensteanbieter (z. B. Anbieter von mobilen Internetdienstleistungen) in strikter Weise zu beschränken und nur auf der Grundlage der informierten Einwilligung der Betroffenen zu gestatten.

**Übereinkommen über Datennetzkriminalität des Europarates**

Am 27. April 2000 veröffentlichte der Europarat auf seiner Website einen Entwurf für ein Übereinkommen über Datennetzkriminalität, das zu diesem Zeitpunkt bereits in der 19. Entwurfsfassung vorlag. Die endgültige Entwurfsfassung sollte bis zum Dezember 2000 fertig gestellt und ab September 2001 zur Unterschrift durch die Vertragspartner bereitgestellt werden. In dem Begleittext hat der Europarat erklärt, dass er daran interessiert ist, den Konsultationsprozess mit interessierten öffentlichen und privaten Einrichtungen auszuweiten.

Die Bemühungen des Europarates stehen im engen Zusammenhang mit entsprechenden Aktivitäten der G 8-Staaten zur Bekämpfung von „Hightech-Kriminalität“[122].

Im Rahmen des Übereinkommens ist die Einführung verschiedener neuer Straftatbestände geplant, die bisher in den Strafgesetzen vieler Mitgliedstaaten des Europarates nicht enthalten sind. Gleichzeitig werden Verfahren zur Verfolgung solcher Verbrechen festgelegt, darunter Maßnahmen zur Verpflichtung von Telekommunikationsanbietern, personenbezogene Daten (sowohl Inhalts- als auch Verkehrsdaten) über Kommunikationsvorgänge in Telekommunikationsnetzen zu speichern und diese Daten nationalen und ausländischen Behörden zur Verfügung zu stellen, die entsprechende Ermittlungen in solchen Strafverfahren durchführen.

Der Berliner Beauftragte für Datenschutz und Akteneinsicht hat in seiner Eigenschaft als Vorsitzender der International Working Group on Data Protection in Telecommunications die Erarbeitung eines gemeinsamen Standpunktes der Arbeitsgruppe zu Datenschutzaspekten des Übereinkommens über Datennetzkriminalität initiiert. Der gemeinsame Standpunkt der Arbeitsgruppe wurde auf der 28. Sitzung der Gruppe am 13./14. September 2000 in Berlin verabschiedet und dem Europarat sowie den Regierungsvertretern, die mit der Erarbeitung des Entwurfs des Übereinkommens beschäftigt waren, zugeleitet. Der diesjährige Vorsitzende der Internationalen Datenschutzkonferenz und Präsident der italienischen Datenschutz-

[122] JB 1999 5.1

kommission hat das Papier ebenfalls namens der Internationalen Konferenz dem Europarat geschickt. Der gemeinsame Standpunkt ist die erste international koordinierte Stellungnahme zu dem Übereinkommen aus Sicht des Datenschutzes. Die Arbeitsgruppe hat darin insbesondere darauf hingewiesen, dass Datenschutzbestimmungen in dem Übereinkommen völlig fehlen, und insofern eine Bezugnahme auf die existierenden Datenschutzregelungen im Rahmen des Europarates[123] sowie die Empfehlung No. R (95) 4 zum Schutze personenbezogener Daten auf dem Gebiet der Telekommunikationsdienste unter besonderer Bezugnahme auf Telefondienste gefordert. Es wurde angeregt, das Expertenkomitee zum Datenschutz des Europarates in die weiteren Entwurfsarbeiten einzubeziehen.

Die Arbeitsgruppe hat nochmals ausdrücklich darauf hingewiesen, dass eine Verpflichtung von Telekommunikations- und Internetdiensteanbietern zur Speicherung von Daten über alle Telekommunikations- und Internetverbindungen für erweiterte Zeiträume ausschließlich für Zwecke der Verbrechensbekämpfung unverhältnismäßig und damit inakzeptabel wäre.

Sie hat gleichzeitig darauf hingewiesen, dass jegliches Abhören privater Kommunikation an angemessene Sicherheitsmaßnahmen gebunden werden muss, wie sie im Übereinkommen zur Rechtshilfe in Stafsachen zwischen den Mitgliedstaaten der Europäischen Union (Artikel 23) niedergelegt sind.

Auch bei der Einführung neuer Straftatbestände hat die Arbeitsgruppe zur Zurückhaltung gemahnt. Die Arbeitsgruppe hat insbesondere darauf hingewiesen, dass zur Verbesserung des Datenschutzstandards im Internet die Verpflichtung von Anbietern entsprechender Dienste zu Sicherungsmaßnahmen der Kriminalisierung von Handlungen, die durch die Sicherheitslücken der Systeme erst ermöglicht werden, vorzuziehen ist.

In der bis zum Ende des Berichtszeitraumes veröffentlichten 24. Entwurfsfassung sind zwei besonders problematische Regelungen aus vorherigen Versionen des Entwurfs nicht mehr enthalten: Die ursprünglich geplante Möglichkeit für die Vertragsparteien, ihre zuständigen Behörden zu befähigen, zu Zwecken strafrechtlicher Ermittlungen und Verfahren unabhängig von Abrechnungsnotwendigkeiten die standardmäßige Speicherung von Verbindungsdaten bei Diensteanbietern für einen Zeitraum von bis zu drei Monaten vorzusehen, damit diese später für evtl. Strafermittlungsverfahren zur Verfügung stehen, ist gestrichen worden. Gleiches gilt auch für die Ermächtigung der Vertragsparteien, die Betreiber von Ano-

[123] Übereinkommen zum Schutze des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (Konvention Nr. 108 vom 28. Januar 1981)

nymisierungsdiensten (z. B. anonyme Remailer) ebenfalls zur vorbeugenden Speicherung personenbezogener Verbindungsdaten über ihre Nutzer zu verpflichten.

Gleichzeitig wird in dem Kapitel über national anwendbare Vorschriften zu den verschiedenen Ermittlungsmaßnahmen ausdrücklich das Erfordernis der Beachtung der Menschenrechte und des Verhältnismäßigkeitsprinzips erwähnt. Auch der von der Arbeitsgruppe als zu allgemein formuliert kritisierte Straftatbestand des Artikel 6 des Entwurfs (unerlaubte Vorrichtung) ist unterdessen ein wenig enger gefasst worden.

Gleichwohl besteht nach wie vor die Gefahr, dass die Umsetzung der sehr allgemein formulierten Straftatbestände der Artikel 4 - 6, bei denen insbesondere auch Beihilfe unter Strafe gestellt werden soll, eine erhebliche Absenkung des Datenschutzstandards für alle Nutzer von Telekommunikationsnetzwerken in den Vertragsstaaten zur Folge haben könnte, da abzusehen ist, dass die Umsetzung dieser Regelung in das nationale Recht zu einer massiven Ausweitung der Speicherung personenbezogener Verbindungsdaten gerade im Bereich des Internet im Rahmen von Ermittlungsmaßnahmen bei solchen Straftaten führen wird.

Bedauerlicherweise ist der Europarat hier den Vorschlägen der Arbeitsgruppe nicht gefolgt, stattdessen Dienstanbieter dazu zu verpflichten, Sicherungsmaßnahmen beim Anschluss ihrer Systeme an ein öffentliches Netzwerk zur Verbesserung des Sicherheitsstandards im Internet im Allgemeinen zu treffen.

**Informationsverarbeitungsgesetz und Beschaffungsmaßnahmen**

Für die Verarbeitung personenbezogener Daten auf Telekommunikationsanlagen des Landes Berlin sind die Regelungen des § 5 Informationsverarbeitungsgesetz (IVG) einzuhalten. Dies bedeutet insbesondere, dass Dienst- und Privatgespräche zu trennen sind; darüber hinaus dürfen Dienstgespräche nicht apparate- bzw. mitarbeiterbezogen gespeichert, sondern müssen Gruppen von Beschäftigten zugeordnet werden, die in der Regel nicht kleiner als zehn Beschäftigte sein dürfen.

In der Vergangenheit ist es hier sowohl bei Neubauten als auch bei Ersatzbeschaffungen zu Unstimmigkeiten zwischen öffentlichen Dienststellen des Landes Berlin und Herstellern von Telekommunikationsanlagen über die technische Realisierung dieser Anforderung gekommen. Bei der Prüfung von einzelnen Ausschreibungsunterlagen hat sich herausgestellt, dass in einigen Fällen vergessen wurde, die Regelungen des § 5 IVG explizit zum Gegenstand der Ausschreibung zu machen.

Wir haben daher die öffentlichen Stellen des Landes Berlin in einem Rundschreiben aufgefordert, in ihrem Geschäftsbereich dafür Sorge zu tragen, dass bei Neubauten und Ersatzbeschaffungen von Telekommunikationsanlagen für den Sprachtelefondienst künftig die Regelungen des § 5 IVG explizit in die Ausschreibungsunterlagen (z. B. Pflichtenhefte) aufgenommen und damit zum Gegenstand der Ausschreibung gemacht werden.

### 5.2 Tele- und Mediendienste

Im zurückliegenden Berichtszeitraum haben uns wiederum zahlreiche Beratungsersuchen von Bürgern im Bereich der Tele- und Mediendienste erreicht. Erheblicher Beratungsbedarf besteht offensichtlich nach wie vor auch bei Berliner Anbietern von Tele- und Mediendiensten; die Anzahl der Beratungsersuchen von Anbietern ist im vergangenen Berichtsjahr wiederum stark angestiegen. Erfreulich ist dabei, dass eine wachsende Anzahl von Anbietern sich bereits in einem sehr frühen Stadium der Planung ihrer Angebote an uns wendet. Dieser Effekt lässt den Schluss zu, dass das Problembewusstsein für Datenschutzfragen bei den Anbietern insgesamt zugenommen hat.

**Novellierung des Teledienstedatenschutzgesetzes**

Bereits in unserem letzten Jahresbericht hatten wir über Bestrebungen der Bundesregierung berichtet, im Rahmen der Evaluierung des Informations- und Kommunikationsdienstegesetzes (IuKDG) das Teledienstedatenschutzgesetz zu novellieren[124].

Bis zum Ende des zurückliegenden Berichtszeitraums ist dieses Vorhaben noch nicht abgeschlossen worden. Derzeit liegt ein Arbeitsentwurf des Bundesministeriums für Wirtschaft und Technologie vor[125]. Ziel der Novellierung ist, den im Bericht der Bundesregierung an den Deutschen Bundestag über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des IuKDG[126] festgestellten gesetzgeberischen Handlungsbedarf umzusetzen.

So sollen unter anderem wesentliche Grundsätze und Verpflichtungen des TDDSG zum Systemdatenschutz (Datenvermeidung, Datensparsamkeit, Grundsätze zur Anonymisierung und Pseudonymisierung), deren Übernahme in ein novelliertes Bundesdatenschutzgesetz geplant ist, aus dem TDDSG gestrichen werden.

Inwieweit dies jedoch aus Sicht der Anbieter zur Verbesserung der Transparenz der Rechtsvorschriften beitragen kann, ist fraglich, da Anbieter von Tele-

---

[124] JB 1999, 5.2

[125] http://www.iid.de/iukdg/eval/index.html

[126] BT-Drs. 14/1191 vom 18. Juni 1999

diensten in dieser Hinsicht zukünftig mehr als bisher gezwungen sein werden, das vergleichsweise unübersichtliche Regelwerk des Bundesdatenschutzgesetzes parallel zu den Bestimmungen des bereits bisher schlanken Teledienstedatenschutzgesetzes anzuwenden.

Abgesehen davon hat das Bundesministerium für Wirtschaft und Technologie in der Vergangenheit mehrfach erklärt, dass eine Änderung des materiell geltenden Datenschutzrechts für den Bereich der Teledienste durch die Novellierung des TDDSG nicht beabsichtigt ist.

Ein Blick in den vorliegenden Entwurf zeigt jedoch, dass die Verarbeitungsbefugnisse der Anbieter von Telediensten in einigen wesentlichen Punkten sehr wohl erweitert werden: So soll auch hier - wie bereits für Anbieter von Telekommunikationsdiensten[127] die Befugnis der Anbieter zur Speicherung von Abrechnungsdaten für Einzelnachweise von bisher 80 Tagen nach Versendung der Rechnung auf 6 Monate ausgedehnt werden (vgl. § 6 Abs. 7 E-TDDSG). Die Begründung führt hierzu lapidar aus, dadurch erfolge eine inhaltliche Anpassung an die Bestimmungen bezüglich der Einzelnachweise in der TDSV, da hier eine vergleichbare Interessenlage besteht, insbesondere bei Diensteanbietern, die zugleich eine Telekommunikationsanlage im Sinne der TDSV betreiben.

Die Ausweitung der Speicherungsdauer hatten wir bereits für Anbieter von Telekommunikationsdienstleistungen im Sinne der TDSV als höchst problematisch kritisiert. Dessen ungeachtet ist der Gesetzgeber offensichtlich entschlossen, diesen Fehler auch im Bereich der Teledienste zu wiederholen.

Wir werden uns im Zuge der anstehenden Beratungen des Ersten Gesetzes zur Änderung des Teledienstedatenschutzgesetzes gegenüber den zuständigen Senatsverwaltungen dafür einsetzen, dass insbesondere diese geplante Absenkung des Datenschutzstandards für Nutzer von Telediensten wieder zurückgenommen wird. Leider sind aufgrund der zurückliegenden Erfahrungen bei der Novellierung der TDSV Zweifel angebracht, ob es uns gelingen wird, den Senat dazu zu bewegen, sich aktiv im Bundesrat für ein höheres Datenschutzniveau einzusetzen.

Siehe hierzu Stellungnahme des Senats zu 5.1 „Telekommunikationsnetze und -dienste“ (ab Seite 167).

**E-Mail-Adressen für alle?**

*Mehrere Bürger hatten von einem in Berlin ansässigen Telediensteanbieter E-Mails erhalten, in denen der Anbieter seine Kunden über die geänderte Preisgestaltung für den von ihm angebotenen Dienst informieren wollte. Dabei wurden den Betroffenen gleich auch noch die E-Mail-Adressen einer großen Anzahl von weiteren Kunden des Unternehmens mit-*

[127] vgl. 5.1

*geteilt, die zusätzlich zu ihrer eigenen E-Mail-Adresse im Anschriftenfeld der E-Mail enthalten waren.*

Bei den E-Mail-Adressen handelt es sich um Bestandsdaten im Sinne des § 5 Teledienstedatenschutzgesetz. Danach darf der Diensteanbieter personenbezogene Daten eines Nutzers erheben, verarbeiten und nutzen, soweit dies für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit ihm über die Nutzung von Telediensten erforderlich ist. Selbstverständlich gehört hierzu nicht die Mitteilung von Bestandsdaten eines Kunden an andere Kunden des Unternehmens, soweit dies nicht Inhalt oder Bestandteil der Dienstleistung ist oder der Betroffene eingewilligt hat. Keine dieser Voraussetzungen lag in diesem Fall vor. Die Übermittlung der E-Mail-Adressen an die anderen Kunden des Unternehmens war somit rechtswidrig.

Die Stellungnahme des Unternehmens ergab, dass bei der Informationsmassnahme zu den neuen Preisen des Unternehmens die Adressen durch ein Versehen im Klartext für einige Buchstabengruppen an alle Empfänger der betreffenden E-Mails versandt worden waren. Das Unternehmen hat uns zugesichert, in Zukunft streng darauf achten zu wollen, dass ein derartiges Missgeschick zukünftig nicht wieder unterläuft.

### 5.3 Datenschutz und Medien

#### Staatsvertrag über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks

Durch den Vierten Rundfunkänderungsstaatsvertrag[128] waren die Datenschutzbestimmungen für Datenschutzvorschriften für die privaten Rundfunkanbieter geändert und an die Bestimmungen des Mediendienste-Staatsvertrages angepasst worden.

Zur Übernahme dieser und weiterer Änderungen in den für die privaten Rundfunkveranstalter in Berlin und Brandenburg geltenden „Staatsvertrag über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks“ hat der Senat im zurückliegenden Berichtszeitraum einen Entwurf vorgelegt[129]. Dieser Entwurf übernimmt die Datenschutzbestimmungen aus dem Vierten Rundfunkänderungsstaatsvertrag vollständig, so dass nach dem In-Kraft-Treten des geänderten Staatsvertrages zwischen Berlin und Brandenburg die Geltung des hohen Datenschutzniveaus des Vierten Rundfunkänderungsstaatsvertrages auch auf private Veranstalter für Rundfunk in Berlin und Brandenburg ausgedehnt wird.

Zwischenzeitlich ist der Rundfunkstaatsvertrag durch den Fünften Rundfunkänderungsstaatsvertrag erneut

Die Novellierung des Staatsvertrages liegt dem Landtag von Brandenburg und dem Abgeordnetenhaus von Berlin zur Ratifizierung vor.

[128] JB 1999, 5.3

[129] Abghs.-Drs. 14/596

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

novelliert worden; die Änderungen betreffen allerdings nicht die im Rundfunkstaatsvertrag enthaltenen Datenschutzbestimmungen. Es ist geplant, die Änderungen des Fünften Rundfunkänderungsstaatsvertrages ebenfalls im Rahmen des Zweiten Staatsvertrages zur Änderung des Staatsvertrages über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks zu übernehmen. Da der Fünfte Rundfunkänderungsstaatsvertrag erst zum 1. Januar 2001 in Kraft tritt, wird der Staatsvertrag zwischen Berlin und Brandenburg voraussichtlich erst im Frühjahr 2001 in Kraft treten.

**Datensparsamkeit bei der Rundfunkfinanzierung**

Im zurückliegenden Berichtszeitraum war die Finanzierung des öffentlich-rechtlichen Rundfunks wiederum Gegenstand einer breiten öffentlichen Diskussion sowohl in der Politik als auch unter den Rundfunkanstalten selbst. Erörtert wurde hierbei auch erneut, ob die Erhebung von Rundfunkgebühren, die an das „Bereithalten des Rundfunkgerätes“ anknüpfen, durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte. Wir hatten in unserem Jahresbericht 1999 über entsprechende Vorschläge des Bundesfachausschusses Medien der CDU berichtet[130].

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat das Thema in einer Entschließung vom 12./13. Oktober 2000[131] aufgegriffen.

Dabei hat die Konferenz insbesondere gefordert, bei der Neuordnung der Rundfunkfinanzierung ein Modell zugrunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung bei der Verarbeitung personenbezogener Daten von Rundfunkteilnehmern orientiert. Nach Auffassung der Datenschutzkonferenz lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen Finanzierungsmodellen gewährleisten, die das Recht auf informationelle Selbstbestimmung der Rundfunkteilnehmer weniger stark einschränken als das derzeit praktizierte Modell.

Die Diskussion auf Ebene der Ministerpräsidenten über die künftige Struktur der Rundfunkgebühren ist noch nicht abgeschlossen. Gesichtspunkte des Datenschutzes werden in die Entscheidung mit einfließen.

**Rundfunkgebühr auch für Kinder?**

*Im zurückliegenden Berichtszeitraum erreichten uns mehrere Eingaben von empörten Eltern, deren minderjährige Kinder von der Gebühreneinzugszentrale im Auftrag des Senders Freies Berlin mit so genannten „werblichen Schreiben“ bedacht worden waren, in denen die Kinder (mit der Anrede „Sehr geehrte Frau“ bzw. „Sehr geehrter Herr“) aufgefordert wurden zu überprüfen, ob sie alle Hörfunk- und Fernsehgeräte auch ordnungsgemäß angemeldet hatten. Die*

[130] JB 1999, 5.3

[131] vgl. Anlagenband „Dokumente zum Datenschutz 2000“, S. 21

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

*Eltern wiesen zu Recht darauf hin, dass ihre Kinder allein schon aufgrund ihres Alters (in einem Fall handelt es sich um ein zehnjähriges Mädchen) keiner Pflicht zur Zahlung von Rundfunkgebühren unterliegen können. Auch wurde die Frage nach der Herkunft der Daten der Kinder aufgeworfen.*

Wie die Stellungnahme des SFB bzw. der GEZ ergab, stammten die Daten der Kinder von einem Adresshandelsunternehmen. Für die Mailing-Aktion waren dabei auch solche „Adressen-Pools“ angemietet worden, die nicht ausdrücklich auf ein bestimmtes Alter begrenzt waren, wobei jedoch die Art des Bestandes darauf hindeutete, dass dort keine Kinder enthalten sind. Um künftig zu verhindern, dass bei derartigen Mailing-Aktionen auch die Anschriften von Kindern verwendet werden, die schon allein wegen ihres Alters für eine Gebührenpflicht nicht in Frage kommen, wird die GEZ jetzt im Adresshandel nur noch solche Adressen anmieten, für die bei dem Anbieter der Adressen das Geburtsjahr zur Verfügung steht und damit die Verschickung der „Werbeschreiben“ an Jugendliche, die im Haushalt der Eltern leben, auf solche Jahrgänge begrenzt werden kann, bei denen der bzw. die Betroffene mindestens theoretisch einer Rundfunkgebührenpflicht unterliegen kann, z. B. weil er oder sie über ein eigenes Einkommen - wie Bafög, eine Ausbildungsvergütung oder eine Rente - verfügt, das den Sozialhilferegelsatz übersteigt.

Die GEZ wird künftig auf die gerügte Datenermittlung verzichten.

**Nochmals: Negative Auskunftspflicht**

Bereits in unserem Jahresbericht 1999 hatten wir uns zum Umfang der Auskunftspflicht von Rundfunkteilnehmern nach § 4 Abs. 5 Rundfunkgebührenstaatsvertrag geäußert. Anlass waren mehrere Eingaben Berliner Rundfunkteilnehmer, die ein Hörfunk-, aber kein Fernsehgerät angemeldet hatten. Die im Auftrag des Senders Freies Berlin tätige GEZ hatte bei den Petenten wiederholt Auskunft darüber begehrt, ob nunmehr Fernsehgeräte zum Empfang bereitgehalten würden. Nach Auffassung des SFB besteht eine Auskunftspflicht nach § 4 Abs. 5 Rundfunkgebührenstaatsvertrag auch dann, wenn von dem Betreffenden weiterhin keine Fernsehgeräte zum Empfang bereitgehalten werden. Der SFB besteht darauf, dass Rundfunkteilnehmer, die nur ein Hörfunkgerät angemeldet haben, der Rundfunkanstalt regelmäßig - die entsprechenden Mailing-Aktionen sollen nach Auskunft der GEZ jährlich wiederholt werden - mitteilen, dass sie weiterhin nicht über ein Fernsehgerät verfügen. Demgegenüber hatte unsere rechtliche Überprüfung ergeben, dass die entsprechende Vorschrift nicht zu einer derartigen „Negativ-Auskunft“ verpflichtet. Diese Rechtsauffassung wird von den anderen Landesbeauftragten für den Datenschutz, die eine eigene Kontrollkompetenz im wirtschaftlich-administrativen Bereich ihrer Landesrundfunkanstalten haben (Bremen, Hessen und Brandenburg) geteilt. In der Stellungnahme des Senats zu unserem Jahresbericht 1999 referiert

Der Senat hält an seiner Stellungnahme zum Datenschutzbericht 1999 fest. Aus Rechtsgründen ist die Rechtsauffassung des SFB nicht zu beanstanden.

Zu dem erwähnten Schreiben der GEZ hat der SFB wie folgt Stellung genommen:

„Das im Bericht erwähnte Schreiben der GEZ ist dem SFB nicht bekannt. Auch die GEZ hat die Existenz von Schreiben mit dem zitierten Wortlaut nicht bestätigt. Die (möglicherweise fehlerhaft) wiedergegebene Passage des Schreibens deutet aber darauf hin, dass es sich um ein werbliches Schreiben der GEZ an einen nicht im Bestand der GEZ registrierten Personenkreis im Rahmen einer Mailingaktion handeln könnte. In solchen Schreiben wird regelmäßig darauf hingewiesen, dass nur diejenigen Personen zur Auskunft verpflichtet sind, die Rundfunkgeräte (nicht wie zitiert Fernsehgeräte) zum Empfang bereithalten und dass für alle anderen Personen eine Antwort freigestellt ist. Bei dem erwähnten Empfänger könnte es sich um eine Person handeln, die versehentlich nicht im Teilnehmerbestand der GEZ gefunden und dadurch in die Mailingaktion miteinbezogen worden war, die aber tatsächlich registrierter Rundfunkteilnehmer ist.“

der Senat nochmals die Rechtsauffassung des SFB. Rundfunkteilnehmer seien nach der entsprechenden Vorschrift nicht nur verpflichtet, auf Verlangen anzugeben, ob und in welchen Zeiträumen ein Rundfunkgerät zum Empfang bereitgehalten wurde, sondern auch, ob und wann dies nicht der Fall war.

Diese Interpretationen ergäben sich sowohl aus dem Wortlaut als auch dem Sinn und Zweck des § 4 Abs. 5 Satz 1 Rundfunkgebührenstaatsvertrag und seien durch entsprechende Gerichtsentscheidungen abgesichert. Zitiert wird lediglich eine Entscheidung des VGH Baden-Württemberg, die sich allerdings auf einen völlig anderen Sachverhalt bezieht[132]: In dem betreffenden Urteil äußerst sich der VGH ausschließlich zu der Frage, wann tatsächliche Anhaltspunkte, dass eine Person nicht angemeldete Rundfunkgeräte zum Empfang bereithält, vorliegen. Dies sei unter anderem dann der Fall, wenn die Wohnung der Person über Einrichtungen verfügt, die aus einer zentralen Hausantennenanlage gespeist werden. Nur soweit solche tatsächlichen Anhaltspunkte vorliegen, die darauf hindeuten, dass Rundfunkgeräte zwar bereitgehalten werden, aber nicht angemeldet sind, müssen sich nach Ansicht des VGH „... diejenigen um Auskunft ersuchten Personen, die nicht Rundfunkteilnehmer sind, ... lediglich der geringen Mühe unterziehen zu bestätigen, dass sie keine Rundfunkgeräte zum Empfang bereithalten." Ohne diese Auffassung des VGH weiter kommentieren zu wollen, ist damit jedenfalls nichts über die vorliegend zu beurteilenden Fälle gesagt. Der SFB stützt sein Auskunftsbegehren gerade nicht darauf, dass ihm tatsächliche Anhaltspunkte vorliegen, dass ein Rundfunkgerät zum Empfang bereitgehalten wird und dies nicht oder nicht umfassend angezeigt wurde (§ 4 Abs. 5 Satz 1 Alternative). Vielmehr soll nach Auffassung des SFB allein die Tatsache, dass jemand als Rundfunkteilnehmer bei der GEZ gemeldet ist, ausreichen, um auch eine „Negativ-Auskunft" zu begründen. Die in Rede stehende Auffassung des SFB kann also mitnichten auf die zitierte Entscheidung des VGH Baden-Württemberg gestützt werden.

Die Rechtsauffassung des SFB wird darüber hinaus anscheinend auch von der GEZ nicht geteilt: Uns liegt ein Schreiben der GEZ an einen Rundfunkteilnehmer in gleicher Angelegenheit vor, in dem Folgendes ausgeführt wird: „Zur Beantwortung ist der Empfänger nur verpflichtet, wenn er tatsächlich ein Fernsehgerät zum Empfang bereithält. Die Ausführungspflicht ist dann auf § 4 Abs. 5 Rundfunkgebührenstaatsvertrag gegründet. Wenn kein Fernsehgerät zum Empfang bereitgehalten wird, besteht keine Verpflichtung zur Rücksendung des Antwortbogens, jedoch sind wir auch in solchen Fällen für eine Antwort dankbar, weil damit der Vorgang abgeschlossen und nochmalige

[132] Urteil vom 7. Oktober 1994, Az.: 10 S 498/94 = DÖV 1995, S. 386

Nachfragen vermieden werden können.“ Dies deckt sich voll inhaltlich mit unserer oben ausgeführten Rechtsauffassung.

Nach alledem ist es bedauerlich, dass der Senat in seiner Stellungnahme zu unserem Jahresbericht 1999 einfach die Rechtsauffassung des SFB übernommen hat mit dem lapidaren Zusatz, diese Ansicht des SFB sei „...aus Rechtsgründen nicht zu beanstanden“[133]. Unter Berufung auf diese Stellungnahme hat der SFB es bisher abgelehnt, in den Vordrucken für die entsprechenden Schreiben darauf hinzuweisen, dass das Ausfüllen und die Rücksendung des Fragebogens dann freiwillig ist, wenn weiterhin keine Fernsehgeräte zum Empfang bereitgehalten werden.

## 6. Aus der Dienststelle

### 6.1. Entwicklung

Die Berliner Verfassung von 1995 sieht vor, dass das Abgeordnetenhaus zur Wahrung des Rechts auf informationelle Selbstbestimmung einen Datenschutzbeauftragten wählt, der vom Präsidenten des Abgeordnetenhauses ernannt wird und dessen Dienstaufsicht unterliegt (Art. 47). Zwischen dieser Vorschrift, die den Datenschutzbeauftragten dem Entscheidungsbereich des Parlaments zuordnet, und der Regelung des bestehenden Berliner Datenschutzgesetzes, nach der der Datenschutzbeauftragte auf Vorschlag des Senats vom Abgeordnetenhaus mit den Stimmen der Mehrheit seiner Mitglieder gewählt und vom Senat ernannt wird (§ 21 BlnDSG), besteht ein offensichtlicher Widerspruch. Da die Amtszeit des bisherigen Berliner Datenschutzbeauftragten am 9. Februar 2000 ablief, enstand die Frage, in welchem Verfahren die Be- bzw. Ernennung für die nächste Amtszeit erfolgen sollte. Nachdem sich Abgeordentenhaus und Senat auf eine einvernehmliche Vorgehensweise geeinigt hatten, wurde der bisherige Amtsinhaber am 9. März 2000 für eine weitere Amtszeit gewählt und am 24. März 2000 durch den Präsidenten des Abgeordnetenhauses ernannt.

Mit Beginn des neuen Jahres wurde die bisherige Stellvertreterin des Datenschutzbeauftragten, Claudia Schmid, zur für den Verfassungsschutz zuständigen Abteilungsleiterin der Senatsverwaltung für Inneres ernannt[134]. Sie war im Juni 1990 in die Dienststelle eingetreten und hatte entscheidend die Fortentwicklung des Datenschutzrechtes insbesondere im Bereich der öffentlichen Sicherheit und Ordnung geprägt. Zuständig für die Öffentlichkeits- und Pressearbeit beeinflusste sie in den vergangenen Jahren entscheidend die Außendarstellung der Dienststelle.

---

[133] Abghs.-Drs. 14/423, S. 155 f.

[134] vgl. 1.2

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

Für die Aufgaben, die dem Datenschutzbeauftragten durch die Tele- und Mediendienstgesetzgebung aus dem Jahr 1997 zugewachsen sind, wurde nach einiger parlamentarischer Diskussion eine Stelle im höheren Dienst bewilligt. Keine Stelle gab es dagegen für die Aufgaben nach dem Informationsfreiheitsgesetz, obwohl sich inzwischen herausgestellt hat, dass dort schwierigste juristische Fragen zu bearbeiten sind.

Auch im Hinblick darauf, dass das neue BDSG im Bereich der Amtsaufsicht über Privatunternehmen einen deutlichen Aufgabenzuwachs mit sich bringen wird, wird eine Aufstockung des Personalbestands unserer Dienststelle unausweichlich bleiben. Es kann nicht angehen, dass angesichts der Entwicklung der Informationstechnologie immer mehr Aufgaben mit Hilfe der Technik bewältigt werden, aus diesem Grund erhebliche Personaleinsparungen erzielt werden, aber auf der anderen Seite die notwendige Kontrolle vollständig vernachlässigt wird.

Bundesweit wird diskutiert, ob eine Gebührenpflicht für die Tätigkeit des Datenschutzbeauftragten gesetzlich eingeführt werden sollte. Wir haben uns hierzu zurückhaltend geäußert, insbesondere da aus Gründen der mangelnden Personalkapazitäten eine Gleichbehandlung bei Prüfungen nicht gewährleistet werden kann, so dass notwendigerweise bei der Gebührenerhebung bei Amtsprüfungen der Verdacht der Willkür nicht auszuschließen ist.

Anders verhält es sich mit den Kosten bei Prüfungen, die aufgrund von Eingaben Betroffener oder konkreter Hinweise getroffen werden müssen. Für diese Fälle hat die Senatsverwaltung für Finanzen unsere Auffassung bestätigt, dass die Erstattung von Barauslagen, zu denen auch Reisekosten und weitere Kosten z. B. durch die notwendige Beauftragung externer Gutachter gehören, nach dem Gebühren- und Beiträgegesetz in Betracht kommt. Dies gilt insbesondere bei Stellen außerhalb Berlins, die im Auftrag für in Berlin gelegene Stellen Daten verarbeiten. Angesichts der zunehmenden Tendenz, Datenverarbeitung im Rahmen des Outsourcing durchführen zu lassen, kann es hier zu erheblichen Aufwendungen kommen, wenn tatsächlich Kontrollen vor Ort (etwa aufgrund von Unterwerfungsklauseln) durchgeführt werden sollen. Von der Möglichkeit der Kostenerstattung werden wir künftig jedenfalls dann Gebrauch machen, wenn Kontrollen außerhalb von Berlin notwendig werden, die von Berliner Stellen veranlasst worden sind.

**6.2 Die Aufgaben**

Bei der Aufgabenentwicklung bestätigt sich die bereits im Vorjahr beobachtete Tendenz, dass sich Bürgerinnen und Bürger zunehmend um den Datenschutz bei elektronischen Medien sorgen. Deutlich über 10% aller Eingaben kamen aus diesem Arbeitsgebiet. Gleichwohl blieben Beschwerden aus den Bereichen

Die Forderung nach zusätzlichen Stellen für einen seit 1997 eingetretenen Aufgabenzuwachs in der Tele- und Mediengesetzgebung ist aufgrund der seit 1994 um 25% erfolgten Aufstockung des Personalbestandes des Berliner Beauftragten für Datenschutz und Akteneinsicht nicht nachvollziehbar. Vielmehr stellt sich die Frage, ob nicht auch beim Beauftragten für Datenschutz und Akteneinsicht Aufgaben aufgrund von Technikeinsatz sowie der Verschiebung von Aufgabenschwerpunkten mittlerweile entbehrlich wurden. Angesichts der Tatsache, dass der Berliner Beauftragte für Datenschutz und Akteneinsicht regelmäßig von den zur Sanierung des Haushalts unabdingbar notwendigen Sparmaßnahmen im Personalbereich ausgenommen wird, während alle anderen Bereiche ihre unverändert wahrzunehmenden Aufgaben mit einem immer geringerem Personalbestand erfüllen müssen, erscheint die Forderung unangemessen. Der Senat geht deshalb davon aus, dass mit dem vorhandenen Personal die Aufgabenwahrnehmung und auch die Erhebung von Gebühren möglich sein müssen. Die Einschätzung, dass eine Aufstockung des Personalbestandes unausweichlich sei, wird nicht geteilt.

Gesundheit und Soziales (17%) neben dem Bereich Wirtschaft (16%) führend. Die Zahlen zu Inneres (9%) und Justiz (7%) zeigen, dass die Besorgnisse sich zunehmend von den Sicherheitsbehörden abwenden. 8% der Eingaben betrafen Fragen des Informationsfreiheitsgesetzes.

### 6.3 Zusammenarbeit mit dem Parlament

Wegen der Wahlen zum Abgeordnetenhaus im Oktober 1999 hatte sich die Beratung des Jahresberichts 1998 verzögert. Unmittelbar nach seiner Konstituierung nahm der neue Unterausschuss Datenschutz des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses im Februar 2000 seine Arbeit unter dem neuen Vorsitzenden Peter Trapp (CDU) auf. Dem Unterauschuss gehören ferner die Abgeordneten Heidemarie Fischer (SPD), Roland Gewalt (CDU), Marion Seelig (PDS) und Wolfgang Wieland (Bündnis 90/ DIE GRÜNEN) an. Im Laufe des Jahres 2000 wurden 14 Sitzungen abgehalten, in denen der Jahresbericht 1998, Teile des Jahresberichtes 1999 sowie aktuelle Themen beraten wurden. Gemäß der 1998 beschlossenen Vorgehensweise sollen Beschlussempfehlungen zu beiden Jahresberichten im Laufe des Jahres ins Plenum des Abgeordnetenhauses eingebracht werden.

### 6.4 Kooperation mit anderen Datenschutzstellen

Das Datenschutzgesetz verpflichtet zur Zusammenarbeit mit allen Stellen, die mit Kontrollaufgaben des Datenschutzes betraut sind (§ 24 Abs. 4 BlnDSG). In der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die im vergangenen Jahr unter dem Vorsitz des niedersächsischen Datenschutzbeauftragten Burkhard Nedden in Hannover (14./15. März 2000) und Braunschweig (12./13. Oktober 2000) tagte, wurde erneut eine Reihe von Beschlüssen gefasst, die die Fortentwicklung des Datenschutzes fördern sollten[135]. Die Ergebnisse sind bei den Berichten aus den Arbeitsgebieten dargestellt worden. Im laufenden Jahr hat die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Bettina Sokol, den Vorsitz übernommen.

Nachdem außer Brandenburg und Berlin auch Schleswig-Holstein über eine Gesetzgebung zur Informationsfreiheit verfügt und in allen Ländern die Landesdatenschutzbeauftragten auch zu Beauftragten für die Akteneinsicht bestimmt wurden, wurde gelegentlich der Datenschutzakademie in Kiel am 29. August 2000 die Gründung der Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID) beschlossen. Eine erste Sitzung, bei der ein Beschluss zur Fortentwicklung der Informationsfreiheit in

[135] vgl. Anlagenband „Dokumente zum Datenschutz 2000“

Deutschland gefasst wurde, fand am 11./12. Dezember 2000 in Potsdam statt[136].

Die besondere Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg wurde fortgesetzt.

Für den Bereich der Aufsicht von Privatunternehmen wurde die Koordinierung im „Düsseldorfer Kreis", dem Gremium der obersten Aufsichtsbehörden für den Datenschutz, ebenso wahrgenommen, wie die Fortführung des Vorsitzes der Arbeitsgruppen „Teledienste und Telekommunikation" sowie „Internationaler Datenverkehr" in dessen Rahmen. Ebenso fortgeführt wurde die Arbeit des *Kooperationskreises IuK*, der Landesbeauftragte und Aufsichtsbehörden gemeinsam berührende Probleme erörterte.

Auf europäischer Ebene ist der Berliner Datenschutzbeauftragte von der Konferenz der Datenschutzbeauftragten als Beauftragter der Länder in der Gruppe nach Art. 29 der Europäischen Richtlinie benannt worden. Zusammen mit dem Bundesdatenschutzbeauftragten nimmt er dort die Interessen der deutschen Datenschutzbehörden wahr, aufgrund seiner Funktionen im Rahmen des „Düsseldorfer Kreises" vertritt er hier auch die Interessen der Aufsicht über die Privatunternehmen.

Die Internationale Arbeitsgruppe Datenschutz in der Telekommunikation ist im Jahr 1983 im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten auf Initiative des Datenschutzbeauftragten gegründet worden, unter dessen Vorsitz sie nach wie vor arbeitet, und hat seither eine Vielzahl von Empfehlungen zur Verbesserung des Datenschutzes in der Telekommunikation erarbeitet. Teilnehmer sind Datenschutzbehörden, aber auch Regierungsstellen, Vertreter internationaler Organisationen und Wissenschaftler aus aller Welt. Seit Anfang der 90er Jahre gilt das besondere Augenmerk der Arbeitsgruppe der Wahrung der Persönlichkeitsrechte im Internet. Im vergangenen Berichtszeitraum hat die Arbeitsgruppe „Gemeinsame Standpunkte" zu folgenden Themengebieten beschlossen:

- Gemeinsamer Standpunkt zur Missbrauchserkennung in der Telekommunikation (Kreta, 4./5.5.2000),
- Gemeinsamer Standpunkt zu Infomediaries (Informationsmakler) - eine datenschutzfreundliche Geschäftsidee? (Kreta, 4./5.2000),
- Gemeinsamer Standpunkt zu Datenschutz und Urheberrechts-Management (Kreta, 4./5.5.2000),

[136] vgl. Anlagenband „Dokumente zum Datenschutz 2000", S. 73

- Gemeinsamer Standpunkt zu Online-Profilen im Internet (Kreta, 4./5.5.2000),
- Gemeinsamer Standpunkt zu Datenschutzaspekten bei der Registrierung von Domain-Namen im Internet (Kreta, 4./5.5.2000),
- Gemeinsamer Standpunkt zu Datenschutzaspekten der Veröffentlichung personenbezogener Daten aus öffentlich zugänglichen Dokumenten im Internet (Kreta, 4./5.5.2000),
- Gemeinsamer Standpunkt zu Datenschutzaspekten des Entwurfs einer Konvention zur Datennetzkriminalität des Europarates (Berlin, 13./14.9.2000),
- Gemeinsamer Standpunkt über die Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Datenschutzabkommen - zehn Gebote zum Schutz der Privatheit im Internet (Berlin, 13./14.9.2000).

Die deutschen Übersetzungen der Gemeinsamen Standpunkte sind im Anlagenband zu diesem Jahresbericht abgedruckt. Sie können darüber hinaus in unserem Internet-Angebot unter http://www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm abgerufen werden.

Fortgeführt wurden auch die Gespräche im Rahmen einer deutsch-amerikanischen Arbeitsgruppe zur Fortentwicklung des Datenschutzes bei Datenflüssen zwischen Deutschland und den USA[137]. Neu aufgenommen wurde eine Kooperation mit dem unter Federführung der Datenschutzkommission der spanischen Hauptstadt Madrid von der Europäischen Kommission geförderten Leonardo-DaVinci-Projekt „DATAPROT“, das ein für ganz Europa gültiges Konzept der Fortbildung für Lehrpersonal im Bereich des Datenschutzes entwickeln soll.

### 6.5. Öffentlichkeitsarbeit

Im Jahr 1986 veröffentlichte der Berliner Datenschutzbeauftragte erstmals seine „Grundsätze für den Datenschutz für isolierte Rechner und Personalcomputer“. Die Broschüre fand lebhaftes Interesse und bis 1992 wurden - inhaltlich an den technologischen Wandel angepasst - vier Auflagen herausgebracht. In dieser Tradition steht die 2., überarbeitete Auflage unserer Broschüre „Materialien zum Datenschutz Nr. 25“, die im Dezember 2000 erschienen ist. Bereits der Titel *„Datenschutz und informationstechnische Sicherheit beim PC-Einsatz“* macht deutlich, dass sich diese Broschüre ausführlich mit den Aspekten der IT-Sicherheit und des Datenschutzes beim Einsatz isolierter oder vernetzter PCs beschäftigt. Neben abstrakten Vorschlägen zur Erfüllung von Sicherheitsanforderungen werden methodische Ansätze zur

[137] JB 1999, 6.4

sinnvollen Auswahl geeigneter Maßnahmen im Einzelfall gegeben.

Ein weiterer Effekt unserer vielfältigen Beratungstätigkeit bestand in der Neufassung der 1994 veröffentlichten Broschüre zum *„Datenschutz in Wissenschaft und Forschung“*. Gemeinsam mit dem Hessischen Datenschutzbeauftragten wurden neue inhaltliche Schwerpunkte aufgenommen. Dabei wird auf die Vorgaben der EG-Datenschutzrichtlinie, die Erfahrungen bei Pseudonymisierungsverfahren, Probleme der Einwilligung bei nichteinwilligungsfähigen Personen, theoretische und praktische Aspekte bei der Nutzung von Datentreuhändern, Maßnahmen zur Sicherung guter wissenschaftlicher Praxis, neue Probleme bei der Genomforschung, Verarbeitung personenbezogener Daten von Personen der Zeitgeschichte sowie Funktions- und Amtsträgern, der zeitweiligen Beschäftigung von Forschern bei Daten besitzenden Stellen sowie Probleme von Forschungsregistern eingegangen.

Mit dem Gesetz zur Förderung der Informationsfreiheit im Land Berlin (Berliner Informationsfreiheitsgesetz - IFG) vom 15. Oktober 1999 hat der Berliner Gesetzgeber jedem Menschen die Möglichkeit eröffnet, in weite Teile der Akten der Berliner Verwaltung Einsicht zu nehmen oder daraus Auskünfte zu erhalten, auch ohne selbst betroffen zu sein. Bereits zuvor gab es eine Vielzahl von Vorschriften, die unter verschiedensten Voraussetzungen Ansprüche auf Zugang zu Verwaltungs- und Justizakten gewährten. In einem neuen Band unseres Berliner Informationsgesetzbuches (Teil 5 - Heft 1) mit dem Titel *„Informationszugangsrecht“* haben wir die wichtigsten Vorschriften, die für die Bürgerinnen und Bürger die Transparenz der staatlichen Institutionen gewährleisten sollen, zusammengestellt.

In einer neuen Schriftenreihe *„Ratgeber zum Datenschutz“* sind Hefte erschienen, in denen wir in kurzer, übersichtlicher Form Hinweise und praktische Tipps zu Datenschutzfragen geben. Die Broschüren beschäftigen sich mit alltäglichen Fragen, die immer wieder an uns herangetragen werden. Wie muss ich ein Schreiben adressieren, damit es ungeöffnet beim Sachbearbeiter in einer Behörde ankommt? Wie kann ich den Handel mit meiner Adresse und an mich gerichtete unerwünschte Werbung verhindern? Wie kann ich meinen PC durch die Vergabe von Passwörtern sichern bzw. einen Softwareangriff verhindern? Welche Rechte habe ich gegenüber Behörden nach dem Informationsfreiheitsgesetz? Mit den Broschüren wollen wir den Bürgerinnen und Bürgern unsere Hilfe zur Selbsthilfe bei diesen Fragen anbieten. Bisher sind folgende Ratgeber erschienen:

- „Schriftwechsel mit Behörden - Ratgeber zum Datenschutz Nr. 1“

| Bericht des Beauftragten für Datenschutz und Akteneinsicht | Stellungnahme des Senats |
|---|---|

- „Adressenhandel und Umgang mit unerwünschter Werbung - Ratgeber zum Datenschutz Nr. 2“
- „Empfehlungen für die Vergabe von Passwörtern - Ratgeber zum Datenschutz Nr. 3“
- „Computerviren und andere Softwareangriffe - Ratgeber zum Datenschutz Nr. 4“
- „Informationsfreiheitsgesetz - Ratgeber zum Datenschutz Nr. 5“.

Berlin, 19. März 2001

Prof. Dr. Hansjürgen Garstka
Berliner Beauftragter für
Datenschutz und Akteneinsicht

Berlin, den 12. Juni 2001

Der Senat von Berlin
Eberhard Diepgen
Regierender Bürgermeister